



Smernica Politiky kybernetickej a informačnej bezpečnosti

MHTH_KB_S01, v2

1. ÚČEL A ROZSAH

Dokument „**Politiky kybernetickej a informačnej bezpečnosti**“ naplňa požiadavky zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení neskorších predpisov a Vyhlášky NBÚ č. 227/2025 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v platnom znení - systém riadenia informačnej bezpečnosti a kybernetickej bezpečnosti, keďže v zmysle platnej legislatívy sa bezpečnostné opatrenia prijímajú a realizujú na základe schválenej bezpečnostnej dokumentácie.

Záväznosť pre: MH Teplárenský holding, a.s.

Tento dokument je aplikovaný v celom rozsahu IB a KB, t. j. na všetky pracoviská, zariadenia a vybavenie nachádzajúce sa v rozsahu IB a KB.

Zmenový list

Dátum	Vydanie	Popis zmeny	Meno zamestnanca vykonávajúceho zmenu
03/2024	1	nový dokument	Róbert Mramúch
03/2026	2	aktualizácia legislatívnych nariadení, aktualizácia kap. 5.19 Riadenie zraniteľností a patch manažment, pridanie kapitoly Politika AI a LLM	Tomáš Baksa

1.	ÚČEL A ROZSAH	1
2.	DEFINÍCIE POJMOV A SKRATKY	4
3.	ZODPOVEDNOSTI A PRÁVOMOCI	9
4.	STRATÉGIA PRE KYBERNETICKÚ A INFORMAČNÚ BEZPEČNOSŤ	10
4.1	ROZSAH A PÔSOBNOSŤ KIB	10
4.2	CIELE KIB	11
4.3	ÚLOHY ŠTATUTÁRNEHO ORGÁNU	13
4.4	ŠTRUKTÚRA A ORGANIZÁCIA BEZPEČNOSTI	13
4.5	RIADENIE AKTÍV	15
4.6	RIADENIE RIZÍK	19
4.7	BEZPEČNOSTNÁ ARCHITEKTÚRA	20
4.8	BEZPEČNOSTNÁ DOKUMENTÁCIA	22
5.	POLITIKY KYBERNETICKEJ A INFORMAČNEJ BEZPEČNOSTI	24
5.1	ÚVODNÉ USTANOVENIA PKIB	24
5.2	SPRÁVA POLITIKY A KONTROLA JEJ DODRŽIAVANIA	24
5.3	URČENIE ROZSAHU A ZODPOVEDNOSTI V OBLASTI IB A KB	24
5.4	SÚLAD S POŽIADAVKAMI	25
5.5	ZÁSADY PRIJATEĽNÉHO POUŽÍVANIA	27
5.6	POLITIKA AI A LLM	33
5.7	POLITIKA PRE KLASIFIKÁCIU INFORMÁCIÍ	35
5.8	POLITIKA RIADENIA PRÍSTUPU	43
5.9	POLITIKA PRÍSTUPOVÝCH HESIEL	45
5.10	POLITIKA ČISTÉHO STOLA A ČISTEJ OBRAZOVKY	45
5.11	POLITIKA LIKVIDÁCIE INFORMAČNÝCH ZARIADENÍ A MÉDIÍ	46
5.12	POLITIKA RIADENIA BEZPEČNOSTI SIETÍ	47
5.13	POLITIKA ZÁLOHOVANIA	51
5.14	POLITIKA PRE PRENOS INFORMÁCIÍ	54
5.15	POLITIKA POUŽÍVANIA KRYPTOGRAFICKÝCH OPATRENÍ	54
5.16	POLITIKA RIADENIA DODÁVATEĽOV	60
5.17	POLITIKA PRE RIADENIE KONTINUITY	61
5.18	RIADENIE BEZPEČNOSTNÝCH INCIDENTOV	65
5.19	RIADENIE ZRANITEĽNOSTÍ A PATCH MANAŽMENT	83
5.20	BEZPEČNOSTNÝ MONITORING A SPRÁVA PREVÁDZKOVÝCH ÚDAJOV	91
5.21	AKVIZÍCIA, VÝVOJ A ÚDRŽBA INFORMAČNÝCH SYSTÉMOV	98
5.22	OCHRANA PRED ŠKODLIVÝM KÓDOM	100
5.23	BEZPEČNOSTNÉ PRAVIDLÁ PRE INŠTALÁCIU A KONFIGURÁCIU IS	101
5.24	PERSONÁLNA BEZPEČNOSŤ	105
5.25	VYKONÁVANIE NÁPRAVNEJ A PREVENTÍVNEJ ČINNOSTI	109
5.26	INTERNÝ AUDIT	111
5.27	METODIKA RIADENIA RIZÍK INFORMAČNÝCH AKTÍV	112
5.28	OCHRANA OSOBNÝCH ÚDAJOV V SÚLADE S POŽIADAVKAMI GDPR	119
5.29	FYZICKÁ BEZPEČNOSŤ	123

<u>6.</u>	<u>SÚVISIACA DOKUMENTÁCIA</u>	<u>127</u>
<u>5.1</u>	<u>INTERNÉ DOKUMENTY</u>	<u>127</u>
<u>5.2</u>	<u>EXTERNÉ DOKUMENTY</u>	<u>128</u>
<u>5.3</u>	<u>PRÍLOHY A FORMULÁRE.....</u>	<u>128</u>
<u>7.</u>	<u>PLATNOSŤ A ÚČINNOSŤ</u>	<u>129</u>

2.DEFINÍCIE POJMOV A SKRATKY

POJMY:

Aktívum - (ang. Asset) čokoľvek potrebné a využívané v biznis procese, úlohách a má pre organizáciu hodnotu – osoba, miesto, vec, proces, technológia, čokoľvek hmotné aj nehmotné.
Bezpečnostná komisia - je poradným orgánom štatutára, definuje a navrhuje bezpečnostnú stratégiu. Bezpečnostnú komisiu schvaľuje štatutár. Bezpečnostná komisia sa vytvára osobami, ktoré sú poverené celkovým riadením a rozvojom informačných systémov, komunikačných systémov a technológií alebo sa významne podieľajú na riadení alebo koordinácii činností spojených s kybernetickou bezpečnosťou.
Bezpečnostná udalosť (BU) - stav systému alebo služby, ktorý signalizuje možnosť narušenia bezpečnosti alebo zlyhania opatrení alebo doposiaľ nezaznamenanú situáciu, ktorá môže byť relevantná z hľadiska bezpečnosti. Je to každá udalosť, ktorá je potenciálne schopná znížiť úroveň bezpečnosti a tým negatívne ovplyvniť aktíva organizácie.
Bezpečnostné opatrenie - je akýkoľvek prostriedok/opatrenie alebo spôsob na zabránenie šírenia BI, neoprávnenej manipulácie s citlivými údajmi, atď.
Bezpečnostný incident (BI) - neplánované prerušenie služby poskytovanej aktívom alebo zníženie jej kvality. Incidentom je aj také zlyhanie aktíva alebo jeho časti, ktoré zatiaľ nemalo dopad na celkovú poskytovanú službu. Jedná sa o neželanú a neočakávanú udalosť bezpečnosti, pri ktorej sa zvýši ohrozenie informačných aktív organizácie. BI môže charakterizovať identifikovaný stav informačného systému, procesu, služby alebo komponentu infraštruktúry, ktorý môže narušiť pravidlá bezpečnostnej politiky ICT, alebo bezpečnostného opatrenia (napr. podozrenie na spáchanie trestného činu, priestupku alebo iného pokusu získať neoprávnený prístup alebo neoprávnene nakladať s informáciami).
Bezpečnostný záznam (BZ alebo log) predstavuje chronologický záznam systémových aktivít dostatočný pre rekonštrukciu, revíziu a skúmanie postupnosti stavov prostredia a aktivít zúčastňujúcich sa na realizácii operácie, postupy, alebo udalosti v transakcii od jej začiatku po jej konečný výsledok.
CMDB - databáza riadenia zmien (CMDB) je databáza, ktorá slúži ako dátový sklad na ukladanie súboru relevantných informácií o hardvérových a softvérových aktívach (bežne označovaných ako konfiguračné položky (CI) v MHTH, ako aj o vzťahoch medzi nimi. Z angl. Configuration Management Database.
Configuration Item (CI) - termín konfiguračná položka (CI) sa vzťahuje na základnú konštrukčnú jednotku systému riadenia konfigurácií. Príklady CI zahŕňajú individuálne aktíva ako napríklad softvér, hardvér, dokumenty, modely a plány.
Dešifrovanie je proces spätnej transformácie zašifrovaného textu na pôvodné vstupné dáta.
Dopad - miera vplyvu incidentu, problému alebo zmeny na procesy organizácie odberateľa a/alebo poskytovateľa služieb. Dopad sa často zakladá na tom, ako budú ovplyvnené úrovne služieb. Dopad a naliehavosť sa používajú pri určovaní priority. Z angl. Impact.
Dopad incidentu - miera vplyvu incidentu na procesy, služby, či ciele organizácie. Dopad a naliehavosť sa používajú pri určovaní priority.
Eskalácia incidentu - pokiaľ nie je možné incident vyriešiť, je nutné ho eskalovať na vyššie úrovne podpory alebo organizačnej hierarchie tak, aby bolo riešenie úspešné. Funkčná eskalácia postupuje incident interným alebo externým podporným tímom, hierarchická eskalácia zapojí príslušné úrovne vedenia organizácie.
Informačný systém - obsahuje všetky servery a personálne počítače, infraštruktúru siete, operačné systémy, aplikačný softvér, údaje a ostatné komponenty, pripojené do počítačovej siete alebo pracujúce samostatne. Informačný systém tiež zahŕňa používanie všetkých interných alebo externých služieb, ako napríklad prístup na Internet, e-mail.

Informačné aktíva - primárne informácie alebo dáta, hlavne v súvislosti s atribútom dôvernosti, ale aj informačné alebo komunikačné systémy, pri ktorých je dôležité zaručiť ich integritu (funkčnosť, neporušenosť, celistvosť, komplexnosť) a dostupnosť (dajú sa používať v definovanom rozsahu). V kontexte tohto dokumentu označuje tiež všetky komponenty informačného systému vrátane údajov, databáz, hardvéru a softvéru.
Katalóg služieb - aktuálny a schválený zoznam služieb organizácie.
Kritickosť služby - je meradlom toho, do akej miery je služba dôležitá, teda ako dlho bude trvať, kým výpadok služby bude mať významný dopad na používateľa služieb a jeho aktivity, ktoré daná služba podporuje. Bližšie v Katalógu služieb. Dopad a kritickosť sa používajú pri určovaní priority. Z angl. Urgency.
Kybernetická bezpečnosť je stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov, alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov.
Manažment služieb (ITSM) - disciplína zaoberajúca sa zabezpečením kvality služieb, pri súčasnom zabezpečení efektivity a účinnosti. Z angl. Information Technology Service Management (ITSM).
Manažment vydaní (Release Management) - proces zabezpečujúci riadenie, plánovanie a kontrolu nasadzovania zmien najmä do prevádzkového prostredia (PROD) prípadne aj iných prostredí (PREPROD, TEST, ...). Manažment vydaní vykonáva svoje aktivity na základe posúdenia a schválenia nasadenia zmien procesom Manažment zmien.
Manažment zmien (Change Management) - proces riadenia žiadosti o zmenu, jej záznam, kategorizácia, posúdenie, schválenie a implementácia.
Manažment žiadosti o službu (RF – Request Fulfilment) - proces spracovania, riadenia a splnenia žiadosti o službu od používateľov týchto služieb. Z angl. Request Fulfilment.
Matica oprávnení - definuje rozsah oprávnení používateľskej triedy/skupiny v aplikácii/IS/RS systémov z hľadiska dostupnosti funkčnosti aplikácie alebo dostupnosti údajov v aplikácii, vlastníkom matice je vlastník systému/aplikácie.
Naliehavosť - subjektívne alebo objektívne definovanie miery, času, závažnosti, či vplyvu incidentu s ohľadom na organizačnú zložku, používateľa, typy služieb.
Nápravné opatrenie - opatrenie, podniknuté s cieľom odstrániť príčiny existujúcej nehody, chyby alebo inej nežiaducej situácie, aby sa zabránilo ich opakovanému výskytu.
Need to Know - je princíp pridelovania prístupových práv k informáciám výlučne v takom rozsahu, ktorý je nevyhnutný pre plnenie pracovných úloh a povinností.
Obnova - návrat systému alebo služby do stavu, definovanom v SLA a Security SLA (SSLA). Poskytovateľ služieb obnovu vykonáva v súlade s SLA a SSLA a požiadavkami pre kontinuitu. Obnova IT služby a OT priemyselného procesu často zahŕňa aj obnovenie dát do známeho stavu (vzťah k zálohovaniu, riadeniu zálohovania a obnovy a jej plánovanie v súlade s SLA a SSLA).
OLA (Operational Level Agreement) - dohoda medzi poskytovateľom IT služby a inou časťou tej istej organizácie. OLA podporuje dodávku IT služieb zákazníkom od poskytovateľa IT služby. OLA definuje produkty alebo služby, ktoré majú byť poskytované a zodpovednosti oboch strán.
Osobný údaj - je informácia týkajúca sa identifikovanej alebo identifikovateľnej fyzickej osoby. Identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

OT - Operational technologies - výrobná a technologická časť (podporuje výrobné a technologické procesy spoločnosti). Podľa medzinárodných štandardov tiež definované ako IACS (Industrial Automation and Control Systems, priemyselná automatizácia a riadiace systémy).
OT manažér - osoba zodpovedná za prevádzku riadiacich a výrobných systémov.
OT operátor - osoba, ktorá riadi a dohľadáva výrobný proces.
OT špecialista - osoba, ktorá vykonáva systémové zmeny v riadiacom systéme.
Podnet na zlepšenie - typ požiadavky týkajúci sa zefektívnenia procesu. Z podnetu na zlepšenie sa môže po jeho analýze, v prípade väčšej realizačnej náročnosti, stať „projekt“.
Používateľ IT/OT - je osoba, ktorá akýmkoľvek spôsobom využíva informačné systémy a služby. Používateľom v zmysle tohto predpisu sa rozumie každý zamestnanec spoločnosti.
Požiadavka na zmenu (RFC - Request for Change) - požiadavka, ktorá sa týka prevádzkovej zmeny v IT / OT systémoch, aplikáciách, prípadne riešenia závažnej chyby. Formálny návrh na vykonanie zmeny. Obsahuje detaily navrhovanej zmeny a môže byť zaznamenaná v elektronickej forme, v zmysle platných interných predpisov a postupov riadenia zmien (Change Management), pričom podlieha schváleniu príslušnými oprávnenými osobami pred jej realizáciou.
Prenosné médium - druh pamäťových médií, ktoré uchovávajú digitálny záznam (patria sem najmä USB dátové médium kľúče, USB hdd, pamäťové karty všetkých druhov, MP3/MP4 prehrávače, digitálne fotoaparáty, atď.).
Priorita - definovaná je maticou priorít riešenia incidentov. Využíva sa najmä pri súčasnom výskyte viacerých incidentov.
Problém - neznáma príčina jedného alebo viacerých incidentov, ktorú je potrebné identifikovať.
Service Desk - útvar, ktorý slúži ako jednotné miesto pre hlásenia od používateľov služieb organizácie. Prijíma, triedi a ak vie, tak rieši všetky požiadavky používateľov služieb a pokiaľ nevie, tak eskaluje požiadavku na ostatné odborné tímy. Požiadavky prijíma formou telefonického volania, elektronického kontaktného formulára alebo emailom. V rámci procesu Manažment incidentov predstavuje úroveň podpory používateľov, resp. prijímateľa požiadavky, teda vykonáva zaznamenanie hlásení, metodickú podporu používateľov služieb, počiatočné riešenie a presmerovanie riešení na L2 (úroveň podpory L2 – špecialista IT/OT), ako aj poskytovanie informácií prípadne asistenčných služieb.
Schvaľovacia komisia zmien (CAB) - je zbor viacerých posudzovateľov a schvaľovateľov zmien, ktorý je zložený tak, aby bola zmena posúdená zo všetkých potrebných hľadísk najmä technického hľadiska a hľadiska rizík a vplyvu na prevádzku služby. Počet členov CAB nie je obmedzený, ale minimálne by mali zmenu schvaľovať 4 členovia. Z angl. Change Advisory Board.
SLA (Service Level Agreement) - dohoda medzi poskytovateľom IT a OT služieb a zákazníkom. SLA popisuje IT alebo OT službu, dokumentuje cieľovú úroveň služieb a špecifikuje zodpovednosti poskytovateľa IT / OT služby a zákazníka. Jedna SLA môže pokrývať niekoľko služieb IT/OT alebo niekoľko zákazníkov.
Služba - nástroj k poskytovaniu hodnoty zákazníkovi (t.j. tomu, kto službu odoberá), pričom táto hodnota pozostáva z toho, čo zákazníkovi pomôže získať také výsledky, ktoré potrebuje, ale bez toho, aby bol zákazník vlastníkom špecifických nákladov a rizík spojených s poskytnutím a dodávkou služby.
Služba IT - explicitne definovaná a popísaná funkcionality, poskytovaná informačnými technológiami, ktorá podporuje, alebo priamo umožňuje fungovanie niektorého obchodného procesu, resp. činnosti. IT službu tvorí kombinácia ľudí, procesov, technológií a mala by byť definovaná dohodou o úrovni služby (SLA).

Šifrovanie je použité kryptografických prostriedkov na zabezpečenie dôvernosti alebo integrity údajov, t.j. transformácia vstupných dát do podoby, v ktorej sú pre potenciálneho útočníka nezrozumiteľné a nie je schopný rekonštruovať ich pôvodnú podobu.
Štandardy - všeobecne schválené MHTH politiky nižšej úrovne (prevádzkové, technické, a bezpečnostné).
Workaround - dočasná oprava alebo riešenie, pokiaľ nie je k dispozícii úplné riešenie.
Zamestnanec - fyzická osoba, ktorá v pracovnoprávných vzťahoch vykonáva pre zamestnávateľa závislú prácu.
Závažný incident - incidenty s kritickou, prípadne vysokou prioritou. Výsledkom závažného incidentu je významný výpadok a dopad na organizáciu, riešenie takéhoto incidentu má vždy najvyššiu prioritu. Závažné incidenty majú dopad na nosné IT a OT procesy a služby spoločnosti.
Záznam o incidente - záznam, ktorý obsahuje detailné informácie o incidente – jeho vzniku, priebehu, postupoch riešenia, riešiteľských tímoch, nápravných opatreniach až po jeho uzavretie. Povinné položky záznamu sú určené v ďalšom texte.
Zmena - pridanie, úprava alebo odstránenie niečoho, čo môže mať vplyv na služby IT a OT.

SKRATKY:

AAA	Identification (vyžiadaná identifikácia), Authentication (overenie identity), Authorization (overenie možnosti prístupu), Auditing (Auditovateľnosť aktivít súvisiace k systému a subjektu), Accounting (overenie vykonaných aktivít)
ACL	Access Control List – riadenie prístupov
Administrátor	Osoba, ktorá spravuje alebo konfiguruje komponenty IT/OT infraštruktúry
AV	Antivírus, antivírusový (napr. program)
BCM	Business Continuity Management – manažment kontinuity činností
BCM	Z angl. Business Continuity Management System – Riadenie kontinuity služieb
BI	Bezpečnostný incident
CA	Certifikačná autorita
CEO	Chief Executive Officer; Generálny riaditeľ
CIA	Z angl. Confidentiality (dôvernosť), Integrity (integrita), Availability (dostupnosť)
CIO	Chief Information Officer (Riaditeľ úseku IT)
CVSS	Common Vulnerability Scoring System
DLP	Data Loss Prevention (nástroj na zabránenie straty alebo úniku citlivých informácií)
DMZ	Z angl. Demilitarized Zone (v počítačovej bezpečnosti fyzická alebo logická podsieť, ktorá je z bezpečnostných dôvodov oddelená od ostatných zariadení)
DOS	Denial of Service, resp. Odoprenie služby (služba sa stane nedostupnou)
DPO	Data Privacy Officer (osoba zodpovedná za ochranu osobných údajov - oblasť ochrany osobných údajov podľa GDPR)
GDPR	General Data Protection Regulation (všeobecné nariadenie o ochrane údajov)
HA	High-Availability, vysoká dostupnosť služieb/komponentu
HSM	Hardware Security Module, hardvérová súčasť

HW	Hardware (fyzická časť výpočtovej techniky)
IB	Informačná bezpečnosť
ICS	Industrial Control System (priemyselný riadiaci systém)
ID	Identifikácia jedinečným kódom
IED	Inteligent Electronic Device, Inteligentné elektronické zariadenie
IS	Informačný systém
IT/ICT	Information Technology (informačno-komunikačné technológie)
ITSM	IT service manažment
KB	Kybernetická bezpečnosť
KIB	Kybernetická a informačná bezpečnosť
MDM	Mobile Device Management, správa a riadenie mobilných zariadení
MHTH	MH Teplárenský holding, a.s (ďalej tiež ako „MHTH“ alebo „spoločnosť“)
MKB	Manažér kybernetickej a informačnej bezpečnosti je zodpovedný za manažment bezpečnosti v spoločnosti a riadenie informačných rizík a zastupuje funkcie bezpečnostného tímu. Táto rola je definovaná v zákone č. 69/2018 Z.z. o kyber. bezpečnosti. V MHTH vykonáva tieto povinnosti manažér bezpečnosti a krízového riadenia.
NBÚ	Národný bezpečnostný úrad
NPO	Nápravné a preventívne opatrenia
OLA	Operational Level Agreement, Dohoda o prevádzkovej úrovni
OT	Operation Technology (výrobné technológie)
PC	Personal Computer (osobný počítač)
PKI	Public Key Infrastructure (infraštruktúra verejných kľúčov)
PKIB	Politika kybernetickej a informačnej bezpečnosti
PLC	Programmable Logic Controller (programovateľný logický automat)
RAT	Risk Analysis Team (špecializovaná medziodborová pracovná skupina s názvom „Tím analýzy KB rizika“, hodnotí úroveň rizika a navrhuje riziká na akceptáciu na stretnutiach Porady vedenia)
RCE	Remote Code Execution (škodlivý kód spustený vzdialene)
RS	Riadiaci systém
RTU	Remote Terminal Unit (bezpečné vzdialené ovládanie)
SCADA	Supervisory Control And Data Acquisition, systém riadenia a dohľadu
SDLC	Software Development Life-Cycle management (správa životného cyklu informačných aktív)
SIEM	Security Incident and Event Management (monitoring bezpečnostných udalostí)
SLA	Service Level Agreement, Dohoda o úrovni poskytovaných služieb
SOA	Statement of Applicability (vyhlásenie o aplikovateľnosti)
SPAN	Mirror port (port na prepínači za účelom monitoringu sieťovej prevádzky)
SRP	Systém riadenia prístupu
SW	Software (programové vybavenie)
TK	Tenký klient

V362	Vyhláška NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v platnom znení
VPN	Virtual Private Network, Virtuálna privátna sieť
Workaround	Náhradné riešenie alebo opatrenie
ZoKB	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení neskorších predpisov
ZoBOaNP	Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností, podľa požiadaviek ZoKB 69/2018 Z. z.
ZS	Základná služba (výroba a distribúcia tepla, výroba elektriny)
PZS	Prevádzkovanie základnej služby (výroba a distribúcia tepla, výroba elektriny)

3. ZODPOVEDNOSTI A PRÁVOMOCI

Zamestnanci zodpovedajú za:

- ochranu im zverených aktív (informácií, osobných údajov, aplikácií, dát, IT/OT zariadení, a pod.),
- dodržiavanie zásad kybernetickej bezpečnosti, opatrení pre elimináciu rizík,
- dodržiavanie pokynov pre prácu s informáciami a osobnými údajmi, a to predovšetkým:
 - chrániť spracúvané informácie a osobné údaje dostupnými a vhodnými prostriedkami, aby nedošlo k ich poškodeniu alebo zneužitiu,
 - zachovávať mlčanlivosť, t. j. nezverejňovať, neposkytovať alebo nesprístupňovať údaje iným osobám, ak to priamo nevyplyva z plnenia pracovných úloh alebo pokynov,
 - pravidelne sa vzdelávať v oblasti informačnej bezpečnosti,

Zamestnanci postupujú v súlade s politikou informačnej a kybernetickej bezpečnosti, sú pozorní, obozretní a pri pochybnostiach alebo neznalosti sa obrátia so žiadosťou o vysvetlenie, či udelenie pokynu na nadriadených pracovníkov alebo osoby poverené presadzovaním politiky.

Riaditelia úsekov zodpovedajú za:

- zavedenie a priebežné zlepšovanie informačnej a kybernetickej bezpečnosti a za zabezpečenie k tomu potrebných zdrojov.

Manažér odboru ľudských zdrojov zodpovedá za:

- výber kvalifikovaných zamestnancov a ich vzdelávanie v oblasti informačnej a kybernetickej bezpečnosti.

Gestor zmluvy zodpovedá za:

- oboznámenie relevantných zmluvných partnerov s Politikami a štandardami kybernetickej a informačnej bezpečnosti pre dodávateľov a tretie strany ([MHTH_KB_S02](#)),

MKB zodpovedá za:

- riadenie a koordináciu kybernetickej bezpečnosti, určovanie zásad, tvorbu, aktualizáciu a presadzovanie bezpečnostnej politiky,
- presadzovanie kybernetickej a informačnej bezpečnosti,
- koordináciu, metodické riadenie a kontrolu dodržiavania informačnej bezpečnosti,

- prípravu a revíziu dokumentácie KB.
- vzdelávanie a zvyšovanie povedomia osôb v súvislosti s KIB IT/OT.
- inventarizáciu príslušných informačných aktív BP pre IT.
- inventarizáciu príslušných informačných aktív.

4. STRATÉGIA PRE KYBERNETICKÚ A INFORMAČNÚ BEZPEČNOSŤ

Účelom tejto stratégie pre informačnú a kybernetickú bezpečnosť je určiť ciele, zásady a princípy ochrany spracúvaných informácií (osobných údajov, verejných, obchodných a prevádzkových dát) a prostriedkov určených na ich spracúvanie (podporných informačných aktív).

Stratégia pre informačnú a kybernetickú bezpečnosť sa prijíma za účelom vytvorenia, zavedenia, udržiavania a zlepšovania procesov, ktoré na základe výsledkov analýzy kybernetických rizík určia opatrenia a postupy na ich znižovanie.

Opatrenia a postupy smerujúce k znižovaniu rizík vychádzajú z tzv. pravidiel „najlepšej praxe“, aby ich aplikovaním bola zabezpečená trvalá integrita, dôvernosť a dostupnosť informačných aktív.

Stratégia bezpečnosti zároveň určuje zodpovedné osoby a ich právomoci za riadenie bezpečnosti, riadenie procesu rizík, zlepšovanie bezpečnostných opatrení a postupov na základe nových poznatkov, ako aj udržiavanie bezpečnostnej dokumentácie v aktuálnom stave.

- **Informačná bezpečnosť** – predstavuje zachovanie základných vlastností - dôvernosti, integrity a dostupnosti údajov, resp. informácií.
- **Kybernetická bezpečnosť** – predstavuje aplikovanie informačnej bezpečnosti elektronicky spracúvaných informácií v prostredí pozostávajúcom z informačných a komunikačných prostriedkov, sietí a zariadení.
- **Dôvernosť** – predstavuje schopnosť zabezpečiť, aby údaje a informácie boli prístupné iba oprávneným osobám a aby sa zabránilo sprístupneniu údajov a informácií neoprávneným osobám, subjektom alebo procesom.
- **Integrita** – predstavuje správnosť, presnosť a celistvosť údajov a informácií. Integrita garantuje, že údaje alebo informácie sú aktuálne a neboli zmenené neoprávneným spôsobom.
- **Dostupnosť** – predstavuje schopnosť zabezpečiť, že údaje alebo informácie sú prístupné pre oprávnené osoby, systémy, alebo procesy v požadovanej dobe a požadovaným spôsobom.

Postavenie a funkcia spoločnosti, vrátane predmetu podnikania je uvedená v [MHTH S11 Organizačný poriadok](#), v kapitole 3.

4.1 ROZSAH A PÔSOBNOSŤ KIB

Táto politika pre informačnú a kybernetickú bezpečnosť sa uplatňuje pri všetkých činnostiach spoločnosti, ktoré MHTH vykonáva, v rámci svojho predmetu podnikania, na základe svojich zákonných povinností alebo záujmov spoločnosti, všetkými organizačnými zložkami (závodmi), všetkými jej zamestnancami a tretími stranami.

Pôsobnosť sa vzťahuje na všetky elektronické informačné systémy a prostriedky, prevádzkové zariadenia, programy a aplikácie, siete a komunikačné systémy.

Týmto dokumentom sa budú riadiť všetky osoby, ktoré spracúvajú informácie alebo ich činnosť má vplyv na spracúvanie informácií alebo s informáciami akokoľvek súvisí (napr. zamestnanci v pracovnom pomere, dočasní zamestnanci, osoby v obdobnom pracovnom vzťahu, zmluvní partneri, pracovníci dodávateľských firiem a pod.).

Pre zabezpečenie dodržiavania zásad bezpečnosti budú s touto stratégiou v primeranom rozsahu oboznámení všetci pracovníci.

Táto stratégia alebo jej časti budú zverejnené a dostupné všetkým zamestnancom a ostatným povinným osobám, aby o nej boli informovaní a mohli v súlade s týmto predpisom postupovať.

Pre zabezpečenie dodržiavania zásad informačnej a kybernetickej bezpečnosti budú požiadavky tejto stratégie v primeranom rozsahu zakotvené aj v zmluvách s dodávateľmi a inými subjektmi, ak budú mať prístup k informáciám a osobným údajom, ktoré spracúva spoločnosť.

4.2 CIELE KIB

4.2.1 STRATEGICKÉ CIELE

Strategickými cieľmi KIB sú:

- Zabezpečiť trvalú integritu, dôvernosť a dostupnosť spracúvaných informácií a údajov a vytvárať tak predpoklady pre napĺňanie záujmov a poslania spoločnosti.
- Zabezpečiť súlad spracúvania informácií a osobných údajov s platnou legislatívou, predovšetkým so:
 - zákonom č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
 - zákonom č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
 - nariadením Európskeho parlamentu a rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov).

4.2.2 HLAVNÉ CIELE

- Zabezpečiť primeranú úroveň ochrany informačných systémov a údajov a navrhovať bezpečnostné riešenia na základe rizík, ktoré ohrozujú informačné aktíva.
- Zabezpečiť správnu a bezpečnú prevádzku systémov, ktoré slúžia na spracúvanie informácií.
- Zabezpečiť fyzické aj logické riadenie prístupu zamestnancov a poverených osôb k spracúvaným informáciám tak, aby nemali prístup k informáciám a systémom, ktoré k výkonu svojich pracovných úloh a funkcie nepotrebujú.
- Zabrániť fyzickému neautorizovanému prístupu osôb do priestorov spoločnosti a k informačným prostriedkom, ako aj zabrániť elektronickému prístupu neoprávnených osôb k informačným systémom a údajom.
- Predchádzať prerušeniam a výpadkom, ktoré môžu pri prevádzke informačných systémov nastať a definovať postupy na obnovu dostupnosti v prípade ich výpadku.
- Monitorovať fyzické prostredie aj prostredie informačných systémov, analyzovať podozrivé udalosti a riešiť bezpečnostné incidenty, aby sa predišlo ich opakovaniu v budúcnosti.
- Zabezpečovať informovanie a školenia zamestnancov, externých pracovníkov a zamestnancov zmluvných strán, aby rozumeli svojim úlohám a činnosti vykonávali v súlade s informačnou, resp. kybernetickou bezpečnosťou.
- Zabezpečiť dodržiavanie zákonných a zmluvných požiadaviek v oblasti informačnej, resp. kybernetickej bezpečnosti a dodržiavať zákonné požiadavky na ochranu osobných údajov.

4.2.3 OPERATÍVNE CIELE

- Vybudovať štruktúru/organizáciu riadenia kybernetickej/informačnej bezpečnosti,
- Vypracovať bezpečnostné predpisy pre zaistenie súladu s legislatívou v oblasti kybernetickej/informačnej bezpečnosti,
- Zabezpečiť evidenciu všetkých používaných aktív a aktualizáciu evidencie v prípade zmien,

- Zabezpečiť klasifikáciu aktív a revidovať/aktualizovať klasifikáciu na základe výsledkov analýzy rizík,
- Pravidelne vykonávať analýzu rizík a venovať sa manažmentu rizík,
- Sledovať a pravidelne vyhodnocovať kritériá zaradenia služieb medzi základné služby,
- Pre včasnú identifikáciu incidentov zefektívniť monitorovanie činností a udalostí v IT a OT infraštruktúre,
- Zabezpečiť pravidelné posúdenie súladu so zmluvnými a legislatívnymi požiadavkami interným a externým auditom,
- Sledovať vývoj legislatívy v oblasti kybernetickej a informačnej bezpečnosti a na základe zmien aktualizovať procesy a dokumentáciu,
- Zabezpečiť nastavenie a zdokumentovanie jednotného procesu nahlasovania a evidencie incidentov,
- Venovať trvalú pozornosť zvyšovaniu bezpečnostného povedomia,
- Zabezpečiť realizáciu relevantných technických opatrení vyplývajúcich zo záverov predošlých analýz a auditov,
- Pravidelné zvyšovanie odborných vedomostí v bezpečnostných technológiách, trendoch a v procesoch.

4.2.4 VYHODNOCOVANIE BEZPEČNOSTNÝCH CIEĽOV

V akčnom pláne budú pre každý cieľ stanovené/rozpracované spôsoby dosiahnutia cieľa, spôsob a kritériá vyhodnocovania, spôsob priebežného vyhodnocovania, zodpovednosť, súčinnosť, časový horizont plnenia a vyhodnotenie plnenia. Bezpečnostná komisia bude v pravidelných intervaloch kontrolovať plnenie cieľov akčného plánu a navrhovať jeho doplnenie a spresnenie podľa aktuálnych potrieb. Súčasne bude plánovať zdroje na plnenie cieľov a kontrolovať ich čerpanie.

Pri vyhodnocovaní bezpečnostných cieľov sa prihliada na:

- skutočnosť, ako sa majú dosahovať bezpečnostné ciele, napr. v kybernetickej bezpečnosti, informačnej bezpečnosti, návrhu nových informačných technológií, atď.,
- skutočnosti, ktorými majú byť podporované (napr. opatrenia v oblasti administratívnej bezpečnosti, opatrenia v oblasti personálnej bezpečnosti, opatrenia v oblasti fyzickej a objektovej bezpečnosti, opatrenia v oblasti bezpečnosti technických prostriedkov vrátane bezpečného prenosu údajov, atď.),
- spôsob dosahovania bezpečnostných cieľov (napr. zavedením systému riadenia, povinnými štandardami, uplatnením bezpečnostných mechanizmov, kontrolou dodržiavania bezpečnostných požiadaviek, atď.),
- spôsoby vyhodnocovania bezpečnostných cieľov (napr. monitorovaním stavu systémov, kontrolou dodržiavania prijatých opatrení, vyhodnocovaním bezpečnostných incidentov, atď.),
- kritériá vyhodnocovania bezpečnostných cieľov (napr. záverečná správa hodnotiaceho bezpečnostného auditu bez závažných nedostatkov, správy z interného auditu, vyhodnotenie penetračného testovania bez zistených kritických slabín, vyhodnocovanie monitorovania systémov, atď.),
- spôsob priebežného hodnotenia adekvátnosti bezpečnostných cieľov (napr. stanovenie periodicity posúdenia hodnotenia adekvátnosti bezpečnostných cieľov zainteresovanými stranami, posúdenie, či plnenie krátkodobých cieľov reálne smeruje k plneniu dlhodobých cieľov, stanovenie systému a termínov na posúdenie adekvátnosti bezpečnostných cieľov bezpečnostnou komisiou, atď.),
- spôsob kontroly postupov využívaných na dosahovanie bezpečnostných cieľov (napr. na základe vypracovaného plánu kontrol v príslušnom kalendárnom roku, formou vykonávania testov podľa stanovených testovacích scenárov, stanovenie obsahu a postupu pre výkon auditu, atď.).

4.3 ÚLOHY ŠTATUTÁRNEHO ORGÁNU

Úlohou štatutárneho orgánu (Predstavenstvo MHTH) pri zabezpečovaní kybernetickej a informačnej bezpečnosti je podporiť plnenie strategického cieľa, definovaných dlhodobých aj krátkodobých bezpečnostných cieľov, a to najmä zabezpečením potrebných ľudských, finančných aj materiálnych zdrojov.

Generálny riaditeľ (CEO) schvaľuje interné dokumenty spoločnosti, ktoré upravujú oblasť informačnej a kybernetickej bezpečnosti v podmienkach MHTH. Schvaľovanie interných dokumentov prebieha v zmysle [MHTH S01 Riadenie dokumentov a procesov](#).

CEO spoločnosti zabezpečuje plnenie cieľov informačnej a kybernetickej bezpečnosti prostredníctvom všetkých organizačných zložiek a v zmysle organizačného poriadku.

4.4 ŠTRUKTÚRA A ORGANIZÁCIA BEZPEČNOSTI

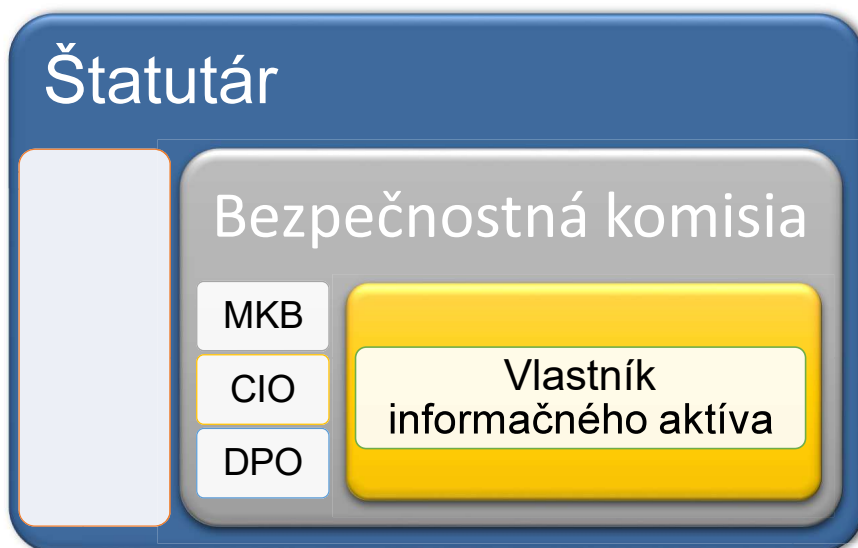
4.4.1 PODPORA ZO STRANY VÝKONNÉHO MANAŽMENTU SPOLOČNOSTI A ZODPOVEDNOSŤ

Výkonný manažment spoločnosti zastupujúci riadiaci orgán Porada vedenia (riaditeľa úsekov) podporujú kybernetickú bezpečnosť deklarováním jej dôležitosti pred zamestnancami, preukazovaním angažovanosti a určovaním zodpovednosti. Základné zodpovednosti v rámci informačnej bezpečnosti sú uvedené v kapitole 3.

Organizácia bezpečnosti stanovuje rozdelenie všeobecných a špecifických zodpovedností a povinností v oblasti kybernetickej a informačnej bezpečnosti a určenie príslušných bezpečnostných rolí potrebných na riadenie kybernetickej a informačnej bezpečnosti vrátane určenia rozsahov činností, kompetencií a úloh.

Vzhľadom na to, že riadenie kybernetickej a informačnej bezpečnosti, ako aj opatrenia na zaistenie kybernetickej a informačnej bezpečnosti nie je možné a ani účelné oddeliť, zahŕňa organizácia bezpečnosti obidve zložky.

Riadenie bezpečnosti, resp. organizácia bezpečnosti MHTH bude mať základnú hierarchickú štruktúru tak, ako je zobrazené na obrázku.



Obr. č. 1: Základná hierarchická štruktúra organizácie bezpečnosti

4.4.2 PRE ORGANIZÁCIU BEZPEČNOSTI PLATIA NASLEDUJÚCE PRAVIDLÁ:

- Vrcholným orgánom, zodpovedným za riadenie KB a IB je štatutár organizácie (predstavenstvo MHTH).
- Bezpečnostná komisia - je poradným orgánom štatutára, definuje a navrhuje bezpečnostnú stratégiu. Bezpečnostnú komisiu schvaľuje štatutár. Bezpečnostná komisia

sa vytvára osobami, ktoré sú poverené celkovým riadením a rozvojom informačných systémov, komunikačných systémov a technológií alebo sa významne podieľajú na riadení alebo koordinácii činností spojených s kybernetickou bezpečnosťou. Vzhľadom na potrebu riešenia KB a IB spoločnosti, pracuje bezpečnostná komisia v zložení:

1. štatutár (predstavenstvo MHTH)
 2. manažér kybernetickej bezpečnosti (MKB)
 3. riaditeľ IT (CIO)
 4. zodpovedná osoba za GDPR oblasť (DPO)
- Členov bezpečnostnej komisie menuje štatutár.
 - MKB musí byť nezávislý od riadenia prevádzky a vývoja služieb informačných technológií.
 - Na procese riadenia a udržiavania kybernetickej a informačnej bezpečnosti sa podieľajú všetky organizačné útvary v rozsahu svojej pôsobnosti prostredníctvom svojich riadiacich pracovníkov.
 - Za jednotlivé aktíva, informácie a procesy zodpovedá zamestnanec, ktorý bol určený ako vlastník daného aktíva.

4.4.3 ORGANIZÁCIA BEZPEČNOSTI

V rámci organizácie bezpečnosti, sú role rozdelené na:

- riadiacu zložku,
- výkonnú zložku,
- kontrolnú zložku,

pričom riadiaca zložka je priamo riadená prevádzkovateľom základnej služby a kontrolná zložka je nezlučiteľná so všetkými ostatnými zložkami.

Riadiaca zložka systému riadenia bezpečnosti zabezpečuje prerokovanie a schválenie koncepčných dokumentov a strategických opatrení týkajúcich sa bezpečnosti informačných technológií, informácií o zaznamenaných bezpečnostných incidentoch spolu s návrhom opatrení na minimalizáciu ich opätovného výskytu a návrhu opatrení vyplývajúcich z analýz, riešených bezpečnostných incidentov, havarijných stavov, kontrol a auditov bezpečnosti informačných technológií.

Z organizácie bezpečnosti sem patria roly:

- **Bezpečnostná komisia** (viď. kapitola 4.5.2)
- **MKB** (Manažér pre kybernetickú a informačnú bezpečnosť),
- **DPO** (osoba zodpovedná za ochranu osobných údajov).

Výkonná zložka systému riadenia bezpečnosti zabezpečuje vypracovanie a aktualizáciu dokumentov upravujúcich systém riadenia bezpečnosti, vyhodnocovanie stavu bezpečnosti informačných technológií, realizáciu bezpečnostných opatrení, plánovanie, koordináciu a vyhodnocovanie činností súvisiacich s riadením bezpečnostných rizík v oblasti bezpečnosti informačných technológií, koordináciu riešenia bezpečnostných incidentov a organizáciu vzdelávacej činnosti pre oblasť bezpečnosti informačných technológií.

Personalizovanie kľúčových rolí sa vykonáva formou RACI matice s prihliadnutím na segregáciu zodpovedností z pohľadu oddelenia exekutívy, výkonu a kontroly.

Z organizácie bezpečnosti sem patria roly:

- **Administrátor** – zamestnanec odborného útvaru IT, alebo OT, ktorého činnosť spočíva v správe implementovaných bezpečnostných mechanizmov alebo dodávateľ.

- **Vlastník** – rola vedúceho zamestnanca – vedúceho organizačného útvaru, zodpovedného za aktívum v jeho správe, alebo za aktívum, ktoré primárne využíva jeho útvar. Vlastník súčasne zodpovedá aj za riziká spojené s používaním týchto aktív.

Kontrolná zložka systému riadenia bezpečnosti zabezpečuje nezávislú kontrolu dodržiavania povinností v oblasti bezpečnosti informačných technológií a hodnotenie súladu stavu bezpečnosti s požiadavkami všeobecne záväzných právnych predpisov.

Z organizácie bezpečnosti sem patria roly:

- **Auditor** - vykonáva audit stavu bezpečnosti, je nezávislý od útvaru bezpečnosti i prevádzky.

4.4.4 MANAŽÉR INFORMAČNEJ A KYBERNETICKEJ BEZPEČNOSTI

Za presadzovanie kybernetickej a informačnej bezpečnosti je zodpovedný Manažér pre kybernetickú bezpečnosť (MKB), ktorého určuje vedenie spoločnosti.

4.4.5 POVINNOSTI ZAMESTNANCOV

Zamestnanci a osoby s prístupom k informačným aktívam (údajom, dátam, softvéru, IT zariadeniam) zodpovedajú za svoju činnosť a sú povinní:

- dodržiavať stratégiu kybernetickej bezpečnosti a súvisiace pokyny, postupy a opatrenia;
- riadiť sa pokynmi nadriadených a manažéra kybernetickej bezpečnosti;
- chrániť informačné aktíva spoločnosti a ohlásiť každé riziko alebo zraniteľnosť, ktoré ich ohrozujú;
- chrániť poskytnuté prístupové údaje (vlastné prístupové práva) a ohlásiť každé ich prezradenie, zneužitie, alebo podozrenie z ich zneužitia;
- pri práci používať iba vlastné prístupové údaje.

4.4.6 ZAMESTNANCI A OSOBY S PRÍSTUPOM K INFORMAČNÝM AKTÍVAM NESMÚ

- zneužívať informačné aktíva, využívať ich nad rozsah alebo v rozpore so svojimi oprávneniami alebo prístupovými právami;
- používať cudzie prístupové práva alebo spracúvať údaje s oprávneniami inej osoby;
- falšovať, meniť, upravovať alebo ničiť záznamy o svojej činnosti;
- usilovať sa o získanie neoprávneného prístupu k informačným aktívam alebo o zmenu prístupových práv;
- brániť iným oprávneným osobám využívať informačné aktíva;
- zamlčovať skutočnosti o bezpečnostných incidentoch alebo bezpečnostných rizikách a hrozbách.

4.5 RIADENIE AKTÍV

Vedenie si uvedomuje hodnotu svojich aktív a dôležitosť poskytovaných služieb. Za aktívum je preto považované všetko, čo má pre spoločnosť hodnotu a čo je potrebné chrániť. Spracovávané údaje a s nimi spojené informačné systémy a technológie predstavujú mimoriadne významné informačné aktíva, o ktoré je nutné sa starať. Riadenie aktív sa systematicky vykonáva počas celého životného cyklu informačného aktíva.

4.5.1 ZÁSADY RIADENIA AKTÍV

- v rámci prevádzkovaného IT/OT systému musia byť identifikované a evidované jeho aktíva;
- aktíva IT/OT systému musia mať určeného svojho vlastníka;

- v rámci prevádzkovaného IT/OT systému musí byť definovaný spôsob používania aktív;
- informácie spracúvané v rámci IT systému musia byť klasifikované a to s ohľadom na ich citlivosť, kritickosť a právne požiadavky;
- tam, kde je to možné, musia byť aktíva IT/OT systému označené v súlade s klasifikačnou schémou,
- prístup zamestnancov tretích strán k dôležitým informačným aktívam môže byť povolený len v nevyhnutných prípadoch a len za účelom realizácie zmluvných prác a len na čas nevyhnutne potrebný na ich realizáciu. Súčasne musia byť stanovené implementované bezpečnostné opatrenia určené analýzou rizík spojených s prístupom tretej strany;
- musia byť vytvorené formálne postupy na správu výmenných počítačových médií;
- musia byť vytvorené formálne postupy na bezpečnú likvidáciu starých, nepoužívaných alebo vyradených médií;
- musia byť vytvorené formálne postupy na manipuláciu s informáciami a na ich bezpečné uchovávanie.

4.5.2 ŽIVOTNÝ CYKLUS INFORMAČNÉHO AKTÍVA:

Správa informačného aktíva počas jeho životného cyklu zahŕňa niekoľko formálnych fáz a to:

- Plánovanie,
- Schválenie,
- Obstaranie,
- Implementácia,
- Testovanie,
- Nastavenie,
- Nastavenie prístupov,
- Prevádzkovanie,
- Udržiavanie,
- Ukončenie.

Cieľom správy životného cyklu informačných aktív (tiež ako „SDLC“ – Software Development Life-Cycle Management) je optimalizovať získavanie informačných aktív, maximalizovať využitie informačného aktíva a znižovať súvisiace servisné a prevádzkové náklady, čo vedie k zvýšeniu výkonnosti informačných aktív a prispieva k bezpečnosti informačného aktíva. Životný cyklus aktív v nižšie uvedenej tabuľke znázorňuje typické základné fázy a ciele riadenia v životnom cykle informačného aktíva.

Fáza	Popis	Proces / vlastník
Plánovanie	Vypracovanie požiadaviek vrátane: obchodné, technické, prevádzkové, bezpečnostné požiadavky. Privacy požiadavky GDPR Klasifikácia Identifikácia rizík Mitigácia rizík BCM (RTO, RPO)	Change Manager / Predkladateľ
Schválenie	Schválenie projektu/ zmeny	Change Manager / MKB

Obstaranie	Vytvorenie alebo obstaranie informačného aktíva.	Nákup/ Nákupca
Implementácia Testovanie Nastavenie	Otestovanie inf. aktíva podľa požiadaviek. Doplnenie do registra inf. aktív Zabezpečiť bezpečné uloženie. Hardening, nastavenie AV, Log manažment, Backup, BCP/DRP	IT/OT Manager/BP
Nastavenie prístupov	Nastavenie prístupov Užívateľské / privilegované Kontrola prístupov	Riadenie prístupov a oprávnení/ IT/OT Manager/BP
Prevádzkovanie	Poskytovanie podpory a školenia Monitorovanie využitia	Vzdelávanie/ IT/OT Manager/BP Monitorovanie/ IT/OT Manager/BP
Udržiavanie	Testovanie zraniteľností Patchovanie Riadenie rizík Monitorovanie Zálohy/ obnovovať Nahradiť – Vyradenie z prevádzky Optimalizácia - Racionalizácia – Vylepšenie	Vulnerability management, Risk management, Monitoring, Backup IT/OT Manager/BP MKB
Ukončenie	Zánik požiadavky na používanie informačného aktíva Odinštalovanie a likvidácia Vyradenie z registra inf. aktív	IT/OT Manager/BP

4.5.3 VLASTNÍCTVO A ZODPOVEDNOSŤ ZA AKTÍVA

Všetky dôležité aktíva spoločnosti musia byť identifikované a zdokumentované, rovnako ako aj ich hodnota a požadovaná úroveň ochrany, ktorú určí zodpovedná osoba (vlastník aktíva, vlastník procesu, atď.).

Všetky aktíva musia byť označené, alebo musia mať vedené záznamy obsahujúce identifikačné informácie (čísla, kódy, inventárne záznamy a pod.).

Informácie uložené v elektronickej alebo fyzickej podobe musia byť jasne identifikovateľné. Tak, aby bolo jasné a nesporné, kto je ich vlastníkom. Uplatňuje sa princíp priradenia vlastníctva – každé aktívum v spoločnosti má určeného konkrétneho vlastníka, ktorý zodpovedá za správu a riadenie príslušných aktív, jeho klasifikáciu a zaradenie do príslušného klasifikačného stupňa, definovanie prístupu k aktívam a pravidelnú revíziu prístupových oprávnení.

Určenie vlastníkov aktív sa vykonáva vždy pri zaradení aktíva do produkčnej prevádzky. Po odchode pôvodného vlastníka musí byť určený nový vlastník. Zodpovednosť za každé aktívum je pripísaná jednoznačnému vlastníkovi aktíva.

Vlastník aktíva (Asset Owner) – táto rola je priradená osobe, ktorá je zodpovedná za klasifikáciu informácií pre určenie miery a spôsobu ochrany daného aktíva. Typicky je to stredný a vyšší manažment, ktorý je zodpovedný za ochranu aktíva (V MHTH túto pozíciu zastáva riaditeľ úseku, príp. riaditeľ závodu).

Vlastník aktíva môže zodpovednosť za aktuálny manažment dať delegovať, teda preukázateľným spôsobom poveriť iného zodpovedného zamestnanca, tzv. správcu aktíva. Právo delegovania prislúcha iba vlastníčkovi daného aktíva.

Vlastník aktíva je povinný zabezpečiť adekvátnu ochranu aktíva tak, aby v prípade zlyhania jedinej ochrany, existovala ďalšia úroveň ochrany a služba tak nedegradovala pod neakceptovateľnú funkciu/úroveň. Kombinovanie viacerých vrstiev ochrany je uplatňovanie princípu „Defense-In-Depth“.

Vlastník aktíva zodpovedá za celkový stav bezpečnosti daného aktíva a zodpovedá za:

- klasifikáciu a kategorizáciu informácií a aktív vo svojej pôsobnosti v zmysle interných predpisov a platnej legislatívy,
- definovanie pravidiel pre prístup k informáciám a aktívam vo svojej pôsobnosti,
- definovanie pravidiel pre pridelovanie rolí a atribútov prístupu,
- definovanie štandardných a privilegovaných prístupov pre definované pracovné roly/pozície,
- definovanie pravidiel segregácie prístupových rolí v MHTH,
- proces schvaľovania a priradzovania prístupov k aktívam vo svojej pôsobnosti,
- pravidelné prehodnocovanie a kontrolu priradených a vytvorených oprávnení.

Správca aktíva (Custodian) – je rola priradená používateľovi, ktorý je zodpovedný za implementáciu predpísaných opatrení definovaných bezpečnostnými politikami a nariadeniami organizácie. Správca vykonáva všetky nevyhnutné aktivity k ochrane a prijatiu adekvátnej ochrany v zmysle CIA (musí byť zaistená Dôvernosť, Dostupnosť, Integrita) dať a naplnené požiadavky manažmentu. Tieto aktivity môžu pozostávať z vykonávania a testovania záloh, overovania dátovej integrity, výkonov pri priradzovaní a zmene prístupov, nasadzovaní

bezpečnostných riešení, implementácii pravidiel pre manažment hesiel, správy dátového úložiska založeného na klasifikácii, atď.

Používateľ (User) – akýkoľvek zamestnanec, ktorý je používateľ IKT, alebo má prístup do informačného systému. Úroveň prístupu závisí vždy od priradených pracovných rolí a je limitovaná iba na úkony spojené s výkonom pracovných povinností v zmysle pracovnej pozície zamestnanca (princíp najnižších oprávnení - Least-Of-Privilege). Používateľ je zodpovedný za bezpečné používanie zverených aktív, dodržiavanie bezpečnostných politík a požiadaviek tak, ako ich nariadila MHTH.

Audítor – je zodpovedný za revíziu a verifikáciu správnosti a úplnosti implementovaných smerníc a politík bezpečnosti. Audítor sa vo svojich reportoch zameriava na súlad a účinnosť, ktorá je revidovaná manažmentom spoločnosti/Porada vedenia. Prípadné nálezy sú transformované do nových direktív a politík, ktoré sú následne uplatňované naprieč celou organizáciou.

4.5.4 SEGREGÁCIA PRÁVOMOCÍ

Je požadované uplatňovať opatrenia princípu „Segregation-Of-Duties“, teda jasne a preukázateľne oddeliť jednotlivé právomoci a to najmä z dôvodu neoprávnenej zmeny, alebo zneužitia aktív. Používanie, prístupovanie, či zmena aktíva je možná len na základe procesu overenia identity používateľa na konkrétnu činnosť. Pre všetky prostredia a procesy organizácie musí byť vždy uplatnený bezpečnostný mechanizmus AAA.

Z dôvodu minimalizácie neoprávneného vykonania neautorizovanej operácie (modifikácia, neoprávnené použitie,...) aktíva, je každý vlastník aktíva povinný definovať segregáciu rolí. Každé operácii nad aktívom, musí predchádzať jej schválenie. Za existenciu a uplatňovanie jednotného procesu je zodpovedný vlastník aktíva. V prípade, ak segregáciu nie je možné jednoducho zabezpečiť, resp. je ťažko realizovateľná, je nutné dodatočne zabezpečiť systém s obmedzením na menšie skupiny aktív (napr. na základe lokality, druhu a pod.), príp. takéto prípady je potrebné zabezpečiť iným spôsobom (zvýšený monitoring, využitie iných technických a organizačných prostriedkov,...)

V prípade, ak správu aktív vykonáva externý subjekt, podmienky sú definované v smernici pre riadenie dodávateľských vzťahov, príp. v príslušnej zmluvnej dokumentácii.

V prípade, ak sa predmet činnosti dotýka základných služieb MHTH, je nutné uzavrieť ZoBOaNP. Za aktuálnosť a dodržanie zodpovedá vlastník aktíva.

4.6 RIADENIE RIZÍK

Vedenie MHTH si uvedomuje skutočnosť, že jeho činnosť a poslanie sú priamo alebo aj nepriamo spojené s rôznymi rizikami. S neustálym rastom rôznych druhov rizík a mierou ich závažnosti rastie aj význam riadenia rizík.

Proaktívny prístup prostredníctvom riadenia rizík umožňuje úspešne zvládať tieto riziká, minimalizovať ich dopady na chod organizácie a náklady na ich elimináciu dostať na predvídateľnú a ekonomicky zodpovedajúcu úroveň.

Riadenie rizík je významnou zložkou zavádzaných bezpečnostných opatrení pre zabezpečenie kybernetickej aj informačnej bezpečnosti počas celého životného cyklu sietí a informačných systémov.

Zásady riadenia rizík:

- analýza rizík kybernetickej/informačnej bezpečnosti sa musí vykonávať periodicky;
- postup pre výkon analýzy rizík musí byť dokumentovaný;
- analýza rizík musí vychádzať z identifikovaných hrozieb, zraniteľností a následkov dopadov na aktíva;
- musia byť určené vlastníci rizík;
- musia byť určené kritériá pre akceptáciu rizík;

- riziká vyššie ako akceptovateľné, na základe stanovených kritérií, je nevyhnutné riadiť;
- výsledky analýzy rizík musí autorizovať vedenie;
- na riadenie neakceptovaných rizík musia byť vyčlenené potrebné zdroje.

Riadenie rizík pre oblasť KIB je rozpracované v kapitole [Metodika riadenia bezpečnostných rizík](#).

4.6.1 OVEROVANIE STAVU KYBERNETICKEJ BEZPEČNOSTI

Pre zistenie stavu kybernetickej a informačnej bezpečnosti a zhodnotenia súladu bezpečnostnej stratégie a bezpečnostných politík s požiadavkami ZoKB, s požiadavkami iných všeobecne záväzných právnych predpisov a so zmluvnými záväzkami, je nevyhnutné vykonávať pravidelné overovanie stavu prostredníctvom externého auditu. Okrem toho je potrebné v prípade mimoriadnych situácií využiť inštitút mimoriadneho auditu.

Overenie stavu kybernetickej a informačnej bezpečnosti sa bude realizovať auditmi v pravidelných intervaloch, určených:

- legislatívou,
- internými predpismi.

Okrem pravidelných auditov bude vykonaný audit relevantných častí prostredia po významných zmenách.

Mimoriadny audit môže nariadiť:

- Bezpečnostná komisia v prípade mimoriadneho zvýšenia počtu incidentov, alebo podozrenia na nízku účinnosť aktuálnych opatrení,
- NBÚ (v zmysle platnej legislatívy).

4.7 BEZPEČNOSTNÁ ARCHITEKTÚRA

Stratégia bezpečnostnej architektúry v spoločnosti je odvodená zo stratégie kybernetickej a informačnej bezpečnosti:

- Všetade, kde je to možné a relevantné, musia byť bezpečnostné mechanizmy aplikované pri zdroji a overené ich používateľom, čomu hovoríme „end-to-end“ bezpečnosť.
- Každý používateľ zdrojov musí byť identifikovaný a autentizovaný skôr ako sa mu povolí prístup (autorizácia) k zdroju.
- Riadenie prístupu k aktívam spoločnosti musí byť funkčné počas celého trvania relácie.
- Všetky bezpečnostne citlivé operácie musia byť overené minimálne dvoma poverenými zamestnancami (pravidlo 4 očí).
- Všetky uložené, archivované a zálohované údaje musia byť v závislosti od citlivosti chránené umiestnením v chránenom priestore alebo budú šifrované.
- Všetky, z pohľadu bezpečnosti kritické udalosti, musia byť zaznamenané. Každý záznam musí byť chránený pred neautorizovaným prezeraním, modifikáciou a zničením.
- Zabezpečenie nemožnosti odmietnutia autorstva a nemožnosti odmietnutia akceptácie transakcie elektronickým podpisom musí byť voliteľné.
- Bezpečnostná architektúra bude implementovaná pre všetky nové informačné systémy. Pre existujúce prevádzkované informačné systémy budú aplikované tie bezpečnostné mechanizmy, ktoré nebudú mať zásadný dopad na prevádzky-schopnosť systému. Pre systémy, kde nebude možné aplikovať navrhované bezpečnostné mechanizmy, bude udelená výnimka. Takéto systémy je potrebné postupne nahradiť novými aj s aplikovaním navrhovaných bezpečnostných mechanizmov.
- Mechanizmy fyzickej a technickej bezpečnosti budú použité ako komplementárne opatrenia na zníženie nárokov na bezpečnostné mechanizmy spoločnosti, nie ako ich náhrada.

4.7.1 BEZPEČNÝ DIZAJN

Požiadavky na informačné systémy podmieňujúce poskytovanie základných služieb, musia odzrkadľovať nasledujúce princípy bezpečného dizajnu.

Systém:

- vyžaduje na svoje používanie len minimálne práva (least privilege),
- oddeľuje používateľov a ich role, práva a privilégia (separation of duties),
- aplikuje viacnásobnú ochranu cez navzájom sa prekrývajúce alebo doplnujúce opatrenia (defense in depth),
- pri zlyhaní nikdy nenaruší svoju vlastnosť bezpečnosť (fail secure),
- má vyvážený pomer bezpečnosti a funkčnosti/použitelnosti (economy of mechanisms)
- má obsahovať len funkcionality, ktoré je nevyhnutná pre jeho podstatu (KISS – Keep It Simple Stupid princíp),
- musí implementovať princíp overovania práv pri každej citlivej aktivite (complete mediation),
- používa také bezpečnostné opatrenia, ktorých preskúmanie/audit nijakým spôsobom neovplyvní samotnú bezpečnosť ich fungovania (open design),
- používa pre privilegovaného používateľa iné funkcie a mechanizmy ako pre bežného používateľa (least common mechanism),
- používa také bezpečnostné mechanizmy, ktoré sú pre používateľa prijateľné a nenúti ho ich obchádzať (psychological acceptability),
- je dizajnový postavený tak, že nemôže kompletne zlyhať len vďaka jedinej chybe alebo bezpečnostnej zraniteľnosti (weakest link),
- musí vychádzať z neproprietárnych, otvorených a kompatibilných štandardov (leveraging existing components).

Všade tam, kde tieto všeobecné princípy nie je možné z objektívnych dôvodov dodržať, musí nastúpiť analýza rizík alebo modelovanie hrozieb, pomocou ktorých sa identifikujú doplnujúce alebo náhradné (work-around) opatrenia.

Bez ohľadu na nedostupnosť opatrení a nemožnosť naplniť zásady bezpečného dizajnu, akékoľvek rozhodnutie musí byť zdôvodnené a zdokumentované a reportované oddeleniu bezpečnosti a krízového riadenia.

4.7.2 ZÁSADY IMPLEMENTÁCIE BEZPEČNOSTNEJ ARCHITEKTÚRY

Pri implementácii bezpečnostnej architektúry spoločnosti, budú dodržané zásady vyplývajúce zo stratégie bezpečnostnej architektúry a požadovanej bezpečnostnej úrovne:

- Použitie minimálneho počtu identifikačných systémov pre všetky prostredia spoločnosti.
- Použitie bezpečnostných mechanizmov autentizácie všetkých používateľov založených na princípe identifikácie jedinečným kódom (ID) a poznaní hesla alebo na overení vlastníctva jedinečného certifikátu v kombinácii s identifikačným číslom a heslom a technickým prostriedkom (tokenom).
- Centralizovaná správa, riadenie bezpečnostného systému a monitorovanie činnosti všetkých používateľov a všetkých administrátorov (správcov) systému v reálnom čase, centralizovaný zber auditných záznamov o činnosti používateľov zdrojov systému a ich centralizované vyhodnocovanie.
- Oddelenie aktív IS spoločnosti od okolitého prostredia pomocou ochranných systémov a ich umiestnenie v chránenom priestore.
- Detekcia narušenia bezpečnosti v reálnom čase aplikovaná priamo pri citlivých procesoch a pri všetkých vstupoch do spoločnosti, umiestneného v chránenom priestore v reálnom čase.
- Vytvorenie bezpečnostného povedomia používateľov a administrátorov IS spoločnosti prostredníctvom výchovno-vzdelávacieho programu.
- Viacnásobné implementovanie tých istých bezpečnostných mechanizmov v jednom prostredí s rôznou silou.

- Implementovanie bezpečnostných mechanizmov pomocou špeciálnych bezpečnostných komponentov alebo pomocou vybraných funkcií a charakteristík komponentov spoločnosti. Z dôvodov cenovej výhodnosti budú využívané predovšetkým softvérové riešenia všade tam, kde to umožní dobrá úroveň technickej a režimovej bezpečnosti. Tam, kde to citlivosť procesov vyžaduje, budú použité hardvérové riešenia.
- Tam, kde je to možné, použijú sa z dôvodu cenovej výhodnosti opatrenia režimovej bezpečnosti podporované mechanizmami technickej bezpečnosti.

Riziko prezradenia pozorovaním čitateľných údajov zobrazených na obrazovkách pracovných staníc, terminálov a iných komponentov spoločnosti je na akceptovateľnej úrovni alebo úplne potlačené zabezpečením:

- umiestnenia komponentov mimo prístupných okien;
- umiestnenia dôležitých komponentov minimálne na druhé poschodie alebo vyššie;
- oddelenia (umiestnením do bezpečnostnej zóny);
- pootočená obrazovky smerom od neautorizovanej osoby,
- vybavením vybraných pracovných staníc a terminálov polarizačným filtrom.

Keďže bezpečnostný profil organizácie MHTH je založený v prvom rade na zaručení dostupnosti a integrity systémov poskytujúcich základné služby, stratégia bezpečnostnej architektúry kladie dôraz na:

- štandardizáciu a homogénnosť kľúčových systémov,
- kompatibilitu používaných systémov a sietí na úrovni binárneho kódu a používaných protokolov,
- dôsledné oddeľovanie dôveryhodných od nedôveryhodných prostredí s využitím firewallov, IPS/IDS a SIEM a bezpečnostných varovaní v reálnom čase,
- dôsledné oddeľovanie kritických, produkčných systémov od podporných a riadiacich (VLAN, VPN),
- kontrolované prepájanie IT a OT systémov tak, aby boli všetky prestupové miesta monitorované a aby zraniteľnosti jedného prostredia nemohli mať dopad na druhé prostredie,
- minimalizáciu priameho prepojenia OT s nedôveryhodnými sieťami ako je internet, pričom všade tam, kde je to možné, je treba vytvoriť prestupnú, nárazníkovú zónu (tzv. DMZ),
- trvalý prehľad o používaných technológiách a systémoch,
- presnú evidenciu informačných zdrojov a
- dôsledné plánovanie a riadenie zmien v architektúre IT/OT systémov.

Aby bola bezpečnostná architektúra účinná, musí vychádzať zo schválenej IT architektúry a celkovej stratégie rozvoja informačných a komunikačných služieb organizácie a tie z celkovej podnikateľskej stratégie organizácie (zosúladenie bezpečnosti s obchodnými a podnikateľskými zámermi).

4.8 BEZPEČNOSTNÁ DOKUMENTÁCIA

Revíziu bezpečnostnej dokumentácie iniciuje a riadi MKB. Revízia sa vykonáva:

- pravidelne každý rok;
- vždy po významnej zmene legislatívy;
- vždy po významnej zmene organizačnej štruktúry;
- po významnej zmene v IS, alebo celej IT/OT infraštruktúre;
- v prípade nariadenia mimoriadnej revízie bezpečnostnou komisiou.

Za vykonanie revízie jednotlivých dokumentov zodpovedá vecne príslušný organizačný útvar v zmysle rozdelenia kompetencií pre oblasť riadenia KB a IB.

Vykonanie revízie bezpečnostnej dokumentácie nariaďuje aj bezpečnostná komisia a to podľa potreby, vzniku mimoriadnych okolností a stanoveného plánu pravidelných revízií.

5. POLITIKY KYBERNETICKEJ A INFORMAČNEJ BEZPEČNOSTI

5.1 ÚVODNÉ USTANOVENIA PKIB

Na zabezpečenie súladu so ZoKB, vyhláškou NBÚ č. 227, vyhláškou NBÚ č. 226/2025 Z. z., ktorou sa určujú identifikačné kritériá závažného narušenia fungovania prevádzkovateľa základnej služby, a vyhláškou NBÚ č. 493/2022 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora, a pre účely plnenia požiadaviek vyplývajúcich z uvedenej legislatívy v prostredí organizácie MHTH, sa ustanovujú Politiky kybernetickej a informačnej bezpečnosti (ďalej tiež ako „PKIB“, alebo „Politika“).

Účelom PKIB je holisticky definovať rámec riadiaceho procesu, ktorý MHTH používa na implementáciu a manažment kvality IT a OT služieb, ktoré podporujú potreby MHTH a pre následné rozsiahle štandardizované zabezpečenie informačnej, technologickej a komunikačnej infraštruktúry MHTH. PKIB rovnako upravuje činnosti súvisiace s riadením IB a KB v spoločnosti a zodpovednosti za ich výkon.

Ustanoveniami smernice sa riadi každý zamestnanec, ktorý vykonáva činnosti upravené v tejto smernici.

5.2 SPRÁVA POLITIKY A KONTROLA JEJ DODRŽIAVANIA

- Za prípravu a revíziu PKIB zodpovedá MKB.
- Politiku musí prerokovať a schváliť vedenie spoločnosti.
- PKIB sa vyhodnocuje, preskúmava a aktualizuje v pravidelných ročných intervaloch,
- V prípade významných legislatívnych, organizačných a technických zmien, pri zistení nových, doteraz neuvažovaných rizík, sa aktualizuje okamžite,
- V prípade zvýšenia počtu bezpečnostných incidentov a kybernetických bezpečnostných incidentov sa aktualizuje podľa potreby.

Zmeny zásad a cieľov stanovených touto Politikou musia, v odôvodnených prípadoch, navrhovať a spracovávať kompetentní odborní pracovníci zabezpečujúci metodické riadenie a výkon činností bezpečnosti a ochrany informačného systému. Zmeny musia byť predkladané na schválenie vedeniu spoločnosti.

Dokument sa aktualizuje a riadi v zmysle [MHTH S01 Riadenie dokumentov a procesov](#).

Kontrola dodržiavania PKIB a jej obsahovej náplne prebieha internou kontrolou informačnej bezpečnosti so zameraním na jednotlivé oblasti kybernetickej a informačnej bezpečnosti. Nedodržanie pravidiel a zásad uvedených v PKIB a prijatých bezpečnostných opatrení bude posudzované ako porušenie pracovnej disciplíny.

5.3 URČENIE ROZSAHU A ZODPOVEDNOSTI V OBLASTI IB A KB

Účelom tejto kapitoly je jasne definovať hranice IB a KB a zodpovednosti pri ich implementácii v MHTH.

5.3.1 DEFINOVANIE ROZSAHU IB A KB

MHTH musí definovať hranice IB a KB a BCM s cieľom rozhodnúť, ktoré informácie chce chrániť. Takéto informácie musia byť chránené bez ohľadu na to, či sa uchovávali, spracovávali alebo posielajú do alebo mimo rozsahu IB a KB a BCM. Skutočnosť, že niektoré informácie sú k dispozícii mimo rozsahu IB a KB a BCM nemá za následok, že nebudú uplatňované bezpečnostné opatrenia. Zodpovednosť bude prevedená na tretiu stranu, ktorá informácie spravuje.

Rozsah IB a KB a BCM na základe právnych, regulačných, zmluvných a iných požiadaviek je definovaný v nasledujúcich bodoch:

5.3.2 PROCESY A SLUŽBY

Prevádzkovanie základných služieb v rozsahu: **Výroba tepla, dodávka tepla, výroba elektrickej energie.**

5.3.3 SIETE A IT INFRAŠTRUKTÚRA

Všetky telekomunikačné siete a počítačové siete spoločnosti sú prevádzkované samostatne alebo dodávateľsky na základe zmluvy.

5.3.4 VYLÚČENIE Z ROZSAHU

Nie sú definované žiadne výluky.

5.3.5 ZODPOVEDNOSŤ ZA DODRŽIAVANIE BEZPEČNOSTI

Bezpečnostná politika spoločnosti musí byť dodržiavaná:

- všetkým zamestnancami spoločnosti,
- zamestnancami tretích strán v rozsahu, ktorý je nevyhnutný na ochranu aktív spoločnosti; tieto povinnosti musia byť stanovené zmluvne, resp. iným záväzným dokumentom,
- pridelenie zodpovedností zamestnancom za bezpečnosť pôsobí preventívne voči narušeniu bezpečnosti spoločnosti. Všetci vedúci zamestnanci spoločnosti sú zodpovední za zavádzanie politiky spoločnosti do každodennej praxe, za podporovanie a presadzovanie zvyšovania úrovne bezpečnosti spoločnosti, prevádzkovaných sietí a IS. Vedúci zamestnanci jednotlivých organizačných útvarov zodpovedajú za to, že ich podriadení konajú v súlade s prijatými bezpečnostnými zásadami a všetky bezpečnostné postupy v rámci ich oblasti zodpovednosti sú vykonávané správne a v súlade s právnymi predpismi a riadiacimi dokumentmi,
- každá tretia strana, podieľajúca sa na prevádzke sietí a IS v spoločnosti, musí mať určenú a poverenú osobu zodpovednú za to, že zamestnanci tretích strán konajú v súlade s prijatými bezpečnostnými zásadami a všetky bezpečnostné postupy v rámci ich oblasti zodpovednosti sú vykonávané správne a v súlade s právnymi predpismi a riadiacimi dokumentmi,
- všetci zamestnanci spoločnosti a zamestnanci tretích strán sú zodpovední za ochranu informačných aktív spoločnosti, prevádzkovaných sietí a IS. Všetci zamestnanci spoločnosti sú povinní dodržiavať pravidlá vyplývajúce z interne riadenej dokumentácie. Taktiež zodpovedajú za všetky činnosti, ktoré vykonávajú v rámci svojej práce,
- zamestnanci tretích strán sú povinní sa oboznámiť s interne riadenou dokumentáciou spoločnosti, v rozsahu potrebnom na výkon činností, ktoré vykonávajú pre spoločnosť. Sprístupnenie interne riadenej dokumentácie im sprostredkuje poverený zamestnanec spoločnosti (koordinátor zmluvného vzťahu za spoločnosť). Môže ísť o excerpt internej smernice, spravidla prostredníctvom samostatnej politiky, alebo metodického predpisu.

Nedodržanie zásad a princípov uvedených v politike spoločnosti a požiadaviek vyplývajúcich z prijatých bezpečnostných opatrení je posudzované ako porušenie pracovnej disciplíny alebo porušenie zmluvných podmienok vo vzťahu k tretej strane.

5.4 SÚLAD S POŽIADAVKAMI

Definuje ako zamedziť porušovaniu zákonných alebo zmluvných povinností súvisiacich s bezpečnosťou.

5.4.1 IDENTIFIKÁCIA POŽIADAVIEK A ZAJINTERESOVANÝCH STRÁN

MKB je zodpovedný za identifikovanie všetkých osôb a organizácií, ktoré môžu ovplyvniť alebo môžu byť ovplyvňované vplyvom implementácie IB a KB alebo BCM (zúčastnené strany), a všetky súvisiace právne, regulačné, zmluvné a iné požiadavky (regulátory).

MKB definuje, kto bude zodpovedný za dodržiavanie jednotlivých požiadaviek a kto bude zodpovedný za informovanie dotknutých strán v prípadoch zmien v požiadavkách.

MKB musí vypracovať zoznam všetkých požiadaviek a zainteresovaných strán a zodpovedných osôb pre právne, regulačné, zmluvné a iné požiadavky a publikovať ich do zoznamu.

Každý zamestnanec spoločnosti musí oznámiť MKB, ak zistí novú právnu, regulačnú, zmluvnú alebo inú požiadavku, ktorá by mohla byť relevantná pre IB a KB alebo BCM.

5.4.1.1 Revízia a hodnotenie

MKB je zodpovedný za preskúmanie zoznamu právnych, regulačných, zmluvných iných požiadaviek minimálne každých 6 mesiacov a aktualizovať podľa potreby. MKB bude informovať všetky zainteresované strany o každej aktualizácii.

MKB je zodpovedný za hodnotenie súladu IB a KB a BCM s relevantnými právnymi, regulačnými a zmluvnými požiadavkami najmenej raz za rok.

5.4.2 PRÁVA K DUŠEVNÉMU VLASTNÍCTVU

Ochrana duševného vlastníctva stanovuje legálne používanie software a informačných produktov, vrátane získavania software prostredníctvom dôveryhodných zdrojov a vytvárania kópií licencovaného software. Udržiavanie povedomia na ochranu práv duševného vlastníctva je zabezpečené vzdelávacím procesom zamestnancov.

5.4.3 OCHRANA ZÁZNAMOV

Záznamy sú chránené pred stratou, zničením, falšovaním, neoprávneným prístupom a neoprávneným vydaním v súlade s legislatívnymi a zmluvnými požiadavkami, ako aj požiadavkami vyplývajúcimi z interných dokumentov upravujúcich činnosť organizácie.

Ochrana záznamov vychádza z politiky pre klasifikáciu informácií a riadenie dokumentov a záznamov.

5.4.4 OCHRANA OSOBNÝCH ÚDAJOV

Ochrana osobných údajov je riadená v súlade so zákonom č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov vymedzuje základné bezpečnostné ciele, ktoré je potrebné dosiahnuť na ochranu informačného systému, v ktorom sú spracúvané osobné údaje, aby sa minimalizovali možné riziká narušenia jeho bezpečnosti.

Ochranu osobných údajov upravuje [MHTH S06 Smernica o ochrane osobných údajov](#).

5.4.5 TYPICKÉ SPÔSOBY SPRACÚVANIA OSOBNÝCH ÚDAJOV

Spracúvaním osobných údajov podľa zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov sa ďalej rozumie vykonávanie operácií alebo súboru operácií s osobnými údajmi, najmä ich získavanie, zhromažďovanie, šírenie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, blokovanie, likvidácia, ich cezhraničný prenos, poskytovanie, sprístupňovanie alebo zverejňovanie.

Spracovanie osobných údajov je popísané v smernici [MHTH S06 Smernica o ochrane osobných údajov](#).

5.4.6 REGULÁCIA KRYPTOGRAFICKÝCH OPATRENÍ

Kryptografické opatrenia musia byť používané v súlade so všetkými prípustnými dohodami, legislatívou a predpismi. Zamestnanci nesmú používať vlastné kryptografické nástroje bez povolenia MKB.

5.4.7 PRESKÚMANIE BEZPEČNOSTI INFORMÁCIÍ

Nezávislé preskúmanie je nevyhnutné pre zaistenie vhodnosti, primeranosti a účinnosti prístupov spoločnosti k riadeniu bezpečnosti informácií. Preskúmanie zahŕňa posúdenie možnosti pre zlepšenie a potreby zmien v prístupe k bezpečnosti vrátane politiky a definovania cieľov opatrení.

Preskúmanie je realizované interným audítorm, nezávislým manažérom alebo externou organizáciou, ktorá sa špecializuje na takéto preskúmavanie.

Výsledky nezávislého preskúmania sú zaznamenané, uchované a oznámené vedeniu spoločnosti. Pokiaľ nezávislé preskúmanie zistí nedostatky, manažment prijme nápravné opatrenia.

5.4.8 SÚLAD S BEZPEČNOSTNÝMI POLITIKAMI A NORMAMI

Vedúci pracovníci v rámci výkonu funkcie preskúmajú plnenie požiadaviek bezpečnosti informácií stanovených v politikách, normách a ďalších platných predpisoch. Pre účinné a pravidelné preskúmanie sú vhodné automatické nástroje so zasielaním notifikácií. V prípade zistenia nesúladu vedúci pracovník musí

- Identifikovať príčiny nesúladu
- Určiť kroky k dosiahnutiu súladu
- Implementovať príslušné nápravné opatrenia
- Preskúmať prijaté nápravné opatrenia s cieľom overiť ich efektívnosť

Výsledky preskúmania prijatých nápravných opatrení sú zaznamenávané a uchovávané pre potreby oznámenia osobám vykonávajúcim nezávislé preskúmanie.

5.4.9 PRESKÚMANIE TECHNICKÉHO SÚLADU

Technický súlad je preskúmaný pomocou automatických nástrojov, ktoré vytvárajú technické správy (majetok, Penetračné testy, testy zraniteľností, súlad s normami,...) Tieto testy sú plánované, dokumentované, vyhodnocované a hlavne opakované. Preskúmanie technického stavu musí byť vykonané len kompetentnou a oprávnenou osobou alebo pod dohľadom takejto osoby.

5.5 ZÁSADY PRIJATEĽNÉHO POUŽÍVANIA

5.5.1 ÚČEL, ROZSAH A POUŽÍVATELIA

Účelom tejto kapitoly je vymedziť jasné pravidlá pre používanie informačného systému a iných informačných aktív spoločnosti.

Tento dokument sa vzťahuje na celý rozsah systému IB a KB, t. J. Na všetky informačné systémy a iné informačné aktíva používané v rámci rozsahu IB a KB.

5.5.2 PRIJATEĽNÉ POUŽÍVANIE

Informačné aktíva je možné použiť len pre potreby spoločnosti s cieľom plnenia úloh týkajúcich sa procesov spoločnosti.

5.5.3 ZODPOVEDNOSŤ ZA MAJETOK

Každé informačné aktívum má definovaného vlastníka. Vlastník aktíva je zodpovedný za dôvernosť, integritu a dostupnosť informačného aktíva.

5.5.4 ZAKÁZANÉ ČINNOSTI

Je zakázané používať informačné aktíva spôsobom, ktorý zbytočne zaberá kapacitu, oslabuje výkon informačného systému alebo ohrozuje bezpečnosť. Je zakázané:

- Sťahovanie nadmerných súborov (grafických, audio, video), ktoré nie sú určené pre obchodné účely spoločnosti, posielanie reťazových správ cez službu e-mail, hranie počítačových hier.
- Používanie firemného emailu na registráciu na mimo firemných platformách/eshopoch.
- Preposielanie firemných dokumentov vo vlastníctve MHTH na súkromné emailové adresy.
- Inštalovať softvér na lokálnom počítači bez výslovného povolenia.

- Inštalovať softvér na prevádzkovaných serveroch mimo schváleného softvérového vybavenia. Používať kryptografické nástroje (šifrovanie) na lokálnom počítači, s výnimkou prípadov uvedených v politike pre klasifikáciu informácií.
- Sťahovať programy z externých médií a internetu.
- Nainštalovať alebo používať periférne zariadenia, ako napríklad modemy, pamäťové karty alebo iné zariadenia pre ukladanie a čítanie údajov (napríklad disky USB flash) bez výslovného povolenia MKB v súlade s politikou pre klasifikáciu informácií.

5.5.5 POUŽÍVANIE MAJETKU MIMO SPOLOČNOSTI

Zariadenia, informácie alebo softvér, bez ohľadu na jeho formu alebo ukladacie médium nemôže byť vyvezené bez predchádzajúceho súhlasu CIO.

5.5.6 VRÁTENIE MAJETKU PO UKONČENÍ ZMLUVY

Pri ukončení pracovného pomeru zamestnanca alebo pri skončení iného zmluvného vzťahu, na základe ktorých sa používali zariadenia, softvér alebo informácie v elektronickej alebo papierovej forme, používateľ musí tieto zariadenia, softvér alebo informácie odovzdať ešte pred samotným skončením pracovného pomeru alebo iného zmluvného vzťahu.

5.5.7 PROCES ZÁLOHOVANIA

Používatelia sú povinní obchodné informácie spracovávať výlučne na pridelených sieťových/cloudových úložiskách, ktoré sú automaticky zálohované.

5.5.8 ANTIVÍRUSOVÁ OCHRANA

Antivírusový softvér musí byť nainštalovaný na každom počítači s aktivovaním automatických aktualizácií.

5.5.9 AUTENTIFIKÁCIA PRE INFORMAČNÉ SYSTÉMY

- Prístup používateľov do informačného systému je možný len na základe jednofaktorovej alebo viacfaktorovej autentifikácie.
- Prístup je schvaľovaný vlastníkom alebo prevádzkovateľom informačného aktíva.
- Užívatelia môžu využívať informačný systém iba na účely, pre ktoré im bol povolený, t. j. pre ktoré dostali prístupové práva.
- Používatelia nesmú vykonávať činnosti, ktoré by umožňovali nepovolený prístup k systému alebo jeho funkcionalitám.

5.5.10 POUŽÍVATEĽSKÝ ÚČET

Používateľ musí používať len svoje prihlasovacie údaje, nesmie používať prihlasovacie údaje inej osoby a nesmie poskytnúť svoje prihlasovacie údaje iným osobám. Je zakázané používanie skupinových účtov, to znamená zdieľanie prihlasovacích údajov viacerými osobami.

Vlastníkom používateľského účtu je jeho užívateľ, ktorý je zodpovedný za jeho použitie a všetky transakcie vykonané prostredníctvom tohto používateľského účtu.

5.5.11 POUŽÍVATEĽSKÉ HESLO

Používatelia musia použiť definovaný bezpečnostný postup pri výbere a používaní hesla:

- heslá sa nesmú oznamovať iným osobám, vrátane nadriadených a správcov systému;
- heslá sa nesmú distribuovať prostredníctvom akéhokoľvek kanála (pomocou ústnej, písomnej alebo elektronickej distribúcie). Výnimku tvoria jednorazové heslá, alebo úvodné heslá, ktoré sú jednorazové a majú časovo obmedzenú platnosť;
- heslá musia byť menené periodicky po definovanej dobe, alebo bezodkladne, ak existujú náznaky, že heslo alebo systém mohol byť kompromitovaný – v takom prípade sa rieši ako bezpečnostný incident;

- komplexita, pravidlá a správa podliehajú definovanej politike hesiel spoločnosti.

5.5.12 OCHRANA ZDIEĽANÝCH ZARIADENÍ A VYBAVENIA

Dokumenty, ktoré obsahujú dôverné informácie musia byť ihneď odobraté z tlačiarňí, faxov a kopírovacích strojov.

5.5.13 POUŽÍVANIE INTERNETU

Prístup na Internet slúži na pracovné účely. Pri používaní Internetu je zakázané:

- vykonávať činnosti, ktoré sú v rozpore s platnou legislatívou,
- vykonávať činnosti, ktoré urážajú politické, etnické, náboženské cítie iných,
- pokúšať sa o:
 - útok s cieľom spomalenia, resp. blokovania poskytovaných služieb,
 - neoprávnené získanie autentifikačných údajov, resp. neoprávnený prístup k iným počítačom a sieťam,
 - neoprávnený prístup k zdrojom a údajom, ich neoprávnené použitie, modifikácia, znehodnotenie alebo zničenie,
 - rozširovanie alebo spúšťanie programov, ktoré ohrozujú bezpečnosť IT (napr. vírusy, trójske kone, hackerské programy, sniffovacie programy, červy, atď.),
- pripájať prenosné zariadenia (notebooky, handheldy), ktoré sú vybavené interným alebo externým HW komponentom (modem, PC-karta, WIFI-karta) umožňujúcim nezávislé pripojenie k Internetu, súčasne do siete spoločnosti a do Internetu,
- používať iný, ako v spoločnosti schválený spôsob pripojenia do siete.

Z prostredia spoločnosti môže byť Internet dostupný iba prostredníctvom definovaného pripojenia spoločnosťou, s pripojením cez firewall alebo proxy server. Priamy prístup na Internet pomocou modemov, mobilný internet, bezdrôtové siete alebo iné zariadenia pre priamy internetový prístup je možný iba so súčasne aktívnou ochranou koncového zariadenia kde sú spoločnosťou definované práva pre sprístupnenie jednotlivých url adries a je využívaná aktívna ochrana voči hrozbám.

Z prevádzkových sietí je akýkoľvek priamy prístup do internetu striktne zakázaný. Prestupy do nedôveryhodných sietí musia byť vopred schválené oddelením bezpečnosti a krízového riadenia.

MKB môže dať blokovat' prístup na niektoré internetové stránky pre jednotlivých používateľov, skupiny používateľov alebo všetkých zamestnancov v spoločnosti. Ak prístup na niektoré webové stránky je zablokovaný, používateľ môže predložiť písomnú žiadosť na povolenie na prístupu na takéto stránky, ktorú posudzuje MKB. Používateľ sa nesmie pokúšať obísť takéto obmedzenia.

5.5.13.1 Všeobecné pravidlá pre používanie internetu:

- Nepoužívať ukladanie údajov na internetové úložiská.
- Nestahovať software alebo iné údaje, ktoré môžu byť chránené autorským právom (video, hudba, hry).
- Nepoužívať aukcie, digitálne trhoviská, alebo E-shopy (facebook marketplace, Temu...).
- Vyhnúť sa stránkam, ktoré sú obscénne, rasistické, urážlivé alebo nezákonné.
- Vyhnúť sa používaniu súkromnej elektronickej pošty (gmail, yahoo, post..).
- Vyhnúť sa používaniu sociálnych sietí, online hier, online hazardu a pornografií.

Používateľ musí považovať informácie získané prostredníctvom neoverených internetových stránok za nespoľahlivé. Takéto informácie pre účely podnikania je potrebné overiť na pravosť a správnosť.

Používateľ je zodpovedný za všetky možné dôsledky vyplývajúce z neoprávneného alebo nevhodného použitia internetových služieb.

5.5.14 E-MAILOVÁ KOMUNIKÁCIA A INÉ METÓDY VÝMENY SPRÁV

Metódy výmeny správ sú verbálne, elektronická pošta, sťahovanie súborov z internetu, prenos dát cez prostriedky instant messages, telefóny, faxy, SMS textové správy, prenosné médiá a sociálne siete a iné špecifické služby.

V súlade s prevádzkovými postupmi pre informačné a komunikačné technológie, politiky elektronického prenosu informácií ako aj politiky pre klasifikáciu informácií MKB určuje komunikačný kanál, ktorý môže byť použitý pre každý typ údajov.

Používatelia musia posilať správy obsahujúce pravdivé informácie. Je zakázané posilať materiály so znepokojujúcim, sexuálnym, hrubým, hanlivým obsahom alebo obsahom porušujúcim zákon. Používatelia nesmú posilať spamové správy osobám, s ktorými nebol preukázateľný žiaden obchodný vzťah alebo osobám, ktoré si takéto informácie nevyžadovali.

Používateľ v prípade nadmerného prijímania SPAM správ musí informovať manažéra MKB.

Správy s obsahom podľa klasifikačného stupňa „Dôverné“ alebo „Prísne Dôverné“ sa musia chrániť v zmysle pokynu o klasifikácii informácií uvedeného v kapitole 5.4.3 tejto smernice.

Každá e-mailová správa musí obsahovať prehlásenie, s výnimkou správ posielaných prostredníctvom automatických komunikačných systémov. Používateľ pri odoslaní správy na informačných kanáloch (sociálne siete, fóra, atď.) musí jednoznačne uviesť, že vyjadrenie alebo názor nepredstavuje názor spoločnosti.

5.5.14.1 POUŽÍVANIE ELEKTRONICKEJ POŠTY

Elektronická pošta slúži na pracovné účely. Používateľ je oprávnený použiť systém elektronickej pošty na prenos údajov podľa ich klasifikácie, pričom je povinný pri prenose zabezpečiť ich ochranu v zmysle klasifikačnej schémy.

Pri používaní elektronickej pošty je zakázané:

- šíriť poplašné správy (hoax),
- správy s obsahom, ktorý uráža politické, etnické, náboženské ctenie iných,
- správy obsahujúce súbory so škodlivým kódom,
- používať elektronickú poшту na neoprávnené zasielanie nadmerného množstva správ, alebo správ s nadmernou veľkosťou,
- preposielanie reťazových emailov, preposielanie materiálov vo vlastníctve spoločnosti na súkromné adresy, používať firemný email na registráciu na portály a online trhoviská.
- používať elektronickú poшту na reklamné a politické ciele, resp. na rušenie alebo ohrozovanie iných používateľov.

Používateľom sa odporúča:

- neotvárať atypický a neočakávaný e-mail prichádzajúci z neznámej, prípadne aj známej adresy, odporúča sa označiť ho ako „nevyžiadanú poшту“ a vymazať bez čítania, nakoľko môže byť nositeľom škodlivého kódu,
- nezadávať e-mailovú adresu na neznámych alebo nekryptovaných webových stránkach, resp. vo webových súťažiach – dôsledkom môže byť príval veľkého množstva nevyžiadanej pošty.

5.5.15 AUTORSKÉ PRÁVA

Používatelia nesmú vytvárať neoprávnené kópie softvéru vo vlastníctve organizácie, s výnimkou prípadov povolených zákonom alebo zmluvou.

Používatelia po skopírovaní softvéru alebo iného licencovaného obsahu z iných zdrojov sú zodpovední za všetky dôsledky, ktoré môžu vyplývať zo zákona o ochrane duševného vlastníctva.

5.5.16 MOBILNÉ ZARIADENIA

Mobilné počítačové vybavenie zahŕňa všetky druhy prenosných počítačov, mobilné telefóny, smart telefóny, pamäťové karty a iné mobilné zariadenia používané na ukladanie, spracovanie alebo prenos údajov.

5.5.16.1 ZÁKLADNÉ PRAVIDLÁ PRE MOBILNÉ ZARIADENIA

Špeciálne pri mobilných zariadeniach (pc, mobilný telefón) treba dbať na ich zabezpečenie v automobiloch alebo iných druhov dopravy, verejných priestoroch, hotelových izbách, zasadačkách, konferenčných centrách a iných nechránených oblastiach mimo priestorov spoločnosti.

Osoby, ktoré mobilné zariadenia používajú mimo priestorov spoločnosti, musia dodržiavať tieto pravidlá:

- mobilné zariadenie obsahujúce dôležité, kritické alebo citlivé informácie nesmú byť ponechané bez dozoru a ak to konkrétne zariadenie umožňuje, musia byť chránené heslom alebo inou formou zabezpečenia;
- pri použití mobilných zariadení na verejných miestach, používateľ musí zabrániť zneužitiu údajov neoprávnenými osobami;
- aktualizácie a bezpečnostné záplaty a ďalšie nastavenia neriadené systémom centrálne, sú vykonávané užívateľom bezodkladne;
- ochrana proti škodlivým kódom je zabezpečená inštalovaním a aktualizáciou AV a IDR ochrany;
- osoba, ktorá používa mobilné zariadenia mimo MHTH je zodpovedná za pravidelné zálohovanie údajov;
- pripojenie do komunikačných sietí a výmena údajov musí odrážať citlivosť údajov;
- údaje v prenosných počítačoch musia byť šifrované (napríklad systémom „BitLocker“);
- ochrana citlivých údajov sa musí vykonávať v súlade s politikou klasifikácie informácií podľa kapitoly 5.4.3 tejto smernice;
- Zariadenie musí byť chránené MDM, resp. MAM systémom.
- v prípade mobilných zariadení je obzvlášť nutné aplikovať politiku čistej obrazovky.

5.5.16.2 VZDIALENÝ PRÍSTUP A PRÁCA NA DIALKU

Vzdialený prístup k aktívam spoločnosti znamená, že informačné a komunikačné zariadenia sú používané za účelom vykonávania práce zamestnancov mimo fyzických priestorov organizácie.

Vzdialený prístup musí byť schválený nadriadeným pracovníkom daného zamestnanca.

Zamestnanec využívajúci vzdialený prístup je zodpovedný za nasledovné:

- ochrana mobilných zariadení uvedených v predchádzajúcej časti;
- zabránenie neoprávnenému prístupu osôb žijúcich alebo pracujúcich na mieste, kde sa pripojenie vykonáva;
- zodpovedajúce nastavenie miestnej siete pre pripojenie k internetu;
- ochrana práv duševného vlastníctva organizácie, softvér alebo iné materiály, ktoré môžu byť chránené právami duševného vlastníctva;
- vrátenie zariadení a dát spoločnosti v prípade ukončenia pracovného pomeru alebo obdobného pracovnoprávneho vzťahu zamestnanca alebo ukončenia iného zmluvného vzťahu používateľa so spoločnosťou;
- zabezpečenie bezpečnej konfigurácie zariadenia, na ktorom sa vzdialený prístup vykonáva, je súčasťou manažmentu koncových staníc v správe úseku IT.

5.5.17 BEZPEČNOSŤ PRI PRÁCI S PRENOSNÝMI MÉDIAMI A MOBILNÝMI ZARIADENIAMÍ

Pre zabezpečenie ochrany údajov nachádzajúcich sa na prenosných a mobilných médiách pred stratou, únikom, alebo iným neoprávneným sprístupnením je špecialista/administrátor úseku IT zodpovedný za nastavenie adekvátnych opatrení, kde musia byť minimálne zohľadnené:

- autorizačný proces pre narábanie s médiami a mobilnými prostriedkami;
- zabezpečenie ochrany médií a mobilných prostriedkov v súlade s minimálnymi bezpečnostnými požiadavkami v súlade s klasifikáciou informácií uchovávaných na médiách;
- uchovávanie a práca s médiami a mobilnými prostriedkami v prostredí v súlade s odporúčaniami výrobcu, resp. dodávateľa;
- špecifiká práce s médiami a mobilnými prostriedkami;
- väzby na procesy riešenia bezpečnostných incidentov a chybových stavov.

Obsahy vybraných prenositeľných médií, ktoré opúšťajú priestory spoločnosti, musia byť zašifrované.

Pásky a zálohovacie médiá (ak sú použité v OT prostredí) sú spravované a v plnej gescii príslušného OT manažéra, resp. spravované dodávateľom technológie.

Na prenos médií je potrebné použiť spoľahlivé prostriedky transportu alebo kuriéra;

Všetky médiá s osobnými a citlivými údajmi musia byť šifrované uložené v bezpečnom, chránenom prostredí, podľa špecifikácie výrobcu;

Informácie, ktoré majú byť uchované dlhšie, ako je doba životnosti média, na ktorom sú uložené (na základe špecifikácie výrobcu), musia byť uložené aj na inom mieste, aby sa tak predišlo ich strate spôsobenej nečitateľnosťou média;

Médiá obsahujúce elektronické dokumenty musia byť zlikvidované bezpečne a spoľahlivo, napr. Spálením, rozrezaním alebo hĺbkovým vymazaním dát, ak nemajú byť použité pre iný účel.

Na pracovných staniciach v IT, sú USB zariadenia mass storage blokovanie celoplošne v rámci IT prostredia, kde špecialista/administrátor úseku IT zabezpečí zablokovanie USB portov. Špecialista/administrátor úseku IT je povinný blokovanie USB centrálnie riadiť a udeľovať výnimky blokovaní v spolupráci s MKB. Ďalej eviduje zoznam pracovných staníc, na ktorých je zablokované a zakázané používanie prenosných USB zariadení;

Na pracovných staniciach, na ktorých je povolené používanie prenosných USB zariadení, zabezpečí Špecialista/administrátor úseku IT automatické šifrovanie vybraných USB médií a kontrolu USB zariadení antivírusovým programom;

Na operátorských staniciach v OT prostredí, musia byť zariadenia USB mass storage celoplošne blokovanie. Dodávateľ v OT zabezpečí zablokovanie USB portov v spolupráci s príslušným OT manažérom. Výnimky musí schváliť MKB.

5.5.18 MONITOROVANIE VYUŽÍVANIA INFORMAČNÝCH A KOMUNIKAČNÝCH SYSTÉMOV

Všetky údaje, ktoré sú vytvorené, uložené, odoslané alebo prijaté prostredníctvom informačných systémov, sa považujú za vlastníctvo spoločnosti.

Používatelia súhlasia, že oprávnené osoby zo spoločnosti môžu pristupovať ku všetkým údajom a prístup týchto osôb sa nebude považovať za porušenie súkromia užívateľov.

MHTH môže používať špecializované nástroje na identifikáciu a blokovanie zakázanej komunikácie a filtrovanie zakázaného obsahu.

Z dôvodu ochrany prevádzkovaných základných služieb sú všetky prístupy ku kritickým aktívam monitorované a činnosti zaznamenávané. V zmysle platnej legislatívy si MHTH vyhradzuje právo záznamy o činnosti použiť, a to najmä pre účely vyšetrovania v prípade kybernetického incidentu alebo udalosti, alebo za účelom povinnosti spolupráce a postúpenia informácií príslušným úradom (§19 ods. 6, §24 ods. 1 ZoKB).

5.5.19 BEZPEČNOSTNÉ INCIDENTY

Každý zamestnanec, dodávateľ alebo tretia osoba, ktorá je v kontakte s údajmi alebo systémami spoločnosti, musí nahlásiť akúkoľvek zraniteľnosť systému, udalosť alebo udalosti poukazujúce na možný bezpečnostný incident podľa pravidiel Incident Managementu.

5.6 POLITIKA AI a LLM

Politika pre používanie umelej inteligencie a aplikácií s podporou LLM modelov a cloudových služieb. Nástroje umelej inteligencie zahŕňajú generatívne AI modely (ChatGPT, Claude, Copilot, Gemini, Grok, Lama), AI asistentov, obrazové generátory, analytické AI nástroje a ďalšie služby založené na strojovom učení alebo spracovaní prirodzeného jazyka.

V súlade s prevádzkovými postupmi pre informačné a komunikačné technológie, politikou pre cloudové služby ako aj politikou pre klasifikáciu informácií MKB určuje, ktoré AI nástroje môžu byť použité pre jednotlivé typy údajov. Zoznam schválených AI nástrojov je vedený oddelením bezpečnosti a krízového riadenia a pravidelne aktualizovaný.

Používatelia musia používať AI nástroje zodpovedne a v súlade s právnymi predpismi (GDPR, AI Act). Je zakázané používať AI na tvorbu zavádzajúceho, diskriminačného, urážlivého obsahu alebo obsahu porušujúceho zákon. Používatelia nesmú vkladať do AI nástrojov citlivé údaje bez oprávnenia. Výstupy AI musia byť vždy overené pred použitím, nakoľko AI sa môže dopúšťať chýb alebo porušovať autorské práva.

Používateľ v prípade podozrivého správania AI nástroja alebo bezpečnostného incidentu súvisiaceho s AI musí okamžite informovať oddelenie bezpečnosti a krízového riadenia.

Údaje podľa klasifikačného stupňa „Dôverné“ alebo „Prísne Dôverné“ nesmú byť vkladané do AI nástrojov, s výnimkou interných AI systémov schválených vedením spoločnosti MHTH v zmysle pokynu o klasifikácii informácií.

Každý AI generovaný obsah určený na publikovanie alebo zdieľanie s externými stranami musí obsahovať označenie, že bol vytvorený s pomocou AI. Používateľ pri použití AI na verejných platformách (sociálne siete, fóra, atď.) musí jednoznačne uviesť, že vyjadrenie alebo obsah vytvorený AI nepredstavuje oficiálny názor spoločnosti.

5.6.1 POUŽÍVANIE AI NÁSTROJOV

AI nástroje slúžia na podporu pracovných úloh. Používateľ je oprávnený použiť AI nástroje na spracovanie údajov podľa ich klasifikácie, pričom je povinný zabezpečiť ich ochranu v zmysle klasifikačnej schémy a tejto smernice.

Pri používaní AI nástrojov je zakázané:

- vkladať osobné údaje fyzických osôb (mená, rodné čísla, adresy, zdravotné záznamy),
- vkladať heslá, API kľúče, prístupové tokeny, certifikáty a iné autentifikačné údaje,
- vkladať obchodné tajomstvá, dôverné stratégie, cenníky a nepublikované obchodné informácie,
- vkladať kompletný produkčný zdrojový kód obsahujúci citlivé konfigurácie,
- vkladať konfigurácie a inštrukcie OT a IT systémov a ich komponentov,
- vkladať mapové podklady a výkresy zakreslenia technologickej infraštruktúry v správe MHTH,
- vkladať zmluvy, dohody o mlčanlivosti (NDA) a právne dokumenty bez schválenia,
- používať neschválené AI nástroje alebo bezplatné verzie bez firemnej licencie,
- vkladať údaje do AI nástrojov poskytovateľov mimo EÚ/EHP bez overenia zmluvných podmienok,
- publikovať AI generovaný obsah bez overenia presnosti, právnej korektnosti a autorských práv,
- používať AI na automatizované rozhodovanie o zamestnancoch alebo zákazníkoch bez ľudského dohľadu,
- vytvárať deepfakes alebo iný zavádzajúci obsah prostredníctvom AI.

Používateľom sa odporúča:

- používať prednostne interné AI nástroje schválené organizáciou pre spracovanie firemných údajov,
- anonymizovať údaje pred vložením do AI (nahradit' skutočné hodnoty fiktívnymi príkladmi, napr. Meno.priezvisko@xyz.sk alebo 192.168.1.1 atď.),
- overiť výstupy AI vždy u odborníka alebo spoľahlivého zdroja pred ich použitím,
- pri generovaní kódu vykonať bezpečnostnú kontrolu (code review) a testovanie na zraniteľnosti,
- označiť AI generovaný obsah tam, kde je to vhodné alebo vyžadované,
- pri pochybnostiach o vhodnosti použitia AI konzultovať s vedúcim pracovníkom alebo oddelením bezpečnosti a krízového riadenia,
- nezdieľať prístupy k AI nástrojom s neoprávnenými osobami,
- hlásiť akékoľvek podozrivé správanie AI alebo potenciálny únik údajov okamžite na oddelenie bezpečnosti a krízového riadenia.

SCHVÁLENÉ AI NÁSTROJE A CLOUDOVÉ SLUŽBY

Používatelia môžu používať výhradne AI nástroje a cloudové služby schválené oddelením bezpečnosti a krízového riadenia. Aktuálny zoznam schválených nástrojov je dostupný na intranete MHTH. Pred použitím nového AI nástroja je nutné podať žiadosť o schválenie cez oddelenie bezpečnosti a krízového riadenia.

Požiadavky na cloudové AI služby (v súlade s prílohou č. 1, položka 151 vyhlášky NBÚ č. 227/2025 Z.z.):

- zadokumentované minimálne bezpečnostné požiadavky pre používanie cloudových služieb,
- riadenie kybernetickej bezpečnosti cloudových služieb v zmysle vyhlášky NBÚ,
- lokalizácia dát v EÚ/EHP alebo v krajinách s rozhodnutím o primeranosti podľa GDPR,
- šifrovanie údajov pri prenose (TLS 1.3+) aj v pokoji (AES-256),
- zmluvné záruky o ochrane údajov, SLA min. 99,5%, možnosť auditu,
- možnosť úplného vymazania údajov do 30 dní,
- kompletné logovanie prístupov (retencia min. 1 rok),
- notifikácia bezpečnostných incidentov do 24 hodín,
- certifikácie ISO 27001, SOC 2 Type II,
- multi-faktorová autentifikácia (MFA),
- transparentný zoznam subdodávateľov,
- možnosť exportu všetkých údajov v štruktúrovanom formáte pre prípad exit stratégie.

Riziká poskytovateľov cloudových služieb:

Aj keď cloudová služba deklaruje ukladanie údajov v EÚ, používatelia musia byť informovaní o nasledujúcich rizikách:

Jurisdikčné riziko: Cloudové služby prevádzkované americkými spoločnosťami (napr. Microsoft, Google, Amazon, SAP, OpenAI) podliehajú americkým zákonom (CLOUD Act, FISA 702), ktoré umožňujú americkým vládnym zložkám (FBI, NSA, CIA) prístup k údajom európskych používateľov bez ich vedomia, aj keď sú údaje fyzicky uložené v EÚ. Poskytovateľ služby nemôže

zaručiť, že údaje neopustia EÚ pri technickom spravovaní systémov alebo pri vynútenom prístupe zo strany USA orgánov.

Technické riziko: Aj pri deklarovanej lokalizácii dát v EÚ môžu údaje dočasne prechádzať cez infraštruktúru mimo EÚ (napr. pri zálohe, replikácii, správe systémov, logovaní, diagnostike). Metadata (kto pristupoval, kedy, odkiaľ) môžu byť ukladané centrálne mimo EÚ.

Zmluvné obmedzenia: Poskytovatelia väčšinou neponúkajú zmluvnú garanciu, že údaje za žiadnych okolností neopustia EÚ. Štandardné zmluvy obsahujú výnimky pre technickú údržbu, právne požiadavky a núdzové situácie.

Každá zmluva s poskytovateľom cloudových AI služieb musí obsahovať komplexnú exit stratégiu zabezpečujúcu možnosť ukončenia služby a prechodu na alternatívne riešenie bez straty údajov alebo kontinuity prevádzky. Poskytovateľ musí umožniť úplný export všetkých údajov (vrátane konfigurácie, logov a metadát) vo všeobecne používanom, strojovo čitateľnom formáte (JSON, XML, CSV) bez dodatočných poplatkov. Po ukončení zmluvy musí byť poskytnutá lehota minimálne 30 dní na stiahnutie údajov pred ich neobnoviteľným vymazaním s vydaním certifikátu o vymazaní. Výpovedná lehota činí minimálne 90 dní, počas ktorých poskytovateľ zachováva plnú funkčnosť služby a poskytuje technickú podporu pri migrácii vrátane možnosti paralelnej prevádzky. Organizácia sa vyhýba vendor lock-in situáciám preferovaním otvorených štandardov, dokumentovaných API a prenositeľných dátových formátov oproti proprietárnym riešeniam. Funkčnosť exit stratégie sa testuje minimálne 1x ročne skúšobným exportom na overenie úplnosti a použiteľnosti exportovaných údajov. Exit stratégia je súčasťou každej zmluvy s cloudovým poskytovateľom a jej plnenie je pravidelne kontrolované oddelením bezpečnosti a krízového riadenia.

Z týchto dôvodov platí:

- pre údaje klasifikované ako „Dôverné“ alebo „Prísne Dôverné“ sa uprednostňujú riešenia európskych poskytovateľov alebo on-premise systémy,
- pri použití cloudových služieb sa vykoná posúdenie vplyvu na ochranu osobných údajov (DPIA) a analýza rizík z pohľadu informačnej a kybernetickej bezpečnosti,
- citlivé obchodné údaje, osobné údaje zamestnancov a zákazníkov, obchodné tajomstvá a interné bezpečnostné konfigurácie nesmú byť ukladané do cloudov mimo Európskych poskytovateľov bez dodatočných technických opatrení (napr. end-to-end šifrovanie s kľúčmi spravovanými výhradne v EÚ),
- používatelia a správcovia sú povinní brať na vedomie toto riziko a voliť komunikačné kanály a nástroje adekvátne citlivosti spracovávaných údajov.

Používanie AI nástrojov a cloudových služieb je monitorované. Oddelenie bezpečnosti a krízového riadenia vykonáva pravidelnú kontrolu dodržiavania tejto politiky a technický monitoring používania AI nástrojov. Porušenie tejto politiky môže viesť k disciplinárnym opatreniam až po ukončenie pracovného pomeru.

5.7 POLITIKA PRE KLASIFIKÁCIU INFORMÁCIÍ

5.7.1 ÚČEL, ROZSAH A UŽÍVATELIA

Účelom tejto kapitoly je zabezpečenie ochrany informácií na primeranej úrovni.

Tento dokument je aplikovaný na celý rozsah IB a KB, t. j. na všetky typy informácií, bez ohľadu na formu tlačенých alebo elektronických dokumentov, aplikácií, databáz, vedomostí, atď.

5.7.2 KLASIFIKÁCIA INFORMAČNÝCH AKTÍV

Hodnota, kritickosť alebo citlivosť informačného aktíva sa určuje prostredníctvom procesu klasifikácie, ktorým sa označuje stupeň hrozby v prípade zneužitia, neautorizovanej zmeny alebo narušenia dostupnosti informačného aktíva.

Pri klasifikácii platia tieto pravidlá:

- určenie CIA – každé klasifikované informačné aktívum má pridelený jeden klasifikačný stupeň pre atribút Dôvernosti, jeden klasifikačný stupeň pre atribút Integrity a jeden klasifikačný stupeň pre atribút Dostupnosti;
- bezpečnostné informácie, nastavenia, postupy, smernice a ostatné úkony súvisiace s riadením aktív sa klasifikujú na rovnaký alebo vyšší klasifikačný stupeň, akým sú označené informačné aktíva, ktorých sa týkajú;
- za priradenie správneho klasifikačného stupňa zodpovedá primárne autor/vlastník informácie alebo funkčný/business vlastník informačného aktíva;
- ak informačné aktívum nemá priradený žiadny klasifikačný stupeň, je potrebné s ním zaobchádzať ako s klasifikačnou úrovňou pre dôvernosť "Interné", integritu "Stredná" a pre dostupnosť "Stredná";
- je povinnosťou každého používateľa informačného aktíva upozorniť na prípadné chybné alebo chýbajúce označenie klasifikačnej úrovne, pretože na toto označenie sa následne viaže náležitá ochrana vo forme procesných, personálnych alebo technických bezpečnostných opatrení.

5.7.3 VÝZNAM KLASIFIKÁCIE INFORMAČNÝCH AKTÍV

- umožňuje naplniť strategické rozhodnutie vrcholového manažmentu o potrebe ochrany kritických aktív organizácie;
- pomáha pri identifikácii tých aktív, ktoré sú pre organizáciu najdôležitejšie alebo najcennejšie;
- zdôvodňuje výber ochranných mechanizmov;
- umožňuje dosiahnuť súlad s právnymi predpismi a nariadeniami;
- pomáha definovať úrovne prístupu, typy oprávneného použitia a podmienky na deklasifikáciu a/alebo kontrolované zničenie informačných aktív, ktoré už nie sú cenné, dôležité alebo citlivé;
- napomáha riadeniu životného cyklu informačných aktív, od ich vzniku, cez používanie, nevyhnutnú dobu uchovávaní až po ich likvidáciu;
- umožňuje rozhodovať o následných a podľa možnosti automatizovaných technologických ochranných mechanizmoch, ako sú napríklad centrálné riadenie prístupov, antimalvérová ochrana, scanovanie na technické zraniteľnosti, IRM (Information Rights Management), DLP (Data Leak Protection) a pod.

5.7.4 DÔVERNOSŤ

Dôvernosť / Confidentiality – informácia je prístupná len autorizovaným osobám

Úroveň dôvernosti je stanovená na základe nasledujúcich kritérií:

- hodnota informácií;
- citlivosť a kritickosť informácií;
- zákonných a zmluvných záväzkov.

ZoKB, resp. prislúchajúca vyhláška V227 predpisuje klasifikačné úrovne pre dôvernosť Verejné, Interné, Chránené, Prísne chránené. Z dôvodu sprehľadnenia a zjednotenia názvosloví sa pre zabezpečenie dôvernosti informačných aktív v MHTH používajú nasledovné úrovne klasifikácie informačných aktív:

Verejné	Sprístupnenie informácie nepredstavuje žiadne riziko, nemajú žiadnu hodnotu pre potenciálneho kybernetického útočníka; informačné aktíva určené pre verejnosť, ktoré sú dostupné z verejných zdrojov a zahŕňajú napríklad informácie z médií, povinne publikované informácie alebo všeobecne dostupné informácie;
Interné	Sprístupnenie informácií predstavuje nízke riziko, lebo nie sú priamo zneužitelné potenciálnym kybernetickým útočníkom, napriek tomu majú slúžiť len na vnútornú potrebu organizácie; informačné aktíva, ktoré sú používané a prístupné pre všetkých používateľov v rámci organizácie prevádzkovateľa základnej služby bez ohľadu na ich pracovnú rolu; <i>následkom neoprávnenej manipulácie alebo únikom môžu byť ohrozené záujmy spoločnosti s nízkym až stredným finančným dopadom, alebo môže byť poškodené obchodné meno spoločnosti;</i> <i>na sprístupnenie týchto aktív tretím stranám je potrebné schválenie zo strany vlastníka informácie;</i>
Dôverné	Sprístupnenie informácie predstavuje vysoké riziko, nakoľko informácie môžu mať zásadnú hodnotu pre potenciálneho kybernetického útočníka a vysokú citlivosť pre organizáciu; patria sem aj také informácie, ktorých dôvernosť je vyžadovaná v rámci platných zákonov; informačné aktíva, ktoré sú používané a prístupné len určeným skupinám oprávnených osôb a ktorých neautorizované sprístupnenie, prezradenie môže mať pre prevádzkovateľa základnej služby negatívny vplyv na poskytovanie služby; <i>následkom neoprávnenej manipulácie alebo únikom môžu byť ohrozené záujmy spoločnosti so stredným až vysokým finančným dopadom, alebo môže byť poškodené obchodné meno spoločnosti;</i> <i>prístup k údajom klasifikovaným ako „Dôverné“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a je vymedzený výhradne vopred definovaným a schváleným útvarom alebo iným jasne vymedzeným skupinám osôb;</i> <i>tretie strany majú k týmto údajom prístup len v nevyhnutných a jednoznačne definovaných prípadoch schválených funkčným (business) vlastníkom;</i> <i>Do tejto kategórie spadajú osobné, zmluvné a finančné údaje zamestnancov/zákazníkov, informácie tretích strán s príslušným stupňom ochrany, daňové tajomstvo, finančné a kontrolované údaje, auditné záznamy, plány obnovy, analýzy a hodnotenie rizík a zraniteľností, konfiguračné a technické nastavenia IS, informácie spadajúce pod obchodné tajomstvo, plány obstarávania, stratégia obstarávania, súťažné podklady, vybrané informácie KB, vybrané skutočnosti obchodnej, výrobné, alebo technickej povahy súvisiace s predmetom činnosti podnikania, ktoré môžu mať akúkoľvek hodnotu a môžu byť materiálneho alebo nemateriálneho charakteru, akékoľvek iné informácie na základe požiadaviek vedúcich pracovníkov a vlastníkov aktív.</i>
Prísne dôverné	Sprístupnenie takýchto informácií predstavuje najväčšie riziko, majú najväčšiu hodnotu pre potenciálneho kybernetického útočníka, najväčšiu citlivosť pre organizáciu;

	<i>informačné aktíva, ktoré sú používané a prístupné len jednotlivým vybraným používateľom prevádzkovateľa základnej služby a ktorých neautorizované odhalenie, prezradenie alebo zničenie, môže mať s vysokou pravdepodobnosťou negatívny vplyv na poskytovanie základnej služby;</i> <i>následkom neoprávnenej manipulácie alebo únikom môžu byť ohrozené záujmy spoločnosti s vysokým až veľmi vysokým finančným dopadom, alebo môže byť poškodené obchodné meno spoločnosti;</i> <i>prístup k údajom klasifikovaným ako „Prísne dôverné“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a výhradne konkrétnym, vopred definovaným a schváleným osobám;</i> <i> tretie strany majú k týmto údajom prístup len vo výnimočných a jednoznačne definovaných prípadoch schválených vlastníkom, alebo na základe ustanovení osobitných predpisov;</i> <i>Do tejto kategórie spadajú skutočnosti obchodnej, výrobnnej, alebo technickej povahy súvisiace s predmetom činnosti podnikania, obchodným tajomstvom, ktoré môžu mať akúkoľvek hodnotu a môžu byť materiálneho alebo nemateriálneho charakteru, informácie o plánovaných akvizíciách, detailné konfigurácie bezpečnostných prvkov a zariadení, detailné informácie k topológiám sietí, autentizačným mechanizmom a samotným údajom používateľov, šifrovacie kľúče, heslá, elektronické podpisy a pečate, akékoľvek iné informácie na základe požiadaviek vedúcich pracovníkov a vlastníkov aktív.</i>
--	---

Základným pravidlom je používať **najnižšiu možnú úroveň** ochrany a zabezpečiť primeranú úroveň ochrany, aby sa predišlo zbytočným nákladom na bezpečnosť.

5.7.5 RE-KLASIFIKÁCIA

Vlastník informácií musí prehodnotiť úroveň dôvernosti svojich informačných aktív každé 2 roky a posúdiť, či netreba zmeniť príslušný stupeň dôvernosti. Ak je to možné, mala by byť úroveň dôvernosti znížená.

5.7.6 OZNAČOVANIE INFORMÁCIÍ

Stupne dôvernosti sú označené nasledujúcim spôsobom:

- **papierové dokumenty** – príslušný stupeň dôvernosti je uvedený v pravom hornom rohu každej stránky dokumentu; na prednej strane obalu takéhoto dokumentu, na zakladači, v ktorom je uložený dokument
- **elektronické dokumenty** – príslušný stupeň dôvernosti je uvedený v pravom hornom rohu každej stránky dokumentu
- **informačné systémy** – príslušný stupeň dôvernosti v aplikácii a databázach musia byť uvedené na obrazovke systému prístupu, ako aj v pravom hornom rohu každej po sebe idúcej obrazovky zobrazujúcej dôverné informácie
- **elektronická pošta** – príslušný stupeň dôvernosti je uvedený v prvej línii tela e-mailu
- **elektronické pamäťové médium** (disky, pamäťové karty, atď.) – príslušný stupeň dôvernosti musí byť uvedený na vrchnej ploche média
- **informácie poskytnuté ústne** – príslušný stupeň dôvernosti informácie postúpenej ústne, telefonicky alebo iným komunikačným prostriedkom musia byť oznámené pred samotnou informáciou.

Označovať príslušným stupňom dôvernosti sa musia aktíva klasifikované ako „Dôverné“
Označovať príslušným stupňom dôvernosti sa musia aktíva klasifikované ako „Prísne Dôverné“

Pri informačných systémoch sa ako minimálna požiadavka vyžaduje všeobecný oznam v znení:

- „Neautorizovaný prístup k tomuto systému je zakázaný. Na prístup do tohto systému patriacemu spoločnosti MHTH musíte mať oprávnenie.“, prípadne:
- „Neoprávnené pokusy o prístup alebo kroky vedúce k obídenu kontrolovaného prístupu a neautorizovanému používaniu tohto systému môžu mať za následok občiansko-právne alebo trestné konanie.“

Kde je to možné, použiť všeobecné znenie: Podmienky používania služieb [Terms of Use]

5.7.7 KLASIFIKÁCIA PROJEKTOV

Spoločnosť zodpovedá za to, že všetky projekty musia byť klasifikované a musia byť definované bezpečnostné a organizačné opatrenia pre ochranu fyzických častí ako aj ochranu údajov.

Pred začatím nového projektu projektový manažér definuje a preškolí celý projektový tím, v zmysle požiadaviek KB, o čom vykoná zápis. Projektový manažér klasifikuje projekt klasifikačným stupňom „Interné“ alebo „Dôverné“.

Klasifikačný stupeň „Interné“ sa aplikuje pre interné projekty.

Označovať príslušným stupňom dôvernosti sa „musia“ projekty klasifikované ako „Dôverné“.

Ochrana projektových údajov sa aplikuje v zmysle kapitoly „SPRACOVANIE KATEGORIZOVANÝCH INFORMÁCIÍ“.

5.7.8 SPRACOVANIE KATEGORIZOVANÝCH INFORMÁCIÍ

Osoby s prístupom ku kategorizovaným informáciám sa musia riadiť pravidlami uvedenými v nasledujúcej tabuľke. MKB musí začať konanie v zmysle platných [Pracovných poriadkov](#) jednotlivých závodov vždy, keď sú porušené pravidlá, alebo ak sa informácie poskytujú neoprávneným osobám. V súlade s postupom riadenia Incidentov sa spíše každá udalosť súvisiaca s ochranou kategorizovaných informácií.

5.7.8.1 Zásady spracovania z pohľadu Dôvernosti:

	Interné	Dôverné	Prísne Dôverné
Papierové dokumenty	- prístup môžu mať iba oprávnené osoby; - ak sa dokument odosiela mimo organizáciu, doklad sa musí zaslať ako doporučená zásielka; - dokumenty sa môžu uchovávať iba v miestnostiach bez prístupu verejnosti; - dokumenty musia byť pravidelne odoberané z tlačiarň alebo faxov	- písomnosti sa musia skladovať bezpečne; - dokument môže byť poslaný v rámci organizácie aj mimo nej iba dôveryhodnou osobou v uzavretej a zalepenej obálke; - faxovanie dokumentu nie je povolené; - dokument môže byť vytlačený iba vtedy, ak oprávnená osoba má tlačiareň pod kontrolou	- písomnosti sa musia skladovať bezpečne; - dokument môže byť poslaný v rámci organizácie aj mimo nej iba dôveryhodnou osobou v uzavretej a zalepenej obálke; - faxovanie dokumentu nie je povolené; - dokument môže byť vytlačený iba vtedy, ak oprávnená osoba má tlačiareň pod kontrolou
Elektronické dokumenty	- prístup môže mať iba oprávnená osoba; - keď sú súbory vymieňané prostredníctvom služby	- dokument musí byť uložený v zašifrovanej podobe; - dokument môže byť uložený iba na serveroch,	- dokument musí byť uložený v zašifrovanej podobe; - dokument môže byť uložený iba na

	Interné	Dôverné	Prísne Dôverné
	ako FTP, chat, atď., musia byť chránené heslom; - prístup do IS, kde je dokument uložený, musí byť chránený komplexným heslom; - obrazovka, na ktorej sa dokument zobrazuje, sa musí automaticky uzamknúť po 10 minútach nečinnosti	ktoré sú riadené spoločnosťou; - dokument sa nesmie vymieňať prostredníctvom služby ako FTP, chatu, atď.	serveroch, ktoré sú riadené spoločnosťou - dokument sa nesmie vymieňať prostredníctvom služby ako FTP, chatu, atď.
Informačné systémy	- prístup môžu mať iba oprávnené osoby; - prístup k IS musí byť chránený komplexným heslom; - obrazovka musí byť automaticky uzamknutá po 10 minútach nečinnosti; - IS sa môže nachádzať iba v priestoroch s kontrolovaným fyzickým prístupom	- prístupy k IS musia byť kontrolované procesom overenia pomocou jedno alebo viac-faktorovou autentifikáciou; - IS môže byť nainštalovaný iba na serveroch riadených spoločnosťou; - IS sa môže nachádzať iba v priestoroch s kontrolovaným fyzickým prístupom a kontrolou identity osôb pri vstupe do miestnosti	- prístupy k IS musia byť kontrolované procesom overenia pomocou jedno alebo viac-faktorovou autentifikáciou; - IS môže byť nainštalovaný iba na serveroch riadených spoločnosťou - IS sa môže nachádzať iba v priestoroch s kontrolovaným fyzickým prístupom a kontrolou identity osôb pri vstupe do miestnosti
Elektronická pošta	- prístup môžu mať iba oprávnené osoby - odosielateľ musí starostlivo skontrolovať meno príjemcu	- musí byť šifrovaná	- musí byť šifrovaná
Elektronické pamäťové médium	- prístup môžu mať iba oprávnené osoby; - médiá pri prenášaní mimo spoločnosti musia byť chránené heslom; - ak sú médiá odosielané mimo organizáciu, médium sa musí zaslať ako doporučená zásielka; - médium sa môže uchovávať iba v priestoroch s kontrolovaným fyzickým prístupom	- médiá sa musia skladovať bezpečne; - médiá môžu byť zaslané v rámci organizácie aj mimo nej iba dôveryhodnou osobou v uzavretej a zapečatenej obálke	- médiá sa musia skladovať bezpečne; - médiá môžu byť zaslané v rámci organizácie aj mimo nej iba dôveryhodnou osobou v uzavretej a zapečatenej obálke

	Interné	Dôverné	Prísne Dôverné
Informácie prenášané ústne	- prístup môžu mať iba oprávnené osoby; - neoprávnené osoby nesmú byť prítomné v miestnosti pri odovzdávaní informácie	- rozhovor vykonávaný prostredníctvom komunikačného prostriedku musí byť šifrovaný; - žiadny prepis konverzácie nesmie byť uchovávaný	- rozhovor vykonávaný prostredníctvom komunikačného prostriedku musí byť šifrovaný; - žiadny prepis konverzácie nesmie byť uchovávaný

5.7.9 INTEGRITA

Integrita/Integrity – informácia je správna a úplná, a počas spracovávania nebola modifikovaná neautorizovaným spôsobom

V MHTH sa používajú nasledovné úrovne klasifikácie informačných aktív pre zabezpečenie integrity informačných aktív:

Nízka	informačné aktíva nepredstavujú žiadne riziko, nemajú žiadnu hodnotu pre potenciálneho kybernetického útočníka; informačné aktíva, ktorých chyba alebo nepresnosť výrazne neohrozí poskytovanú základnú službu;
Stredná	informačné aktíva predstavujú určité riziko, ale nie sú priamo zneužitelné potenciálnym kybernetickým útočníkom, napriek tomu majú slúžiť len pre vnútornú potrebu organizácie; informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých chyba alebo nepresnosť môže spôsobiť dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká
Vysoká	informačné aktíva predstavujú vysoké riziko, majú vysokú hodnotu pre potenciálneho kybernetického útočníka, vysokú citlivosť pre organizáciu; vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých chyba, nepresnosť bezprostredne ohrozuje poskytovanú základnú službu, s ňou spojené aktivity a reputáciu prevádzkovateľa základnej služby

5.7.9.1 Zásady spracovania z pohľadu Integrity:

Inf. Aktívum	Požiadavka na integritu: Stredná	Požiadavka na integritu: Vysoká
Informačné systémy: overenie vstupov/výstupov	Vykonáva sa overenie vstupov a výstupov	Musí byť vykonávané overenie vstupov a výstupov
Duplicitné údaje	Udržiavanie údajov len na mieste určenia. Zabránenie prevádzkovania na viacerých miestach	Udržiavanie údajov len na mieste určenia. Zabránenie prevádzkovania na viacerých miestach
Auditné záznamy	Uchovávajú sa záznamy o zmene	Musia sa uchovávať záznamy o zmene
Prenos súborov	Vykonáva sa kontrola prenášaných súborov napríklad HASH funkciou. Porovnanie Fingerprintu pred odoslaním a po prijatí.	Musí sa vykonávať kontrola prenášaných súborov napríklad HASH funkciou. Porovnanie Fingerprintu pred odoslaním a po prijatí.
Dokumenty	Aplikujú sa nástroje eIDAS na podpisovanie dokumentu pomocou	Musia sa aplikovať nástroje eIDAS na podpisovanie dokumentu pomocou

	dôveryhodného kvalifikovaného podpisu alebo pečate.	dôveryhodného kvalifikovaného podpisu alebo pečate.
--	--	--

5.7.10 DOSTUPNOSŤ

Dostupnosť/Availability – informácia je na požiadanie autorizovanej osoby/procesu prístupná a použiteľná

V MHTH sa používajú nasledovné úrovne klasifikácie informačných aktív pre zabezpečenie dostupnosti informačných aktív:

Nízka	informačné aktíva nepredstavujú žiadne riziko, nemajú žiadnu hodnotu pre potenciálneho kybernetického útočníka; informačné aktíva, ktorých chyba alebo nepresnosť výrazne neohroží poskytovanú základnú službu, alebo pre ktoré existujú alternatívne postupy; stupeň: „Non-Commercial“ • doba obnovy aktíva nesmie presiahnuť 30 pracovných dní • nedostupnosť aktíva môže spôsobiť úroveň škody „nízka“ stupeň: „Commercial“ • doba obnovy aktíva nesmie presiahnuť 10 pracovných dní • nedostupnosť aktíva môže spôsobiť úroveň škody „nízka“
Stredná	informačné aktíva predstavujú určité riziko, ale nie sú priamo zneužiteľné potenciálnym kybernetickým útočníkom, avšak majú slúžiť len pre vnútornú potrebu organizácie; informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie môže spôsobiť dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká; stupeň: „Business Critical“ • doba obnovy aktíva nesmie presiahnuť 1 pracovný deň • nedostupnosť aktíva môže spôsobiť úroveň škody „stredná“
Vysoká	informačné aktíva predstavujú vysoké riziko, majú vysokú hodnotu pre potenciálneho kybernetického útočníka, vysokú citlivosť pre organizáciu; vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie bezprostredne ohrozuje poskytovanú základnú službu, s ňou spojené aktivity a dobrú povesť prevádzkovateľa základnej služby; stupeň: „Mission Critical“ • doba obnovy aktíva nesmie presiahnuť 8 hodín • nedostupnosť aktíva môže spôsobiť úroveň škody „vysoká“

5.7.10.1 Zásady spracovania z pohľadu Dostupnosti:

Inf. Aktívum	Požiadavka na dostupnosť: Stredná	Požiadavka na dostupnosť: Vysoká
Informačné systémy	Vykonanie BIA (RTO,RPO)	Vykonanie BIA (RTO,RPO)
Architektúra	Zmapovanie úzkeho hrdla (points of failure)	HA architektúra
Prevádzka systémov	Mali by byť navrhnuté BCP pre obnovenie služby	Musia by byť navrhnuté BCP pre obnovenie služby

Prevádzka systémov	Mali by byť testované BCP pre obnovenie služby	Musia byť testované BCP pre obnovenie služby
Dokumenty	Mali by sa aplikovať nástroje eIDAS na podpisovanie dokumentu pomocou dôveryhodného kvalifikovaného podpisu alebo pečate.	Musia sa aplikovať nástroje eIDAS na podpisovanie dokumentu pomocou dôveryhodného kvalifikovaného podpisu alebo pečate

5.7.11 KLASIFIKAČNÁ SCHÉMA

Bezpečnosť informácií spočíva v ochrane na klasifikačných atribútoch:

Dôvernosc', Integrita a

Dostupnosť (z angl. CIA – Confidentiality, Integrity, Availability).

Vzhľadom na praktickú použiteľnosť je možné zjednodušiť označenie klasifikačnej úrovne a klasifikovať informačné aktíva jednotne a len na stupeň dôvernosti. Vychádza sa z predpokladu, že aj pri sprístupnení alebo zneužití informácie, ktorá v konečnom dôsledku ohrozuje len integritu alebo dostupnosť informačného aktíva (nie jeho dôvernosc'), ide primárne vždy o narušenie dôvernosti, ktoré malo za následok ohrozenie integrity alebo dostupnosti.

Praktická klasifikačná schéma:

Aplikovaná klasifikačná úroveň:	Ohrozenie aktíva / stupeň (z pohľadu Dôvernosti; Integrity; Dostupnosti)
Verejnosc'	Dôvernosc': Verejnosc' ; Integrita: Nízka ; Dostupnosť: Nízka
Internosc'	Dôvernosc': Internosc' ; Integrita: Stredná ; Dostupnosť: Stredná
Dôvernosc'	Dôvernosc': Chránenosc' ; Integrita: Stredná ; Dostupnosť: Stredná
Prísne dôvernosc'	Dôvernosc': Prísne Chránenosc' ; Integrita: Vysoká ; Dostupnosť: Vysoká

5.8 POLITIKA RIADENIA PRÍSTUPU

5.8.1 ÚČEL, ROZSAH A UŽÍVATELIA

Politika riadenia prístupu definuje bezpečnostné pravidlá pre prístup do rôznych systémov a informačných zariadení organizácie.

Politika je aplikovaná v celom rozsahu IB a KB, t. j. na všetky systémy a zariadenia použité v rozsahu IB a KB.

5.8.2 RIADENIE PRÍSTUPU

Základným princípom riadenia prístupu je zakázanie prístupu na všetky systémy, aplikácie, siete, služby a informácie, ak nie je výslovne povolený jednotlivým používateľom alebo skupinám používateľov. Je definovaný proces riadenia prístupu pre každý systém a službu cez formalizovaný formulár.

- Žiadateľ o Zriadenie/ Zmenu / Odobranie prístupu: Nadriadený zamestnanec
- Schvaľovateľ o Zriadenie/ Zmenu / Odobranie prístupu: IT/OT manažér
- Vykonávateľ Zriadenia/ Zmeny / Odobrania prístupu plus notifikácia: IT/OT Administrátor

Formulár Žiadosti o Zriadenie/ Zmenu / Odobranie prístupu sa archivuje u: IT. V rámci riadenia IT služieb (známe ako ITIL metodológia), budú jednotlivé žiadosti vedené v ITMS nástroji.

Prístup do všetkých fyzických oblastí spoločnosti je povolený, s výnimkou oblastí, pre ktoré musia byť udelené špeciálne oprávnenia.

Táto politika určuje pravidlá pre prístup k systémom, službám a zariadeniam, zatiaľ čo politika klasifikácie informácií definuje pravidlá pre prístupy na individuálne dokumenty a záznamy.

5.8.3 RIADENIE PRIVILÉGIÍ

Zodpovedná osoba pri pridelení oprávnenia musí zohľadniť obchodný účel a bezpečnostné požiadavky na prístup (definícia rizika), ako aj klasifikáciu informácií, ktoré sú sprístupnené s takýmto prístupovým právom, v súlade s politikou pre klasifikáciu informácií.

5.8.4 PRAVIDELNÉ PRESKÚMANIE PRÍSTUPOVÝCH PRÁV

Vlastníctvo každého systému/zariadenia, pre ktoré sú potrebné špeciálne prístupové práva, je potrebné v pravidelných intervaloch kontrolovať, či udelené prístupové práva sú v súlade s procesmi a bezpečnostnými požiadavkami.

Interný audítor vykonáva overenie kontroly prístupov polročne, o vykonaní je potrebné vykonať písomný záznam.

5.8.5 ZMENY A UKONČENIE PRÍSTUPU

Pri zmene pracovnej pozície alebo ukončení zamestnania, HR musí bezodkladne informovať zodpovedné osoby, ktoré schvaľujú/odoberajú oprávnenia pre zamestnanca.

Pri zmene zmluvných vzťahov s externými partnermi, ktorí majú prístup k systémom, službám a zariadeniam, alebo po uplynutí platnosti zmluvy, musia byť bezodkladne informované zodpovedné osoby pre riadenie privilégii externých partnerov.

Prístupové práva pre všetky osoby, ktoré zmenili pracovnú pozíciu v spoločnosti alebo zmluvný vzťah, musia byť bezodkladne odstránené alebo zmenené.

5.8.6 SPRÁVA HESIEL

Pravidlá pre používanie používateľských autentifikačných údajov:

- Každý užívateľ používa len vlastné, jednoznačne pridelené užívateľské meno.
- Každý používateľ má možnosť vybrať si svoje vlastné heslo.
- Dočasné heslo používané pre prvé prihlásenie do systému musí byť jedinečné a silné (je komplexné)
- Dočasné heslo sa oznámi užívateľovi bezpečným spôsobom a identita používateľa je skontrolovaná pred poskytnutím hesla.
- Systém po prihlásení jednorazovým heslom automaticky požaduje zmenu dočasného hesla do systému.
- Systém riadenia hesiel musí požadovať od užívateľa zadať len silné heslo.
- Systém riadenia hesla musí vyžadovať zmenu užívateľského hesla v definovanom intervale.
- Ak používateľ vyžaduje zmenu hesla, systém musí určiť totožnosť používateľa zadaním starého hesla.
- Užívateľ musí opätovne potvrdiť nové heslo.
- Heslo nesmie byť viditeľné na obrazovke počas prihlásenia alebo zmeny hesla.
- Ak používateľ zadá trikrát po sebe nesprávne heslo, systém musí zablokovat používateľské konto.
- Preddefinované heslá nastavené výrobcom softvéru alebo hardvéru musia byť zmenené počas počiatočnej inštalácie.
- Súborny, ktoré obsahujú heslá musia byť ukladané v kryptovanom tvare.

5.8.7 KONTROLA

V pravidelných intervaloch, minimálne 1x ročne, sa vykonáva preverenie bezpečnostných pravidiel a konfigurácií definovaných touto smernicou za účelom identifikácie nesúladu s týmito požiadavkami a zabezpečenia ich následnej nápravy.

Za vykonanie kontroly zodpovedá príslušný manažér IT a príslušný manažér OT. Kontrolu vykonáva špecialista/administrátor IT/OT, ktorý o jej výsledku informuje riaditeľa úseku informačných systémov a MKB.

5.9 POLITIKA PRÍSTUPOVÝCH HESIEL

5.9.1 ÚČEL, ROZSAH A UŽÍVATELIA

Účelom tejto kapitoly je stanoviť pravidlá, ktoré zabezpečia riadenie bezpečného hesla a bezpečné používanie hesiel.

Tento dokument je aplikovaný na celom rozsahu IB a KB a BCM, t. j. na všetky pracoviská a systémy umiestnené v rozsahu IB a KB.

Používatelia tohto dokumentu sú všetci zamestnanci spoločnosti.

5.9.2 POVINNOSTI POUŽÍVATEĽOV

Používatelia musia použiť spoľahlivé bezpečnostné postupy pri výbere a používaní hesla:

- heslá sa nesmú oznamovať iným osobám, vrátane vedenia a správcov systému;
- užívateľsky generované heslá sa nesmú distribuovať prostredníctvom žiadnych komunikačných kanálov (ústne, písomne alebo elektronická distribúcia, atď.); používateľ je povinný heslá zmeniť, ak existujú náznaky, že heslá alebo systém môže byť kompromitovaný – v takom prípade sa spracuje bezpečnostné hlásenie.

Účinné heslá sa vyberú nasledujúcim spôsobom:

- pomocou najmenej 12 znakov pre používateľské konto, najmenej 20 pre privilegovaný účet;
- pomocou najmenej jedného numerického znaku;
- použitím aspoň jedného veľkého písmena a malého abecedného znaku;
- heslo nesmie byť zo slovníka, nesmie byť dialektické alebo žargónové slovo z akéhokoľvek jazyka, alebo akéhokoľvek takéto slová napísané odzadu;
- heslá nesmú vychádzať z osobných údajov (napr. dátum narodenia, adresa, meno člena rodiny, mačky, psa, atď.);
- posledných 10 hesiel sa nesmú opätovne použiť;
- heslo musí byť zmenené do definovanej doby (exspirácia 180 dní v prípade použitia MFA)
- heslo musí byť zmenené po prvom prihlásení do systému;
- minimálna platnosť hesla je 1 deň;
- heslo sa nesmie ukladať v automatizovaných prihláseniach systému (napríklad makro alebo prehliadač);
- Je zakázané používať heslá používané na súkromné účely a súčasne na podnikateľské/pracovné účely;
- Je zakázané používať rovnaké heslo pre viac podnikových systémov.

5.10 POLITIKA ČISTÉHO STOLA A ČISTEJ OBRAZOVKY

5.10.1 ÚČEL, ROZSAH A UŽÍVATELIA

Táto časť dokumentu vymedzuje pravidlá, ktoré zabráňujú neoprávnenému prístupu k informáciám na pracoviskách, zaoberá sa ochranou citlivých informácií na pracovisku kategorizovaných ako "Dôverné" alebo "Prísne Dôverné" podľa politiky pre klasifikáciu informácií.

Pravidlá sú aplikované na všetky pracoviská, zariadenia a vybavenie nachádzajúcom sa v rozsahu IB a KB.

5.10.2 POLITIKA ČISTÉHO STOLA

Ak oprávnená osoba nie je na pracovisku, všetky tlačené dokumenty, ako aj dátové pamäťové médiá musia byť odstránené zo stola alebo iných miest (tlačiarne, faxy, kopírky, atď.) na zabránenie prístupu neoprávnených osôb.

Takéto dokumenty a médiá sa musia skladovať bezpečným spôsobom v súlade s politikou pre klasifikáciu informácií.

5.10.3 POLITIKA ČISTEJ OBRAZOVKY

Ak nie je oprávnená osoba na pracovisku, musí byť zamedzený prístup k informáciám uzamknutím (napr. ctrl+alt+delete/zamknúť).

V prípade krátkej neprítomnosti sa politika čistej obrazovky aplikuje odhlásením všetkých systémov alebo uzamknutím obrazovky pomocou hesla (napr. ctrl+alt+delete/zamknúť). Ak osoba, ktorá je neprítomná dlhšiu dobu, politika čistej obrazovky sa aplikuje odhlásením všetkých systémov a vypnutím pracovnej stanice.

5.10.4 TLAČIARNE A SCANNERY

Dokumenty, ktoré obsahujú citlivé informácie musia byť ihneď odstránené z tlačiarňí, faxov a kopírovacích strojov.

5.11 POLITIKA LIKVIDÁCIE INFORMAČNÝCH ZARIADENÍ A MÉDIÍ

Táto časť dokumentu sa zameriava na to, aby informácie uložené na zariadeniach a médiách boli bezpečne odstránené alebo zlikvidované. Táto časť je aplikovaná v celom rozsahu, t. j. na všetky informačné a komunikačné technológie.

5.11.1 LIKVIDÁCIA ZARIADENIA A MÉDIÍ

Všetky údaje a licencovaný softvér uložený na prenosných pamäťových médiách (napríklad na CD, DVD, USB flash diskoch, pamäťových kartách, ale aj na papieri) a na všetkých zariadeniach obsahujúcich uložené údaje (napr. počítače, mobilné telefóny, atď.) je nutné vymazať pamäťové médiá skôr, než budú zlikvidované, odpredané, opakovane použité alebo zaslané na servis.

Osoba zodpovedná za mazanie dát / zničenie médií, musí informovať vlastníka príslušného aktíva o vymazaní / likvidácii údajov a iniciovať aktualizáciu inventárneho zoznam. Túto skutočnosť je potrebné zaznamenať v protokole o likvidácii.

5.11.2 ZARIADENIA

MKB je zodpovedný za dodržiavanie vymazania údajov zo zariadenia, pokiaľ politika pre kategorizáciu informácií nepredpisuje inak. Údaje sa musia vymazať nízko úrovňovým formátovaním. Ak proces nie je dostatočne zabezpečený vzhľadom na citlivosť údajov, potom pamäťové médium musí byť zničené fyzickým spôsobom.

5.11.3 PRENOSNÉ MÉDIÁ

MKB je zodpovedný za kontrolu mazania dát z prenosných nosičov, pokiaľ politika pre kategorizáciu informácií nepredpisuje inak. Údaje sa musia vymazať nízko úrovňovým formátovaním. Ak proces nie je dostatočne zabezpečený vzhľadom na citlivosť údajov, potom pamäťové médium musí byť zničené fyzickým spôsobom.

5.11.4 PAPIEROVÉ DOKUMENTY

Zamestnanci spoločnosti používajúci papierové dokumenty sú zodpovední za zničenie, resp. Archiváciu papierových dokumentov ([MHTH S47 Registratúrny plán](#)). Papierové dokumenty sú likvidované skartovacím strojom.

5.11.5 VYMAZANIE A LIKVIDÁCIA MÉDIÍ,

Záznamy o vymazaní/zničení médií pre údaje klasifikované ako "Dôverné" alebo "Prísne Dôverné", musia obsahovať nasledujúce informácie:

- informácie o médiách,
- dátum vymazania/zničenia,
- metóda vymazanie/zničenie
- osoba, ktorá vykonáva proces.

Všetky informácie klasifikované ako "Dôverné" a "Prísne Dôverné" sú vymazané/zničené v prítomnosti Likvidačnej komisie pozostávajúcej z osôb oprávnených na prístup k informáciám.

Bližšie proces upravuje:

- Likvidačná komisia v zmysle [MHTH S09 Správa majetku a budov \(bod 4.4\)](#)
- Proces odpredaja.

5.12 POLITIKA RIADENIA BEZPEČNOSTI SIETÍ

5.12.1 HLAVNÉ ZÁSADY OCHRANY SIETÍ A INFORMAČNÝCH SYSTÉMOV

Táto bezpečnostná politika rovnako vychádza z požiadaviek na kategorizáciu sietí a informačných systémov pre poskytovateľov základnej služby uvedených v Prílohe č. 2 Vyhlášky NBÚ č. 227/2025 Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Táto bezpečnostná politika v zmysle ochrany sietí a informačných systémov formou ich kategorizácie, má tieto hlavné ciele:

- vedieť identifikovať počítačové siete a informačné systémy spracúvajúce alebo prenášajúce informácie alebo predstavujúce súvisiace informačné aktíva, ktoré sú kľúčové pre poskytovanie základných služieb;
- vedieť stanoviť stupeň hrozby, ktoré by narušenie ich prevádzky z pohľadu integrity, dôvernosti alebo dostupnosti mohli pre organizáciu znamenať;
- definovať a implementovať bezpečnostné opatrenia adekvátne pre každý stupeň ohrozenia týchto sietí a informačných systémov, pričom platí, čím vyššia kategória, tým viac bezpečnostných opatrení je povinných (identifikácia a autorizácia, audit
- ná stopa, monitorovanie bezpečnostných udalostí).

5.12.2 KATEGORIZÁCIA SIETÍ A INFORMAČNÝCH SYSTÉMOV

Hodnota, význam alebo kritickosť sietí a informačných systémov sa určuje prostredníctvom procesu klasifikácie, ktorým sa označuje stupeň hrozby v prípade neautorizovanej zmeny alebo narušenia dostupnosti sietí a informačných systémov.

Pri kategorizácii platia tieto pravidlá:

- kategorizácia sietí a informačných systémov je založená na klasifikácii informácií;
- kategorizácia sietí a informačných systémov sa vykonáva pre každú sieť a informačný systém vytvorením zoznamu vybraných komponentov sietí a informačných systémov, ktorý identifikuje jednotlivé siete a informačné systémy, ich podporné systémy a podsystémy s uvedením ich bezpečnostnej funkcie a zaradenia do príslušných bezpečnostných kategórií;
- zoznam komponentov sietí a informačných systémov identifikujúci jednotlivé siete a informačné systémy sa môže skladať z textovej, tabuľkovej alebo grafickej časti tak, že sú jednoznačne definované hranice vybranej siete a informačného systému, rozhrania medzi definovanými hranicami, bezpečnostné funkcie komponentov, ktoré majú byť zahrnuté v posudzovaní úrovne bezpečnosti a požiadavky príslušných regulačných požiadaviek a technických noriem alebo iných vecne obdobných postupov a metód na ich projektovanie, vytváranie, implementáciu a kontrolu;

- siete a informačné systémy tvoriace hranicu medzi rôznymi bezpečnostnými kategóriami v bezpečnostnom systéme sa zaradia do vyššej bezpečnostnej kategórie;
- kategorizácia sietí a informačných systémov zohľadňuje, že zlyhanie siete alebo informačného systému v ľubovoľnej bezpečnostnej úrovni nespôsobí zlyhanie vybranej siete a informačného systému zaradeného do bezpečnostnej úrovne s vyššou kategóriou. Pomocné siete a informačné systémy a podsystémy, ktoré pomáhajú funkciám vybraných informačných systémov, musia byť zaradené do príslušnej bezpečnostnej kategórie s ohľadom na zaradenie nadradeného systému;
- každé klasifikované informačné aktívum má pridelený jeden klasifikačný stupeň pre atribút dôvernosti, jeden klasifikačný stupeň pre atribút integrity a jeden klasifikačný stupeň pre atribút dostupnosti;
- bezpečnostné informácie, nastavenia, postupy, smernice a ostatné úkony súvisiace s riadením aktív sa klasifikujú na rovnaký alebo vyšší klasifikačný stupeň, akým sú označené informačné aktíva, ktorých sa týkajú;
- za priradenie správneho klasifikačného stupňa zodpovedá primárne autor/vlastník informácie alebo funkčný/business vlastník informačného aktíva.

5.12.3 VÝZNAM KATEGORIZÁCIE SIETÍ A INFORMAČNÝCH SYSTÉMOV

- umožňuje naplniť strategické rozhodnutie vrcholového manažmentu o potrebe ochrany kritických aktív organizácie;
- pomáha pri identifikácii tých aktív, ktoré sú pre organizáciu najdôležitejšie alebo najcennejšie;
- zdôvodňuje výber ochranných mechanizmov a bezpečnostných opatrení;
- umožňuje dosiahnuť súlad s právnymi predpismi a nariadeniami;
- umožňuje prioritizovať nasadzovanie automatizovaných technologických opatrení, ako sú napríklad nasadzovanie firewallov, virtualizácia a segregácia sietí, šifrovanie prenosových ciest, bezpečná konfigurácia sieťových prvkov a kritických serverov, zbieranie, centrálna monitorovanie a korelácia bezpečnostných udalostí (SEM alebo SIEM), atď.

5.12.4 KLASIFIKAČNÉ KATEGÓRIE PRE SIETE A INFORMAČNÉ SYSTÉMY

V MHTH sa používajú nasledovné kategórie (klasifikačné stupne) pre siete a informačné systémy súvisiace s prevádzkou základných služieb:

Kategória	Sieť alebo informačný systém zaradíme do príslušajúcej kategórie, ak existuje minimálne jeden z nasledovných dôvodov:	Zjednodušené vysvetlenie požiadavky (hlavné kritérium)
I.	ohrozenie nemá žiadny negatívny dopad na poskytovanú základnú službu; obsahujú alebo spracúvajú informačné aktíva klasifikované z hľadiska dôvernosti ako „verejné“ alebo v odôvodnených prípadoch „interné“, obsahuje alebo spracúva informačné aktíva klasifikované z hľadiska dostupnosti klasifikačným stupňom „nízka“ alebo v odôvodnených prípadoch „stredná“, obsahujú alebo spracúvajú informačné aktíva klasifikované z hľadiska integrity klasifikačným stupňom „nízka“ alebo v odôvodnených prípadoch „stredná“, obsahujú alebo spracúvajú informačné aktíva, pri ktorých nie je potrebné identifikovať používateľov,	systémy a siete, ktoré nijak nesúvisia so základnou službou (ZS), resp. ohrozenie atribútov CIA nespôsobí MHTH žiadnu škodu

	obsahujú alebo spracúvajú informačné aktíva, pri ktorých nie je potrebné vykonávať kontrolnú činnosť (ukladanie a analýza bezpečnostných prevádzkových záznamov (logov)).	
II.	obsahujú alebo spracúvajú informačné aktíva, ktorých ohrozenie môže spôsobiť kybernetický bezpečnostný incident I. stupňa, obsahujú alebo spracúvajú informačné aktíva, ktoré sú klasifikované z hľadiska dôvernosti ako „interné“, „dôverné“ alebo v odôvodnených prípadoch „prísne dôverné“, obsahujú alebo spracúvajú informačné aktíva, ktoré sú klasifikované z hľadiska dostupnosti klasifikačným stupňom „stredná“ alebo v odôvodnených prípadoch „vysoká“, obsahujú alebo spracúvajú informačné aktíva, ktoré sú klasifikované z hľadiska integrity klasifikačným stupňom „stredná“ alebo v odôvodnených prípadoch „vysoká“, obsahujú alebo spracúvajú informačné aktíva, pri ktorých je potrebné identifikovať používateľov (najmä privilegovaných) takým spôsobom, aby ich aktivity významné pre informačnú bezpečnosť, mohli byť vždy dostatočne preukázané, obsahujú alebo spracúvajú informačné aktíva, pri ktorých je potrebné vykonávať kontrolnú činnosť (ukladanie a analýza bezpečnostných prevádzkových záznamov (logov)).	systémy a siete, ktoré súvisia so základnými službami tak, že môžu viesť ku kybernetickému incidentu I. stupňa - napr. vďaka agendového systému; Active Directory pre doménu, ktorou sa riadia prístupy do systémov poskytujúcich ZS, možno považovať za agendový alebo „podporný“ systém
III.	obsahujú alebo spracúvajú informačné aktíva, ktorých ohrozenie môže spôsobiť kybernetický bezpečnostný incident II. a III. stupňa, obsahujú alebo spracúvajú informačné aktíva, ktoré sú klasifikované z hľadiska dôvernosti ako „prísne dôverné“, obsahujú alebo spracúvajú informačné aktíva, ktoré sú klasifikované z hľadiska dostupnosti klasifikačným stupňom „vysoká“, obsahujú alebo spracúvajú informačné aktíva, ktoré sú klasifikované z hľadiska integrity klasifikačným stupňom „vysoká“, obsahujú alebo spracúvajú informačné aktíva, pri ktorých je potrebné identifikovať všetkých používateľov takým spôsobom, aby ich aktivity kritické pre informačnú bezpečnosť, mohli byť vždy dostatočne preukázané (auditovateľnosť), obsahujú alebo spracúvajú informačné aktíva, pri ktorých je potrebné vykonávať kontrolnú činnosť (ukladanie a analýza bezpečnostných prevádzkových záznamov (logov)).	siete a informačné systémy, prostredníctvom ktorých sa poskytuje základná služba, ktorých výpadok alebo poškodenie spôsobí poškodenie alebo znemožnenie poskytovania základnej služby a ktorých ohrozenie môže viesť k kybernetickému bezpečnostnému incidentu II. a III. stupňa

5.12.5 PREHĽAD ZÁVAŽNÝCH KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV PODĽA NBÚ

Národný bezpečnostný úrad podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a vyhlášky č. 226/2025 Z.z. ustanovuje:

- Vymedzenie identifikačných kritérií závažného narušenia fungovania prevádzkovateľa základnej služby. Uvedené je v [prílohe č. 1.](#)
- Náležitosti hlásenia závažného kybernetického bezpečnostného incidentu podľa § 24 ods. 3 písm. a) a b) zákona. Uvedené sú v [prílohe č. 2.](#)
- Náležitosti hlásenia významnej kybernetickej hrozby, udalosti odvrátenej v poslednej chvíli a zraniteľnosti podľa § 24 ods. 5 zákona a hlásenia kybernetického bezpečnostného incidentu, kybernetickej hrozby a udalosti odvrátenej v poslednej chvíli podľa § 24 ods. 6 zákona. Uvedené sú v [prílohe č. 3.](#)

Na základe uvedených ustanovení, boli v MHTH zavedené indikátory závažnosti incidentov a ich nahlasovanie.

5.12.6 ROZSAH BEZPEČNOSTNÝCH OPATRENÍ PRE OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Rozsah všeobecných bezpečnostných opatrení pre oblasti kybernetickej bezpečnosti podľa § 20 ods. 2 zákona je uvedený v [prílohe č. 1](#) vyhlášky 227/2025 Z.z. a určuje sa na základe analýzy rizík.

5.12.7 RIADENIE BEZPEČNOSTI V SIETACH

Sieťové prostredie je riadené a spravované

- interne – LAN a zariadenia LAN, WAN
- externe – LAN, WAN a pripojenie do Internetu dodávateľom na základe zmluvy so stanovenými parametrami SLA.

Prístup do siete spoločnosti je riadený, prístupové práva sú pridelené na základe interných predpisov.

Riadenie zmien v sieťach sa vykonáva štandardným zmenovým konaním. Činnosti v sieťach sú monitorované, o udalostiach sa vytvárajú audítne záznamy.

Sieťové zásuvky, ktoré sa nepoužívajú musia byť deaktivované.

Prístup do sieťového prostredia je zabezpečený autentifikačnými mechanizmami.

Prístup k diagnostickým a konfiguračným portom IT komponentov musí byť riadený a chránený (fyzickým i logickým prístupom).

Pre zisťovanie efektívnosti použitých sieťových opatrení sa vykonáva pravidelne kontrola sieťových nastavení, minimálne 1-krát ročne.

5.12.8 ODDEĽOVANIE SIETÍ

Sieťové prostredie spoločnosti je členené do viacerých logických segmentov – samostatných VLAN pre pracovné stanice, servery, WiFi, atď. Pre jednotlivé samostatné siete VLAN musia byť definované pravidlá (access listy), ktoré povolia / blokujú komunikáciu na úrovni zdrojovej a cieľovej IP adresy a definovanej služby. Pravidlá sú pravidelne preskúmané a aktualizované.

Sieťové prostredie musí byť chránené technológiou so zabezpečením funkcií umožňujúcich ochranu proti útokom z Internetu (firewall).

5.12.9 BEZDRÔTOVÉ SIETE A DRÔTOVÉ SIETE

5.12.9.1 Bezdrôtové siete

Vytvorenie každej bezdrôtovej siete musí schváliť oddelenie bezpečnosti a krízového riadenia.

Všetky bezdrôtové siete musia byť zabezpečené primeranými bezpečnostnými nastaveniami.

Prístup do bezdrôtovej siete povoľuje pre zamestnanca na základe žiadosti priamy nadriadený.

Bezdrôtová sieť pre zamestnancov tretích strán musí byť oddelená od bezdrôtovej siete pre zamestnancov a nesmie umožňovať prístup k IS a údajom spoločnosti. Pridelenie prístupu do tejto siete (SSID a heslo) musí byť časovo obmedzené na dobu potrebnú pre výkon práce zamestnanca tretej strany. O prístup do bezdrôtových sietí pre zamestnancov tretej strany žiada Vlastník, pre ktorého zamestnanci tretej strany vykonávajú činnosť. K žiadosti sa vyjadruje MKB. Bezdrôtové siete sú monitorované, auditné záznamy sú ukladané a pravidelne vyhodnocované oddelením bezpečnosti a krízového riadenia.

5.12.9.2 Drôtové siete

Pripojenie počítačov a sieťových periférií je realizovaný cez štruktúrovanú kabeláž formou kabeláže ETHERNET 5 a vyššej. Prípojné body sú realizované v chránených dátových skrinách, ktoré sú trvalo uzamknuté. Kabeláž nie je vedená cez nechránené dátové trasy, kde by bolo možné realizovať kompromitáciu siete.

5.12.10 PRENOS INFORMÁCIÍ

Pri prenose informácií prostredníctvom sietí sa postupuje na základe klasifikácie informácií, ktoré majú byť prenášané sieťovým prostredím v zmysle požiadaviek interných predpisov pre daný stupeň klasifikácie. Súčasne je potrebné zohľadniť aj požiadavky na integritu informácií, prípadne na ich autenticitu, nepopierateľnosť a časovú následnosť.

Vo všeobecnosti platí, že dôvernosť citlivých informácií je potrebné chrániť šifrovaním a všade kde je to technicky možné používať zabezpečené verzie prenosových protokolov (HTTPS, FTPS, SFTP, SSH, SMIME a pod.).

5.13 POLITIKA ZÁLOHOVANIA

5.13.1 ÚČEL, ROZSAH A UŽÍVATELIA

Účelom je zabezpečiť, aby boli vytvorené záložné kópie a aby boli pravidelne testované v definovaných intervaloch.

Uplatňuje sa pre celý rozsah IB a KB, t. j. na všetky informačné a komunikačné technológie.

Zálohovanie a obnova dát a systémov

Rozhodovanie o tom, ktoré systémy a siete, ich časti, komponenty alebo iné dáta, ktoré sú kľúčové pre obnovenie prevádzky pri poskytovaní základných služieb, musí vždy vychádzať z:

- a) posúdenia možného dopadu na organizáciu a jej skutočných potrieb (BIA),
- b) technických možností konkrétnych systémov
 - pri vytváraní záloh,
 - ich bezpečného uloženia tak, aby im nehrozilo narušenie alebo zničenie, a
 - ich spätného obnovovania zo záloh.

V procese BIA ide primárne o zaradenie systémov a sietí do kategórií I., II., III. (podľa Kategorizácia sietí a informačných systémov), tieto kategórie však nepredpisujú konkrétne požiadavky na plány záloh jednotlivých systémov alebo sietí.

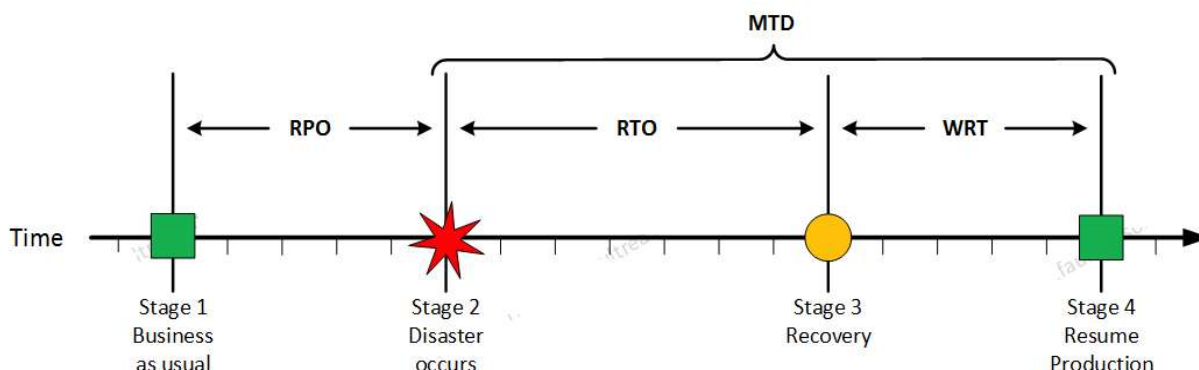
Preto musí každý plán záloh vychádzať z analýzy následkov možného dopadu nedostupnosti konkrétneho systému, siete alebo dát, ktorá sa realizuje cez BIA a teda odhadovaný:

- a) finančný dopad (ušlý zisk, pokuty a sankcie),
- b) dopad na meno a reputáciu,
- c) dopad na dotknuté osoby (klienti, zamestnanci, tretie strany), a
- d) dopad na dostupnosť služieb.

Na základe odhadnutého celkového dopadu definujú funkční (business) vlastníci konkrétne požiadavky na predmet zálohovania (len dáta, časti systémov alebo celé systémy) a na obnoviteľnosť systému alebo siete prostredníctvom vybraných parametrov ako **cieľový čas na**

zotavenie (RTO), cieľový bod obnovenia (RPO), čas potrebný na overenie integrity obnoveného systému alebo dát, (WRT, Work Recovery Time) tak, aby pre každý systém alebo sieť existoval definovaný a schválený **maximálne tolerovateľný výpadok (MTD, Maximum Tolerable Downtime)**.

Maximálne tolerovateľný výpadok (MTD) = cieľový čas na zotavenie (RTO) + čas potrebný na overenie integrity obnoveného systému alebo dát (WRT)



Obr. č. 2: Ilustrácia časovej závislosti pri havárii IS

5.13.2 TECHNICKÉ MOŽNOSTI ZÁLOHOVANIA A OBNOVOVANIA ZO ZÁLOH

Technické možnosti zálohovania systémov, sietí, komponentov a kľúčových dát vychádzajú z:

- možností riadenia procesu (online, near-line, off-line, kompletný backup site);
- úložných médií (magnetické pásky, hard disk a SSD disky, optické úložiská, vzdialené zálohovacie služby);
- zálohovacích metód (plná záloha systému (imaging), inkrementálne zálohy, near-CDP (continuous data protection), reverzne inkrementálne zálohy, diferenčné zálohy);
- Predmetu zálohovania (fyzické médium (disk), logické médium (volume), virtuálny systém (VM), OS a súborový systém, databáza, aplikácia, užívateľské dáta, konfiguračné dáta);
- periodicity záloh (okamžite pri zmene, denne, týždenne, mesačne, kvartálne, polročne, ročne, nikdy, nie je možné);
- spôsobu overenia použiteľnosti zálohovaných dát (obnovenie iba časti zálohovaných dát a overenie ich integrity, obnovenie komponentu a overenie jeho funkčnosti, obnovenie systému alebo aplikácia a overenie ich funkčnosti, použitie typických základných funkcií v systéme, porovnanie počtu záznamov v databáze, žiadne overenie).

Výber procesu, médií a metód závisí od požiadaviek na Maximálne tolerovateľný výpadok (MTD) pre každý systém alebo sieť samostatne.

5.13.3 PROCES ZÁLOHOVANIA

Záložné kópie musia byť vytvorené pre všetky systémy identifikované v stratégii obchodnej kontinuity a v intervaloch.

Každý plán záloh pre konkrétny systém, sieť alebo dáta musí obsahovať informácie o Vlastníkoch:

- Business/funkčný vlastník;
- Útvar, oddelenie business vlastníka;
- Technický vlastník;
- Útvar, oddelenie technického vlastníka (správca systému, siete).

IT/OT manažér je zodpovedný za zálohovanie informácií, softvéru a systémov.

Zálohy sa ukládajú na diskový priestor s vysokou dostupnosťou.

Protokoly o procese zálohovania sa vytvárajú automaticky v systémoch, kde sa vytvára záložná kópia.

- Špecialista/Administrátor úseku IT vykonáva zálohovanie a archiváciu údajov v zmysle interných dokumentov a vytvára záložné kópie dôležitých informácií a softvéru.

- b) Špecialista/Administrátor je zodpovedný za vypracovanie interného dokumentu zálohy a obnovy dát, ktorá by mala obsahovať požiadavky MHTH na zálohovanie (parametre RTO a RPO), retenciu údajov, testovanie záloh ako aj adekvátnu ochranu záložných médií proti environmentálnym a kybernetickým hrozbám.
- c) Požiadavky na zálohovanie sú definované s vlastníkom aktíva
- d) V internom dokumente pre zálohovanie a obnovu musí byť minimálne zohľadnené:
 - vymedzenie rozsahu zálohovaných údajov s cieľom zabezpečenia kontinuity činností,
 - určenie spôsobu, frekvencie a času vykonávania zálohovania,
 - systém testovania médií a vykonaných záloh na zabezpečenie ich integrity,
 - spôsob manipulácie so zálohami so zabezpečením ich ochrany na úrovni, ktorá zodpovedá v zmysle klasifikácie informácií MHTH,
 - požiadavky na ochranu zálohovaného informačného systému,
 - spôsob uchovávanía záloh,
 - podmienky vyradovania a spôsob likvidácie zálohovacích médií.

V internom dokumente upravujúcom spravovanie dokumentov spoločnosti, vzhľadom na legislatívu, musia byť zohľadnené, napr.:

- vymedzenie rozsahu archivovaných údajov vzhľadom na požiadavky legislatívy SR a interných predpisov MHTH – [MHTH S47 Registratúrny plán](#),
- zabezpečenia prístupu k archivovaným údajom (vzhľadom na možné zmeny v štruktúrach databáz, konfiguráciách IS a pod.),
- určenie spôsobu, frekvencie a času vykonávania archivácie,
- výber typu médií s ohľadom na životnosť médií, požadovanú dobu archivácie, a kompatibilitu zariadení na spracovanie médií,
- systém testovania médií a vykonaných archivov na zabezpečenie ich integrity,
- spôsob obnovy archívnych médií,
- spôsob manipulácie s médiami so zabezpečením ich ochrany na úrovni v zmysle klasifikácie informácií v MHTH,
- systém uchovávanía médií,
- podmienky vyradovania a spôsob likvidácie médií.

Médiá so záložnými údajmi sú uložené v inej fyzickej miestnosti, alebo lokalite a to pre prípady živelných pohrôm atď. Pokiaľ nie je možné túto podmienku splniť, musia byť médiá s archívными údajmi uložené oddelene od médií so záložnými údajmi tak, aby sa v maximálnej možnej miere zamedzilo súčasnému zničeniu záložných aj archívnych médií v prípade živelnej pohromy alebo ich odcudzenia, či straty prekonaním jednej a tej istej prekážky. V MHTH sa uplatňuje tzv. pravidlo 3-2-1. Za nakladanie s médiami je zodpovedný Špecialista/Administrátor úseku IT.

Špecialista/Administrátor úseku IT je povinný minimálne raz za rok otestovať obnovu dát podľa definovaného pracovného postupu a je povinný vypracovať testovací protokol z každého testu zálohovania a obnovy zápisom do manažmentu zmien.

Zálohovanie a obnova je definovaná interným dokumentom pre každý systém zvlášť a je uchovávaná v digitálnej alebo papierovej podobe. Pracovný postup vypracováva Špecialista/Administrátor úseku IT.

5.13.4 TESTOVANIE ZÁLOŽNÝCH KÓPIÍ

Záložné kópie a proces ich obnovy sa testujú v definovaných intervaloch. Test obsahuje schopnosti obnovenia systému a obnovenia údajov.

IT/OT manažér je zodpovedný za:

- overovanie záložných kópií,
- za vyhotovenie záznamu o testovaní záložných kópií.

5.14 POLITIKA PRE PRENOS INFORMÁCIÍ

5.14.1 ÚČEL, ROZSAH A UŽÍVATELIA

Účelom tejto kapitoly je popísanie bezpečného vymieňania informácií.

táto kapitola sa aplikuje na celý rozsah IB a KB, t. j. na všetky informácie a komunikačné a informačné technológie.

PRENOS INFORMÁCIÍ

Spoločnosť môže vymieňať údaje prostredníctvom nasledujúcich elektronických komunikačných kanálov:

- a) e-mailov;
- b) sťahovanie súborov z internetu;
- c) prenos dát cez špecializované komunikačné systémy;
- d) telefóny, faxy, SMS textové správy;
- e) prenosné médiá, fóra a sociálne siete.

MKB určuje komunikačný kanál, ktorý môže byť použitý pre každý druh informácií a prípadne obmedziť oprávnenia týkajúce sa používania komunikačných kanálov, t. j. vymedziť, ktoré činnosti sú zakázané.

Okrem šifrovacích bezpečnostných opatrení predpísaných v PKIB, MKB stanovuje dodatočné opatrenia pre každý typ údajov a komunikačných kanálov, na základe výsledkov analýzy rizík.

5.14.2 VZŤAHY S EXTERNÝMI SPOLOČNOSŤAMI

Externé spoločnosti zahŕňajú rôznych poskytovateľov služieb, hardvéru, softvéru, alebo spracovania údajov.

Pred výmenou informácií s akoukoľvek externou stranou, musí byť podpísaná zmluva, za ktorú zodpovedá vlastník/gestor ([Dohoda o mlčanlivosti](#) - NDA). Zmluva obsahuje klauzuly v súlade s posúdením rizík a obsahuje nasledovné časti:

- spôsob identifikácie druhej strany;
- povolenia na prístup k informáciám;
- zabezpečenie nepopierateľnosti;
- technické pravidlá pre prenos dát;
- reakcia na incident;
- označovanie a spracovanie citlivých informácií;
- kopírovanie informácií.

Zmluva s externými stranami musí byť vypracovaná podľa politiky externých dodávateľov.

5.15 POLITIKA POUŽÍVANIA KRYPTOGRAFICKÝCH OPATRENÍ

5.15.1 ÚČEL, ROZSAH A UŽÍVATELIA

Účelom tejto kapitoly je vymedziť pravidlá pre používanie kryptografických metód, ako aj pravidlá pre používanie kryptografických kľúčov pre ochranu dôvernosti, integrity, pravosti a nepopierateľnosti informácií.

Ďalším účelom je zaviesť uplatňovanie kryptografických opatrení s postupmi, ktoré poskytujú primeranú úroveň ochrany citlivých informácií organizácie a zároveň zabezpečujú súlad so zákonnými, regulačnými a zmluvnými požiadavkami. Postupy narábania s údajmi stanovujú požiadavky na používanie techník šifrovania, na ochranu citlivých údajov na úložiskách (Data-At-Rest) aj pri prenose (Data-In-Transit). Táto politika definuje opatrenia a súvisiace postupy pre rôzne oblasti a domény, kde sa používa šifrovanie a šifrovacie techniky.

Kryptografický mechanizmus je aplikovaný v celom rozsahu IB a KB, t. j. na všetky systémy a informácie použité v rozsahu IB a KB.

5.15.2 KRYPTOGRAFIA

Kryptografia je metóda ochrany údajov pomocou mechanizmov umožňujúcich zobrazit' obsah správy iba jej odosielateľovi a príjemcovi, pre ktorého je určená. Týka sa bezpečných informačných a komunikačných techník odvodených z matematických konceptov a súboru výpočtov založených na pravidlách (algoritmoch) na transformáciu správ spôsobmi, ktoré je ťažké dešifrovať. Tieto algoritmy sa používajú na generovanie kryptografických (šifrovacích) kľúčov, digitálne podpisovanie, prehliadanie webových stránok na internete a zabezpečenie dôvernosti komunikácie, napr. pri transakciách platobnými kartami alebo v e-mailovej komunikácii.

Kryptografické prostriedky sa používajú na zabezpečenie:

- a) dôvernosti údajov,
- b) integrity údajov,
- c) autentizácie odosielateľa (digitálny podpis),
- d) nepopierateľnosti vykonanej činnosti (non-repudiation).

Kryptografické prostriedky sa používajú najmä na ochranu citlivých údajov:

- a) prenášaných cez nezabezpečené prostredie (napr. internetová alebo e-mailová komunikácia),
- b) uložených na lokálnych diskoch (koncové stanice, zdieľané úložiská údajov a pod.),
- c) prenosných zariadeniach (notebooky, tablety, smartfóny a pod.),
- d) prenosných médiách (CD, DVD, USB a pod.).

5.15.3 ŠIFROVANIE ÚDAJOV

Používanie kryptografických opatrení musí byť riadené. Jednotlivé roly a zodpovednosti v procese riadenia kryptografických opatrení sú popísané v nasledujúcich článkoch tohto dokumentu.

Šifrovanie a dešifrovanie je realizované pomocou šifrovacích a dešifrovacích algoritmov (matematických funkcií).

Použitý šifrovací algoritmus musí byť vhodne zvolený tak, aby zabezpečil dostatočnú úroveň ochrany údajov. Úroveň zabezpečenia údajov vyplýva z ich citlivosti, resp. klasifikačného stupňa.

Na základe použitého algoritmu sa metódy šifrovania delia na:

- a) symetrické šifrovanie,
- b) asymetrické šifrovanie.

Symetrické šifrovanie používa na šifrovanie aj na dešifrovanie správy jeden rovnaký kľúč. Pri tejto metóde šifrovania je nevyhnutné zabezpečiť dôvernosť šifrovacieho kľúča, aby ho poznali len osoby, ktoré navzájom pomocou tohto kľúča informácie šifrujú. Správa, ktorá sa zašifruje týmto tajným kľúčom sa dá dešifrovať len opätovným použitím toho istého tajného kľúča. Výhodou použitia tejto metódy je rýchlosť šifrovania, nakoľko proces symetrického šifrovania nie je náročný na výpočtové kapacity. Nevýhodou je nutnosť zabezpečiť dôvernosť šifrovacieho kľúča. Príkladom symetrického šifrovania je použitie archivačného programu s možnosťou zaheslovať vzniknutý súbor (napr. WinRAR, WinZip, 7-Zip a pod.).

Pri rozhodovaní o použití tejto kryptografickej metódy je potrebné zvážiť:

- a) možnosť prelomiť šifrovanie brute-force útokom v prípade použitia príliš krátkeho šifrovacieho kľúča,
- b) potrebu použitia dostatočne silného hesla šifrovaného súboru (minimálna dĺžka hesla 2010 znakov, kombinácia malých a veľkých písmen, číslíc, prípadne špeciálnych znakov), ideálne dlhá fráza,
- c) potrebu utajenia hesla použitého na zašifrovanie súboru (napr. poslanie hesla iným komunikačným kanálom než bol poslaný samotný súbor – heslo cez SMS, Signal alebo

iné aplikácie slúžiace na šifrovanú komunikáciu, ktorých používanie je v podniku akceptované).

Asymetrické šifrovanie používa na šifrovanie a dešifrovanie správy dva rozdielne kľúče:

- a) **privátny kľúč** – tajný šifrovací kľúč, ktorý pozná len jeho majiteľ; používa sa na dešifrovanie zašifrovaných správ a na vyhotovovanie elektronického podpisu správ,
- b) **verejný kľúč** – šifrovací kľúč, ktorý sa používa na šifrovanie správ; tento kľúč je verejný a majú ho k dispozícii všetci používatelia komunikujúci s majiteľom verejného kľúča; verejný kľúč obsahuje certifikát vystavený certifikačnou autoritou (CA).

Digitálny podpis slúži ako prostriedok zabezpečenia autenticity a integrity elektronických dokumentov. Používa sa na overenie elektronickej totožnosti osoby, ktorá podpísala konkrétny elektronický dokument (autenticita odosielateľa) a kontrolu, či obsah podpísaného dokumentu nebol počas jeho prenosu zmenený (integrita dokumentu).

O použití a potrebnom rozsahu kryptografickej ochrany informačných aktív rozhoduje vlastník aktíva, ktorý vhodný spôsob a metódu šifrovania konzultuje s MKB.

Výber použitej kryptografickej metódy závisí najmä na:

- a) posúdení rizík spojených s ochranou aktíva,
- b) požadovanej úrovni ochrany aktíva,
- c) technických možnostiach prevádzkovaných systémov a
- d) ekonomickej náročnosti opatrenia vzhľadom na hodnotu chráneného aktíva.

Minimálne požiadavky kryptografickej ochrany aktív podniku sú definované nasledovne:

- a) šifrovací algoritmus symetrického šifrovania: AES-256,
- b) šifrovací algoritmus asymetrického šifrovania: RSA,
- c) dĺžka kryptografického kľúča RSA: najmenej 2048 bitov,
- d) expirácia kryptografického kľúča: 1 rok,
- e) funkcia používaná na hashovanie: SHA-256.

Za definovanie minimálnych požiadaviek kryptografickej ochrany aktív zodpovedá MKB.

Všetky prípady využitia kryptografických metód a prostriedkov sú zdokumentované. V prípade informačných a riadiacich systémov je tento popis uvedený v prevádzkovej dokumentácii príslušného IS alebo RS a v prípade všeobecných požiadaviek na šifrovanie údajov stanovuje minimálne požiadavky táto príručka. Za existenciu popisu kryptografických opatrení v prevádzkovej dokumentácii IS alebo RS zodpovedá vlastník daného IS alebo RS. Popis kryptografických opatrení v prevádzkovej dokumentácii IS alebo RS vykonáva dodávateľ príslušného IS alebo RS.

Všetky prípady využitia kryptografických metód a prostriedkov sú priebežne sledované a vyhodnocované z hľadiska odolnosti použitých kryptografických prostriedkov voči známym zraniteľnostiam a hrozbám. Za priebežné sledovanie a vyhodnocovanie vhodnosti používaných kryptografických prostriedkov zodpovedá MKB. Sledovanie a vyhodnocovanie vykonáva vlastník aktíva, ktorý v prípade identifikácie zraniteľnosti alebo nevhodnosti niektorej z používaných kryptografických metód alebo prostriedkov o tejto skutočnosti informuje MKB. Definovanie nových a vyhovujúcich kryptografických metód a prostriedkov vykonáva vlastník aktíva, ktorý ich vhodnosť a rozsah konzultuje s MKB a špecialistami úseku informačných technológií.

Nasadenie kryptografických prostriedkov vykonáva:

- a) zamestnanec dodávateľa v prípade externe vyvíjaného alebo nasadzovaného IS alebo RS,
- b) špecialista/administrátor úseku informačných technológií v prípade interných aplikácií alebo nástrojov.

Správu nasadených kryptografických prostriedkov vykonáva špecialista/administrátor úseku informačných technológií.

5.15.4 INFRAŠTRUKTÚRA VEREJNÝCH KĹÚČOV

Pre účely využívania asymetrického šifrovania je potrebné vytvoriť infraštruktúru verejných kľúčov (PKI – Public Key Infrastructure). Táto infraštruktúra slúži na riadenie životného cyklu kryptografických kľúčov a ich správu.

Správa kryptografických kľúčov a certifikátov v rámci ich životného cyklu zahŕňa procesy na ich:

- a) vytváranie,
- b) distribúciu,
- c) uchovávanie,
- d) archiváciu,
- e) obnovu,
- f) ukončenie platnosti (revokáciu) a
- g) likvidáciu.

Špecialista/administrátor úseku informačných systémov vykonáva v súvislosti s PKI nasledujúce činnosti:

- a) vytváranie privátnych a verejných šifrovacích kľúčov,
- b) aktiváciu šifrovacích kľúčov,
- c) distribúciu šifrovacích kľúčov používateľom,
- d) archiváciu neaktívnych šifrovacích kľúčov potrebných pre prístup k šifrovaným elektronickým archívom,
- e) likvidáciu šifrovacích kľúčov,
- f) poskytovanie podpory používateľom v súvislosti s kryptografickými kľúčmi.

Na správu kryptografických kľúčov a certifikátov slúži certifikačná autorita. V prostredí podniku slúži na účely certifikačnej autority Microsoft Active Directory Certificate Services.

Certifikačná autorita musí byť nakonfigurovaná tak, aby vydávané certifikáty spĺňali schválené požiadavky na použitý šifrovací algoritmus, minimálnu dĺžku kľúča a hashovaciu funkciu.

Certifikát vydaný certifikačnou autoritou obsahuje verejný kľúč vlastníka certifikátu.

Certifikáty môžu byť vydané osobám alebo zariadeniam (napr. serverom alebo koncovým staniciam) a potvrdzujú totožnosť danej osoby alebo zariadenia.

Certifikát musí byť obnovený vždy pred jeho expiráciou alebo v prípade, ak nastane zmena v údajoch, ktoré certifikát obsahuje, napr. zmena domény, mena alebo e-mailovej adresy vlastníka certifikátu.

Každý používateľ ručí za zabezpečenie dôvernosti svojho privátneho šifrovacieho kľúča. Každé vyzradenie alebo kompromitácia súkromného šifrovacieho kľúča sa považuje za bezpečnostný incident. V prípade straty dôvernosti privátneho šifrovacieho kľúča sa certifikát súvisiaci s týmto kľúčom bezodkladne zbaví platnosti (revokácia).

Pozbavenie platnosti certifikátu sa bezodkladne vykoná aj v prípade ukončenia zamestnaneckého pomeru so zamestnancom, a to najneskôr v deň ukončenia tohto pomeru.

Všetky činnosti v súvislosti s riadením životného cyklu kryptografických kľúčov a ich správou, vrátane správnej konfigurácie CA, vykonáva špecialista/administrátor úseku informačných systémov.

5.15.5 ŠIFROVANIE LOKÁLNYCH DISKOV

Lokálne disky na všetkých koncových staniciach, stolových aj prenosných, sú šifrované. Na tento účel sa v prostredí podniku používa aplikácia BitLocker, ktorá je súčasťou systému Windows, obdobne pre Mac OS a distribúcie OS Linux/Unix.

Šifrovanie lokálnych diskov je aplikované aj na prenosných zariadeniach v majetku podniku, t. j. tabletoch a smartfónoch.

Šifrovanie lokálnych diskov na koncových staniciach je vynucované centrálnym nástrojom na správu koncových staníc.

Šifrovanie lokálnych diskov na prenosných zariadeniach je vynucované centrálnym nástrojom na správu mobilných zariadení (MDM).

Zabezpečenie centrálneho šifrovania a overenie, že disky na všetkých serveroch, dátových úložiskách a koncových staniciach, prípadne iných aktívnych prvkoch a prenosných zariadeniach sú šifrované ak to zariadenie a výrobca umožňuje, vykonáva špecialista/administrátor úseku informačných systémov.

5.15.6 ŠIFROVANIE PRENOSNÝCH MÉDIÍ

Ak zamestnanci organizácie ukladajú citlivé údaje na prenosné médiá (CD, DVD, USB a pod.), musia byť tieto údaje chránené pred stratou dôvernosti použitím nástrojov šifrovej ochrany informácií.

Za citlivé údaje sa na tento účel považujú údaje označené klasifikačným stupňom „dôverné“ a „prísne dôverné“. V prípade pochybnosti o citlivosti informácií alebo ich klasifikačnom stupni je zamestnanec povinný konzultovať ich s vlastníkom aktíva. V prípade, ak vlastníka aktíva nevie určiť, osloví nadriadeného, MKB alebo osobu zodpovednú za ochranu osobných údajov (DPO), ktorí mu poskytnú informáciu o tom, kto je vlastníkom aktíva. O citlivosti a klasifikačnom stupni údajov rozhoduje príslušný vlastník aktíva.

Na tento účel je akceptovanou metódou použitie nástrojov umožňujúcich symetrické šifrovanie s použitím šifrovacieho algoritmu najmenej AES-256, napr. 7-Zip, WinRAR alebo WinZip. Heslo na ochranu takto zašifrovaného súboru musí spĺňať požiadavky v zmysle politiky hesiel.

Heslá na dešifrovanie súborov umiestnených na prenosných médiách nesmú byť uložené v priečinkoch týchto prenosných médií alebo uvedené na ich obale.

5.15.7 E-MAILOVÁ KOMUNIKÁCIA

V prípade potreby výmeny citlivých údajov elektronickou poštou sú zamestnanci spoločnosti povinní chrániť tieto údaje pred stratou dôvernosti a pred odoslaním takýchto údajov použiť nástroje šifrovej ochrany informácií. Za citlivé údaje sa na tento účel považujú údaje označené klasifikačným stupňom „dôverné“ a „prísne dôverné“. V prípade pochybnosti o citlivosti informácií alebo ich klasifikačnom stupni je zamestnanec povinný konzultovať ich s nadriadeným, MKB alebo osobou zodpovednou za ochranu osobných údajov (DPO).

Na tento účel je akceptovanou metódou použitie nástrojov umožňujúcich vykonávať symetrické šifrovanie s použitím šifrovacieho algoritmu najmenej AES-256, napr. 7-Zip, WinRAR alebo WinZip. Heslo na ochranu takto zašifrovaného súboru musí spĺňať požiadavky v zmysle kap. 5 Šifrovanie údajov.

Heslo na otvorenie zašifrovaného súboru nesmie byť obsahom textu samotného e-mailu, ale musí byť adresátovi oznámené iným akceptovaným komunikačným kanálom, napr. cez SMS alebo aplikáciu Signal a pod.

V prípade, že zamestnancovi bude na základe hlásenia z dohľadových nástrojov alebo informácie od iného zamestnanca spoločnosti alebo tretej strany preukázané odoslanie e-mailu s nezašifrovanou prílohou, ktorej obsahom sú citlivé údaje, bude takéto konanie považované za porušenie pracovnej disciplíny a bezpečnostný incident. O tejto skutočnosti bude oboznámený nadriadený príslušného zamestnanca, MKB a v prípade ohrozenia ochrany osobných údajov, aj osoba zodpovedná za ochranu osobných údajov (DPO).

5.15.8 PRÍSTUP DO INTERNEJ SIETE Z EXTERNÉHO PROSTREDIA

Priamy prístup z externého prostredia do interných sietí a k informačným systémom spoločnosti nie je možný. Na tento účel slúži najmä segmentácia siete, VPN a správne nastavenie pravidiel brány firewall. Za definovanie sieťových segmentov, pravidiel prestupov medzi týmito segmentmi a pravidiel brány firewall zodpovedá manažér oddelenia rozvoja a prevádzky IT infraštruktúry. Bezpečnostné nastavenia vyplývajúce z týchto pravidiel vykonáva špecialista/administrátor úseku IT, ktorý tieto nastavenia zároveň priebežne monitoruje a vyhodnocuje a v prípade identifikovania

nedostatkov o tejto skutočnosti informuje za účelom úpravy pravidiel manažéra odd. bezpečnosti a krízového riadenia, ktorý rozhodne o ďalšom postupe.

Na tento účel musia zamestnanci spoločnosti, dodávateľov alebo tretích strán použiť VPN klienta nainštalovaného na koncovú stanicu, ktorý zabezpečuje šifrovanie komunikácie medzi koncovou stanicou nachádzajúcou sa v externej nezabezpečenej sieti a interným prostredím podniku, t. j. dôvernosť tejto komunikácie.

Pri prihlásení sa do VPN klienta sa vyžaduje overenie identity používateľa viacfaktorovou autentifikáciou.

Zamestnanec spoločnosti požiada o nainštalovanie VPN klienta prostredníctvom ITSM nástroja HelpDesk (<https://mhth.xurrent.com/self-service>) a táto požiadavka musí byť schválená v súlade s postupmi pre riadenie prístupov.

VPN klienta na koncovú stanicu zamestnancovi nainštaluje a nakonfiguruje špecialista/administrátor úseku informačných systémov.

Postup pri inštalácii VPN klienta na koncové stanice zamestnancov dodávateľov alebo tretích strán určuje príslušný manažér úseku informačných systémov v závislosti od konkrétneho prípadu.

VPN spojenia sú terminované v DMZ segmente, ktorý je oddelený od ostatných segmentov internej siete.

5.15.9 SIEŤOVÁ KOMUNIKÁCIA

Pri sieťovej komunikácii musí byť zabezpečená dôvernosť a integrita prenášaných údajov.

Dôvernosť a integrita údajov prenášaných pri sieťovej komunikácii je zabezpečená šifrovaním tejto komunikácie prostredníctvom sieťových bezpečnostných protokolov. Ich účelom je zabrániť neoprávnenému používateľovi, aplikácii, službe alebo zariadeniu v prístupe k údajom prenášaných po sieti.

Dôvernosť komunikácie typu klient-server je zabezpečená použitím protokolu SSL alebo TLS.

Dôvernosť komunikácie prostredníctvom webovej stránky podniku je zabezpečená použitím protokolu HTTPS.

Dôvernosť komunikácie prostredníctvom Wi-Fi sietí je zabezpečená použitím protokolu WPA2 alebo vyššieho.

Pravidlá pre zabezpečenie sieťovej komunikácie požadovaným spôsobom šifrovania určuje MKB. Za výber vhodných šifrovacích mechanizmov zodpovedá manažér oddelenia rozvoja a prevádzky IT infraštruktúry.

Nasadenie a správu šifrovacích mechanizmov vykonáva špecialista/administrátor na úseku IT.

5.15.10 ŠIFROVANIE V OT PROSTREDÍ

IEC 60870-5-104 je medzinárodný protokol a štandard, ktorý sa používa na diaľkové ovládanie v energetike a v aplikáciách energetických systémov. Je to jeden z hlavných riadiacich protokolov v systéme SCADA ICS v spoločnosti. Jedným z najčastejších útokov, ktorý môže mať katastrofický dopad na priemyselné riadiace systémy, je útok na riadiace príkazy v IEC 104. Dochádza k nemu vtedy, keď útočník do riadiaceho systému vloží falošné riadiace príkazy, tzv. vkladanie príkazov (command injection attack) a informačných údajov. Tento protokol je natívne nešifrovaný.

V prípade nasadenia šifrovania nad protokolom IEC 60870-5-104 je nutné nasadiť jeho rozšírenie cez protokol IEC 62351, ktorý podporuje šifrovanie SSL/TLS medzi stanicou a transformátorovou ochranou (IED). Postup a technické riešenie musí byť konzultované s dodávateľom riadiaceho systému.

Šifrovanie na sieťovej úrovni pomocou SSL/TLS IEC 62351-9 (napr. pre podporované Siemens IED) musí byť schválené a odporučené dodávateľom podľa bezpečnostných štandardov výrobcu konkrétneho riadiaceho systému, alebo jeho prvku.

Šifrovanie v OT sieti môže zvýšiť latencie signalizačnej prevádzky a spôsobiť negatívne dopady. Akékoľvek šifrovacie riešenie tretej strany, ktoré nie je natívne integrované v komponentoch riadiaceho systému, ju nutné konzultovať s dodávateľom riadiaceho systému.

V prípade použitia industrial Wi-Fi ako ISA 100 alebo Wireless HART je nutné použiť symetrické šifrovanie a to minimálne AES 128 bit.

Dôvernosť komunikácie typu SCADA klient-server je zabezpečená použitím protokolu SSL alebo TLS, všade tam, kde je to technicky možné.

Dôvernosť komunikácie prostredníctvom využívania webových stránok pre technologické portály a technologické kamerové systémy podniku je zabezpečená použitím protokolu HTTPS.

Technologické laptopy slúžiace na programovanie riadiaceho systému musia mať zabezpečené harddisky a prenosné média šifrovaním, napr. nástrojmi BitLocker alebo VeraCrypt.

Priame VPN prístupy do OT siete sú zakázané ako tiež inštalácia takýchto zariadení v technických miestnostiach podniku.

Za zabezpečenie šifrovania v OT prostredí zodpovedá MKB.

Za výber vhodných šifrovacích mechanizmov zodpovedá príslušný OT manažér v súčinnosti s dodávateľmi riadiacich systémov. Nasadenie vykonáva dodávateľ riadiacich systémov a správu šifrovacích mechanizmov vykonáva špecialista/administrátor úseku IT.

5.15.11 KONTROLA

V pravidelných intervaloch, minimálne 1x ročne, sa vykonáva kontrola bezpečnostných pravidiel a konfigurácií definovaných touto smernicou za účelom identifikácie nesúladu s týmito požiadavkami a ich následnej nápravy.

Za vykonanie kontroly zodpovedá príslušný manažér IT a príslušný manažér OT. Kontrolu vykonáva špecialista/administrátor IT/OT, ktorý o jej výsledku informuje riaditeľa úseku informačných systémov a manažéra kybernetickej bezpečnosti.

5.16 POLITIKA RIADENIA DODÁVATEĽOV

5.16.1 ÚČEL, ROZSAH A UŽÍVATELIA

Účelom tejto kapitoly je vymedziť pravidlá vzťahov s dodávateľmi a partnermi a inými tretími stranami.

táto časť dokumentu je záväzná pre všetkých dodávateľov a partnerov, ktorí môžu ovplyvniť dôvernosť, integritu a dostupnosť poskytovaných služieb spoločnosti.

Používatelia tohto dokumentu sú vedúci pracovníci a osoby zodpovedné za riadenie vzťahov s dodávateľmi a partnermi v spoločnosti.

5.16.2 VZŤAHY S DODÁVATEĽMI A PARTNERMI

5.16.2.1 IDENTIFIKÁCIA RIZÍK

Bezpečnostné riziká súvisiace s dodávateľmi a partnermi sú identifikované počas hodnotenia rizík, podľa metodiky riadenia rizík. Počas analýzy rizík treba venovať osobitnú pozornosť rizikám súvisiacim s prístupom dodávateľov k informačným aktívam.

5.16.2.2 PREVEROVANIE

MKB rozhodne, či je potrebné vykonať overenie pre jednotlivých dodávateľov a partnerov, a ak áno – ktoré metódy sa musia použiť.

5.16.2.3 ZMLUVY

MKB je zodpovedný za rozhodovanie o tom, ktoré bezpečnostné opatrenia budú zahrnuté v zmluve s dodávateľom alebo partnerom.

Zamestnanec požiada dodávateľa, aby zabezpečil segregáciu jeho vývojových prác pre daného zákazníka od iných vývojových prác pre iného zákazníka.

Takéto rozhodnutia musia byť založené na výsledkoch posúdenia rizika a opatrení; klauzuly, ktoré stanovujú uchovanie mlčanlivosti a vrátenia aktív po skončení dohody sú povinné. Poverený zamestnanec dohodne s dodávateľom spôsob pre segregáciu vývojových prác u dodávateľa. Segregácia znamená, že dodávateľ je povinný rozlíšiť projekty podľa zákazníkov a zabezpečiť pri návštevách jeho zákazníkov nemožnosť nahliadať na praktiky (dôverné informácie) realizované u inej firmy.

Zmluva musí zabezpečiť spoľahlivé dodávky výrobkov a služieb.

MKB rozhodne, či jednotliví zamestnanci dodávateľa/partnera budú musieť podpísať vyhlásenie o zachovaní mlčanlivosti pri práci v spoločnosti.

5.16.2.4 ŠKOLENIA A BUDOVANIE POVEDOMIA

Gestor/vlastník zmluvy rozhodne, ktorých zamestnancov dodávateľov a partnerov je potrebné preškoliť v oblasti informačnej a kybernetickej bezpečnosti.

5.16.3 MONITORING A PRESKÚMANIE

Vlastník zmluvy musí pravidelne kontrolovať a monitorovať úroveň plnených služieb a plnenie bezpečnostných požiadaviek dodávateľov alebo partnerov. Hodnotenie poskytovaných služieb formou kontroly treba vykonať 1-krát ročne.

Všetky bezpečnostné incidenty súvisiace so spoločnosťou musí dodávateľ/partner bezodkladne nahlásiť MKB.

5.16.3.1 ODOBRA Tie PRÍSTUPOVÝCH PRÁV / NÁVRAT MAJETKU

Pri zmene zmluvy, alebo jej ukončení, prístupové práva zamestnancov partnera /dodávateľa musia byť odstránené podľa politiky riadenie prístupu.

Vlastník zmluvy po ukončení zmluvy je povinný sa uistiť, či bolo vrátené všetko vybavenie, softvér alebo informácie v elektronickej alebo papierovej forme.

Pre riadenie dodávateľov platia povinnosti podľa ZoKB a PKIB.

5.16.3.2 Súvisiaca dokumentácia

Ďalšie informácie uvedené v smernici [MHTH_S39_Dodávateľsko odberateľské vzťahy](#).

5.17 POLITIKA PRE RIADENIE KONTINUITY

5.17.1 ÚČEL, ROZSAH A UŽÍVATELIA

Účelom tejto časti dokumentu je vymedziť cieľ, rozsah a základné pravidlá pre riadenie kontinuity podnikania.

Táto politika je aplikovaná na celý Business Continuity Management System (BCM).

5.17.2 RIADENIE BCM

Predmetom riadenia kontinuity podnikania je identifikovať potenciálne hrozby pre organizáciu a dopady na obchodné operácie, a poskytnúť rámec pre vytváranie organizačnej odolnosti so schopnosťou účinne na hrozby reagovať.

5.17.3 CIELE BCM

- Systém BCM musí spĺňať všetky požiadavky zákonných, regulačných a zmluvných povinností.
- Vyvinúť, implementovať, udržiavať a neustále zlepšovať systém BCM vrátane stratégií, politiky a plánov obnovy.
- Zaisťovať, aby všetky funkcie a činnosti stratégie a plánov obnovy boli funkčné a efektívne.

- Plniť opatrenia z riadenia rizík týkajúce sa BCM.
- Vytvoriť stratégiu a plány obnovy na nové hrozby, ktoré boli identifikované ako výsledok procesu riadenia rizík a navrhnuť a implementovať zodpovedajúce opatrenia.
- Poskytnúť záruky všetkým zainteresovaným stranám prostredníctvom zavedenia a udržiavania stratégie a plánov obnovy.
- Uplatňovať túto politiku do všetkých činností v rámci spoločnosti.
- Poskytnúť dostatočné zdroje, školenia a zamestnancov potrebných na vytvorenie, zavedenie, prevádzku a údržbu systému BCM.
- Každoročne preskúmať systém kontinuity prevádzky.
- Zabezpečiť, aby spoločnosť implementovala osvedčené postupy a nové trendy, prostredníctvom ktorých je možné dosiahnuť zlepšenie mechanizmov BCM.

5.17.4 ROZSAH

Business Continuity Management System musí byť implementovaný pre celú organizáciu, pričom osobitnú pozornosť treba venovať činnostiam zisteným počas BIA - analýzy obchodných dopadov na základné služby (PZS).

5.17.5 HLAVNÉ PRODUKTY A SLUŽBY

Nasledujúce kľúčové produkty a služby sú poskytované spoločnosťou v rozsahu stanovenom v predchádzajúcej časti:

- Zabezpečenie základnej služby podľa ZoKB

Obchodné riadenie kontinuity musí zabezpečiť, že vyššie uvedené služby sa opätovne podarí sprevádzkovať na vopred definovanú úroveň.

5.17.6 ZODPOVEDNOSŤ ZA RIADENIE KONTINUITY PODNIKANIA

Všeobecné povinnosti:

- Business Continuity Manager – BCM, je zodpovedný za to, že riadenie kontinuity podnikania je vybudované a plní svoju funkciu v súlade s touto politikou. Je zodpovedný za zabezpečenie všetkých potrebných zdrojov;
- BCM zodpovedá za operatívne zavedenie a udržiavanie kontinuity podnikania BCM na úrovni DR plánov;
- Výkonný manažment spoločnosti (Porada vedenia) je zodpovedný za preskúmanie BCM minimálne raz za rok alebo vždy, keď dôjde k významnej zmene. Z preskúmania je nutné vyhotoviť hodnotiacu správu. Účelom preskúmania manažmentom je stanoviť vhodnosť, primeranosť a efektívnosť BCM;

Konkrétne úlohy:

- BCM je zodpovedný za vypracovanie plánu a vykonanie školení, ktorý sa vzťahuje na všetky osoby, ktoré plnia úlohy pri riadení obchodnej kontinuity;
- Opatrenia na zabezpečenie kontinuity činností musia byť vykonávané a testované minimálne raz ročne za použitia rôznych metód, s cieľom posúdiť, ako môžu chrániť činnosti organizácie;
- BCM musí vykonávať nácvik a plán testovania, ktorý musí byť schválený vedením spoločnosti; Po každom nácviku a testovaní musí byť vyhotovená hodnotiacia správa;
- BCM je zodpovedný za prijímanie a vykonávanie údržby a aktualizácie plánu BCM, takže všetky prvky BCM musia byť udržiavané a aktualizované;
- Vždy, keď je Business Continuity Plan, plán obnovy alebo Plan Incident Response aktivovaný, BCM je zodpovedný za kontrolu účinnosti BCM;
- BCM je zodpovedný za sledovanie nezhôd, falošných poplachov, aktuálnych udalostí, atď.

5.17.7 MERANIE

Spoločnosť je povinná pre zabezpečenie BCM plánovať a merať aktivity spojené s prevádzkovaním základných služieb (PZS):

- Splnenie stanovených cieľov v súlade s touto politikou - aspoň raz za rok, obvykle v rámci orgánu Porada vedenia;
- Účinnosť a primeranosť plánov kontinuity podnikania - na frekvencii nastavenej v pláne kontinuity;

BCM vypracuje správu o výsledkoch meraní, zatiaľ čo analýza a vyhodnotenie výsledkov sa uskutoční za predpokladu preskúmania vedením spoločnosti.

5.17.8 METODOLÓGIA ANALÝZY OBCHODNÝCH DOPADOV NA PODNIKANIA BIA

Dopady vyvolané incidentom sú posudzované z hľadiska celkového vplyvu na fungovanie spoločnosti a poskytovaných služieb (kvalitatívne posúdenie) a finančný dopad (kvantitatívne posúdenie).

5.17.9 MAXIMÁLNY PRIJATEĽNÝ VÝPADOK (RTO)

Maximálny prijateľný výpadok / maximálne prípustné obdobie prerušenia poskytovania služieb sa určuje v hodinách alebo dňoch.

Klasifikácia úrovne dopadu po incidente na spoločnosť:

Okrajový dopad	1	Trvanie incidentu spôsobuje zanedbateľné poškodenie spoločnosti, peňažného toku, zákonných, regulačných alebo zmluvných povinností alebo dobrú povesť spoločnosti.
Prijateľný dopad	2	Trvanie incidentu spôsobuje poškodenie spoločnosti, peňažného toku, zákonných, regulačných alebo zmluvných povinností alebo dobrú povesť spoločnosti, ale takéto škody sú stále prijateľné.
Vysoký dopad	3	Trvanie incidentu spôsobuje poškodenie spoločnosti, peňažného toku, zákonných, regulačných alebo zmluvných povinností alebo dobrú povesť spoločnosti a takéto škody sú neprijateľné.
Katastrofický dopad	4	Trvanie incidentu spôsobuje fatálne škody spoločnosti, peňažného toku, zákonných, regulačných alebo zmluvných povinností alebo dobrú povesť spoločnosti.

5.17.10 MAXIMÁLNE STRATY DÁT (RPO)

Maximálne množstvo údajov, ktoré môžu byť stratené pre každý IS (databázu, aplikáciu alebo informáciu,...).

Klasifikácia úrovne dopadu po incidente na spoločnosť:

Okrajový dopad	1	Počet stratených dát spôsobí zanedbateľné poškodenie spoločnosti, peňažného toku, zákonných, regulačných alebo zmluvných povinností alebo jej dobrú povesť.
Prijateľný dopad	2	Počet stratených dát spôsobí poškodenie spoločnosti, peňažného toku, zákonných, regulačných alebo zmluvných povinností alebo jej dobrú povesť, ale takáto škoda je stále prijateľná pre spoločnosť.
Vysoký dopad	3	Počet stratených dát spôsobí poškodenie spoločnosti, peňažného toku, zákonných, regulačných alebo zmluvných

		povinností alebo jej dobrú povesť, takáto škoda je neprijateľná pre spoločnosť.
Katastrofický dopad	4	Počet stratených dát spôsobí poškodenie spoločnosti, peňažného toku, zákonných, regulačných alebo zmluvných povinností alebo jej dobrú povesť, takáto škoda je fatálna až likvidačná pre spoločnosť.

5.17.11 PRAVIDELNÉ PRESKÚMANIE ANALÝZY OBCHODNÉHO DOPADU

BCM musí vykonať preskúmanie analýzy obchodného dopadu a obchodnej stratégie. Preskúmanie sa vykonáva aspoň raz za rok alebo častejšie v prípade značných organizačných zmien, významných zmien v technológii, zmeny podnikových cieľov, zmien v podnikateľskom prostredí.

5.17.12 PLÁNY OBCHODNEJ KONTINUITY

Plán obchodnej kontinuity pozostáva z dvoch hlavných častí:

- Plán reakcie na incident, ktorý vymedzuje priamo reakciu na výskyt rôznych typov udalostí;
- Plánov na obnovu jednotlivých aktivít.

5.17.13 ZÁVISLOSTI

Pre účinnosť plánu je nevyhnutné, aby boli všetky zdroje a vybavenie stanovené v stratégii kontinuity podnikania dostupné a pripravené.

5.17.14 AKTIVÁCIA A DEAKTIVÁCIA PLÁNOV

Plán reakcie na Incident sa aktivuje automaticky v prípade, ak dôjde k mimoriadnej udalosti, alebo potenciálne hrozí jej vzniknutie. Plán reakcie na Incident bude deaktivovaný po vymedzení alebo odstránení incidentu.

Plány na obnovu pre konkrétne činnosti sú aktivované výlučne rozhodnutím zodpovedného povereného riešiteľa v roli krízového manažéra, ak zhodnotí, že konkrétna činnosť bude prerušená na obdobie dlhšie ako je čas obnovy. Rozhodnutie krízového manažéra môže byť písomné alebo ústne (len vo výnimočných prípadoch, keď vec neznesie odklad).

Plány na obnovu môžu deaktivovať zodpovedného povereného riešiteľa v roli recovery manažéra pre jednotlivé činnosti keď zistia, že boli splnené všetky podmienky na pokračovanie podnikateľskej činnosti. Plány na obnovu sú deaktivované obnovením bežných podnikateľských činností.

5.17.15 PRÍPRAVA AKČNÝCH PLÁNOV

Každá zodpovedná osoba musí vypracovať akčný plán pre svoju oblasť zodpovednosti, ktorý okrem iných informácií obsahuje nasledovné:

- jednotlivé kroky,
- potrebné ľudské zdroje,
- požadované finančné zdroje
- termíny.

5.17.16 TESTOVANIE BCP/DRP PLÁNOV

Za účelom overenia funkčnosti BCP a DRP plánov ako aj overenia, že zamestnanci organizácie zúčastňujúci sa na zabezpečení kontinuity procesov a obnovy systémov po havárii tieto plány ovládajú a vedia ich realizovať v určených časových lehotách, sa jednotlivé plány tieto pravidelne testujú. Pravidelné testovanie vykonáva Špecialista/Administrátor úseku IT v spolupráci s príslušnými manažérmi IT, business partnermi IT a manažérmi OT, ktorí o jej výsledku informujú MKB.

Špecialisti a administrátori úseku IT a príslušní OT manažéri, sú zodpovední za identifikovanie požiadaviek na dostupnosť jednotlivých IT, resp. OT systémov, kritických komponentov, služieb alebo aplikácií ako aj preverenie možnosti aktuálnej garancie požadovanej úrovne dostupnosti. Dostupnosť je preskúmaná, prípadne testovaná v pravidelných intervaloch a to minimálne raz za rok.

V prípade, že požadovaná úroveň dostupnosti systémov nie je zaručená v súčasnej architektúre, sú zvážené možnosti vytvorenia redundantnej architektúry, alebo ďalšie možnosti pre dosiahnutie požadovanej úrovne dostupnosti (napr. spare hardware).

5.18 RIADENIE BEZPEČNOSTNÝCH INCIDENTOV

5.18.1 ÚČEL, ROZSAH A UŽÍVATELIA

Cieľom je určenie účinných a efektívnych postupov identifikovania, reagovania, dokumentovania, vyšetrovania a odstránenia bezpečnostných incidentov akýchkoľvek informačných aktív ako aj bezpečnostných incidentov definovaných v zákone o ochrane osobných údajov a ZoKB – od ich zachytenia až po celkové vyriešenie.

Bezpečnostný incident je jedna alebo viac nečakaných alebo nežiaducich bezpečnostných udalostí, ktoré môžu ohroziť informačnú/kybernetickú bezpečnosť a tým aj obchodné procesy spoločnosti.

5.18.2 PRINCÍPY RIADENIA INCIDENTOV

Definícia kybernetického incidentu

- a) Bezpečnostným incidentom sa rozumie identifikovaný neštandardný stav IT/OT systému, procesu, služby, alebo komponentu infraštruktúry, ktorý môže narušiť pravidlá bezpečnostnej politiky, alebo bezpečnostného opatrenia. Patrí sem aj akýkoľvek prípad zlyhania bezpečnostných opatrení s negatívnym, alebo potenciálne negatívnym dopadom na informačné aktíva.
- b) Bezpečnostným incidentom je aj podozrenie na spáchanie trestného činu v IT a OT prostredí, priestupku alebo iného pokusu získať neoprávnený prístup alebo neoprávnene nakladať s informáciami;
- c) Podľa tejto smernice sa postupuje pri riešení incidentov informačnej a kybernetickej bezpečnosti. Za proces riešenia ostatných bezpečnostných incidentov (fyzická alebo funkčná ochrana) je zodpovedný útvar OBKR;
- d) Úsek IT a OBKR sú povinní spolupracovať pri riešení bezpečnostných incidentov, a to najmä v prípadoch pokiaľ sa jedná o kombináciu bezpečnostných incidentov informačnej a fyzickej bezpečnosti;
- e) Zamestnanci spoločnosti ako aj zamestnanci tretích strán sú povinní ohlasovať incidenty nadriadenému, MKB (alebo bezpečnostný tím), administrátorovi IT, RIS manažérovi aj možné bezpečnostné nedostatky, alebo slabiny informačných systémov, služieb a aplikácií spoločnosti, ktoré zistili pri ich používaní, alebo správe;

5.18.3 ŽIVOTNÝ CYKLUS KYBERNETICKÉHO INCIDENTU

Životný cyklus bezpečnostného incidentu sa skladá z piatich fáz:

- 1) **Identifikácia** – proces rozpoznania vzniku bezpečnostného incidentu, jeho registrácia v systéme riadenia incidentov a priradenie zodpovednej osoby pre riešenie daného incidentu;
- 2) **Riešenie** – proces, v ktorom zodpovedné osoby analyzujú stav a príčiny incidentu, hľadajú riešenie vedúce k minimalizácii škôd spôsobených bezpečnostným incidentom a prijímajú okamžité opatrenia, vedúce k eliminácii bezpečnostného incidentu, resp. vyhlasujú krízový stav, ak to vážnosť a povaha incidentu vyžadujú;
- 3) **Neutralizácia/izolácia** – proces realizácie opatrení, vedúcich k trvalému odstráneniu rizika výskytu identifikovaného typu bezpečnostného incidentu, izolácia

kompromitovaného systému od zbytku siete, tak aby nedošlo k ďalšiemu šíreniu do iných segmentov a zón.

- 4) **Obnova** – proces obnovy systému späť do normálneho prevádzkového stavu a obnovenie služieb a priemyselných procesov.
- 5) **Ponaučenie** – zdokumentované vyšetrenie incidentu, ktoré obsahuje aj zoznam nápravných opatrení, ktoré budú slúžiť ako prevencia a zamedzenie incidentu v budúcnosti, ponaučenie vo forme edukácie osôb, zmena technických opatrení a bezpečnostných smerníc, atď.

5.18.4 OSOBY ZODPOVEDNÉ ZA RIEŠENIE INCIDENTOV

Pri riešení bezpečnostného incidentu spolupracujú nasledovné zodpovedné osoby, resp. tímy:

- Manažér kybernetickej bezpečnosti (MKB)
- Bezpečnostný tím riešenia kybernetických incidentov
- Administrátor IT/OT, resp. špecialista IT/OT
- Používateľ IT/OT
- Zodpovedná osoba – DPO (pre GDPR incidenty)

5.18.5 ŽIVOTNÝ CYKLUS INCIDENTU A MATICA ZODPOVEDNOSTÍ PRE JEDNOTLIVÉ ROLE

	Identifikácia	Riešenie	Neutralizácia	Obnova	Ponaučenie
IT/OT používateľ	X				X
IT/OT administrátor	X	X	X	X	X
MKB	X	X			X
MKB, Bezpečnostný tím, IT/OT špecialista	X	X	X		X
Zodpovedná osoba (DPO)	X	X			X

5.18.6 STRUČNÝ POPIS JEDNOTLIVÝCH ROLÍ A ZODPOVEDNOSTÍ:

Používateľ IT: ako i každý iný zamestnanec spoločnosti je v procese prvej identifikácie bezpečnostného incidentu zodpovedný za nahlásenie bezpečnostného incidentu na IT Helpdesk, a to emailom na helpdesk alebo cez self-portal. Používateľ IT nesmie samostatne vyvíjať akékoľvek aktivity, ktorými by sa pokúsil vyriešiť vzniknutý bezpečnostný incident, okrem prípadov, keď musí vykonať kroky vedúce k minimalizácii ďalších škôd na majetku alebo zraneniu osôb v prípade živeľnej pohromy.

OT používateľ je povinný nahlásiť bezpečnostný incident OT manažérovi. OT operátor/špecialista nesmie samostatne vyvíjať akékoľvek aktivity, ktorými by sa pokúsil vyriešiť vzniknutý bezpečnostný incident, okrem prípadov, keď musí vykonať kroky vedúce k minimalizácii ďalších škôd na majetku alebo zraneniu osôb v prípade živeľnej pohromy.

MKB participuje a metodicky riadi proces manažmentu kybernetického incidentu, a v prípade potreby spúšťa eskalačný proces a informuje manažment o dopadoch a následkoch incidentu na spoločnosť, zvoláva krízový tím, koordinuje a zostavuje Bezpečnostný tím.

Administrátor IT a OT špecialista je zodpovedný za jednoznačnú identifikáciu nahláseného bezpečnostného incidentu. Ďalej zabezpečuje zber údajov pre následnú analýzu vzniku bezpečnostného incidentu, je zodpovedný za riešenie bezpečnostného incidentu a jeho evidenciu a zber dôkazov, koordinuje a informuje osoby zodpovedné za riešenie. Je zodpovedný za

neutralizáciu/izoláciu kompromitovaného systému (odpojenie napadnutého systému malvérom od počítačovej siete) pomocou technických opatrení a obnovu systému zo záloh.

Bezpečnostný tím zabezpečuje podrobnú analýzu bezpečnostného incidentu a navrhuje opatrenia s cieľom v čo najkratšom čase eliminovať výskyt bezpečnostného incidentu. Koordináciu a informovanosť v rámci Bezpečnostného tímu pri riešení BI zabezpečuje MKB. Zodpovedá tiež za posúdenie vážnosti bezpečnostného incidentu ako podklad pre bezpečnostnú komisiu, kt. vyhlasuje krízový stav, ak je to pre prevádzku spoločnosti nevyhnutné. Členov menuje MKB na základe typu a rozsahu incidentu (napr. administrátor IT, špecialista OT, zástupca pre komunikáciu apod.)

Bezpečnostná komisia – riadiaca komisia pre oblasť KB, vyhlasuje krízový stav pre oblasť KB

Zodpovedná osoba (DPO) je určená osoba, ktorá zabezpečuje dohľad nad ochranou osobných údajov pri spracúvaní osobných údajov. Dohľad nad ochranou osobných údajov predstavuje viacero úloh a činností, ktoré je zodpovedná osoba povinná plniť podľa nariadenia GDPR, zákona o ochrane osobných údajov a internej smernice MHTH o ochrane osobných údajov. Nariadenie GDPR definuje požiadavku nahlásenia incidentu súvisiaceho s porušením práv a slobôd dotknutých osôb bez zbytočného odkladu, najneskôr však do 72 hod. od jeho zistenia na Úrad na ochranu osobných údajov Slovenskej republiky.

Tím interných predpisov – zabezpečuje preukázateľné oboznámenie všetkých zamestnancov s touto smernicou, v zmysle postupov uvedených v [smernici MHTH S01 Riadenie dokumentov a procesov](#).

5.18.7 IDENTIFIKÁCIA A HLÁSENIE BEZPEČNOSTNÝCH SLABÍN (ZRANITEĽNOSTÍ)

Bezpečnostnou slabinou (vulnerability) je všetko, čo môže viesť k bezpečnostnému incidentu.

V prípade, ak zamestnanec odhalí bezpečnostnú slabinu, jedná rovnako ako v prípade odhalenia bezpečnostnej udalosti/incidentu.

Medzi základné kategórie zraniteľností patria najmä:

- nedostatočná údržba informačného a komunikačného systému;
- zastaranosť informačného a komunikačného systému;
- nedostatočná ochrana vonkajšieho perimetra;
- nedostatočné bezpečnostné povedomie používateľov a administrátorov;
- nevhodné nastavenia prístupových oprávnení;
- Chybná konfigurácia prvkov infraštruktúry, alebo riadiacich prvkov,
- nedostatočné postupy pri identifikovaní a odhalení negatívnych bezpečnostných javov, kybernetických bezpečnostných udalostí a kybernetických bezpečnostných incidentov;
- nedostatočné monitorovanie činnosti používateľov a administrátorov a neschopnosť odhaliť ich nevhodné alebo závadné spôsoby správania;
- nedostatočné stanovenie bezpečnostných pravidiel, nepresné alebo nejednoznačné vymedzenie práv a povinností používateľov, administrátorov a bezpečnostných rolí;
- nedostatočná ochrana aktív;
- nevhodná bezpečnostná architektúra;
- nedostatočná miera nezávislej kontroly;
- neschopnosť včasného odhalenia pochybenia zo strany zamestnancov.

5.18.8 DETEKCIA BEZPEČNOSTNÝCH UDALOSTÍ A INCIDENTOV

Spoločnosť v rámci komunikačnej siete, ktorej súčasťou je informačný a komunikačný systém, minimálne v rozsahu prevádzkovaných základných služieb kybernetickej bezpečnosti, používa nástroje pre detekciu kybernetických bezpečnostných udalostí, ktoré zaistia:

- overenie a kontrolu prenášaných dát v rámci komunikačnej siete a medzi komunikačnými sieťami,
- overenie a kontrolu prenášaných dát na perimetri komunikačnej siete a
- blokovanie nežiaducej komunikácie.

Spoločnosť zabezpečuje detekciu kybernetických bezpečnostných udalostí primerane s ohľadom na dôležitosť aktív v rámci IT/OT systémov, min. v rozsahu:

- koncových staníc;
- mobilných zariadení;
- serverov;
- dátových úložísk a výmenných dátových nosičov;
- sieťových aktívnych prvkov a
- iných aktív priamo/nepriamo podieľajúcich sa na prevádzkovaní základnej služby.

Proces detekcie kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom nástroja na detekciu kybernetických bezpečnostných incidentov, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát.

Proces zberu a vyhodnocovania kybernetických bezpečnostných incidentov sa zabezpečuje prostredníctvom nástroja na zber a nepretržité vyhodnocovanie kybernetických bezpečnostných udalostí, ktorý umožňuje:

- zber a vyhodnocovanie informácií o kybernetických bezpečnostných incidentoch;
- vyhľadávanie a zoskupovanie záznamov súvisiacich s kybernetickým bezpečnostným incidentom;
- vyhodnocovanie bezpečnostných udalostí a na ich identifikáciu ako kybernetických bezpečnostných incidentov;
- revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných kybernetických bezpečnostných incidentoch.

5.18.9 RIEŠENIE BEZPEČNOSTNÝCH UDALOSTÍ A INCIDENTOV

V rámci riešenia bezpečnostných udalostí je potrebné naplňať tieto ciele:

- potvrdiť alebo vyvrátiť, či skutočne k incidentu došlo;
- zhromaždiť presné a objektívne informácie;
- nastaviť mechanizmy získavania a spracovania dôkazov; zachovať privátnosť informácií garantovanú zákonom;
- minimalizovať dopady incidentu na normálne fungovanie organizácie;
- umožniť stíhanie útočníkov;
- vytvoriť podrobné protokoly a odporúčenie.

5.18.10 POSTUP PRE EVIDENCIU A RIEŠENIE BEZPEČNOSTNÝCH INCIDENTOV

O tom, či ide o bezpečnostnú udalosť alebo bezpečnostný incident, rozhoduje vždy na základe získaných informácií manažér kybernetickej bezpečnosti.

Aktivity pri evidencii a riešení BI:

- vyšetrenie bezpečnostného incidentu;
- spoluprácu s NBÚ SR a ústrednými orgánmi pri riešení hláseného kybernetického bezpečnostného incidentu, poskytovanie potrebnej súčinnosti pre tieto orgány, ako aj informácií získaných z vlastnej činnosti dôležitých pre riešenie kybernetického bezpečnostného incidentu;
- zistenie účastníkov;
- určenie závažnosti a škôd;
- stanovenie postupu pre odstránenie následkov;

- podľa potreby úprava pravidiel a smerníc;
- vyvolanie rokovania škodovej komisie;
- vyvolanie rokovania disciplinárnej komisie;
- vyvolanie trestného vyšetrovania;
- dokumentácia incidentu, v čase bezpečnostného incidentu zabezpečenie dôkazu alebo dôkazného prostriedok tak, aby mohol byť použitý v trestnom konaní zabezpečenie dôkazných materiálov a ich ochrany pred zmenami;
- určenie postupu pri jeho riešení;
- určenie pracovníkov zodpovedných za odstránenie incidentu (prípadne jeho následkov).

Po zaevidovaní bezpečnostného incidentu MKB riadi všetky následné činnosti (ak ich typ bezpečnostného incidentu vyžaduje):

- Integrita dôkazného materiálu by sa mala chrániť tak, aby mohol byť použitý v trestnom konaní. Kopírovanie dôkazného materiálu by sa malo vykonávať pod dohľadom dôveryhodného personálu a informácie o tom, kde a kedy sa kopírovanie uskutočnilo, o tom kto ho vykonal, ako aj to, aké nástroje a programy boli pritom použité, by sa mali zaznamenať vo forme log záznamov.
- Súčasťou evidencie kybernetických bezpečnostných incidentov, sa na zabezpečenie dôkazu alebo dôkazného prostriedku, evidujú aj informácie identifikujúce kybernetický bezpečnostný incident, ako napríklad lokalita, hostname, MAC adresy, IP adresy, identifikačné údaje všetkých zariadení a zúčastnených osôb a dátum, čas manipulácie s údajmi a vymedzenie miesta ich uloženia.
- Za týmto účelom, v prípade závažných incidentov, u ktorých je možné predpokladať disciplinárne alebo právne konanie, je potrebné zabezpečiť dôkazný materiál nasledovne:
 - pre papierové dokumenty: originál sa uchováva v bezpečí a sú uložené dôkazy o tom, kto ho našiel, kde a kedy bol nájdený a kto bol svedkom tohto objavenia. Každé prešetrenie by malo uistiť o tom, že originály neboli sfalšované;
 - pre informácie na počítačových médiách: aby sa zaistila dostupnosť, vytvoria sa kópie alebo „zrkadlové obrazy“ všetkých prenosných médií, informácií na pevných diskoch alebo v pamäti (v závislosti od platných požiadaviek); uchováva sa log záznam všetkých činností;
 - počas procesu kopírovania dôkazného materiálu by mali byť pri tomto procese svedkovia; pôvodné médium a log záznam (ak to nie je možné, tak aspoň jedna kópia alebo „zrkadlový obraz“) sa držia v bezpečí a nedotknuté.

Akékoľvek úkony s dôkazným materiálom v súdnom konaní sa môžu vykonávať iba na jeho kópiách. Je potrebné chrániť integritu dôkazného materiálu tak, aby mohol byť použitý v trestnom konaní. Kopírovanie dôkazného materiálu sa vykonáva iba pod dohľadom dôveryhodného personálu a informácie o tom, kde a kedy sa kopírovanie uskutočnilo, o tom kto ho vykonal, ako aj to, aké nástroje a programy boli pritom použité, by sa mali zaznamenať vo forme bezpečnostných (log) záznamov.

5.18.11 RACI MATICA PRE AKTIVITY INCIDENT MANAŽMENTU

	Aktivita/ Vlastník	CEO	MKB	CIO	Úrad	Zamestnanci	DPO
R - Zodpovedný za vykonanie A - Zodpovedný za úlohu C - Konzultované s kým? I – Informovaný (kto)?							
1	Prijímanie varovaní o potenciálne kritických bezpečnostných udalostiach (útoky, kampane, Zraniteľnosti vrátane Breaches) Zabezpečí, aby sa príslušné incidenty hlásili v súlade s postupmi jednotlivých regulácií. ASAP	A	R	I	C		C
2	Ak je pravdepodobné, že porušenie bezpečnosti alebo strata integrity bude mať nepriaznivý dopad na fyzickú alebo právnickú osobu, spoločnosť bez zbytočného odkladu informuje fyzickú alebo právnickú osobu aj o porušení bezpečnosti alebo strate integrity. ASAP	A	R	I	I	I	I
3	V prípade akejkoľvek zraniteľnosti, vzhľadom na potenciálny dopad, spoločnosť: - vytvorí a implementuje plán na zmiernenie zraniteľnosti; ASAP	A	R	I	I	I	
4	Zdokumentované rozhodnutie o prijatí rizika v prípade hrozby alebo zraniteľnosti. ASAP	R	C	I		I	
5	Registrácia Incidentu a bezpečnostných udalostí v ITSM nástroji, návrh nápravných a preventívnych opatrení	I	C	I		R	I
6	Ukončenie incidentu, vyhodnotenie nápravných a preventívnych opatrení	A	R	I		I	I
7	Monitorovanie celého environmentu bezpečnostných systémov formou prijímania notifikácií o bezpečnostných udalostiach a Bezpečnostných incidentoch a následné vyhodnotenie a vykonanie opatrení	A	R	C			
8	Vyhlásenie krízového stavu a spustenie BCM	R	C	C	I		
9	Ukončenie krízového stavu a návrat do štandardnej prevádzky	R	C	C	I		

5.18.12 POSTUP RIADENIA KYBERNETICKÉHO INCIDENTU

5.18.12.1 Identifikácia incidentu

Proces riadenia incidentov pozostáva z množstva na seba nadväzujúcich aktivít, ktoré sú popísané v nasledujúcich bodoch.

Krok1: Identifikácia incidentu

Vstup: Nástroj na monitorovanie bezpečnostných hrozieb, fyzickej bezpečnosti, nahlásenie osobou

Výstup: Vylúčenie udalosti a identifikácia incidentu na základe indikátorov kompromitácie

Kto: hociktorý používateľ IT / OT alebo OT operátor

Kedy: v prípade spozorovania indikátorov kompromitácie, alebo anomálii IT / OT systému

Čo: Identifikovať, či sa jedná o udalosť, alebo incident

Prvým krokom je identifikovať, či sa naozaj jedná o bezpečnostný incident. Incident môže zistiť hociktorý používateľ IT / OT, administrátori systému, dodávateľa alebo iné tretie strany, alebo môže vyplývať z informácie automatizovaného bezpečnostného monitoringu.

Identifikácia incidentu	Rýchly checklist
Otázky, ktoré si kladieme	• Kde sa to stalo? • Kto hlásil alebo objavil incident? • Ako to bolo objavené? • Existujú nejaké ďalšie oblasti, ktoré boli incidentom ohrozené? Ak áno, aké sú a kedy boli objavené? • Aký je rozsah dopadu? • Unikli osobné údaje? Koľko? • Aký je dopad na biznis?

Na identifikáciu, či sa jedná o udalosť, alebo o incident, pomôžu indikátory kompromitácie systému (IoC), ktoré môžu byť nasledovné:

- a) zjavné prejavy vírusovej nákazy, prípady fatálnej nedostupnosti služby IS, strata alebo porušenie dôvernosti informácií, podozrenie na kompromitáciu hesla, fyzické narušenie chránených priestorov, krádež nosiča informácií, havária, požiar apod.,
- b) poruchy, zlyhanie služieb informačného systému (napríklad porucha HW, nefunkčnosť IS, výpadok pripojenia do počítačovej siete, výpadok dodávky el. energie apod.),
- c) akékoľvek podozrenia týkajúce sa bezpečnosti IS,
- d) vedomé aj nedbanlivostné porušenia vnútorných predpisov spoločnosti, ktoré môžu spôsobiť zníženie úrovne bezpečnosti osôb, objektov alebo informácií,
- e) akékoľvek pokusy prekonať bezpečnostné opatrenia s cieľom získať neoprávnený prístup k informáciám alebo za účelom vyradiť časť alebo celý informačný systém z prevádzky,
- f) chyby v konfigurácii informačných systémov, ktoré umožňujú prístup k údajom alebo funkcionalitám užívateľom informačného systému nad rámec schválených oprávnení.

Používateľ, ktorý identifikuje bezpečnostný incident, informuje Helpdesk cez self-service portal <https://mhth.xurrent.com/self-service>, príp. emailom na it-servicedesk@mhth.sk.

OT operátor nahlasuje bezpečnostný incident OT manažérovi a MKB, ktorý ho ďalej smeruje na správcu OT systému, ktorý je zaň zodpovedný. Incident je rovnako hlásený cez ITSM nástroj (<https://mhth.4me.com/self-service>).

Nezáleží na forme oznámenia – môže to byť emailom, telefonicky, ústne alebo hlásením z monitorovacieho systému. Upresnenie a záznam zistenia je úlohou a zodpovednosťou Helpdesk, ktorý môže oznamovateľa späťne kontaktovať, aby zistil ďalšie podrobnosti alebo súvislosti.

Na základe získaných informácií a vlastného preverenia situácie určí Helpdesk, či je udalosť bezpečnostným incidentom alebo sa jedná o falošný alarm (false positive).

5.18.12.2 Nahlasovanie na Helpdesk a vytvorenie záznamu o incidente

Vstup: Identifikovaný incident

Výstup: Vytvorenie záznamu o incidente

Kto: Všetci zamestnanci

Kedy: Keď sa usúdi, že môže ísť o kybernetický bezpečnostný incident

Čo: Klasifikovať a vytvoriť záznam o incidente

5.18.12.3 Postup nahlasovania bezpečnostného incidentu:

Každý incident musí byť samostatne zaevidovaný a musia byť zachytené všetky informácie podstatné pre jeho riešenie. Okrem uľahčenia práce riešiteľskému tímu Helpdesku, to je nevyhnutné aj v prípade neskoršej forenznej analýzy incidentu (viď sekcia Zber dôkazov).

Okamžite zabezpečiť informácie o incidente tak, aby s nimi nebolo možné neoprávnene manipulovať, jedná sa predovšetkým o informácie nižšie (pokiaľ sú známe):

Zároveň je nutné záznamy o incidente priebežne dopĺňať spolu s tým, ako prebieha jeho riešenie. Záznam údajov o incidente musí obsahovať:

- Názov a popis služby alebo informácie, ktorá je predmetom incidentu alebo ktorá je narušením ohrozená – názov dotknutého IT / OT aktíva (v popise incidentu),
- Oblasť zasiahnutých aktív (IT / OT, lokality a priestory, ľudské zdroje),
- Prostriedok poskytujúci službu, správca služby, správca prostriedku,
- Zdroj narušenia,
- Cieľ narušenia,
- Účastníci incidentu, ak sú známi,
- Príslušné prevádzkové záznamy (Logy) o narušení,
- Dátum a čas zaznamenania,
- Zadávateľ incidentu, osoba ktorá incident zistila,
- Identifikátor incidentu,
- Vlastník aktíva,
- Kategória incidentu (malware, kompromitácia hesla,...),
- Stupeň naliehavosti incidentu (klasifikácia incidentu),
- Stavový kód incidentu (otvorený, spracovávaný, vyriešený, uzavretý),
- Popis príznakov incidentu,
- Komu bol incident priradený na riešenie,
- Známy typ chyby alebo incidentu, ak sa jedná o opakovaný incident,
- História incidentu – sled činností vykonaných pri riešení incidentu spolu s časom realizácie a osobami, ktoré ich vykonali,
- Dátum a čas vyriešenia,
- Osoba, ktorá potvrdila funkčnosť riešenia,
- Dátum a čas uzavretia incidentu.

Ak bezpečnostný incident narušia pracovnú činnosť a povinnosti zamestnanca, ktorý bezpečnostný incident zistil, je potrebné okamžite informovať aj priameho nadriadeného a bezodkladne informovať MKB.

Pri narušení bezpečnosti objektu / chráneného priestoru je pracovník, ktorý narušenie zistí, povinný toto bezodkladne nahlásiť ako bezpečnostný incident špecialistovi FOB; v prípade nebezpečenstva je potrebné upovedomiť aj strážnu službu objektu, resp. podľa charakteru incidentu inú prítomnú zodpovednú osobu (napr. priameho nadriadeného, osobu zodpovedajúcu za objekt, prítomného člena manažmentu a pod.).

V prípade zrejmej nezákonnej narušenia bezpečnosti (napr. násilné vniknutie) je potrebné bezodkladne volať políciu (v prípade požiaru – požiarnu záchrannú službu a pod.).

Zamestnanec je súčasne povinný, podľa svojich možností, prispieť k okamžitému odstráneniu bezpečnostného incidentu a jeho následkov. Jedná sa predovšetkým o izoláciu zdroja narušenia alebo ohrozenia. Takou izoláciou môže byť odpojenie zariadenia od sietí, odstránenie používateľa alebo počítača z domény, zakázanie prístupu počítača alebo užívateľa k službe alebo službám. Toto je potrebné vykonať podľa možnosti okamžite po zabezpečení informácií o bezpečnostnom incidente, ktoré boli popísané vyššie. Ak je incident takého charakteru, že v jeho priebehu dochádza k významným ekonomickým alebo morálnym stratám spoločnosti, je prvoradou povinnosťou zamestnanca zabrániť týmto stratám.

Zamĺčanie bezpečnostného incidentu je samo o sebe bezpečnostným incidentom.

Tretie strany, najmä prevádzkovatelia základnej alebo poskytovatelia digitálnej služby v zmysle ZoKB č. 69/2018 Z. z. o kybernetickej bezpečnosti v platnom znení a dodávateľa, s ktorými spoločnosť uzatvorila zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ZoBOaNP) nahlasujú kybernetické bezpečnostné incidenty podľa ZoBOaNP.

5.18.12.4 Klasifikácia závažnosti incidentu

Vstup: Zaznamenaný incident s potrebnými informáciami

Výstup: Klasifikácia incidentu podľa závažnosti a dopadu

Kto: IT Helpdesk, IT administrátor, IT/OT špecialista

Kedy: Pri vytvorení záznamu o kybernetickom incidente

Čo: Určenie dôležitosti incidentu, na základe požiadaviek biznisu

Klasifikácia incidentu podľa závažnosti a dopadu	Popis
Kritický incident (Critical incident)	Predstavuje výpadok dôležitého komponentu IT /OT produkčnej infraštruktúry, dátového centra alebo zdieľanej aplikácie/služby. Taktiež zahŕňa incidenty, ktoré predstavujú nedostupnosť základnej služby, príp. zlyhanie kritickej aplikácie alebo systému. Došlo k ohrozeniu zdravia zamestnancov, environmentálnemu hazardu v rámci OT prostredia. Došlo k úniku veľkého objemu osobných údajov (GDPR). Pre tento incident neexistuje žiadny workaround alebo náhrada.
Dôležitý incident (Important incident)	Predstavujú výpadok IT služieb alebo OT riadiacich procesov s dopadom na malú skupinu koncových používateľov, technológií, ktorý môže mať dopad na dodanie základnej služby (vrátane oneskorenia, dostupnosti atď.). Výpadok IT / OT technológie s redundanciou.
Normálny incident (Normal incident)	Ktorý ovplyvňuje jedného koncového používateľa alebo má minimálny dopad na biznis alebo sa jedná o výpadok neprodukčného systému. Prevádzkové incidenty zahŕňajú aj servisné IT požiadavky v rámci definovaného času odozvy.

5.18.12.5 Kategorizácia typu incidentu

Vstup: Klasifikovaný incident s potrebnými informáciami

Výstup: Kategorizácia incidentu podľa závažnosti a dopadu

Kto: IT Helpdesk, IT administrátor, IT/OT špecialista

Kedy: Pri vytvorení záznamu o kybernetickom incidente

Čo: Určenie dôležitosti incidentu, na základe požiadaviek biznisu

Terminológia	Popis
Anomália systému	Neznáme sieťové aktivity ovplyvňujúce / degradujúce výkonnosť IT / OT siete so zvýšeným využitím šírky pásma siete a skráteným časom odozvy, nadmerným výkonom procesorov, zvýšenými podozrivými požiadavkami na sieť alebo zvýšenými výstrahami systému IDS (Intrusion Detection System) alebo systémom prevencie narušenia (IPS), ktoré vedú k zlyhaniu aplikácie. Zahŕňa výpadky v elektronických obvodoch, elektromechanické komponenty počítačového / komunikačného systému alebo poruchu / neschopnosť programu pokračovať v spracovaní v dôsledku nesprávnej logiky.
Fyzická bezpečnosť	Narušenie fyzickej bezpečnosti technických miestností a dátových centier napr. identifikovaný alarmom narušenia, kamerovým systémom alebo systémom prístupových kariet.
Fraud (podvody)	Neoprávnené použitie zdrojov a Phishing Napr. používanie zdrojov pre neautorizované účely, vrátane vytvárania ziskov. Napr. maskovanie sa ako iná entita s cieľom presvedčiť užívateľa, aby previedol finančné prostriedky na vybraný účet, napr. účet dodávateľa.
Neautorizovaná zmena	Akékoľvek neoprávnené zmeny nastavenia IT / OT systému, vložením, úpravou alebo vymazaním. Napríklad zmeny štandardných operačných prostredí, pridanie spustiteľných súborov alebo úprava konfigurácie spustiteľného súboru. Inštalácia neschválených aplikácií a programov. Akúkoľvek neoprávnenú inštaláciu dodatočných zariadení na spracovanie, komunikáciu alebo ukladanie dát v IT / OT sieti. Toto zahŕňa, ale nie je obmedzené na: • sieťové prvky • servery a pracovné stanice • smart telefóny • prenositeľné médiá (USB, externé disky) • bezdrôtové prístupové body.
Neautorizovaný prístup	Neoprávnený prístup z vnútorných a vonkajších zdrojov k informáciám a IT / OT systémom.
Porušenie politík IT/OT bezpečnosti	Akékoľvek porušenie pravidiel bezpečnosti informácií alebo aspektov kódexu týkajúcich sa bezpečnosti informácií.
Prienik do IT / OT siete	Prieniky konkrétne zamerané na vnútornú IT / OT. Toto zahŕňa, ale nie je obmedzené na:

		- odmietnutie služby (DoS) / distribuované odmietnutie služby (DDoS) - prerušenie/zastavenie biznis alebo riadiacich procesov - pokusy o lámanie/zneužitie hesiel - pokusy o zneužitie sieťových a industriálnych komunikačných protokolov - skenovanie a zahlcovanie siete
Strata/krádež zariadenia	IT/OT	Krádež alebo strata akéhokoľvek informačného alebo technologického aktíva / zariadenia (vrátane prenosných a pevných médií), ktoré mohli byť alebo boli použité na spracovanie alebo uchovávanie informácií.
Únik / krádež dát		Krádež alebo strata akýchkoľvek dát vrátane osobných informácií.
Vírusová infekcia		Softvérové programy, ktoré majú spôsobiť poškodenie IT / OT systémov (vírus, ransomware, malware, atď.)
Zneužitie hesiel		Zdieľanie / krádež / strata hesiel alebo iného autentizačného tokenu.
Zneužitie privilégií		Zmeny v nastaveniach používania privilégií na samostatných alebo sieťových zariadeniach vrátane sieťových profilov, miestnych konfiguračných súborov používateľov alebo zariadení, ktoré neboli schválené prostredníctvom procesu riadenia zmeny.

5.18.12.6 Pridelovanie incidentov

Vstup: Klasifikovaný incident s priradenou závažnosťou a kategóriou

Výstup: Incident eskalovaný do vyšších úrovní

Kto: IT Helpdesk, IT administrátor, MKB, IT/OT špecialista, Bezpečnostný tím, Zodpovedná osoba

Kedy: V procese klasifikácie incidentov

Čo: Prideliť incident správnej osobe a úrovni riešenia

Klasifikácia incidentu	Riešiteľ incidentu	Úroveň riešenia	Pridelenie a eskalácia
Kritické incidenty (Critical incidents)	- Administrátor IT - OT špecialista - MKB - Bezpečnostný tím - Vedenie spoločnosti - Zodpovedná osoba za ochranu osobných údajov (DPO)	Level 3	Závažný IT/ OT bezpečnostný incident je riešený na tímovej úrovni zahŕňa viacerých vlastníkov aktív a procesov. V prípade, že sa závažný incident nepodarí vyriešiť do 1 hod., vlastník incidentu eskaluje riešenie a hlási incident nadriadenému. Závažný incident zahŕňa kooperáciu a súčinnosť všetkých dotknutých zamestnancov vrátane manažmentu, ktorý musí byť informovaný o priebehu riešenia.

			V prípade prekročenia kritérií požiadaviek ZoKB, hlási MKB BI na NBÚ. V prípade úniku osobných údajov, zodpovedná osoba DPO (Data Protection Officer) kontaktuje Úrad na ochranu osobných údajov SR a nahlási tento incident.
Dôležité incidenty (Important incident)	• IT Helpdesk • Administrátor IT • OT špecialista • Môže asistovať MKB	Level 2	IT Incident klasifikovaný ako dôležitý sa oznamuje IT Helpdesku, ktorý ho prideli oddeleniu IT. OT Incident klasifikovaný ako dôležitý sa oznamuje OT špecialistovi, ktorý ho následne rieši v spolupráci s oddelením IT. Ak sa administrátorovi IT nepodari stabilizovať IT prostredie alebo komponent v primeranom čase (do 2 hod.), bezpečnostný incident sa považuje za závažný a daný administrátor IT je povinný to okamžite nahlásiť manažérovi IT a podľa potreby MKB, prípadne Bezpečnostnému tímu. Ak sa IT/OT špecialistovi nepodari stabilizovať prostredie alebo komponent v primeranom čase (do 2 hod), bezpečnostný incident sa považuje za závažný a daný špecialista je povinný to okamžite nahlásiť príslušnému manažérovi, výrobnému manažérovi a podľa potreby MKB, prípadne Bezpečnostnému tímu.
Normálny incident (Normal incident)	• IT Helpdesk • OT špecialista	Level 1	Prevádzkový (bežný) incident súvisiaci s výpočtovou technikou oznamujú zamestnanci IT Helpdesku a IT/OT špecialistovi. Všetky ostatné incidenty nesúvisiace s výpočtovou technikou sú zamestnanci povinní hlásiť svojmu nadriadenému.

5.18.12.7 RIEŠENIE A ANALÝZA INCIDENTU

Krok 2: Detailná analýza incidentu (Root Cause Analysis)

Vstup: Incident je klasifikovaný, priradený na analýzu

Výstup: Skúmanie dôkazov, analýza hlavnej príčiny incidentu

Kto: IT administrátor, MKB, IT/OT špecialista, Bezpečnostný tím

Kedy: Keď je jasné, že sa jedná o kybernetický incident

Čo: Vytvoriť záznam o incidente

Pridelený incident je potrebné zanalyzovať, aby sa našlo vhodné riešenie a aby sa prípadne zabránilo jeho výskytu v budúcnosti. Ak je k dispozícii databáza minulých incidentov, mala by sa prehľadať, či neobsahuje známe riešenie. V prípade potreby môže riešiteľ upraviť klasifikáciu alebo kategorizáciu bezpečnostného incidentu.

Analyzovanie incidentu zahŕňa nasledujúce činnosti:

Postup analýzy incidentu	Popis akcie
Kedy sa to stalo?	• Zistenie presného časového poradia udalostí, ktoré predchádzali incidentu • Identifikáciu činností alebo udalostí, ktoré mohli byť priamou príčinou incidentu • Preskúmanie iných špecifických súvislostí (korelácie), aby boli zistené okolnosti vedúce ku vzniku incidentu napr. fyzická bezpečnosť
Čo sa stalo?	• Presné ohraničenie incidentu – či unikli osobné údaje a koľko toho uniklo • Skúma sa, či postup riešenia nie je zahrnutý v existujúcej databáze incidentov, pracovných postupoch alebo iných zdokladovaných riešeniach. Ak takýto postup riešenia existuje, použije sa na vyriešenie incidentu. • Identifikácia vstupného vektora útoku, ktorým smerom prišla nákaza • Aké kroky podniknúť, aby sa malware ďalej nešíril (patchovanie, blokovanie portov na Firewallle) • Analýza záznamov a logov z bezpečnostného monitoringu (SIEM, syslog) • Analýza monitoringu kapacít, akú šírku pásma spotreboval malware, cez ktoré komunikačné kanály a porty sa šíri DDoS útok, atď.
Aký je dopad?	• Analýza, ktoré prevádzky OT nefungujú a aká časť organizácie je postihnutá, ktoré ďalšie systémy sú ovplyvnené alebo ohrozené • V prípade OT prostredia, analýza prerušenia a výpadku priemyselných procesov alebo strata kontroly nad procesmi • Analýza, aké služby sú ohrozené a aká veľká je škála výpadku • Určenie zdrojov a prostriedkov potrebných na obnovu systému

5.18.12.8 Hierarchická eskalácia

Vstup: Eskalácia na riešiteľov vyšších úrovní

Výstup: Rozhodnutie na základe eskalácie

Kto: IT administrátor, MKB, IT/OT špecialista, Bezpečnostný tím

Kedy: V procese eskalácie incidentov

Čo: Eskalovať incident a informovať zodpovedných pracovníkov

V prípade incidentov so Závažnou až Kritickou klasifikáciou je nutné informovať o incidente nadriadených a vedenie spoločnosti. Mnohé situácie si vyžadujú zásah vedenia spoločnosti.

Vedenie spoločnosti sa tak na základe včasných informácií môže pripraviť na vyplývajúce komplikácie a vykonať nutné opatrenia. Taktiež môže v záujme urýchleného vyriešenia incidentu zasiahnuť do procesu riešenia a schváliť priradenie zdrojov, s ktorými sa pôvodne nerátalo.

5.18.12.9 Porušenia ochrany osobných údajov v rámci nariadenia GDPR

Vstup: Eskalácia na riešiteľov vyšších úrovní

Výstup: Rozhodnutie na základe eskalácie

Kto: Zodpovedná osoba (DPO)

Kedy: V procese eskalácie incidentov

Čo: Eskalovať incident a informovať zodpovedných pracovníkov a Úrad na ochranu osobných údajov Slovenskej republiky (ďalej len „úrad“)

Podľa nariadenia GDPR (ďalej len „nariadenie“) porušením ochrany osobných údajov je porušenie bezpečnosti, ktoré vedie k:

- náhodnému alebo nezákonnému zničeniu prenášaných, uchovávaných osobných údajov (osobné údaje už neexistujú),
- strate prenášaných, uchovávaných osobných údajov (osobné údaje existujú, ale sa nad nimi stratila kontrola, alebo k nim stratil prístup),
- zmene prenášaných, uchovávaných osobných údajov (osobné údaje boli poškodené, pozmenené, nie sú úplné),
- neoprávnenému prístupu prenášaných, uchovávaných osobných údajov (k osobným údajom sa dostala tretia osoba, ktorá nie je oprávnená ich spracúvať), alebo
- neoprávnenému poskytnutiu prenášaných, uchovávaných osobných údajov (osobné údaje boli poskytnuté tretej osobe, ktorá nie je oprávnená ich spracúvať).

V prípade porušenia ochrany osobných údajov je potrebné postupovať podľa článku 33 nariadenia alebo § 40 zákona o ochrane osobných údajov a tento incident oznámiť v zákonných lehotách úradu alebo prevádzkovateľovi, ak MHTH spracúva osobné údaje ako sprostredkovateľ v mene iného prevádzkovateľa.

Proces nahlásovania bezpečnostného incidentu úradu, je popísaný na konci tohto dokumentu.

Klasifikácia incidentu	Riešiteľ incidentu	Eskalácia smerovaná na:	Popis eskalácie
Kritické incidenty (Critical incident)	• Administrátor IT • OT špecialista • MKB • Bezpečnostný tím • Zodpovedná osoba za ochranu osobných údajov (DPO)	• Vedenie spoločnosti • IT manažment • Úrad na ochranu osobných údajov SR	• je potrebné prizvať externých konzultantov alebo tretie strany z dôvodu analýzy a vyšetrenia hlavnej príčiny incidentu, prípadne foréznej analýzy • je potrebné komunikovať s dotknutými osobami • majú byť kontaktované orgány činné v trestnom konaní, Úrad na

ochranu osobných údajov SR, Národný bezpečnostný úrad

- hlásenia úniku osobných údajov Úradu na ochranu osobných údajov SR
- oznámenie o porušení ochrany osobných údajov inému prevádzkovateľovi, ak MHTH koná v postavení sprostredkovateľa

5.18.12.10 Proces nahlasovania incidentu pri porušení ochrany osobných údajov

MHTH spracúva osobné údaje vo vlastnom mene, musí porušenie ochrany osobných údajov oznámiť úradu bez zbytočného odkladu a podľa možnosti do 72 hodín po tom, čo sa o tejto skutočnosti dozvedel.

V prípade, že MHTH spracúva v postavení sprostredkovateľa osobné údaje v mene iného prevádzkovateľa, v takom prípade MHTH podá prevádzkovateľovi oznámenie bez zbytočného odkladu po tom, čo sa o porušení ochrany osobných údajov dozvedel.

Určenie momentu, kedy je nutné nahlásiť incident môže byť v praxi problematické. Týmto momentom treba rozumieť situáciu, keď nadobudneme vysoký stupeň istoty, že došlo k bezpečnostnému incidentu spôsobujúcemu zásah do osobných údajov. Napríklad to môže byť vtedy, ak sa potvrdí prienik útočníka do siete a následne sa zistí, že týmto konaním bolo zasiahnuté do uchovávaných osobných údajov.

Jedinou výnimkou, kedy si prevádzkovateľ nemusí oznamovaciu povinnosť splniť je prípad, keď nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby. Nutnosť podať oznámenie posudzuje v každom prípade zodpovedná osoba (DPO).

5.18.12.11 Oznámenie adresované úradu musí podľa nariadenia obsahovať tieto náležitosti:

- opis povahy porušenia ochrany osobných údajov vrátane, ak je to možné, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch,
- kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,
- opis pravdepodobných následkov porušenia ochrany osobných údajov,
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.

Formulár pre nahlasovanie bezpečnostných incidentov pri porušení ochrany osobných údajov je na adrese:

<https://schranka.slovensko.sk/FormConstructor/Default.aspx?IdService=434885>

5.18.12.12 Neutralizácia a izolácia incidentu

Vstup: Závažnosť incidentu

Výstup: Izolácia a neutralizácia problematického alebo kompromitovaného aktíva na základe závažnosti

Kto: IT administrátor, IT/OT špecialista, Bezpečnostný tím

Kedy: Keď je identifikované, že incident by mohol mať rozsiahly dopad na IT / OT infraštruktúru

Čo: Izolovať a neutralizovať kompromitovaný IT / OT komponent od zbytku siete

Hlavným účelom tejto fázy je obmedzenie poškodenia a zabránenie ďalšiemu poškodeniu IT / OT aktív alebo infraštruktúry.

Izolácia kompromitovaných systémov sa skladá z nasledovných krokov:

Postup pri neutralizácii a izolácii kompromitovaného systému	
Prvý krok (Short-term containment)	Prvým krokom je eliminácia okamžitých škôd spôsobených napríklad malvérom a krátkodobé obmedzenie prístupu ku zdrojom, vo forme izolácie od siete segmentu infikovaných pracovných staníc alebo serverov, ktoré boli napadnuté. Ak je to možné, kompromitovaný systém nevypínať od elektrickej energie, aby neznehodnotil dôkazový materiál. V tejto fáze je všetka prevádzka presmerovaná na záložné servery. Krátkodobé obmedzenie zdrojov nemá byť dlhodobé riešenie problému; je určená len na dočasnú izoláciu incidentu aby nedošlo k väčším škodám.
Druhý krok (Forensic analysis)	Druhým krokom je zálohovanie kompromitovaného systému; pred vypnutím napadnutého systému je nutné vytvoriť image harddisku na bitovej úrovni pomocou forenzných nástrojov, ako napríklad forenzná sada nástrojov (FTK), EnCase a pod. Dôvodom je to, že forenzný softvér zazálohuje postihnutý systém (systémy) tak, ako boli počas incidentu v originálnom stave čím sa uchovávajú dôkazy v prípade, že incident sa transformoval do trestného činu, prípadne spôsobil ohrozenie zdravia osôb v OT.
Tretí krok (Long-term containment)	Posledným krokom je dlhodobá izolácia, čo je v podstate krok, kde sú postihnuté systémy trvalo odpojené od siete a sú kompletne reінštalované z dôvodu kompromitácie útokom. Primárne zameranie v tomto kroku je bezpečné formátovanie (aspoň 16x), tak aby sa odstránili zadné vrátka (backdoor), ktoré zanechali útočníci na postihnutých systémoch. Následne inštalácia bezpečnostných záplat na ďalších postihnutých a susedných systémoch a vykonanie bezpečnostných opatrení na obmedzenie akýchkoľvek ďalších eskalácií incidentu.

Príklad izolácie systému:

Odpojenie postihnutých systémov buď odpojením sieťového UTP kábla od siete alebo vypnutie napájania prepínačov a / alebo smerovačov na časti siete. Izolovať ohrozené systémy od tých, ktoré neboli ohrozené. Izolovať problém od zvyšku výrobnjej siete OT a obmedziť šírenie akéhokoľvek malware alebo znížiť riziko ďalších útokov.

Izolácia systémov	Rýchly checklist
Otázky, ktoré si kladieme:	• Môže byť napadnutý systém izolovaný? • Ak áno, pokračujte s izolovaním postihnutých systémov. • Ak nie, potom pracujte s vlastníkami a / alebo manažérmi systému a zistite ďalšie opatrenia potrebné na vyriešenie problému. • Sú všetky postihnuté systémy izolované od neovplyvnených systémov? • Ak áno, pokračujte ďalším krokom. • Ak nie, pokračujte v izolácii postihnutých systémov, aby sa zabránilo ďalším incidentom

5.18.12.13 Zber dôkazov a evidencie

Vstup: Neutralizácia a Izolácia systému

Výstup: Zber dôkazov a evidencie

Kto: Externý forenzný expert, IT administrátor, MKB, Bezpečnostný tím

Kedy: Keď sa jedná o závažný a kritický incident

Čo: Zozbierať dôkazy o incidente

Pre efektívne riešenie incidentu je kľúčové získať hneď na začiatku čo najviac informácií o prejavoch incidentu. Na ich základe je prípadne možné využiť existujúcu databázu znalostí alebo pripravené modelové riešenia a incident vyriešiť na mieste, vrátane odsúhlasenia riešenia priamo s nahlásujúcim.

Používateľ IT/OT nesmie samostatne vyvíjať akékoľvek aktivity, ktorými by sa pokúsil vyriešiť vzniknutý bezpečnostný incident a to z dôvodu znehodnotenia dôkazovej evidencie (tzv. chain of custody) okrem prípadov, keď musí vykonať kroky vedúce k minimalizácii ďalších škôd na majetku alebo zraneniu osôb v prípade živeľnej pohromy.

Pre identifikáciu, zber, získavanie a uchovávanie dôkazov pri riešení bezpečnostných incidentov sú stanovené postupy a princípy, ktoré zaručia možnosť použitia dôkazu v sporových konaniach podľa platnej legislatívy (trestnoprávne, pracovnoprávne, občianskoprávne, obchodnoprávne spory) v prípadoch, kde je pravdepodobné, že k takým sporom dôjde.

Zoznam dôkazového materiálu môže byť:

1. Logy a správy v IT / OT systémoch
2. Papierová dokumentácia
3. Screenshoty obrazoviek
4. Fotografie
5. Pamäťové záznamy a dumpy
6. Kópia hardisk image

Pravidlá týkajúce sa dôkazového materiálu vo všeobecnosti zahŕňajú:

- A. prípustnosť dôkazov: či dôkazy môžu byť použité na súde alebo nie;
- B. závažnosť dôkazov: kvalita a úplnosť dôkazov;

Aby sa dosiahla prípustnosť dôkazov, vyšetrovateľ incidentu musí zabezpečiť, aby ich informačné systémy boli v súlade s akýmkoľvek uverejneným štandardom alebo kódexom postupov pre tvorbu prípustných dôkazov.

Aby sa dosiahla vysoká dôveryhodnosť dôkazov o incidente, kvalita a úplnosť postupov používaných na zber a dôsledné ochraňovanie dôkazov, je absolútne nevyhnutné. Je nutné zabezpečiť dôkazy o incidente, ktoré budú získavané, tieto musia byť bezpečne uložené a spracované. A to za týchto podmienok:

- a) papierové dokumenty: originál je zabezpečený a je vedený záznamom o osobe, ktorá našla dokument, kde bol dokument nájdený a kto bol svedkom tohto objavu;
- b) vyšetrowanie by malo zabezpečiť, že originály nebudú manipulované;
- c) informácie o počítačových médiách: zrkadlové obrazy, snapshoty alebo kópie akýchkoľvek vymeniteľných médií, musia byť zabezpečené a informácie o pevných diskoch alebo pamäťových médiách musia byť dostupné;
- d) zoznam všetkých činností počas procesu kopírovania musí byť registrovaný a zachovaný;
- e) akékoľvek forenzné práce sa musia vykonávať len na kópiách dôkazného materiálu. Mala by sa chrániť celistvosť všetkých dôkazných materiálov;
- f) kopírovanie dôkazných materiálov musí byť zaznamenávané pod dohľadom dôveryhodného personálu (MKB) a informácie o tom, min. kedy a kde bol proces kopírovania vykonaný, kto vykonal kopírovacie činnosti a ktoré nástroje a programy boli použité.

5.18.12.14 OBNOVA

Obnova kompromitovaných alebo poškodených systémov

Vstup: Incident eliminovaný, situácia je stabilizovaná

Výstup: Obnova kompromitovaných systémov

Kto: IT/OT administrátor, Bezpečnostný tím

Kedy: Keď došlo k napadnutiu systémov útočníkom alebo zákerným kódom

Čo: Obnova systémov zo záloh

Účelom tejto fázy je priviesť postihnuté systémy späť do pôvodného a stabilného prostredia opatrne, aby sa zabezpečilo, že to nepovedie k inému incidentu. Je nevyhnutné testovať, monitorovať a verifikovať systémy, ktoré sa vrátia do pôvodného stavu, aby sa overilo, či nie sú znova napadnuté škodlivým softvérom alebo napadnuté inými prostriedkami. Niektoré dôležité rozhodnutia počas tejto fázy sú:

- Čas a dátum obnovenia priemyselných procesov a biznis operácií - je nevyhnutné, aby prevádzkovatelia / vlastníci systému vytvorili konečné rozhodnutie, kedy bude obnovený systém vrátený do prevádzky
- Ako testovať a overiť, či sú kompromitované systémy čisté a plne funkčné
- Trvanie monitorovania, ktoré sa má dodržiavať pri abnormálnom správaní po incidente
- Nástroje na testovanie, monitorovanie a overovanie správania systému

Obnova systémov	Rýchly checklist
Otázky, ktoré si kladieme:	• Existuje záloha kompromitovaného systému? • Ak áno, aké staré sú dáta? • Ak nie, inštalujeme systém nanovo • Sme si istí, že zálohované dáta nie sú napadnuté zákerným kódom? • Kedy by bolo možné obnoviť postihnuté systémy späť do funkčného stavu? • Aké nástroje použijeme na testovanie, monitorovanie a overenie toho, či sú systémy správne a nie sú

5.18.12.15 PONAUCENIE

Ponaučenie z kybernetických incidentov

Vstup: Kompromitovaný systém bol obnovený a uvedený späť do prevádzky

Výstup: Ponaučenie pre všetky ovplyvnené strany incidentom a implementácia bezpečnostných opatrení

Kto: IT administrátor, IT/OT Špecialista, Bezpečnostný tím, vedenie spoločnosti

Kedy: Po vyriešení incidentu

Čo: Zlepšenie technických opatrení, preškolenie personálu, zlepšenie politik a postupov

Účelom tejto fázy je dopracovať akúkoľvek dokumentáciu, ktorá nebola vykonaná počas incidentu, ako aj akúkoľvek ďalšiu dokumentáciu, ktorá môže byť prínosom pre budúce incidenty. Dokument by mal byť tiež napísaný vo forme správy, ktorá by poskytla prehľad o priebehu incidentu.

Príklad správy, ktorá by mala zhrňať nasledujúce informácie:

- 1) Kedy bol incident zistený a kým;
- 2) Rozsah a dopad incidentu na biznis;
- 3) Ako bol incident riešený a odstránený;
- 4) Aké aktivity boli vykonané počas obnovy systémov;
- 5) Oblasti, kde boli tímy efektívne;
- 6) Oblasti, kde boli tímy neefektívne a potrebujú zlepšenie.

5.19 RIADENIE ZRANITEĽNOSTÍ A PATCH MANAŽMENT

5.19.1 ZÁVÄZNÉ RÁMCE, REGULAČNÉ OPATRENIA A INTERNÉ PRAVIDLÁ

PLÁN SKENOV ZRANITEĽNOSTI

Plán skenov zraniteľností pre jednotlivé roky pripravuje oddelenie kybernetickej bezpečnosti.

Skeny jednotlivých systémov sa vykonávajú periodicky v pravidelných definovaných cykloch v IT prostredí. V OT prostredí sú skeny realizované manuálne plánovaným a riadeným procesom.

Zariadenia	Minimálny počet skenov mesačne
Servery	2 krát
Pracovné stanice	2 krát
Aktívne sieťové prvky (roure, switche, FW,..)	2 krát

Mimo plánovaných testov sa musia vykonať testy aj po zásadných zmenách konfigurácie systémov alebo prostredia. Oddelenie IT a OT má povinnosť bezodkladne informovať o zmenách oddelenie KB. Pri Implementácii nových projektov musia byť všetky servery a novovzniknutá infraštruktúra otestované na potenciálne zraniteľnosti.

Prístup k reportom skenov zraniteľností majú:

- Oddelenie bezpečnosti a krízového riadenia;
- Aplikační vlastníci;

- Vlastníci systému;
- Systémoví administrátori;
- Vlastníci HW;
- Audit IT/OT.

5.19.2 ÚLOHY A ZODPOVEDNOSTI

Manažment zraniteľností definuje nasledovné role identifikované v rámci spoločnosti:

- **Špecialista kybernetickej bezpečnosti zodpovedá za:**
 - konfiguráciu skenovacieho nástroja plánuje,
 - konfiguráciu a výkon testov zraniteľností,
 - riadenie procesu odstraňovania zraniteľností,
 - riadenie plánu sanácie (Remediation Plan).
 - prípravu ročného plánu skenovania zraniteľností,
 - notifikáciu dotknutých osôb o čase, kedy sa budú skeny vykonávať.
 - vyhodnocovanie skenov zraniteľnosti.
- **Špecialista KB:**
 - je poverený správou aplikácie IDR/SIEM.
 - zabezpečuje súčinnosť IDR/SIEM scenárov pri vykonávaní testov zraniteľností.
- **Aplikačný (business) vlastník zodpovedá za:**
 - nastavenie aplikácie z pohľadu aplikačnej funkcionality.
- **Vlastník systémovej oblasti IS zodpovedá za:**
 - prevádzku systému
 - realizáciu opatrení stanovených v dôsledku zistených zraniteľností (patch management).
- **Vlastník aplikačnej oblasti IS zodpovedá za:**
 - plynulý chod aplikácie z pohľadu systémových komponentov (DB, systémy, služby,...).
- **Risk Analysis Team (RAT):**
špecializovaná medziodborová pracovná skupina s názvom „Tím analýzy KB rizika“:
 - hodnotí úroveň rizika,
 - navrhuje riziká na akceptáciu na stretnutiach Porady vedenia.

5.19.3 PROCES RIADENIA ZRANITEĽNOSTÍ

Cyklus procesu riadenia zraniteľností pozostáva z nasledujúcich fáz:

- a) Prípravná fáza
- b) Sken zraniteľností
- c) Plán sanácie a vykonávanie sanácie (tzv. Remediation Plan)
- d) Opakovaná kontrola stavu zraniteľností.

5.19.4 PRÍPRAVNÁ FÁZA

Hlavnou aktivitou tejto fázy je príprava ročného plánu skenovania, v ktorom je uvedené, aké systémy a kedy budú skenované. Tento plán pripravuje poverený špecialista KB a musí byť pripravený do 31.1. daného roku. Na základe tohto plánu sa v aplikácii na sledovanie zraniteľností naplňujú a nakonfigurujú skeny.

Plán je možné počas roku meniť podľa potrieb.

Aplikační (business) vlastníci, vlastník systémovej oblasti IS a vlastník aplikačnej oblasti IS, musia byť minimálne 7 dní pred vykonaním skenu notifikovaní formou pripomienky v ich firemnom kalendári. Počas tejto doby je možné odmietnuť naplánovanú úlohu a navrhnúť alternatívny dátum, kedy bude možné skeny vykonať. Účastník, ktorý vzniesol námietku, je povinný uviesť dôvod a navrhnúť nový termín. V prípade, že dotknuté strany sa do času vykonania skenu nevyjadria, termín skenu sa považuje automaticky za akceptovaný.

5.19.5 SKEN ZRANITEĽNOSTÍ

- Skenovanie sa vykonáva automaticky v čase, v akom bol naplánovaný.
- Akékoľvek problémy, ktoré sa vyskytnú počas, ako aj v čase po ukončení skenov, ako napríklad nedostupnosť systémov, služieb, alebo zlé odozvy aplikácií, musia byť nahlásené a špecialistom KB zaznamenané v samostatnom zozname.

V prípade, že sken spôsobil nedostupnosť, alebo obmedzenie funkčnosti systému, alebo služby, pri opätovnom skene, špecialista KB musí túto skutočnosť spomenúť pri notifikácii o plánovanom skene a upozorniť na túto skutočnosť dotknuté strany.

Tiež musí túto skutočnosť zohľadniť pri plánovaní skenov a nastaviť skeny tak, aby sa minimalizovalo riziko výpadku systému, alebo služby.

Výstupom z testovania je protokol o zistených zraniteľnostiach, na základe ktorého sa vyhotoví sanačný plán.

5.19.6 PLÁN SANÁCIE A VYKONÁVANIE SANÁCIE

Sanačný plán pripravuje oddelenie KB. Tento plán obsahuje zoznam zraniteľností, ktoré je nutné odstrániť, dátum, do ktorého treba zraniteľnosť odstrániť a navrhované riešenia na odstránenie zraniteľností.

Aplikační vlastníci, systémoví vlastníci a systémoví administrátori majú prístup k výsledkom skenov, aby si mohli pozrieť výsledky pre systémy, za ktoré sú zodpovední.

Plánované nápravné opatrenia musia byť vykonané v časovom rámci 30 dní od zaslania výsledkov testov. Zodpovední vlastníci informačných systémov sú povinní informovať oddelenie bezpečnosti a krízového riadenia o vykonaní sanačného plánu. Pre daný systém túto informáciu zaznamenávajú do samostatného súboru *plánu remediácie, alebo priamo do ticketu ITSM nástroja*. Pri aplikovaní sanačných aktivít je potrebné zvážiť možné závislosti na aplikačných úrovniach a spätnej kompatibilitate celého prostredia s ohľadom na funkčnosť samotných systémov.

V prípade, ak danú zraniteľnosť do uvedeného dátumu nie je možné odstrániť, musí aplikačný vlastník túto skutočnosť komunikovať so špecialistom oddelenia bezpečnosti a krízového riadenia povereným tvorbou sanačného plánu a určiť nový termín na odstránenie rizika, navrhnúť náhradné riešenie, alebo zdôvodniť, prečo nápravné opatrenie nie je možné vykonať.

5.19.7 OPAKOVANÁ KONTROLA STAVU ZRANITEĽNOSTÍ

Po vykonaní sanácie musí byť spolu so špecialistom KB naplánované overenie, ktorého cieľom je zistiť, či aktivity vykonané na odstránenie zraniteľností boli úspešné, alebo nie. Tento test sa musí vykonať do 7 dní od vykonania nápravných opatrení, najneskôr však po uplynutí doby 30 dní – času na vykonanie sanačného plánu. Overovací test sa musí vykonať pomocou rovnakej techniky s rovnakým nastavením konfigurácie ako pri počiatkovej kontrole. Pri overovaní teste musia byť splnené rovnaké formálne kroky ako pri počiatkovom testovaní.

Vlastníci aktív budú informovaní, či sanácia bola účinná alebo reziduálne riziko zostáva.

5.19.8 VYHODNOTENIE PROCESU RIADENIA ZRANITEĽNOSTÍ

Po ukončení cyklu testovania informačného systému na jeho zraniteľnosti, musia byť výsledky analyzované a riziká z toho vyplývajúce musia byť ohodnotené a zaznamenané do katalógu rizík.

5.19.9 RACI MATICA ROLÍ A ZODPOVEDNOSTÍ

R - Zodpovedný za vykonanie A - Zodpovedný za úlohu C - Konzultované s kým? I – Informovaný (kto)?		Vlastník Aplikácie	Správca aplikácie	Správca systému	Špecialista KB	MKB	CIO
Prípravná fáza	Definovanie rozsahu testovania (VA plán)				R	A	I
	Definovanie času testovania (VA plán)				R	A	I
	Upozornenie všetkých dotknutých strán o čase a rozsahu testovania	I	I	I	R	A	
Sken zraniteľností	Spustenie skenu zraniteľností	I	I	I	R	A	
	Monitorovanie stability a výkonu systémov počas doby skenovania	R	R	R	I	A	
	Komunikácia ohľadom vzniknutých problémov počas skenovania	C	R	R	C	A	
	Analýza zistených zraniteľností	I	I	I	R	A	I
Vykonávanie sanácie	Plán sanácie	I	I	I	R	A	I
	Vykonávanie sanačných opatrení	C	R	R	C	A	
	Upozornenie na vykonanie sanačných opatrení	C	R	R	I	A	
Opakovaná kontrola	Upozornenie všetkých dotknutých strán o čase, v ktorom bude vykonaný opakovaný sken	I	I	I	R	A	
	Spustenie opakovaného skenu zraniteľností				R	A	
	Analýza a porovnanie výsledkov s prvým skenom	I	I	I	R	A	I
Posúdenie a akceptácia rizika	Analýza a ohodnotenie rizika	RAT					
	Formálne akceptovanie rizika	CEO					

5.19.10 PATCH MANAŽMENT PROCES

Hlavným cieľom procesu Patch manažment je zabezpečiť bezpečné a konzistentné nasadzovanie potrebných SW opráv (patchov) na ICT a ICS zariadenia spoločnosti, tiež:

- Identifikovanie SW záplat / patchov;
- Evidenciu SW záplat / patchov;
- Zvolenie vhodného prístupu pre otestovanie SW záplat / patchov a vyhodnotenie testu;
- Zabezpečenie implementácie SW záplat / patchov;
- Vyhodnotenie implementácie SW záplat / patchov.

Patch manažment - príprava a nasadenie záplat (vo forme bezpečnostných balíkov, alebo vydání) do prevádzky alebo do prípravného (testovacieho) prostredia. Cieľom je zabezpečiť:

- minimalizovať bezpečnostné riziko organizácie prostredníctvom včasného a efektívneho riadenia bezpečnostných záplat
- stanoviť jasné zodpovednosti a vlastníctvo v procese riadenia patch manažmentu
- zabezpečiť viditeľnosť a kontrolu nad všetkými aktualizáciami procesmi
- odstránenie známych zraniteľností ako i funkčných nedostatkov,
- zníženie počtu bezpečnostných, ale i prevádzkových incidentov a nežiadúcich stavov,
- nasadenie záplaty na „prvý pokus“ a bez chýb,

- plánovanie a nasadenie záplat,
- overenie vydania záplat pred nasadením a identifikáciu rizík nasadenia a opatrení na ich eliminovanie,
- ochranu prevádzkového prostredia pred neriadenými záplatami, ktoré môžu narušiť chod IT a OT systémov,

IT/OT manažér je na základe odporúčaní tímu KB, zodpovedný za definovanú oblasť IS a v procese patch manažment zodpovedný za:

- kontrolu dostupnosti nových patchov;
- naplánovanie nasadzovania patchu;
- nasadenie patchu;
- v prípade neúspešného nasadenia patchu, vytvorenie incidentu a zabezpečenie nápravy v ITSM.

Security záplaty (patche) sa aplikujú bezodkladne.

Špecialista/administrátor úseku informačných systémov je zodpovedný za:

- pravidelné sledovanie nových bezpečnostných záplat konkrétnym výrobcom IT, príp. OT systému,
- zabezpečuje inštaláciu týchto záplat pre IT a OT prostredie podľa potreby aj v súčinnosti s dodávateľmi. (Pre OT prostredie je implementácia plne v kompetencii príslušného OT manažéra),
- navrátenie IT/OT systému do pôvodného stavu,
- deinštaláciu záplaty (roll back plán) v prípade, že inštalácia bezpečnostnej záplaty zlyhá.

Špecialista/administrátor úseku informačných systémov v súčinnosti s dodávateľmi IT/OT systémov je zodpovedný za:

- inštaláciu bezpečnostných záplat, vrátane aplikačných záplat (knižnice a podporné programy).
- implementáciu doplnkových opatrení a analýzu dopadov a rizík v súvislosti s aplikovaním záplat v IT/OT prostredí.

Riadenie záplat musí byť súčasťou procesu riadenia zraniteľností, za účelom zvyšovania kybernetickej bezpečnosti prostredníctvom inštalácie záplat, nazývaných aj aktualizácie softvéru, aktualizácie firmvéru, balíky Service Pack, rýchle opravy, aktualizácie systému BIOS (Basic Input Output System) a ďalšie aktualizácie digitálnych elektronických programov, ktoré riešia chyby, funkčnosť, spoľahlivosť a zraniteľnosti v oblasti kybernetickej bezpečnosti.

Proces riadenia záplat zahŕňa inštaláciu záplat:

- Testovanie záplat v pred produkčnom (testovacím) prostredí,
- Zabezpečenie aktivít procesu a riadenie záplat podľa ich typu v produkčnom prostredí
- Kritické záplaty (critical updates): inštalujú sa okamžite, čo najskôr, ako to situácia dovoľí (napr. patch proti ransomware, Zero Day),
- Vydanie nových definícií (definition updates): špecifikuje vírusové a iné aktualizácie,
- Bezpečnostné záplaty (security updates): určujú všeobecne vydanú aktualizáciu pre problém súvisiaci so zabezpečením pre špecifický produkt,
- Balíky service packs: určujú kumulatívnu množinu rýchlych opráv, ktoré sa použijú v aplikáciách a systémoch. Tieto opravy môžu zahŕňať: aktualizácie zabezpečenia, kritické aktualizácie, aktualizácie softvéru, atď.
- Aktualizácie (updates): určujú aktualizáciu aktuálne nainštalovanej aplikácie alebo súboru,

5.19.11 PROCES KLASIFIKÁCIA A PRIORITIZÁCIA ZRANITEĽNOSTÍ

CVSS Skóre

- Kritické (CVSS 9.0-10.0): Ihneď hroziaca exploitácia, vysoký dopad
- Vysoké (CVSS 7.0-8.9): Značný bezpečnostný vplyv, vysoká pravdepodobnosť zneužitia
- Stredné (CVSS 4.0-6.9): Umiernenosť, vyžaduje špecifické podmienky
- Nízke (CVSS 0.1-3.9): Minimálny priamy bezpečnostný vplyv

5.19.11.1 Stupne kritičnosti systému

- **Kritičnosť 1 - Kritická:**

Charakteristika:

Systém je nevyhnutný pre bezpečnosť, kontinuitu prevádzky alebo ochranu života a zdravia.

Výpadok alebo kompromitácia môže viesť k:

ohrozeniu života a zdravia,
environmentálnym škodám,
porušeniu legislatívnych povinností.
Neustála dostupnosť je nevyhnutná.

Príklady:

SCADA / PLC systémy priamo riadiace výrobu
Bezpečnostné systémy
Autentifikačné systémy
Kritická infraštruktúra podľa NIS2

Dopad zlyhania:

Neakceptovateľný, vyžaduje okamžité krízové riadenie.

- **Kritičnosť 2 - Vysoká:**

Charakteristika:

Systém je nevyhnutný pre hlavné obchodné alebo technologické procesy.
Výpadok spôsobí významné finančné straty alebo prevádzkové riziká.
Spracúva citlivé alebo osobné údaje.

Príklady:

Produkčné databázové systémy
Autentifikačné a autorizačné systémy
Riadiace OT systémy s nepriamym dopadom na výrobu

Dopad zlyhania:

Závažné narušenie prevádzky, vyžaduje okamžitú reakciu

- **Kritičnosť 3 - Stredná:**

Charakteristika:

Podporný systém pre hlavné procesy.
Krátkodobý výpadok je akceptovateľný, ale ovplyvňuje efektivitu práce.

Môže spracúvať interné alebo mierne citlivé údaje.

Príklady:

Súborové servery

ERP podporné moduly

Monitorovacie OT systémy bez priameho riadenia procesu

Dopad zlyhania:

Obmedzenie prevádzky, nutnosť nápravných opatrení.

• **Kritičnosť 4 - Nízka:**

Charakteristika:

Systém nemá priamy vplyv na kľúčové procesy organizácie.

Výpadok nespôsobí významné prevádzkové ani finančné škody.

Neobsahuje citlivé ani regulované údaje.

Príklady:

Testovacie a vývojové systémy

Interné informačné portály

Neprodukčné OT zariadenia

Dopad zlyhania:

Minimálny, tolerovateľný bez okamžitého zásahu.

Kritickosť systému	Kritické (CVSS 9.0–10.0)	Vysoké (CVSS 7.0–8.9)	Stredné (CVSS 4.0–6.9)	Nízke (CVSS 0.1–3.9)
Kritická	Bezodkladne, do 72 hodín	Do 7 dní	Do 30 dní	Do 90 dní
Vysoká	Do 72 hodín	Do 14 dní	Do 60 dní	Do 120 dní
Stredná	Do 7 dní	Do 30 dní	Do 90 dní	Do 180 dní
Nízka	Do 14 dní	Do 60 dní	Do 180 dní	Podľa harmonogramu / voliteľné

5.19.11.2 Doplnujúce pravidlá

1. **Zero-Day a aktívne zneužívané zraniteľnosti** musia byť riešené okamžite bez ohľadu na CVSS skóre alebo kritickosť systému.
2. **OT systémy** môžu vyžadovať plánované údržbové okná; v takom prípade sa uplatňujú **kompensačné opatrenia** (segmentácia siete, zvýšený monitoring).
3. Ak nie je možné dodržať stanovený termín, musí byť:
 - o vykonané hodnotenie rizika,
 - o zdokumentovaná výnimka,
 - o schválené vedením alebo MKB.
4. Pri kumulácii viacerých zraniteľností sa uplatňuje **najprísnejší termín**.

5.19.12 PATCH MANAŽMENT PRE KONCOVÉ UŽÍVATEĽSKÉ ZARIADENIA

5.19.12.1 Zásady patch manažmentu

1. Všetky koncové zariadenia musia byť spravované centrálnym nástrojom.
2. Automatické aktualizácie sú preferované, ak nie je stanovená výnimka.
3. Používatelia nesmú:
 - vypínať aktualizácie,
 - inštalovať neautorizovaný softvér,
 - odkladať povinné reštarty nad stanovený limit.
4. Neaktualizované alebo nepodporované zariadenia nesmú mať prístup do siete.

Každé koncové zariadenie musí byť:

- evidované v CMDB alebo MDM,
- priradené ku konkrétnemu používateľovi,
- klasifikované podľa kritickosti.

Testovanie patchov

- Patche sa testujú na:
 - referenčnej skupine zariadení,
 - pilotných používateľoch.
- Kritické patche môžu byť nasadené okamžite bez úplného testovania.

Nasadzovanie patchov

- Patche sa nasadzujú:
 - automaticky počas definovaných údržbových okien.
- Reštart zariadenia:
 - je povinný,
 - môže byť odložený maximálne na definovaný čas (24–48 hodín).

5.19.12.2 Stupne kritičnosti užívateľov

- **Kritický užívateľ**
(vedenie, administrátori, používatelia s prístupom k citlivým údajom alebo kľúčovým systémom)
- **Dôležitý užívateľ**
(používatelia podporujúci hlavné procesy organizácie)
- **Bežný užívateľ**
(administratívni a podporní používatelia)

Kritičnosť užívateľa	Kritické (CVSS 9.0–10.0)	Vysoké (CVSS 7.0–8.9)	Stredné (CVSS 4.0–6.9)	Nízke (CVSS 0.1–3.9)
Kritický	Bezodkladne, do 24 hodín	do 3 dní	do 14 dní	do 60 dní
Dôležitý	do 48 hodín	do 7 dní	do 30 dní	do 90 dní
Bežný	do 72 hodín	do 14 dní	do 60 dní	do 120 dní

5.20 BEZPEČNOSTNÝ MONITORING A SPRÁVA PREVÁDZKOVÝCH ÚDAJOV

5.20.1 ÚČEL A ROZSAH

táto kapitola definuje štandard pre vytváranie, uchovávanie a poskytovanie bezpečnostných záznamov (logov), prevádzkových a lokalizačných údajov a podmienky ďalšej komunikácie s orgánmi činnými v trestnom konaní a s inými orgánmi štátu v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti.

5.20.2 RIADENIE KONFIGURÁCIÍ

Riadenie konfigurácie (Configuration Management) je proces poskytujúci logický model infraštruktúry a služieb prostredníctvom identifikácie, kontroly, merania a verifikácie existujúcich konfiguračných položiek.

Hlavnými úlohami procesu riadenia konfigurácie sú:

- Dokumentovanie životného cyklu konfiguračných položiek,
- Udržiavanie systému konfiguračného manažmentu CMDB a informácie v ňom uložené sprístupňovať rolám a funkciám, ktoré ich potrebujú,
- Údržba knižnice dokumentácie a softvéru,
- Udržiavanie evidencie licencií softvéru.
- Proces riadenia konfigurácií zodpovedá najmä za to, že aktíva požadované pre dodávku IT/OT služieb sú správne riadené, a že o týchto aktívach sú k dispozícii presné a spoľahlivé informácie kedykoľvek a kdekoľvek sú potrebné.
- Za proces riadenia konfigurácií je zodpovedný CIO.

Zodpovednosťou procesu riadenia konfigurácie je tiež vlastníctvo systému konfiguračného manažmentu CMDB (ktorý sa typicky skladá z niekoľkých konfiguračných databáz a prípadne ďalších integrovaných dátových zdrojov) a z toho vyplývajúca zodpovednosť za aktuálnosť údajov a informácií v ňom uložených.

Za CMDB je zodpovedný manažér IT, príp. iný poverený pracovník úseku IT.

5.20.3 RIADENIE KAPACÍT

IT a OT infraštruktúra je monitorovaná za účelom identifikácie ich kapacitných požiadaviek a ich trendov tak, aby nedošlo ku kritickému výpadku, spomaleniu, alebo inej neočakávanej poruche funkčnosti.

Špecialista/Administrátor úseku IT zodpovedá za:

- správnu implementáciu, údržbu a správu monitorovacích nástrojov a utilít v IT a OT infraštruktúre pre systémy v jeho zodpovednosti,
- sledovanie kapacít,
- monitoring systémových prostriedkov diskových kapacít,
- optimalizáciu dávkových procesov,
- optimalizáciu databázových dopytov,
- nastavenie reštrikcie nekritických služieb náročných na zdroje a pod.

Riadenie kapacít je sledované oficiálne schváleným nástrojom na monitoring a sledovanie kapacít, kde musia byť monitorované minimálne nasledovné parametre systému ako je:

- Sieťová prevádzka (dostupnosť zariadení atď.)
- Vyťaženie šírky pásma v sieti
- Vyťaženosť systémov (CPU, Memory)
- Voľné miesto lokálnych úložísk zariadení, alebo systémov (storage)
- Monitoring HW komponentov (výpadky a zlyhania komponentov)

5.20.4 HLAVNÉ ZÁSADY TVORBY A SPRÁVY BEZPEČNOSTNÝCH ZÁZNAMOV

V rámci prevádzky vznikajú Bezpečnostné záznamy generované rozličnými softvérovými komponentmi a zariadeniami prevádzkovanými v IT/OT infraštruktúre. Bezpečnostné záznamy môžu podľa charakteru obsahovať: Osobné údaje, Údaje klienta, Údaje zamestnanca a Prevádzkové údaje.

Bezpečnostné záznamy môžu byť použité na posúdenie funkčnosti nastavenia systému vzhľadom na jeho funkciu a bezpečnosť, na vyšetrovanie vzniknutých incidentov a poskytujú hlavný zdroj informácií pre systémový bezpečnostný audit a tiež môžu byť kľúčovým dôkazom pri forenznej analýze v súdnom vyšetrovaní.

Bezpečnostné záznamy sú tvorené a uchovávané tak, aby boli dôveryhodné, relevantné a dostatočne detailné.

Všetky udalosti a činnosti musia byť výsledovateľné.

Systémoví administrátori a správcovia informačných aktív pravidelne kontrolujú Bezpečnostné záznamy, ktoré sa uchovávajú najmenej po dobu stanovenú pre príslušnú kategóriu údajov zahrnutých v Bezpečnostných záznamoch alebo stanovených pre príslušný proces v súlade s legislatívnyymi, klientskymi a firemnými potrebami.

5.20.5 MONITORING BEZPEČNOSTNÝCH ZÁZNAMOV

V prípade neobvyklej udalosti je notifikovaný systémový administrátor a to minimálne v týchto prípadoch:

- blížiac sa zaplnenie kapacity úložného priestoru;
- neštandardne vysoká záťaž systému (load);
- detegovaná neobvyklá bezpečnostná udalosť.

Musí byť implementovaný unifikovaný centrálny monitorovací systém s nastavenými metrikami pre každé monitorované zariadenie/systém (príklady nastavenia metrik: upozornenie e-mailom pri 80% zaplnenia diskovej partície, e-mailom a notifikáciou v rámci monitorovacej aplikácie alert pri 95% zaplnení diskovej partície, upozornenie pri 50% využití CPU počas 5 minút, e-mailom a notifikáciou v rámci monitorovacej aplikácie alert pri nedostupnosti kritickej služby viac ako 5 minút.)

Musia byť monitorované všetky aktíva vysokej hodnoty (významu) pre MHTH na základe analýzy rizík alebo iného posúdenia, najmä centrálné sieťové prvky a servery a služby prístupné do externých sietí ako aj kritické interné servery a služby.

Musia byť monitorované všetky sieťové prvky a servery a služby. Každý nový systém musí byť zaradený do bezpečnostného monitoringu, rozsah navrhuje systémový administrátor, o prípadnej výnimke informuje MKB.

Musí byť poverený personál zodpovedný za monitorovanie bezpečnostných záznamov a upozornení a vykonanie potrebnej akcie v prípade incidentu. Odporúča sa vytvoriť prvú líniu operátorov, ktorí obsluhujú monitorovací systém a korigujú nápravné opatrenia.

Odporúča sa nastaviť monitorovací systém tak, aby v prípade vážnych udalostí produkoval aj upozornenie cez "out-of-band" kanál (napríklad e-mail, SMS, slack a pod.).

5.20.6 ZABEZPEČENIE A RIADENIE PRÍSTUPU K BEZPEČNOSTNÝM ZÁZNAMOM

Súbory s bezpečnostnými záznamami by mali byť zabezpečené aspoň takýmto spôsobom:

- Sú čitateľné len administrátorom (osobami poverenými ich analýzou).
- Nesmú byť prepisovateľné a vymazateľné (mal by byť možný len zápis na koniec súboru).
- Odporúča sa komprimovať a šifrovať archivované logovacie súbory. Pri ručnej archivácii sa odporúča aj podpisovať logovacie súbory.

- Záznamy prenášané alebo presmerované od pôvodného zdrojového zariadenia do bezpečnostného monitorovacieho systému sú presmerované prostredníctvom zabezpečených kanálov alebo prostredníctvom dedikovanej správcovskej siete.

5.20.7 MINIMÁLNY ROZSAH TVORBY BEZPEČNOSTNÝCH ZÁZNAMOV (LOGOVANIA):

Bezpečnostné záznamy sa tvoria minimálne na úrovniach:

- a) Udalosti operačného systému
- b) Auditné záznamy OS
- c) Informácie týkajúce sa aplikačných účtov
- d) Udalosti aplikácie

Rozsah údajov zaznamenávaných pre každú udalosť sa môže značne líšiť, minimálne by sa mala zaznamenať: časová stopa, kódy udalostí/stavu/alebo chýb, názov služby/príkazu/aplikácie, používateľský alebo systémový účet priradený k udalosti, použité zariadenie (napr. zdrojové a cieľové adresy IP, ID relácie terminálu, webový prehliadač), atď.

5.20.8 ODPORÚČANÝ ROZSAH TVORBY BEZPEČNOSTNÝCH ZÁZNAMOV (LOGOVANIA):

Odporúča sa zaznamenávať aspoň tieto činnosti:

- Neúspešné pokusy o prihlásenie;
- Používatelia, ktorí boli pridaní alebo odstránení zo systému;
- Priradenie a použitie špeciálnych systémových privilegovaných účtov;
- Úspešné pokusy o prihlásenie.

Odporúčané nastavenia pre systémy Windows

Bezpečnostný monitoring zbiera minimálne tieto informácie z pracovných staníc a serverov:

- Zmeny v privilegovaných skupinách (Domain Admins, Enterprise Admins...) (Windows Event ID 4728, 4729, 4732, 4733, 4756 a 4757)
- Zmeny v skupinových politikách (Windows Event ID 4735 a 4737)
- Security logy (najmä Windows Event ID 4624, 4625, 4672, 4688, 4720–4726, 4740 a 1102)
- Nainštalovanie novej služby (Windows System Event ID 7045, 7030);
- Vypnutie lokálneho firewallu (Windows Event ID 2003);
- Nepovolenie spustenia vykonateľného súboru, kvôli whitelisting pravidlu (Windows Applocker: Event ID 8004);
- Detekcia škodlivého kódu antimalware riešením, napríklad Windows Defender event ID:
 - **1116** – Malware detected
 - **1117** – Malware action taken
 - **5007** – Configuration changed
 - **5010** – Real-time protection disabled
- Informácie o všetkých spustených procesoch aj s plným príkazovým riadkom;
- Odporúča sa implementovať logovanie prístupu k citlivým aktívam (napríklad súbory, riadky databázovej tabuľky apod.).

Odporúča sa, aby bezpečnostný monitoring zbieral aspoň tieto informácie zo sieťového monitoringu:

- skenovanie sietí a portov;

- pokus o prístup do nevyužíteho IP rozsahu Spoločnosti;
- pokus o prístup na honeypot;
- história dotazov na DNS mená a vyhodnocovanie podozrivých DNS mien (napríklad na základe entropie, reputačných databáz, alebo štatistiky využitia).

5.20.9 PRESKÚMAVANIE SPRÁVNOSTI NASTAVENIA

Správcovia systémov a správcovia zariadení vedú evidenciu o tvorených Bezpečnostných záznamoch a vykonávajú pravidelné preskúmania funkčnosti ich tvorby a parametrov nastavenia najmenej raz ročne, aby sa zabezpečilo zachovanie dôvernosti, integrity, dostupnosti a autenticity informačných aktív, pričom preskúmanie prebieha za účasti nadriadeného alebo MKB a výsledok preskúmania je zaznamenaný do nezmeniteľného záznamu.

5.20.10 CENTRÁLNY NÁSTROJ NA MONITOROVANIE BEZPEČNOSTI SIETÍ A INFORMAČNÝCH SYSTÉMOV

Monitorovanie bezpečnosti sietí a informačných systémov sa tam, kde je to možné, musí uskutočňovať implementáciou centrálného nástroja na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov, zabezpečujúceho bezpečnostný dohľad nad sieťami a informačnými systémami, zaznamenávaním prevádzky týchto sietí a informačných systémov.

Monitorovanie bezpečnosti sietí a informačných systémov sa realizuje minimálne v rozsahu monitorovania centrálnych sieťových prvkov a serverov, služieb prístupných z/do externých sietí a kritických interných serverov a služieb.

Nástroj na zaznamenávanie činnosti sietí a informačných systémov zaznamenáva:

- aktivity v podobe vytvorenia, čítania, aktualizácie alebo odstránenia dôverných a prísne dôverných informácií a údajov alebo ďalších informačných aktív s nimi spojených;
- iniciáciu pripojenia do siete alebo informačného systému a akceptáciu alebo odmietnutie pripojenia do siete alebo informačného systému zaznamenaním aspoň dátumu a času aktivity, identifikácie technického prostriedku, v rámci ktorého je činnosť zaznamenaná, identifikáciu osoby a zdroja vo forme IP adresy;
- pridelenie, úpravu alebo zrušenie prístupových práv používateľa vrátane pridania nového používateľa alebo skupiny používateľov, zmenu úrovne oprávnenia používateľa, zmenu pravidiel firewallu alebo zmenu hesla;
- automatické varovné alebo chybové hlásenia systémov;
- detegované podozrivé alebo škodlivé aktivity;
- pohyb a prístup k dokumentom vo vlastníctve MHTH
- ďalšie informácie nevyhnutné na posúdenie závažnosti kybernetického bezpečnostného incidentu v spojení s kritickosťou danej služby alebo zariadenia a korektné informácie o dátume, čase a použitej časovej zóne.

5.20.11 ZDROJE SPRACOVANIA BEZPEČNOSTNÝCH PROTOKOLOV

Antimalwérový softvér – najbežnejšou formou antivírusového softvéru je antivírusový softvér, ktorý zvyčajne zaznamenáva všetky prípady zisteného škodlivého softvéru, pokusy o nakazenie súborov alebo systému.

Aplikácie – operačné systémy a bezpečnostný softvér poskytujú základ a ochranu pre aplikácie, ktoré sa používajú na ukladanie, prístup a manipuláciu s údajmi používanými v obchodných procesoch organizácie. Požiadavky klientov a odpovede servera, ktoré môžu byť užitočné pri rekonštrukcii sekvencií udalostí a určovaní ich zjavných výsledkov. Ak aplikácia zaznamená úspešné autentifikácie používateľov, je zvyčajne možné určiť, ktorý používateľ zadal každú požiadavku.

Auditorské záznamy – záznamy auditu obsahujú informácie o bezpečnostných udalostiach, ako sú úspešné a neúspešné pokusy o autentifikáciu, prístup k súborom, zmeny bezpečnostných politík, zmeny účtov (napr. Vytvorenie a odstránenie účtu, priradenie privilégií účtu) a použitie privilégií. OS umožňujú správcovi systému určiť, ktoré typy udalostí sa budú auditovať a či sa majú zaznamenávať úspešné a / alebo neúspešné pokusy o vykonanie určitých akcií.

Autentifikačné servery (AD) – autentifikačné servery vrátane serverov jednotného prihlásenia zaznamenávajú každý pokus o autentizáciu vrátane jeho pôvodu, používateľského mena, úspechu alebo neúspechu a dátumu a času.

Firewall - rovnako ako smerovače, firewall povoľujú alebo blokujú činnosť na základe pravidiel; firewall však používajú oveľa sofistikovanejšie metódy na preskúvanie sieťového prenosu. Firewall môže tiež sledovať stav sieťovej prevádzky a vykonávať kontrolu obsahu. Firewally majú zložitejšie zásady a generujú podrobnejšie protokoly činnosti ako smerovače.

Informácie o použití – ako napríklad počet transakcií uskutočnených v určitom období (napr. minúta, hodina) a veľkosť transakcií (napr. veľkosť e-mailovej správy, veľkosť prenosu súboru). To môže byť užitočné pre určité typy monitorovania zabezpečenia (napr. Desaťnásobné zvýšenie aktivity e-mailu môže naznačovať novú hrozbu škodlivého softvéru prenášaného e-mailom; neobvykle veľká odchádzajúca e-mailová správa môže naznačovať nevhodné zverejnenie informácií).

Informácie o účte – napríklad úspešné a neúspešné pokusy o autentifikáciu, zmeny účtu (napr. vytvorenie a odstránenie účtu, priradenie privilégií účtu) a použitie privilégií. Okrem identifikácie bezpečnostných udalostí, ako je napríklad hádanie hesla hrubou silou a eskalácia práv, sa dá použiť na identifikáciu toho, kto aplikáciu použil a kedy ju každá osoba použila.

Jump server – je systém v sieti, ktorý slúži k prístupu a správe zariadení v samostatnej bezpečnostnej zóne. Jump server je bezpečnostné a monitorované zariadenie, ktoré pokrýva dve rozdielne bezpečnostné zóny a poskytuje kontrolovaný prístup medzi nimi.

Monitorovacie systémy – systémy schopné monitorovať IP konektivitu sieťových zariadení ale aj prevádzkové služby, limitné stavy CPU, sieťových úložísk, atď. (napr. Zabbix, Nagios atď.).

Operačné systémy (OS) pre servery, pracovné stanice a sieťové zariadenia (napr. Smerovače, prepínače) zaznamenávajú rôzne informácie súvisiace so zabezpečením. Najbežnejšie typy údajov OS týkajúcich sa zabezpečenia sú nasledujúce:

Router – smerovače sú nakonfigurované tak, aby povoľovali alebo blokovali určité typy sieťového prenosu na základe politiky. Smerovače, ktoré blokujú prenos, sú zvyčajne nakonfigurované tak, aby protokolovali iba tie najzákladnejšie charakteristiky blokovanej aktivity.

Sieťové karanténne servery – pred povolením pripojenia k sieti kontrolujú úroveň zabezpečenia každého vzdialeného zariadenia. Často sa to deje prostredníctvom karanténnej siete. Hostitelia, ktorí nereagujú na kontroly servera alebo zlyhajú pri kontrole, sú umiestnení do karantény v samostatnom segmente virtuálnej lokálnej siete (VLAN). Karanténne servery v sieti zaznamenávajú informácie o stave kontrol vrátane toho, ktorí hostitelia boli umiestnení do karantény a z akých dôvodov.

Softvér na správu zraniteľnosti – softvér na správu chýb zabezpečenia, ktorý obsahuje softvér na správu opráv a softvér na hodnotenie zraniteľnosti, zaznamenáva históriu inštalácie opráv a stav zraniteľnosti každého zariadenia, ktorý obsahuje známe chyby zabezpečenia a chýbajúce aktualizácie softvéru.

Softvér pre vzdialený prístup (VPN) – vzdialený prístup je poskytovaný a zabezpečovaný prostredníctvom virtuálnych privátnych sietí (VPN). Systém VPN zaznamenáva úspešné a neúspešné pokusy o prihlásenie, ako aj dátumy a časy, keď sa každý používateľ pripojil a odpojil, a množstvo dát odoslaných a prijatých v každej relácii používateľa.

System Events – udalosti systému sú prevádzkové akcie vykonávané súčasťami OS, napríklad vypnutie systému alebo spustenie služby. Zaznamenávajú zlyhané udalosti a najvýznamnejšie úspešné udalosti, ale veľa OS umožňuje správcovi určiť, ktoré typy udalostí sa budú zaznamenávať.

Systémy detekcie a prevencie narušenia (IDS/IPS) – systémy detekcie a prevencie narušenia zaznamenávajú podrobné informácie o podozrivom správaní a zistených útokoch, ako aj o všetkých činnostiach, ktoré systémy prevencie narušenia vykonávajú na zastavenie prebiehajúcej škodlivej činnosti.

Významné operatívne činnosti – ako je spustenie a vypnutie aplikácie, zlyhania aplikácie a veľké zmeny v konfigurácii aplikácie. To možno použiť na identifikáciu bezpečnostných kompromisov a prevádzkových zlyhaní.

Webové servery proxy – sú sprostredkujúcim hosťiteľom, prostredníctvom ktorého sú prístupné webové stránky. Webové proxy spracovávajú žiadosti vo webovej stránke v mene používateľov a ukladajú do medzi-pamäti kópie načítaných webových stránok, aby boli ďalšie prístupy na tieto stránky efektívnejšie.

5.20.12 INFRAŠTRUKTÚRA SPRÁVY PROTOKOLOV

Infraštruktúra na správu protokolov, pozostáva z hardvéru, softvéru, sietí a médií používaných na generovanie, prenos, ukladanie, analýzu a likvidáciu údajov protokolu.

Správa protokolov zabezpečuje, aby sa bezpečnostné záznamy ukladali dostatočne podrobne počas primeraného časového obdobia pre zaistenie identifikácie bezpečnostných incidentov, porušenia zásad, podvodné aktivity a prevádzkové problémy krátko po ich vzniku a na poskytnutie informácií užitočných na ich riešenie. Protokoly sú nevyhnutné aj na vykonávanie auditov a forenzných analýz, podporu interných vyšetrovaní organizácie a dlhodobých problémov.

5.20.13 GENEROVANIE A UKLADANIE PROTOKOLOV

Lokálne na mieste vzniku – protokoly sú umiestnené na mnohých hosťiteľoch v celej spoločnosti MHTH, čo si vyžaduje vykonanie správy protokolov v celej MHTH. Jeden zdroj denníka môže tiež generovať viac denníkov - napríklad aplikáciu. Miesto uloženia protokolu je v mieste vzniku.

Vzdialene nezávislé forenzné repository – pre ochranu protokolov pred zmenou integrity, alebo vymazaním sa z koncových bodov zariadení, v reálnom čase zasielajú protokoly na nezávislé forenzné úložisko, kde nemajú zriadené prístupové oprávnenia ani administrátori systému. Napríklad central syslog server. V prípade kompromitácie servera aj po vymazaní protokolov na kompromitovanom zariadení, stále zostávajú zachované forenzné údaje na vzdialenom úložisku.

Nekonzistentný čas - každé zariadenie/software, ktorý generuje protokoly, odkazuje na svoje interné hodiny, pri nastavovaní časovej pečiatky, pre každú položku protokolu. Ak sú hodiny zariadenia nepresné, nepresné budú aj záznamy v jeho denníkoch. To môže sťažiť analýzu protokolov, najmä keď sa analyzujú protokoly z viacerých zariadení. Je nevyhnutné mať nastavený systém centrálného času (NTP server) na úrovni celej IT, resp. OT infraštruktúry.

Ochrana protokolov – pretože protokoly obsahujú záznamy o zabezpečení systému a siete, je potrebné ich chrániť pred narušením ich dôvernosti a integrity.

5.20.14 BEZPEČNOSTNÉ INFORMÁCIE A SOFTVÉR NA SPRÁVU UDALOSTÍ (SIEM)

SIEM umožňuje koreláciu udalostí, čo je hľadanie vzťahov medzi dvoma alebo viacerými položkami protokolu. Najbežnejšou formou korelácie udalostí je korelácia založená na pravidlách,

ktorá sa zhoduje s viacerými protokolmi položky z jedného zdroja alebo z viacerých zdrojov na základe zaznamenaných hodnôt, ako sú časové pečiatky, adresy IP a typy udalostí. Koreláciu udalostí možno vykonať aj inými spôsobmi, napríklad pomocou štatistických metód alebo vizualizačných nástrojov. Ak sa korelácia vykonáva pomocou automatizovaných metód, výsledkom úspešnej korelácie je spravidla nový záznam protokolu, ktorý spája informácie na jednom mieste. V závislosti od povahy týchto informácií, môže infraštruktúra tiež generovať výstrahu, ktorá naznačuje, že identifikovaná udalosť si vyžaduje ďalšie prešetrenie.

Pre vyhodnocovanie jednotlivých tipov incidentov slúžia základné pravidlá tzv. Use-Case, aplikovaním ktorých systém vie automaticky založiť bezpečnostný incident pre konkrétny vektor útoku alebo porušeniu bezpečnostnej politiky.

5.20.15 PREVÁDZKOVÉ PROCESY PROTOKOLOV

Správcovia na úrovni systému a infraštruktúry sa riadia štandardnými procesmi správy protokolov, za ktoré sú zodpovední. Táto časť popisuje hlavné operačné procesy správy protokolov.

- Konfigurácie zdrojov protokolov;
- Generovanie protokolov;
- Ukladanie a zabezpečenie protokolov;
- Vykonanie analýzy údajov protokolu;
- Iniciujte príslušné reakcie na identifikované udalosti;
- Správa pre dlhodobé ukladanie údajov denníka.

5.20.16 KONFIGURÁCIA ZDROJOV PROTOKOLU

Správcovia na úrovni systému musia nakonfigurovať zdroje protokolov tak, aby zachytávali potrebné informácie v požadovanom formáte a umiestneniach a aby si ich uchovali po príslušné časové obdobie.

Na základe zásad organizácie správcovia určujú, ktorý z ich hostiteľov a komponentov hostiteľa sa musí alebo má podieľať na infraštruktúre správy protokolov. Jeden súbor protokolu môže obsahovať informácie z niekoľkých zdrojov,

5.20.17 GENEROVANIE PROTOKOLOV

Za predpokladu, že zdroj protokolu ponúka možnosti konfigurácie, pri výbere počiatočného nastavenia protokolovania treba zvážiť kapacitné možnosti a predpokladaný objem údajov pre zaznamenanie každého typu udalosti.

5.20.18 SKLADOVANIE A LIKVIDÁCIA PROTOKOLOV

Správcovia na úrovni systému určia ako má každý zdroj denníka ukladať svoje údaje. To by malo byť riadené predovšetkým organizačnými politikami týkajúcimi sa ukladania protokolov, najmä požiadavkami na preposielanie záznamov do infraštruktúry správy protokolov.

5.20.19 ZABEZPEČENIE DENNÍKA

Správcovia infraštruktúry a systému chránia dôvernosť, integritu a dostupnosť údajov denníka.

5.20.20 OBMEDZENIE PRÍSTUPU K SÚBOROM DENNÍKA

Používatelia by nemali mať prístup k súborom denníka. V nevyhnutných prípadoch by mali mať oprávnenie iba na pripojenie s prístupom na čítanie. Používatelia by nemali byť schopní premenovať, vymazať alebo vykonať iné operácie na úrovni súborov so súbormi denníka.

Ukladanie citlivých údajov

Niektoré protokoly zaznamenávajú citlivé údaje, napríklad heslá, osobné údaje, atď. Ak je to možné, protokolovanie by malo byť nakonfigurované tak, aby nezaznamenávalo informácie, ktoré sa nevyžadujú, a predstavovali by značné riziko, ak by k nim mali prístup neoprávnené strany.

Ochrana archivovaných súborov denníka

Zahrňa vytvorenie a zabezpečenie prehľadov správ pre súbory, šifrovanie súborov denníka a zabezpečenie primeranej fyzickej ochrany k archívnym médiám.

Zabezpečenie procesov, ktoré generujú položky protokolu.

Neoprávnené strany nesmú manipulovať s procesmi zdrojových protokolov, spustiteľnými súbormi, konfiguračnými súbormi alebo inými súčasťami zdrojov protokolov, ktoré by mohli mať vplyv na protokolovanie.

Nakonfigurovanie každého zdroja denníka tak, aby sa správal primerane, keď sa vyskytnú chyby protokolovania. Protokolovanie sa môže považovať za také dôležité pre konkrétny zdroj protokolu, že by zdroj protokolu mal byť nakonfigurovaný tak, aby úplne zastavil svoju funkčnosť pri zlyhaní protokolovania.

Implementácia bezpečných mechanizmov na prepravu údajov protokolu zo systému na centralizované servery správ protokolov.

Nastavenie zabezpečenia aplikovaním šifrovania komunikácie prostredníctvom samostatného protokolu, napríklad IPsec alebo SSL.

Analýza údajov protokolu – potrebné efektívne analyzovať s použitím automatizovaných prostriedkov.

Stanovenie priorít v záznamoch – stanovenie priorít pri analýze položiek protokolu napr. vysoké / stredné / nízke.

Reakcia na identifikované udalosti – počas analýzy protokolov môžu správcovia identifikovať udalosti, ako sú napríklad incidenty a prevádzkové problémy, ktoré si vyžadujú určitý druh reakcie.

5.21 AKVIZÍCIA, VÝVOJ A ÚDRŽBA INFORMAČNÝCH SYSTÉMOV

5.21.1 VÄZBA NA NORMY

Táto časť primárne vychádza z normy ISO/IEC 27001:2022 Informačné technológie – Bezpečnostné metódy – Systémy riadenia informačnej bezpečnosti – Požiadavky. Dokument sa zameriava najmä na opatrenia a požiadavky uvedenej normy v súvislosti s akvizíciou, vývojom a údržbou informačných systémov.

5.21.2 VÝVOJ NOVÉHO/EXISTUJÚCEHO IS

Pri vývoji je potrebné:

- určiť bezpečnostné požiadavky na vyvíjaný IS na základe analýzy rizík, požiadaviek na dostupnosť a klasifikáciu spracúvaných údajov;
- zabezpečiť oddelenie prostredí prevádzky, vývoja a testovania pre minimalizáciu neautorizovaného prístupu alebo zmien v prevádzkovom prostredí;
- zabezpečiť kvalifikovaný interný alebo externý personál na vývoj;
- evidenciu zmien v rámci projektu vývoja;
- riadenie verzií (najlepšie prostredníctvom automatizovaného prostriedku);
- testovanie pred každým nasadením do prevádzky, vrátane testovania bezpečnostných funkcií;
- spracovanie dokumentácie.

5.21.3 INTERNÝ A EXTERNÝ VÝVOJ IS

Bez ohľadu na to, či ide o interný alebo externý vývoj IS, každý vývoj IS vyžaduje štandardný projektový prístup, pričom súčasťou projektového tímu sú vždy interní pracovníci a v prípade externého vývoja aj externí pracovníci. Interní pracovníci zabezpečujú minimálne koordináciu a

dohľad nad projektom. Každý vývoj zároveň znamená dodržiavanie bezpečnostných požiadaviek spoločnosti.

5.21.4 EVIDENCIA A RIADENIE ZMIEN

Požiadavky na zmeny od útvarov používateľov sa zadávajú cez špeciálne, na tento účel vytvorené aplikácie ITSM, kde je zabezpečené automatizované sledovanie priebehu riešenia – od evidencie zadáných požiadaviek až po akceptovanie žiadateľom po otestovaní.

Riadenie zmien v IT prebieha podľa interného dokumentu [MHTH IT S01 Proces riadenia zmien v IT \(Change Management process\)](#) úseku IT.

5.21.5 KONFIGURAČNÉ RIADENIE VÝVOJA SW

Cieľom konfiguračného riadenia pri vývoji, dodávke a údržbe softvéru, je jednoznačne identifikovať verzie každého programu, umožniť riadenú aktualizáciu daného programu a sledovať všetky zmeny softvéru počas jeho životného cyklu.

Riadenie verzií sa má realizovať využitím automatizovaného mechanizmu vždy pre daný aplikačný software. Súčasťou riadenia verzií má byť aj informácia o obsahu danej verzie a možnosť vypršania platnosti danej verzie, pričom na základe definovaného časového parametra sa daná verzia automaticky zablokuje.

Súčasťou konfiguračného riadenia sú dedikované prostredia pre vývoj, testovanie a prevádzku.

5.21.6 INTERNÉ TESTOVANIE SW

Pred odovzdaním softvéru do prevádzky, musí prebehnúť testovanie softvéru. Proces testovania softvéru pozostáva z nasledovných krokov:

5.21.6.1 NÁVRH TESTOVACÍCH SCENÁROV

V prípade rozsiahlejších dodávok alebo kritických funkčných častí je nutné zabezpečiť prípravu testovacích scenárov. V prípade menších zmien je možné, po dohode testovanie realizovať bez formálnych testovacích scenárov.

5.21.6.2 TESTOVANIE FUNKCIONALITY

Čiastkové testovanie softvéru počas vývoja tzv. Unit testy vykonávajú členovia vývojového tímu podľa pokynov Vedúceho tímu.

V prípade externého vývoja toto testovanie realizujú pracovníci dodávateľa.

Pred odovzdaním SW do prevádzky musí prebehnúť tzv. akceptačné testovanie softvéru (User Acceptance Test – UAT). Realizáciu UAT zabezpečuje Vlastník v spolupráci s oddelením rozvoja a prevádzky aplikácií, v súlade s definovanými testovacími scenármi.

5.21.6.3 TESTOVANIE BEZPEČNOSTI

Pred nasadením novej verzie SW do prevádzky, musí byť vykonaná statická, alebo dynamická analýza kódu automatizovaným prostriedkom vhodným pre dané vývojové prostredie (napr. PMD a Findbugs, Snyk, Detendabot a pod.), o výstupe analýzy a odstránení prípadných zistených chýb sa vykoná záznam. V rámci automatizovaného procesu nasadzovania SW CI/CD je potrebné aplikovať mechanizmy kontroly závislostí a zraniteľností.

Minimálne raz ročne, resp. pri zásadných zmenách SW (zmena bezpečnostných princípov, zmena architektúry, použitých platforiem a pod.), sa vykonajú penetračné testy aplikácie (presná špecifikácia testovania a jeho zameranie sa určí pred začiatkom testovania na základe vstupných parametrov – podľa druhu aplikácie a vykonaných zmien). Testovanie zmien musí prebiehať v testovacom prostredí, ktoré je oddelené (fyzicky aj logicky) od prevádzkového prostredia.

Výstupom tohto procesu je záznam o testovaní s popisom zistených chýb a zraniteľnosti a popisom prijatých opatrení na ich odstránenie.

5.21.6.4 OPRAVA NÁJDENÝCH CHÝB

V prípade nájdania chýb počas testovania a ich následného odstránenia je nutné opakovane vykonať testovanie v celom rozsahu testovacích scenárov, týkajúcich sa danej časti SW. V

případe menších zmien je možné po dohode s oddelením rozvoja a prevádzky aplikácií, testovanie realizovať bez formálnych testovacích scenárov.

5.21.6.5 DOKUMENTÁCIA

Po každej významnej zmene SW je potrebné zabezpečiť aktualizáciu systémovej, prevádzkovej a používateľskej dokumentácie v rozsahu a kvalite zodpovedajúcej rozsahu a povahe vykonanej zmeny.

5.22 OCHRANA PRED ŠKODLIVÝM KÓDOM

Spoločnosť MHTH prijala vhodné nástroje a infraštruktúru, vrátane antivírusových systémov, aby sa zabránilo vniknutiu a pôsobeniu potenciálne škodlivého softvéru. Úsek IT je zodpovedný za inštaláciu a hodnotenie nových verzií a aktualizácií a na stanovenie spôsobov odozvy a opatrení v prípade, že sa v informačných systémoch zistí potenciálne škodlivý softvér.

- Aplikovaný systém na serverovú platformu
- Aplikovaný systém na WS a notebooky
- Aplikovaný systém pre GW (SMTP, WWW)

5.22.1 BEZPEČNOSTNÉ OPATRENIA PROTI ŠKODLIVÉMU KÓDU

Úsek IT je zodpovedný za prijímanie vhodných opatrení na zisťovanie a blokovanie počítačových vírusov a iného potenciálne škodlivého softvéru, aby sa zabezpečila okamžitá identifikácia, zastavenie šírenia a odstránenie škodlivého programu, rovnako ako aj oprava jeho následkov. MKB priebežne vzdeláva personál, aby sa zvýšila informovanosť o tejto problematike.

Úsek IT je tiež zodpovedný za:

- správu vhodných nástrojov a infraštruktúry na zabránenie vniknutiu a následnému pôsobeniu potenciálne škodlivého softvéru;
- centrálnu správu antivírusového systému, posudzovanie nových verzií a inštaláciu aktualizácií;
- stanovenie vhodného používateľského pravidla týkajúceho sa prevencie a ochrany pred škodlivým kódom;
- zabránenie samostatnej inštalácii softvéru používateľmi alebo ich deaktivácie okrem schváleného SW vybavenia MHTH;
- neustále aktualizovanie antivírusových systémov na všetkých serveroch a pracovných staniciach a implementovať opatrenia, aby sa zabránilo ich vypnutiu používateľmi. Skontrolovať, či antivírusové systémy boli správne nainštalované a povolené vo všetkých systémoch potenciálne ohrozených vniknutím škodlivého kódu. Antivírusový softvér musí byť vždy aktívny, povolený a aktualizovaný na najnovšiu dostupnú verziu a ak to výslovne vyžaduje zákon, musia generovať denníky udalostí;
- je zodpovedný v prípade, že softvér inštalujú tretie strany, prijať preventívne kontrolné opatrenia na zabránenie prítomnosti potenciálne škodlivého kódu.

Špecialista/administrátor úseku IT je povinný:

- zabezpečiť inštaláciu a pravidelnú aktualizáciu antivírusových detekčných a prevenčných nástrojov slúžiacim na kontrolu a ochranu IT a OT aktív. Antivírusové a antimalvérové opatrenia musia zhŕňať:
 - a) **Kontrolu súborov** (s výnimkou schválených výnimiek) na všetkých elektronických, optických a sieťových médiách pred ich použitím.
 - b) **Kontrolu príloh elektronickej pošty a stiahnutých súborov** pred ich otvorením, pričom kontrola musí prebiehať na viacerých úrovniach (e-mailové brány, koncové zariadenia, sieťové vstupné body).

- c) **Ochranu pred nevyžiadanou poštou**, phishingom, škodlivými odkazmi a ďalšími formami sociálneho inžinierstva.
 - d) **Ochranu pred exploitáciou**, vrátane detekcie a blokovania pokusov o zneužitie zraniteľností aplikácií, operačného systému a prehliadačov.
 - e) **Aplikačnú kontrolu (whitelisting)**, ktorá povoľuje spúšťanie len autorizovaných aplikácií, binárnych súborov a skriptov.
 - f) **Kontrolu a ochranu webových stránok** z hľadiska výskytu škodlivého kódu, rizikových kategórií a podozrivých domén.
- venovať zvýšenú pozornosť tomu, aby škodlivý kód nebol zavedený počas výkonu pohotovostných postupov alebo postupov údržby;
 - nasadiť hardening nastavenia do používania (deaktivácia nepotrebných a nezabezpečených služieb a protokolov).
 - nastaviť internetový prehliadač tak, aby si používateľ nemohol sám doinštalovať plugin, add-on, alebo rozšírenia, ktoré nie sú povolené.

5.23 BEZPEČNOSTNÉ PRAVIDLÁ PRE INŠTALÁCIU A KONFIGURÁCIU IS

Inštaláciu a konfiguráciu systémov a aplikácií je kompetentný vykonávať len administrátor ICT, ktorý má na takéto činnosti privilegované prístupy. Užívatelia majú pridelené základné prístupy do systémov bez možnosti inštalácie softvérového vybavenia a vypínania bezpečnostných nastavení zariadení (ako je napríklad antivírusová ochrana a pod.).

Je zakázané inštalovať si z webového prehliadača rozširujúce softvérové vybavenia bez výslovného odsúhlasenia administrátorom ICT.

5.23.1 ZÁKLADNÁ OCHRANA

Táto časť popisuje opatrenia na zabezpečenie základnej úrovne ochrany, ktoré sa majú aplikovať v počiatočných konfiguračných fázach a následných operáciách všetkých typov systémov (pracovné stanice, servery, sieťové zariadenia), s osobitným dôrazom na aspekty:

- kontroly prístupu;
- inštalácie a bezpečnej konfigurácie (hardening);
- optimalizácie služieb;
- opravovania a odstránenia slabých miest;
- umiestnenia systémov.

5.23.1.1 KONTROLA PRÍSTUPOV

Opatrenia prijaté pre kontrolu prístupov nariaďujú administrátorovi IS:

- deaktivovať všetkých nepotrebných používateľov zabudovaných v systéme (ako napr.: Guest, TsInternetUser v prípade, že ich nevyužíva terminálový server);
- zabezpečiť autentifikačné mechanizmy pre prístup u správcov systému, ktoré spĺňajú minimálne ustanovenia dobrej praxe bezpečnostných pravidiel pre autentifikáciu;
- nakonfigurovať systém, ak takýto krok neznamená prerušenie technickej podpory a garancií dodávateľov a neohrozuje správne fungovanie aplikácie tak, aby nezobrazoval informácie o systéme a používateľoch až kým prihlasovanie nebude úspešne ukončené, konkrétne v priebehu týchto fáz:
 - prvý vstup do systému;
 - nové pripojenie do systému;
 - zablokovanie a odblokovanie pracovnej relácie;

- informovať používateľov pred vstupom do systému, že zariadenie môžu využívať výlučne na služobné účely.

5.23.1.2 BEZPEČNÁ INŠTALÁCIA A KONFIGURÁCIA

Opatrenia pre bezpečnú inštaláciu a konfiguráciu systémov stanovujú:

- odstrániť, alebo ak to nie je možné, odstaviť tie časti technického vybavenia, ktoré nie sú potrebné k prevádzke systému alebo sa využívajú len počas fázy inštalácie. Odstrániť alebo deaktivovať systémové služby, ktoré nie sú nevyhnutné pre správne fungovanie zariadenia (hardening na základe CIS frameworku);
- v prípade potreby deaktivovať možnosť spustenia systému z externého média (napr. disketa, CD), ak je operačný systém nainštalovaný na takomto informačnom médiu;
- tam, kde je to možné, deaktivovať možnosť automatického stiahnutia konfigurácie z externého servera (napr. TFTP server), po inštalácii a nakonfigurovaní ICT zariadenia;
- tam, kde je to možné, deaktivovať automatické spracovanie obsahu z externého média (napr. CD-ROMy, USB kľúče);
- tam, kde je to možné, zablokovat' prístup na diaľku do diagnostických a správcofských portov systému, alebo chrániť prístup cez autentifikačné mechanizmy;
- odstrániť pre operačné systémy nepotrebné, pred-inštalované programy (napr. nástroje týkajúce sa správ, e-maily neoprávneným klientom, alebo klientom, ktorých MHTH nepoužíva), za predpokladu, že takýto krok nespôsobí prerušenie technickej podpory a garancií dodávateľov;
- vymazať dočasné súbory, ktoré vytvorili používatelia, procesy a aplikácie, ak ich už systém nepoužíva na sledovania činností;
- zosynchronizovať systémové hodiny a skontrolovať nadväzujúce oblasti ako sú: časové pečiatky, registrácie udalostí, zaznamenávanie verzií, atď.;
- zjednotiť formát hodín na všetkých systémoch;
- pre hodiny používať licencované a certifikované referenčné zdroje.

5.23.1.3 OPTIMALIZÁCIA POSKYTOVANÝCH SLUŽIEB

Opatrenia pre optimalizáciu poskytovaných služieb stanovujú:

- za účasti pracovníkov zodpovedajúcich za konfigurovanie systému, pri každom systéme definovať služby, ktoré je potrebné udržiavať aktívne a tie, ktoré možno deaktivovať;
- deaktivovať služby, ktoré nie sú výslovne potrebné pre chod systému, nakoľko môžu byť zraniteľné;
- odstrániť z každej aktívnej služby nepotrebné nástroje a funkcie (napr. pri inštalácii prednastavené „vzorové súbory“, alebo „testovacie súbory“, on-line dokumentácia);
- tam, kde je to možné bez vplyvu na činnosť firmy zabezpečiť, aby správy, ktoré sa pomocou aktívnych služieb na systéme zobrazujúce používateľom, neobsahovali informácie o konfigurácii, druhu, alebo verzii nainštalovaného softwaru.

5.23.1.4 UMIESTNENIE SYSTÉMOV

Opatrenia zabezpečujúce primeraný stupeň fyzickej bezpečnosti:

- zabezpečiť primerané opatrenia fyzickej ochrany priestorov a zón, ktoré sú vyhradené pre servery a sieťové zariadenia (technické priestory, skrinky,...) a sprístupniť ich len oprávneným osobám prostredníctvom monitoringu a zaznamenávania prístupov.
- zdokumentovať umiestnenie vybavenia zápisom do inventáru majetku;

5.23.1.5 OPATRENIA PRE PRACOVNÉ STANICE A SERVERY

Opatrenia prijaté v súvislosti s inštaláciou softwaru nariaďujú:

- inštalovať na pracovné stanice a servery len povolený software s riadnou licenciou, aby sa zabezpečilo plnenie právnych obmedzení týkajúcich sa používania materiálov, ktoré spadajú do oblasti ochrany duševného vlastníctva, alebo sú chránené licenciami;
- inštalácie vykonáva výhradne administrátor ICT.

5.23.1.6 NASTAVENIA SIETE

Tieto opatrenia prijaté pre sieťové nastavenia nariaďujú:

- nastaviť konfiguračné parametre rozhrania a sieťových protokolov tak, aby sa minimalizovala zraniteľnosť systému voči kybernetickým útokom mimo sieťového protokolu (napr. DoS cez zaplavenie SYN, IP alebo MAC spoofing, unesenie relácie a pod.);
- deaktivovať autentifikačné mechanizmy umožňujúce prístup do systémov len na základe IP adresy zdrojového systému bez vyžiadania explicitnej identifikácie používateľa, ktorý sa chce pripojiť;
- zdefinovať a chrániť sieťové zdieľanie pracovných staníc a systémov, ktoré sú dostupné z internej siete, pomocou vhodných mechanizmov kontroly prístupov, zameraných predovšetkým na:
 - SMB zdieľanie na pracovných staniciach musí byť zakázané, pokiaľ nie je výslovne schválené bezpečnostným oddelením a technicky kontrolované.
 - Prístup k SMB službám na pracovných staniciach musí byť blokovaný firewallom, s výnimkou komunikácie so schválenými servermi (napr. file servery, doménové radiče).
 - Prenos súborov medzi používateľmi musí prebiehať výhradne cez schválené a monitorované kanály, ako sú:
 - centrálné file servery,
 - cloudové úložiská organizácie,
 - schválené kolaboračné platformy.

5.23.1.7 SYSTÉM SÚBOROV

Opatrenia na nastavenie súborov nariaďujú:

- nakonfigurovať prístup do súborov a adresárov tak, aby boli chránené pred nepovoleným vstupom odstránením nepotrebných povolení;
- zapnúť predchádzajúce povolenia týkajúce sa systému súborov, aby novo-vytvorené súbory a adresáre mali pridelené rovnaké prístupové povolenia, ako adresár, ktorý ich obsahuje;
- používanie nástrojov správcu umožniť výlučne používateľom s profilom správcu (napr. konfiguračné zariadenia, nástroje na správu disku, pracovné zariadenia a pod);
- prístup do konfiguračných súborov a adresárov je umožnený výlučne používateľom s administrátorskými oprávneniami;
- umožniť výlučne užívateľom s administrátorskými oprávneniami nainštalovať do systému nové softwarové aplikácie.

5.23.1.8 ANTIVÍRUSOVÝ SOFTVÉR

Opatrenia týkajúce sa správy antivírusového softwaru nariaďujú:

- centrálné riadenie antivírusového softwaru, a pravidelné overovanie správnosti konfigurácie;
- inštalovať, aktivovať a vždy udržiavať antivírusový software v chode, aktualizovať ho a zabrániť koncovým používateľom, aby ho mohli deaktivovať, alebo pozmeniť nastavenia;
- nakonfigurovať antivírusové programy tak, aby automaticky a periodicky skontrolovali zariadenie, na ktorom sú nainštalované, vrátane aktívnych procesov v pamäti a lokálnych pevných diskov a prenosných médií;
- nainštalovať dočasné opravy a nové verzie antivírusových aplikácií ihneď po posúdení dopadov ich inštalácie ako aj neuskutočnenej inštalácie;
- sledovať zisťovanie vírusov a nekalých softwarových aktivít.

5.23.1.9 INŠTALÁCIA SOFTVÉRU A ZARIADENÍ

Špecialista/administrátor úseku IT je povinný:

- inštalovať len autorizovaný software, ktorý je v MHTH oficiálne schválený a v súlade s licenčnými podmienkami. Výnimky schvaľuje a eviduje ;
- Služby a aplikácie musia byť výhradne inštalované v súlade s licenčnými podmienkami. Z toho dôvodu musia byť pri ich nákupe preskúmané všetky licenčné podmienky stanovené výrobcom, alebo autorom a identifikované všetky prípadné obmedzenia, alebo iné kritériá, ktoré môžu mať negatívny dopad na používanie produktu v spoločnosti.
- V OT prostredí je manažment licencií riadený licenčným manažérom v rámci SCADA komponentov (EWS, operátorské stanice, procesné stanice, PLC kontrolér, atď.). Niektoré systémy vyžadujú použitie hardvérového kľúča (USB) pri inštalácii licencie (napr. Siemens).
- Inštalácia a aktualizácia operačných systémov, aplikácií a programových knižníc je vykonávaná výhradne špecialistom/administrátorom úseku IT v súčinnosti a schválením vlastníkom aktív.
- Software a operačné systémy môžu byť inštalované iba v súlade s platnými štandardami MHTH pre operačné systémy;
- Špecialista/administrátor úseku IT je zodpovedný za pripojenie pracovnej stanice do lokálnej počítačovej siete IT, inštaláciu operačného systému a všetkého ostatného programového vybavenia. Je tiež povinný pripojiť zariadenie do monitorovacieho nástroja;
- Používateľ má zakázané pripájať súkromné zariadenia do IT a OT siete, alebo prepájať tieto siete s Internetom.
- OT manažér samostatne, alebo v spolupráci s dodávateľom automatizácie zodpovedá za pripojenie operátorskej stanice, inžinierskej do počítačovej siete SCADA, inštaláciu operačného systému a všetkého ostatného programového vybavenia.
- Vlastník aktíva schváli a zabezpečí inštaláciu len takých programových prostriedkov, ktoré zamestnanec potrebuje ku svojej práci. Prístupové práva schváli tak, aby zamestnanec nemohol na pracovnej stanici meniť žiadne programové vybavenie, a tiež meniť konfiguráciu programového vybavenia;
- Servery, dátové úložiská, procesné stanice a ostatné kritické zariadenia, musia byť zabezpečené pred zneužitím alebo poškodením, umiestnená v uzamykateľných technických miestnostiach, alebo dátových centrách. V prípade OT prostredia v osobitnej a uzamykateľnej miestnosti (IT/OT serverovni), s potrebným technickým, klimatickým a bezpečnostným vybavením;
- Nová aplikácia, alebo iný software je pred inštaláciou adekvátne otestovaná špecialistom/administrátorom úseku IT za účelom overenia funkčnosti, vplyvu na operačný systém a bezpečnostných vlastností.
- V OT je software a aplikácie vopred testované dodávateľom OT technológií.

5.23.2 KONTROLA

V pravidelných intervaloch, minimálne 1x ročne, dohliada MKB na vykonávanie kontroly bezpečnostných pravidiel súvisiacich s riadením prevádzky sietí a konfigurácií bezpečnostných nástrojov definovaných touto smernicou za účelom identifikácie nesúlady s týmito požiadavkami a ich následnej nápravy.

Za vykonanie kontroly na úseku IT zodpovedá CIO.

Kontrolu vykonáva špecialista/administrátor úseku IT, ktorý o jej výsledku informuje CIO a MKB.

5.23.3 ĎALŠIE USTANOVENIA

Na základe tohto predpisu užívatelia nemajú právo inštalácie softvéru na prostriedky ICT, ani manipulovať s bezpečnostným nastavením zariadení. Je zakázané inštalovať softvérové rozšírenia na úrovni webového prehliadača. Je zakázané kopírovať a spúšťať portable aplikácie.

Na kontrolu prítomnosti nelegálneho softvéru sa vykonáva softvérová inventúra inštalovaného a kopírovaného softvéru minimálne 2 x ročne administrátorom ICT.

5.24 PERSONÁLNA BEZPEČNOSŤ

Personálna bezpečnosť je súbor opatrení, ktoré sú zamerané na výber vhodných zamestnancov a na zabezpečenie kontroly ich dôveryhodnosti a lojálnosti.

Činnosti popisujú informačnú a kybernetickú bezpečnosť pri uzatváraní pracovného pomeru, počas pracovného pomeru a pri ukončení pracovného pomeru.

Smernica upravuje oblasti:

1. prijímanie nových zamestnancov – preverenie ich vhodnosti pre pozíciu, pridelenie prístupových práv a zariadení potrebných pre výkon práce,
2. trvanie pracovného pomeru - zavedenie programov budovania bezpečnostného povedomia, zvyšovanie úrovne povedomia zamestnancov, overovanie účinnosti, disciplinárny proces,
3. zmien pracovných pozícií a s nimi súvisiace zmeny v prístupových právach a potrebách pridelenia zariadení pre výkon práce,
4. ukončenie pracovného pomeru a odobratie prístupových práv a pridelených zariadení.

5.24.1 PROCES BUDOVANIA POVEDOMIA INFORMAČNEJ BEZPEČNOSTI

5.24.1.1 ČINNOSTI PRED NÁSTUPOM DO ZAMESTNANIA

Pri vzniku potreby na obsadenie pracovného miesta zabezpečí odbor ľudských zdrojov výber vhodných uchádzačov v zmysle [MHTH S21 Riadenie ľudských zdrojov](#).

Všetky spisy pri výberovom konaní sú dôverného charakteru a sú bezpečne uložené na odbore ľudských zdrojov, prípadne skartované. Prístup (nahliadnutie) do spisu výberového konania majú výhradne členovia výberového tímu (spravidla priamy nadriadený nového zamestnanca, recrutier, príp. HR BP).

5.24.1.2 Stanovenie prístupových práv k aktívam spoločnosti

V súlade s pracovnou pozíciou o prístupové práva pre zamestnanca žiada priamy nadriadený. Požiadavku schvaľuje príslušný gestor/vlastník a realizuje príslušný administrátor, ktorý zodpovedá za kompletnú prípravu pracovného miesta v súlade so zaužívanými štandardami, prípadné špeciálne požiadavky rieši podľa dohovoru s nadriadeným, vždy je informovaný MKB.

5.24.1.3 Zaškolenie v oblasti informačnej bezpečnosti

Pri nástupe je zamestnanec preukázateľne zaškolený v oblasti informačnej bezpečnosti. Školenie vykoná MKB predovšetkým informuje zamestnancov o:

- a) základných pravidiel používania autentizačných prostriedkov,
- b) klasifikácii aktív a ochrane aktív,

- c) spôsobe hlásenia incidentov,
- d) základoch antivírusovej ochrany,
- e) používaní internetu a elektronickej pošty,
- f) používaní softvéru (ochrana autorských práv),
- g) prípadných postihoch v prípade porušenia pravidiel informačnej/kybernetickej bezpečnosti.

5.24.1.4 Mlčanlivosť

Každý zo zamestnancov spoločnosti povinne podpisuje vyhlásenie o mlčanlivosti, ako súčasť pracovnej zmluvy.

Táto povinnosť mlčanlivosti platí počas celej existencie pracovného pomeru a po jeho zániku.

Porušenie povinnosti mlčanlivosti môže mať aj právne následky.

Partneri a subdodávatelia v zmluvnom vzťahu s organizáciou sú taktiež viazaní povinnosťou mlčanlivosti, ktorá sa uplatňuje v uzavretých zmluvách a aj vo vzorových podnikových zmluvách.

Základom pre uplatnenie zodpovednosti v prípade porušenia povinnosti mlčanlivosti je vyhlásenie o mlčanlivosti v pracovnej zmluve a v prípade cudzích osôb časť zmluvy o spolupráci týkajúca sa mlčanlivosti.

5.24.2 PERSONÁLNA BEZPEČNOSŤ POČAS ZAMESTNANIA

Počas pracovného pomeru je potrebné pri každej zmene zaradenia zamestnanca preskúmať jeho prístupové práva a prispôbiť ich novému stavu. O zmene zaradenia zamestnanca informuje odbor ľudských zdrojov cez ITSM nástroj. Vykonané zmeny sú uložené v ITSM nástroji. Evidencia, revalidácia a odoberanie prístupových práv sa vykonáva podľa interných nariadení pre riadenie prístupových práv.

5.24.3 ŠKOLENIA

Počas zamestnania sú zamestnanci pravidelne školení v oblasti IB a KB. Za organizáciu školení zodpovedá MKB.

Dodržiavanie pravidiel IB a KB kontroluje priebežne priamy nadriadený zamestnanca. Minimálne raz ročne MKB vykoná kontrolu dodržiavania pravidiel bezpečnosti.

Minimálne raz ročne zabezpečí oddelenie vzdelávania a HR služieb školenie / preškolenie pracovníkov na požiadavky IB a KB.

5.24.4 UKONČENIE ZAMESTNANIA

Pri ukončení pracovného pomeru, obdobného pracovnoprávneho vzťahu alebo iného zmluvného vzťahu je odbor ľudských zdrojov zodpovedný za informovanie úseku IT, aby k stanovenému dňu boli zamestnancovi odobraté prístupové práva (elektronický výstupný list).

V prípade okamžitého skončenia pracovného pomeru zo strany zamestnávateľa, alebo okamžitého skončenia pracovného pomeru zo strany zamestnanca je potrebné zvážiť okamžité zrušenie jeho prístupových práv.

Záznam o zrušení prístupových práv potvrdí Administrátor elektronicky na „Výstupnom liste“, ktorý je súčasťou spisu zamestnanca.

5.24.5 DISCIPLINÁRNY PROCES

Porušenie ustanovení pravidiel informačnej bezpečnosti vo vzťahu k politikám informačnej a kybernetickej bezpečnosti bude u zamestnancov považované za porušenie základných povinností zamestnanca (§ 81 písm. A), c), e) a f) Zákonníka práce) a je možné z neho vyvodit' príslušné pracovno-právne dôsledky, vrátane skončenia pracovného pomeru výpoveďou alebo okamžitým ukončením v zmysle platného [Pracovného poriadku](#).

Pri zistení porušenia pravidiel platných bezpečnostných politík (ďalej len „pravidlá“) MKB, alebo ním poverená osoba písomne alebo telefonicky na to upozorní zamestnanca, ktorý pravidlá

porušil; V prípade hrubého porušenia pravidiel, je na túto skutočnosť upozornený aj priamy nadriadený.

Opakované alebo hrubé porušenie pravidiel zo strany zamestnanca bude riešené nasledovne:

- dňom zistenia porušení pravidiel stráca zamestnanec právo používať služby informačných systémov a sietí zamestnávateľa,
- nadriadený zamestnanca s personálnou právomocou rozhodne o prípadnom pracovno-právnom postihu zamestnanca,
- prípadná trestno-právna zodpovednosť nie je týmto postupom dotknutá.

5.24.6 CIELE BUDOVANIA POVEDOMIA KYBERNETICKEJ A INFORMAČNEJ BEZPEČNOSTI (KIB)

Povedomie o kybernetickej a informačnej bezpečnosti je prvou líniou obrany pre bezpečnosť informačných systémov a sietí. Je to nevyhnutná požiadavka riadenia informačnej bezpečnosti, v prípade jej absencie sú náklady vynaložené na technickú a organizačnú bezpečnosť neefektívnym vynakladaním finančných prostriedkov.

Základné ciele na dosiahnutie a udržanie potrebnej úrovne bezpečnostného povedomia a kompetentnosti sú:

- zvyšovanie úrovne poznania zamestnancov a tretích strán o rizikách spojených s používaním ICT a možnostiach ochrany pred hrozbami.
- rozšírenie vzdelávania začlenením základov KIB do systému vzdelávania zamestnancov – nie len pri nástupe do zamestnania ale aj v priebehu celého životného cyklu zamestnania.
- zavedenie programov budovania bezpečnostného povedomia a kompetentnosti používateľov so špeciálnymi nárokmi na znalosť KIB (bezpečnostní špecialisti, analytici, programátori, audítori).

5.24.6.1 Definovanie kategórií

Pri definovaní kategórií sa vychádza z predpokladu, že každý účastník má také znalosti z KB, aby plnohodnotne pokryl plnenie svojich úloh, keďže nedostatočné vedomosti vedú k chybám z neznalosti.

S prihliadnutím na nutnosť kategorizácie zamestnancov, návrh definuje nasledovné kategórie používateľov IT:

- Zamestnanci používajúci k svojej práci prostriedky IT / informačné a telekomunikačné technológie/
- Manažéri a vedúci pracovníci
- Informatici bez špecializácie v IB
- Špecialisti v IB

5.24.6.2 OBSAH VZDELÁVANIA PRE JEDNOTLIVÉ KATEGÓRIE

Návrh vychádza z definície troch úrovní poznania a pre vyššie uvedené kategórie účastníkov digitálneho priestoru špecifikujeme, ktoré oblasti poznania a na akej úrovni by mali mať. Sú to:

Úroveň A

Znalosť vybraných základných pojmov a ich významu (schopnosť porozumieť pojmom, postupom, hotovým bezpečnostným riešeniam a vyvarovať sa základných rizík).

Úroveň B

Znalosť a použitie mechanizmov a procesov v bezpečnostných riešeniach (kvalifikovaná orientácia v oblasti, schopnosť zdôvodniť a realizovať navrhnuté riešenia).

Úroveň C

Schopnosť navrhovať, analyzovať, uplatniť a hodnotiť bezpečnostné požiadavky, riešenia a mechanizmy.

Návrh požadovanej úrovne znalostí pre jednotlivé kategórie používateľov IT prostriedkov:

Oblasti IB		Zamestnanci	Riadiaci zamestnanci	IT/OT špecialisti	IB/KB špecialisti
1	Manažment IB	A	A	B	B
2	Architektúra, modely a hodnotenie	-	A	B	C
3	Riadenie prístupu	A	A	B	B
4	Aplikačná bezpečnosť	A	B	C	C
5	Bezpečnosť prevádzky	A	A	C	C
6	Fyzická bezpečnosť	-	A	B	C
7	Kryptografia	A	A	B	C
8	Siete, internet, telekomunikácie	A	A	C	C
9	Incident Manažment	A	A	B	C
9	Plánovanie kontinuity činností	A	A	B	C
10	Ochrana osobných údajov – GDPR	A	B	C	C
11	Legislatíva a regulácie	A	B	A	C

5.24.7 BEZPEČNOSTNÉ ŠKOLENIA

5.24.7.1 VSTUPNÉ ŠKOLENIE

V súlade s plánom rozvoja bezpečnostného povedomia bude zabezpečené poučenie používateľov, administrátorov, osôb zastávajúcich bezpečnostné role a dodávateľov o ich povinnostiach a o bezpečnostnej politike formou vstupného školenia.

Vstupné vzdelávanie zamestnancov organizácie je riešené formou prezenčného (distančného) školenia pre prácu v informačnom systéme organizácie a zoznámenie so základnými pravidlami pracovníkmi úseku IT.

Vstupné školenia sa konajú najneskôr v deň nástupu nových zamestnancov, väčšinou k 1. a 15. dňu kalendárneho mesiaca. Iné termíny školenia, príp. absolvovanie online, po dohode so zodpovedným zamestnancom. Užívateľ je povinný sa školenia zúčastniť. Po zaškolení a oboznámení sa so základnými pravidlami, sa užívateľ písomne zaviaže podmienky dodržiavať. V prípade absolvovania školenia online, je potrebné zabezpečiť preukázateľné oboznámenie sa so školiacim materiálom.

5.24.7.2 PRAVIDELNÉ ŠKOLENIA

MKB spracuje a priebežne aktualizuje vzdelávací kurz pre základné zoznámenie užívateľov organizácie s problematikou informačnej a kybernetickej bezpečnosti, bezpečnostného povedomia pri práci s IS / IT organizácie v súlade s platnou legislatívou.

Povinnosť absolvovať školenia pre konkrétne role pracovníkov organizácie a frekvencia školení, je stanovená v pláne rozvoja bezpečnostného povedomia.

5.24.7.3 ODBORNÉ ŠKOLENIA

Pre osoby zastávajúce bezpečnostné úlohy v súlade s Plánom rozvoja bezpečnostného povedomia zabezpečí pravidelné odborné školenia príslušný riaditeľ úseku v spolupráci s odborom ľudských zdrojov, pričom vychádza z aktuálnych potrieb povinnej osoby v oblasti kybernetickej bezpečnosti.

V prípade potreby odborného školenia v oblasti kybernetickej bezpečnosti, je odovzdaná požiadavka na odbor ľudských zdrojov k zabezpečeniu odborného školenia.

5.24.7.4 HODNOTENIE ÚČINNOSTI

Za hodnotenie účinnosti plánu rozvoja bezpečnostného povedomia, vykonaných školení a ďalších činností spojených so zlepšovaním bezpečnostného povedomia zodpovedá MKB.

Oblasť vzdelávania a rozvoja bezpečnostného povedomia je tak isto podrobená kontrole v rámci pravidelného auditu kybernetickej bezpečnosti, prípadne ad hoc kontrolám a auditu podľa rozhodnutia Audítora kybernetickej bezpečnosti.

5.25 VYKONÁVANIE NÁPRAVNEJ A PREVENTÍVNEJ ČINNOSTI

5.25.1 ZÁSADY UPLATŇOVANIA NÁPRAVNEJ A PREVENTÍVNEJ ČINNOSTI

Uplatňovanie nápravnej a preventívnej činnosti je zabezpečované prijatím, realizáciou, kontrolou plnenia a vyhodnocovaním nápravných a preventívnych opatrení (NPO). Opatrenia sú zamerané na odstránenie a vylúčenie už existujúcich príčin a možných nezhôd alebo iných nežiadúcich situácií, predovšetkým ich opakovaného výskytu. Existujúce a možné nezhody sa vzťahujú k celému systému IB a KB.

Povinnosťou každého zamestnanca je všimnúť si, či sa vyskytla nejaká nezhoda predovšetkým na vlastnom pracovisku, resp. všimnúť si, či sa okolie, podmienky, prostredie atď. nemenia tak, že by nezhoda mohla nastať.

Každá už vzniknutá nezhoda sa rieši prijatím takých nápravných opatrení, realizáciou ktorých sa táto nezhoda odstráni. Možným nezhodám sa je potrebné vyhnúť systémovým prístupom založeným na prevencii. Prevencia spočíva v zisťovaní či už prišlo k nezhode, či sa sledovaný stav zhoršuje a či je stav vyhovujúci. Ak sa súčasný stav zhoršuje a v budúcnosti môže viesť k nezhode, je potrebné prijať preventívne opatrenia. Preventívne opatrenia môže navrhnúť každý zamestnanec zodpovednej osobe za útvar.

5.25.2 ZDROJE INFORMÁCIÍ PRE PRIJÍMANIE NÁPRAVNÝCH A PREVENTÍVNYCH OPATRENÍ

Informácie pre prijímanie NPO sú zistenia:

- z preverovania MKB (interné audity, dozorný audit a certifikačný audit, a pod.);
- z procesov vyplývajúcich z riadenia kybernetickej a informačnej bezpečnosti;
- z výsledkov kontrol;
- z reklamácií a sťažností;
- z dodávok prác, služieb a tovarov.

5.25.3 POSTUP UPLATŇOVANIA NÁPRAVNÝCH A PREVENTÍVNYCH OPATRENÍ

Nápravné opatrenia prijíma zodpovedný za útvar ku každej závažnej nezhode, ktorá už nastala. Pri prijímaní nápravných opatrení sa použije tento postup:

- zistenie nezhody a výkon operatívnej nápravy (v prípade, ak je to možné);
- kvantifikácia problému;

- analýza príčin, preskúmanie potreby aktualizovať analýzu rizík procesu alebo zainteresovanej strany;
- prijatie a dokumentovanie nápravných opatrení;
- realizácia nápravných opatrení;
- kontrola plnenia a vyhodnotenie účinnosti nápravných opatrení.

Pri prevencii vzniku možných nezhôd uplatňuje zodpovedný za útvary systémový prístup, ktorý realizuje nasledovne:

- monitorovanie a vyhodnocovanie zdrojov informácií o možných nezhodách;
- ak je vyhodnotenie stavu uspokojivé, proces môže pokračovať;
- vykonanie analýzy príčin zhoršeného stavu (ak vyhodnotenie poukazuje na nepriaznivé trendy vývoja);
- prijatie a dokumentovanie preventívnych opatrení;
- realizácia preventívnych opatrení;
- kontrola plnenia a vyhodnotenie účinnosti preventívnych opatrení.

5.25.4 ZISŤOVANIE NEZHÔD, ANALÝZA PRÍČIN VZNIKU NEZHÔD A SPÔSOB ICH VYSPORIADANIA

- a) V prípade ak sa zistí nehoda, zistenú nehodu oznámi zamestnanec svojmu nadriadenému, ktorý podľa stupňa závažnosti nehody rozhodne, či odstránenie nehody zabezpečí vo vlastnej kompetencii a to buď operatívne (bez prijatia NPO) alebo prijatím NPO. Nadriadený, ktorý je vedúcim organizačného útvaru na najvyššom stupni riadenia môže odstrániť nehodu vo vlastnej kompetencii alebo rozhodne o prijatí NPO (napr. formou Listu NPO, ktorý postúpi poverenej osobe).
- b) Každý zamestnanec zodpovedný za útvary po hlásení zistenej nehody hľadá možnosti riešenia vzniknutej situácie so zainteresovanými zamestnancami. Ak sa nedarí príčiny nehody odstrániť, problém rieši so svojim nadriadeným, prípadne vedúci organizačného útvaru na najvyššom stupni riadenia rozhodne o prijatí NPO.
- c) Každý zodpovedný za útvary vykonáva analýzu príčin v procese riešenia nezhôd na organizačných útvaroch na jednotlivých stupňoch riadenia, v ktorých sa nehoda vyskytla alebo môže vyskytnúť. Podľa potreby môže zodpovedný za útvary prizvať aj zamestnancov organizačných útvarov na vyššom stupni riadenia alebo zamestnancov iných organizačných útvarov.
- d) Pri odstraňovaní nezhôd sa postupuje podľa ich závažnosti. Jednoduché problémy sú riešené operatívne a príslušné opatrenia sa nedokumentujú. Ich realizáciu a účinnosť kontroluje príslušný zodpovedný za útvary. O nehode a jej riešení informuje svojho nadriadeného. Pri riešení závažnejších nezhôd (prijatí, realizácii a kontrole NPO) postupuje zodpovedný za útvary na jednotlivých riadiacich stupňoch spôsobom podľa pokynov vyššie.
- e) Z hľadiska prevencie možných nezhôd sa analýza vykoná vtedy, keď informácie zo sledovaných zdrojov signalizujú zhoršenie stavu. O prijatí, realizácii a kontrole preventívneho opatrenia na odstránenie vzniku potencionálnej nehody, rozhoduje zodpovedný za útvary podľa stupňa závažnosti nehody spôsobom podľa pokynov vyššie.

5.25.5 PRIJÍMANIE A SCHVAĽOVANIE NÁPRAVNÝCH A PREVENTÍVNYCH OPATRENÍ

Zodpovedný za útvary prijíma NPO k zisteniam/odporúčaniam

- z interného auditu v zmysle platnej [MHTH S30 Interné audity](#).

- k zisteniam z ostatných previerok MKB (certifikačný audit, dozorný audit, recertifikačný audit, ročná správa o hodnotení) do 10 pracovných dní od doručenia správy, resp. prerokovania správy manažmentom úradu,
- k zisteniam z ďalších oblastí (z procesov, z výsledkov kontrol, z reklamácií a sťažností, z dodávok prác, služieb a tovarov) neodkladne po zistení nezhody, najneskôr však do 5 pracovných dní.

Obdobne sú prijímané aj preventívne opatrenia na odstránenie vzniku potencionálnej nezhody.

5.25.6 ZAVEDENIE A KONTROLA NÁPRAVNÝCH A PREVENTÍVNYCH OPATRENÍ

- Kontrolu plnenia a vyhodnotenie účinnosti zavedených opatrení vykonáva (v stanovenom termíne na splnenie opatrenia, resp. na mimoriadne vyžiadanie poverenej osoby) zodpovedný útvar. O výsledku informuje svojho nadriadeného a poverenú osobu zaslaním vyhodnotenia NPO.
- Súhrnné vyhodnotenie plnenia a účinnosti prijatých a realizovaných NPO vykonáva každoročne poverená osoba (na základe hodnotení predkladaných zodpovednými za útvar/úsek) a predkladá ho na prerokovanie manažmentu.

5.26 INTERNÝ AUDIT

5.26.1 ÚČEL, ROZSAH A UŽÍVATEĽOV

Všetky súvisiace činnosti s interným auditom, ako napr. príprava programu auditu, výber audítora, vedenie jednotlivých auditov a podávanie správ sú zadefinované v smernici [MHTH_S30 Interné auditu](#) a nazývame ich interná kontrola.

Cieľom interného auditu vo vzťahu k požiadavkám KIB, je určiť, či postupy, kontroly, procesy, mechanizmy a ďalšie činnosti v rámci IB a KB a BCM sú v súlade s ISO 27001, normami ISO 22301, príp. NIST framework a IEC62443, platnými predpismi, internou dokumentáciou spoločnosti. Účinne zaviesť, udržiavať a spĺňať požiadavky bezpečnostnej politiky.

5.26.2 PLÁNOVANIE INTERNÉHO AUDITU

MKB schvaľuje ročný program pre interný audit.

Interné auditu by sa mali vykonávať v priebehu jedného roka pre zabezpečenie pokrytia celého rozsahu IB a KB. Interné auditu sú plánované podľa úrovne rizík pre jednotlivé oblasti a podľa výsledkov z predchádzajúcich auditov.

Ročný plán interného auditu musí obsahovať nasledovné informácie o každom individuálnom internom audite:

- Obdobie auditu (s uvedením dátumu, alebo mesiaca, v ktorom sa plánuje audit)
- Rozsah auditu (oddelenia, procesy, doložky štandard, atď.)
- Audítorské kritériá (normy, legislatívu a predpisy, interná dokumentácia, firemné štandardy a zmluvné záväzky)
- Metóda auditu (preskúmanie dokumentácie, rozhovory so zamestnancami, preskúmanie záznamov, preskúmanie informačných systémov, atď.)
- Audítori, ktorí budú vykonávať audit (ak existuje viac ako jeden audítor, určiť vedúceho tímu auditu)

Vykonané auditu musia byť zaznamenané v programe ročných interných auditov.

PZS je povinný preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek ZoKB vykonaním auditu kybernetickej bezpečnosti a to v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov

- po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a
- v určenom časovom intervale.

Audit vykonaný nezávislým audítorom KB, vykonávaný podľa požiadaviek ZoKB môže nahradiť opakovaný ročný interný audit.

5.26.3 MENOVANIE INTERNÝCH AUDÍTOROV

CEO vymenuje interných audítorov.

Interný audítor môže byť zamestnanec spoločnosti alebo osoba mimo spoločnosti. Kritériá vymenovania interného audítora sú:

- znalosť ISO/IEC 27001, resp. metodiky pre audit podľa ZoKB (príp. normy ISO 22301)
- znalosti techník systému riadenia auditu
- znalosti informačných a komunikačných technológií, znalosť IT procesov a IT security procesov

Interní audítori musia byť vybraní tak, aby sa zabezpečila objektivnosť a nestrannosť, t. j. vyhnúť sa konfliktu záujmov, pretože audítori nie sú oprávnení auditovať ich vlastnú prácu.

Odporúča sa absolvovať kurz interných audítorov podľa ISO/IEC 27001.

5.26.4 VEDENIE JEDNOTLIVÝCH INTERNÝCH AUDITOV

Osoby zodpovedné za jednotlivé interné audity sú identifikované v ročnom pláne interných auditov. Ak audit vykonáva tím pozostávajúci z niekoľkých audítorov, osoba zodpovedná za audit je vedúci audítor.

Zohľadnenie kritérií počas vnútorného auditu:

- kritéria stanovené v programe ročného vnútorného auditu
- výsledky predchádzajúcich interných alebo externých auditov
- výsledky hodnotenia rizík, kontroly implementácie, analýza vplyvu podnikania, atď.
- vnútorný audit kontrolný

Výsledok auditu musí byť zdokumentovaný a reportovaný a:

- výsledok interného auditu musí byť zaslaný na MKB
- nápravné opatrenia musia byť zdokumentované vo formulári nápravné opatrenia.

5.27 METODIKA RIADENIA RIZÍK INFORMAČNÝCH AKTÍV

5.27.1 PRIORITY A CIELE ANALÝZY RIZÍK

Informačné aktíva pre väčšinu organizácií predstavujú súčasnú, alebo potenciálnu hodnotu a preto musia byť primeraným spôsobom chránené. Bezpečnosť informačných aktív je založená na udržiavaní akceptovateľnej miery identifikovaného rizika prostredníctvom komplexných procesov a činností zameraných na odvrátenie, alebo zmenšenie identifikovaných rizík, resp. prejavov a dopadov hrozieb, ktoré pôsobia na informačné aktíva.

Podľa všeobecnej definície je riziko chápané ako „vplyv neistoty na ciele“. Termín „kybernetické bezpečnostné riziko“ je tiež ekvivalentom výrazu „IT riziko“.

5.27.2 ZÁSADY NAVRHOVANEJ METODIKY

Analýza rizík má slúžiť k podrobnému rozboru stavu kybernetickej a informačnej bezpečnosti v MHTH. Cieľom analýzy rizík má byť identifikácia okolností, ktoré potenciálne môžu narušiť bezpečnosť (t.j. zraniteľností, hrozieb a škodlivých udalostí).

Výsledkom analýzy rizík musí byť ohodnotený zoznam identifikovaných rizík a návrh bezpečnostných opatrení, ktoré slúžia na ošetrovanie týchto rizík.

Preferovanou metódou ošetrovania rizika má byť redukcia rizika na akceptovateľnú úroveň. Riziká majú byť primárne ošetrované v poradí od najvyšších po najnižšie.

Analýza rizík musí byť vykonaná v takom detaile, ktorý umožní určiť, či je riziko akceptovateľné (t.j. či hodnota zvyškového rizika je na zanedbateľnej úrovni).

Odhad pravdepodobnosti zohľadňuje najpravdepodobnejšiu kombináciu hrozieb, ktorej je následne priradená slovná, alebo číselná hodnota pravdepodobnosti naplnenia, v rámci stanovenej metriky.

Odhad závažnosti potenciálnych dopadov zohľadňuje najhorší možný dopad hrozieb, ktorému je následne priradená slovná, alebo číselná hodnota závažnosti dopadu, v rámci stanovenej metriky.

Vyhodnotenie výsledného rizika je vyjadrené ako násobok odhadu pravdepodobnosti a odhadu závažnosti dopadov plynúcich z možného naplnenia hrozby, škodlivej udalosti, alebo kombinácie hrozieb, po zohľadnení existujúcich bezpečnostných opatrení.

Identifikované zraniteľnosti, hrozby, potenciálne škodlivé udalosti sú sumarizované do konkrétnych scenárov rizík, v kontexte príslušného informačného aktíva.

Pre riziká týkajúce sa okolia, na ktoré v rámci analýzy rizík konkrétného aktíva nie je dosah, sú bezpečnostné opatrenia popísané formou požiadaviek, resp. odporúčaní na okolie.

5.27.3 PREHL'AD PROCESOV RIADENIA RIZÍK

Analýza rizík je základnou súčasťou riadenia IB a KB a pozostáva z viacerých navzájom prepojených častí, a to:

- Klasifikácia aktív v projekte,
- Zoznam analyzovaných aktív a pôsobiacich hrozieb na tieto aktíva,
- Vyhodnotenie rizík,
- Návrh bezpečnostných opatrení,
- Zhmutie výsledkov analýzy rizík.

Proces riadenia rizík podľa ISO27005 popisuje obr. Určenie kontextu – predstavuje popis vnútorného a vonkajšieho prostredia, v ktorom sa MHTH snaží o dosiahnutie svojich cieľov. Následne sa vykonáva posúdenie rizika. Riziko sa znižuje opatreniami na zníženie rizika až na prijateľnú úroveň rizika.

Ak sú opatrenia na zníženie rizika nedostatočné, nasleduje ďalšia iterácia posúdenia rizík a definovanie prídavných bezpečnostných opatrení.

Ošetrovanie rizika je vykonávanie cyklického procesu pozostávajúceho z nasledujúcich zložiek:

- Posúdenie/ošetrovanie rizika,
- rozhodnutie, či zvyškové riziko je prijateľné,
- vytvorenie nového ošetrovania rizika, ak úroveň rizika nie je prijateľná,
- posúdenie účinnosti ošetrovania.



1. Identifikácia a klasifikácia informačných aktív
2. Identifikácia relevantných zraniteľností a hrozieb
3. Posúdenie rizika:
 - a) určenie hodnoty pravdepodobnosti jednotlivých hrozieb v súvislosti s daným aktívom a zraniteľnosťou,
 - b) určenie hodnoty dopadu jednotlivých hrozieb v súvislosti s daným aktívom a zraniteľnosťou,
 - c) výpočet úrovne závažnosti výsledných rizík,
 - d) klasifikácia úrovni závažnosti rizík,
 - e) zníženie rizika na akceptovateľnú úroveň,
 - f) akceptácia zvyškového rizika.

113 z 129

1. Objekt (sídlo, lokalita, zóna, všetky fyzické priestory organizácie, organizačná štruktúra)
2. Hardvér
3. Softvér
4. Komunikácia (sieť, všetky telekomunikačné zariadenia slúžiace na prepojenie)
5. Dokumenty
6. Personál (personál, vedenie, používatelia, administrátori, dodávatelia a tretie strany)
7. Procesy

5.27.4 ZOZNAM RELEVANTNÝCH ZRANITEĽNOSTÍ A HROZIEB

Zraniteľnosti sú slabé miesta v postupoch, manažmente, MHTH, personálnej oblasti, hardvéri, softvéri, komunikačnom zariadení a vo fyzickom prostredí, ktoré môžu byť využité pri hrozbe. Zraniteľnosť konkrétneho aktíva je určovaná vo vzťahu ku každej hrozbe osobitne, ktorá by mohla túto zraniteľnosť v špecifickej situácii využiť. Identifikácia zraniteľností je vykonaná prostredníctvom príkladov zraniteľností uvedených v STN ISO/IEC 27005, podľa znalostí a zverejnených slabín použitých technológií v informačnom systéme a využitých organizačných opatrení na riadenie informačnej bezpečnosti posudzovaného systému.

Zoznam zraniteľností vychádza z STN ISO 27005, ktorá pokrýva manažment rizík informačných systémov. Zoznam je doplnený o zraniteľnosti uvedené v štandardoch BSI a NIST.

5.27.5 ODHAD DOPADOV HROZBY PRI NAPLNENÍ SCENÁRA RIZIKA

Pri ohodnocovaní závažnosti dopadov v rámci jednotlivých scenárov rizík sú dopady klasifikované podľa úrovne ich závažnosti. Úroveň závažnosti dopadov je vyjadrená podľa nasledovných významov:

Dopad	Popis	Hodnota
Zanedbateľný	Dopad akceptovateľného charakteru, ktorý môže byť zvládnutý v rámci plnenia bežných pracovných povinností bez potreby dodatočných zdrojov na odstránenie dôsledkov.	5
Minimálny	Dopad neakceptovateľného charakteru, ktorý však môže byť zvládnutý v rámci plnenia bežných pracovných povinností s minimálnymi personálnymi a finančnými nárokmi.	20
Stredný	Dopad neakceptovateľného charakteru, ktorý nie je zvládnuteľný v rámci plnenia bežných pracovných povinností a generuje mimoriadne personálne a finančné nároky (napr. zapojenie externých špecialistov a zdroje nad rámec bežného rozpočtu).	50
Závažný	Prerušenie výkonu určitej konkrétnej služby alebo spôsobenie preukázateľného narušenia bezpečnosti, výdavky na riešenie bezpečnostného incidentu, zvýšené nároky na použitie mimoriadnych personálnych a finančných zdrojov na odstránenie dôsledkov, resp. prerušenie stredne významných činností.	70
Katastrofický	Zásadné ohrozenie výkonu a funkčnosti primárnych procesov, kľúčových aktív; v extrémnom prípade ohrozenie bezpečnosti až existencie kritických aktív vo veľkom rozsahu, resp. celej organizácie.	100

Tabuľka hodnotenia dopadov

Do výsledného posúdenia budú zahrnuté len tieto identifikované hrozby. Pre každú z týchto hrozieb sa musí jednotlivo určiť hodnota jej pravdepodobnosti a určiť hodnota dopadu.

5.27.6 URČENIE HODNOTY PRAVDEPODOBNOTI HROZIEB

Na určenie celkovej pravdepodobnosti, ktorá naznačuje šancu, že potenciálna zraniteľnosť môže byť zneužitá v rámci existujúcej infraštruktúry a prostredia, musia byť zvážené nasledujúce faktory:

1. motivácia a zdatnosť zdroja hrozby,
2. podstata zraniteľnosti,
3. existencia a efektivita aktuálne uplatnených opatrení.

Pri stanovovaní pravdepodobnosti je potrebné prihliadať aj na frekvenciu výskytu incidentov v minulosti, ktorých podstatou bolo zneužitie príslušnej zraniteľnosti. Ak takýto údaj existuje, mal by byť v súlade so stanovenou úrovňou pravdepodobnosti.

Pravdepodobnosť, že potenciálna zraniteľnosť môže byť zneužitá zo strany zdroja hrozby, môže byť popísaná ako vysoká, stredná, nízka alebo veľmi nízka. Podrobnejšie rozdelenie a popis je v nasledujúcej tabuľke:

Pravdepodobnosť	%	Frekvencia slovne	Pravdepodobnosť popisne	Hodnota
Vysoká	81 – 100	Veľmi často	Zdroj hrozby je vysoko motivovaný a je dostatočne technicky zdatný; uplatnené opatrenia na prevenciu identifikovanej zraniteľnosti sú neefektívne. Existuje skúsenosť z minulosti, že daná zraniteľnosť bola už mnohokrát zneužitá.	1
Stredná	51 – 80	Často	Zdroj hrozby je motivovaný a technicky zdatný; uplatnené opatrenia čiastočne bránia úspešnému zneužitiu zraniteľností. Existuje skúsenosť z minulosti, že daná zraniteľnosť bola už niekoľkokrát zneužitá.	0,8
Nízka	11 – 50	Niekedy	Zdroj hrozby nemá dostatočnú motiváciu ani zručnosti; uplatnené opatrenia preventívne predchádzajú a významným spôsobom zabraňujú zneužitiu zraniteľností. Z minulosti existuje ojedinelá skúsenosť zneužitia danej zraniteľnosti.	0,5
Veľmi nízka	0 – 10	Málokedy	Zdroj hrozby nemá dostatočnú motiváciu ani zručnosti; uplatnené opatrenia preventívne predchádzajú a významným spôsobom zabraňujú zneužitiu zraniteľností. Neexistuje historická skúsenosť so zneužitím danej zraniteľnosti.	0,1

Tabuľka hodnotenia pravdepodobnosti

5.27.6.1 Výpočet úrovne závažnosti rizík

Úroveň závažnosti rizika [R] je vyhodnocovaná ako násobok stanovenej pravdepodobnosti rizika [P] a stanoveného dopadu rizika [D]. Všeobecne je funkcia pre výpočet rizika v prístupe orientovanom na hrozby uvádzaná ako:

$$R = P \times D$$

Pre jednotlivé aktíva sú hodnotené len tie položky z katalógu hrozieb, ktoré sú relevantné pre konkrétne aktívum. Pre každú z relevantných hrozieb pre príslušné aktívum sa vypočíta úroveň závažnosti rizika. Výsledná hodnota úrovne závažnosti rizika v kontexte informačného aktíva [R] bude potom súčtom rizika každej z relevantných hrozieb z referenčného katalógu hrozieb, t.j.:

$$R = \sum R_1 \dots R_n$$

Riziková expozícia informačného aktíva sa vypočítava ako aritmetický priemer tak, že súčet rizík relevantných hrozieb vstupujúcich do scenára sa vydolí počtom relevantných hrozieb vstupujúcich do scenára.

5.27.6.2 Stanovenie jednotného indexu rizika

Pre stanovenie úrovne závažnosti rizika v metodike riadenia rizika je možné použiť napr. nasledovný index:

Úroveň závažnosti	Dolný interval	Horný interval
Mimoriadne závažné	81	100
Vysoké	51	80
Nízke	21	50
Zanedbateľné	1	20

5.27.7 OŠETROVANIE RIZIKA

Metódy ošetrovania rizika

Pri výbere a prijímaní opatrení sa zohľadňujú nasledovné základné prístupy k riziku:

Zníženie rizika

Zníženie rizika je najčastejšou metódou ošetrovania rizika. Uplatnený je výber vhodných opatrení tak, aby riziko bolo znížené až na úroveň zvyškového rizika, ktoré môže byť následne prehodnotené ako akceptovateľné.

Zníženie rizika je možné dosiahnuť pomocou vhodných opatrení na zníženie následkov rizika alebo na zníženie pravdepodobnosti realizácie rizika (napr. pri riziku útoku na IS alebo infiltrácie zo siete internet sa nasadia adekvátne nakonfigurované firewally a ďalšie bezpečnostné nástroje).

Vyhnutie sa riziku

Keď je identifikované riziko považované za príliš vysoké, alebo náklady na implementáciu ošetrovania rizika presahujú prínosy, rozhodnutím môže byť aj úplné vyhnutie sa riziku, a to nevykonaním plánovanej alebo existujúcej aktivity alebo súboru aktivít, resp. zmenou podmienok, podľa ktorých bude činnosť vykonávaná.

Najčastejším spôsobom vyhnutia sa riziku je rozhodnutie zmeniť prostredie, v ktorom sa riziko vyskytuje tak, aby toto riziko neprichádzalo do úvahy (napr. v prípade ohrozenia dôvernosti údajov pri ich prenose nedôveryhodným komunikačným kanálom sa použije iný komunikačný kanál).

Presun rizika

Presun rizika je metóda ošetrovania rizika, pri ktorej bude určitá časť následkov rizika zdieľaná s externými subjektmi. Typickým presunom rizika je poistenie, alebo výber zmluvného partnera, ktorého úlohou bude monitorovať proces a prijať okamžité opatrenia na zastavenie hrozby skôr, ako vznikne škoda (napr. pri zvýšenom riziku požiaru sa MHTH poistí proti stratám spôsobeným požiarom).

Zachovanie rizika

Ak úroveň rizika spĺňa kritériá na akceptáciu rizika, nie je potrebné implementovať opatrenia a riziko môže zostať zachované v pôvodne ohodnotenej úrovni.

Návrh bezpečnostných opatrení

V zmysle všeobecných zásad tejto metodiky majú byť riziká ošetrované v poradí od najvyšších po najnižšie. Bezpečnostné opatrenia musia byť preto prijímané v závislosti na stanovenej úrovni rizika.

Návrh opatrení v závislosti na stanovenej úrovni závažnosti rizika:

Závažnosť rizika	Úroveň závažnosti rizika	Opatrenia
A	Mimoriadne vysoké riziko	Rozšírené a dodatočné bezpečnostné opatrenia sú bezpodmienečne nutné a je nutné prijať ich bezodkladne. Výkon kľúčových procesov a ďalšia prevádzka systému je podmienená prijatím opatrení.
B	Vysoké riziko	Rozšírené a dodatočné bezpečnostné opatrenia sú potrebné a mali by byť prijaté v dohľadnej dobe. Výkon kľúčových procesov organizácie ani prevádzka systému sa nepovažujú za akútne ohrozené.
C	Nízke riziko	Vlastník aktíva musí stanoviť, či je nutné prijať rozšírené bezpečnostné opatrenia, alebo či v minulosti prijaté opatrenia sú ešte potrebné. Riziko je možné akceptovať ako prijateľné len v prípade, že boli prijaté rozšírené bezpečnostné opatrenia.
D	Zanedbateľné riziko	Nie je nutné prijať dodatočné ani rozšírené bezpečnostné opatrenia. Riziko je možné akceptovať ako prijateľné.

Návrh bezpečnostných opatrení vychádza z nasledovných princípov:

- 1) pri návrhu opatrení sa vychádza z hodnoty a charakteru výsledného rizika určeného podľa stanovenej metodiky,
- 2) pre každé výsledné riziko, ktoré nie je akceptovateľné, je popísaný spôsob jeho ošetrenia pomocou navrhovaných bezpečnostných opatrení,
- 3) opatrenia sú navrhované v kontexte identifikovaných hrozieb,
- 4) cieľom je navrhnuť systém bezpečnostných opatrení takým spôsobom, aby po ich implementácii boli všetky riziká znížené na úroveň zodpovedajúcu akceptovateľným rizikám.

Postupnosť, akou budú navrhované opatrenia realizované, tzv. implementačný plán, je rozpracovaná v rámci bezpečnostnej stratégie (kap. 4). Tento program závisí od viacerých faktorov, ktoré je potrebné pri jeho návrhu zohľadniť. K takýmto faktorom prináležia:

- 1) priority vyplývajúce z ohodnotenia rizík,
- 2) výška nákladov potrebných na realizáciu opatrení,
- 3) pripravenosť a spôsobilosť organizácie na realizáciu opatrení (technická, organizačná, finančná),
- 4) podpora manažmentu organizácie na realizáciu opatrení.

5.27.8 AKCEPTÁCIA ZVÝŠKOVÉHO RIZIKA

5.27.8.1 Zvyškové riziko

Zvyškové je také riziko, ktorého hodnota po komplexnom ošetrení rizík implementáciou pôvodných, dodatočných a rozšírených opatrení je taká nízka, že je pre organizáciu prijateľné a nie je nutné uplatniť ďalšie opatrenia na jeho zníženie.

Výsledné riziko môže byť v rámci analýzy rizík označené ako akceptovateľné len za predpokladu splnenia nasledovných podmienok:

- 1) pravdepodobnosť realizácie rizika je príliš nízka,
- 2) straty spôsobené realizáciou rizika sú nepatrné,
- 3) realizácia rizika výrazne nenaruší stanovenú / očakávanú úroveň bezpečnosti,
- 4) opatrenia minimalizujúce pravdepodobnosť jeho realizácie sú nákladnejšie ako prípadné straty,
- 5) opatrenia minimalizujúce pravdepodobnosť jeho realizácie výrazne prevyšujú štandardnú úroveň bezpečnosti v prostredí nasadenia,
- 6) pri presune rizika na iný subjekt.

Referenčná hodnota zvyškového rizika by mala byť stanovená na takej úrovni, aby riziko bolo možné zanedbať. Keďže zvyškové riziko musí byť zanedbateľné, vylučuje to možnosť označiť vysoké riziko za zvyškové.

5.27.8.2 Kritériá akceptácie zvyškového rizika

Návrhy možných prístupov (resp. hodnotiacich kritérií) pre prijatie zvyškového rizika:

1. vyjadrenie kritérií prijatia rizika ako pomeru odhadnutého zisku (alebo iného podnikateľského prospechu) k odhadnutému riziku
2. stanovenie rôznych tried rizík (napr. rizík ktoré by mohli viesť k nesúladu s právnymi a regulačnými požiadavkami, resp. rizík stanovených zmluvnými požiadavkami)
3. požiadavky na budúce dodatočné ošetrovanie (napr. riziko môže byť prijaté, ak existuje schválenie a záväzok zníženia rizika na prijateľnú úroveň v stanovenom časovom období)

Kritériá prijatia rizík sa môžu líšiť v závislosti na tom, ako dlho sa očakáva, že riziko bude existovať, napr. riziko môže byť spojené s dočasnou, alebo krátkodobou aktivitou. Kritériá pre prijatie rizika by mali byť stanovené so zreteľom na:

- Obchodné požiadavky
- Právne a regulačné aspekty
- Bežnú prevádzku
- Technológie
- Financie
- Sociálne a humanitárne faktory

5.27.8.3 Proces akceptácie rizika

Akceptácia zvyškového rizika je proces, v ktorom štatutár alebo štatutárnym zástupcom poverený organizačný útvar formálne odsúhlasí eskalované zvyškové riziko.

Všetky akceptované riziká musia byť prehodnocované minimálne raz ročne a to až do doby, pokiaľ riziko neprestane byť relevantné, alebo sa nepristúpi k inému spôsobu ošetrovania identifikovaného a trvajúceho rizika.

Predložené riziká sú posudzované štatutárom ako vlastníkom rizík, spravidla na Porade vedenia.

5.28 OCHRANA OSOBNÝCH ÚDAJOV V SÚLADE S POŽIADAVKAMI GDPR

Spoločnosť s cieľom zaistiť vysokú úroveň ochrany osobných údajov, a to aj s prihliadnutím na úroveň potenciálneho rizika pri spracúvaní osobných údajov, prijala zoznam adekvátnych technických a organizačných opatrení (bezpečnostné opatrenia).

Spoločnosť vypracovala smernicu [MHTH_S06 Smernica o ochrane osobných údajov](#).

5.28.1 TECHNICKÉ OPATRENIA

5.28.1.1 Technické opatrenia realizované prostriedkami fyzickej povahy

- Zabezpečenie objektu pomocou mechanických zábranných prostriedkov (napr. uzamykateľné dvere, okná, mreže) a v prípade potreby aj pomocou technických zabezpečovacích prostriedkov (napr. elektrický zabezpečovací systém objektu, elektrická požiarňa signalizácia).

- Zabezpečenie chráneného priestoru jeho oddelením od ostatných častí objektu (napr. steny, zábrany v podobe prepážok, mreží alebo presklenia).
- Umiestnenie dôležitých prostriedkov informačných technológií v chránenom priestore a ochrana IT/OT infraštruktúry pred fyzickým prístupom neoprávnených osôb a nepriaznivými vplyvmi okolia.
- Bezpečné uloženie fyzických nosičov osobných údajov vrátane bezpečného uloženia listinných dokumentov.
- Opatrenie na zamedzenie náhodného prečítania osobných údajov zo zobrazovacích jednotiek (napr. vhodné umiestnenie zobrazovacích jednotiek).

5.28.1.2 Ochrana pred neoprávneným prístupom

- Šifrová ochrana uložených a prenášaných údajov, pravidiel pre kryptografické opatrenia.
- Pravidlá prístupu tretích strán k informačnému systému, ak k takému prístupu dochádza.

5.28.1.3 Riadenie prístupu oprávnených osôb

- Riadenie prístupov a opatrenia na zaručene platných politík riadenia prístupov (napr. identifikácia, autentizácia a autorizácia osôb v informačnom systéme).
- Riadenie privilegovaných prístupov v informačnom systéme.
- Zaznamenávanie prístupu a aktivít poverených osôb v informačnom systéme.

5.28.1.4 Riadenie zraniteľností

- Opatrenia na detekciu a odstránenie škodlivého kódu a nápravu následkov škodlivého kódu.
- Ochrana pred nevyžiadanou elektronickou poštou.
- Používanie legálneho a prevádzkovateľom schváleného softvéru.
- Opatrenia na zaručenie pravidelnej aktualizácie operačných systémov a programového aplikačného vybavenia.
- Pravidlá sťahovania súborov z verejne prístupnej počítačovej siete a spôsob ich overovania. Filtrovanie sieťovej komunikácie.
- Zhromažďovanie informácií o technických zraniteľnostiach informačných systémov, vyhodnocovanie úrovne rizík a implementácia opatrení na potlačenie týchto rizík.

5.28.1.5 Sieťová bezpečnosť

- Kontrola, obmedzenie alebo zamedzenie prepojenia informačného systému, v ktorom sú spracúvané osobné údaje s verejne prístupnou počítačovou sieťou
- Ochrana vonkajšieho a vnútorného prostredia prostredníctvom nástrojov sieťovej bezpečnosti (napr. firewall), segmentácia počítačovej siete.
- Pravidlá prístupu do verejne prístupnej počítačovej siete, opatrenia na zamedzenie pripojenia k určitým adresám, pravidlá používania sieťových protokolov.
- Ochrana proti iným hrozbám pochádzajúcim z verejne prístupnej počítačovej siete (napr. hackerský útok).
- Aktualizácia operačného systému a programového aplikačného vybavenia.

5.28.1.6 Zálohovanie

- Test funkčnosti záložných dátových nosičov.
- Vytváranie záloh s vopred zvolenou periodicitou.
- Určenie doby uchovávanía záloh a kontrola je dodržiavania.
- Test obnovy informačného systému so zálohami.

- Bezpečné ukladanie záloh.

5.28.1.7 Likvidácia osobných údajov a dátových nosičov

- Technické opatrenia na bezpečné vymazanie osobných údajov z dátových nosičov.
- Zariadenie na mechanické zničenie dátových nosičov osobných údajov (napr. zariadenie na skartovanie listín a dátových médií).

5.28.2 ORGANIZAČNÉ OPATRENIA

5.28.2.1 Personálne opatrenia

- Poverenie osoby prevádzkovateľom alebo sprostredkovateľom, ktorý má prístup k osobným údajom.
- Pokyny prevádzkovateľa na spracúvanie osobných údajov, najmä:
- Vymedzenie osobných údajov, ku ktorým má mať konkrétna osoba prístup na plnenie jej povinností alebo úloh,
- Určenie postupov, ktoré je poverená osoba povinná uplatňovať pri spracúvaní osobných údajov,
- Vymedzenie základných postupov alebo operácií s osobnými údajmi,
- Vymedzenie zodpovednosti za porušenie zákona,
- Poučenie poverených osôb o postupoch spojených s automatizovanými prostriedkami spracúvania a súvisiacich právach a povinnostiach (v priestoroch prevádzkovateľa a mimo týchto priestorov),
- Určenie zodpovednej osoby podľa § 44 zákona,
- Vzdelávanie poverených osôb (napr. právna oblasť, oblasť informačných technológií),
- Postup pri ukončení pracovného alebo obdobného pracovného vzťahu alebo obdobného pomeru poverenej osoby (napr. odovzdanie pridelených aktív, zrušenie prístupových práv, poučenie o následkoch porušenia zákonnej alebo zmluvnej povinnosti mlčanlivosti),
- Práca na diaľku a pravidlá mobilného spracovania dát.

5.28.2.2 Riadenie aktív

- Technické, organizačné a personálne opatrenia na vedenie inventárneho zoznamu aktív a jeho pravidelná aktualizácia.
- Evidencia všetkých miest prepojenia sietí vrátane prepojení s verejne prístupnou počítačovou sieťou.
- Určenie vlastníctva aktív a zodpovednosti za riziká.
- Pravidlá a postupy klasifikácie informácií.
- Pravidlá a postupy na označovanie informácií a zaobchádzanie s nimi v súlade s platnou klasifikačnou schémou.
- Pravidlá na prijateľné používanie informácií a aktív spojených s prostriedkami na spracúvanie informácií.
- Opatrenia na vrátenie aktív (napr. prostriedkov spracúvania osobných údajov) patriacich prevádzkovateľovi po ukončení pracovného pomeru, po vypršaní uzatvorenej dohody alebo zmluvy, pri zmene pracovného miesta alebo pracovného zaradenia a pod.

5.28.2.3 Riadenie prístupu oprávnených osôb k osobným údajom

- Pravidlá fyzického vstupu do objektu a chránených priestorov prevádzkovateľa
- Správa prístupových prostriedkov a zariadení do objektov (individuálne pridelenie kľúčov, elektronických kľúčov, vstupných kariet a bezpečné ukladanie ich rezerv).
- Pravidlá pridelovania prístupových práv a úrovni prístupu (rolí) povereným osobám.

- Politika hesiel a pravidiel používania autorizačných a autentizačných prostriedkov.
- Pravidlá vzájomného zastupovania poverených osôb (napr. pri nehode, dočasnej pracovnej neschopnosti, ukončení pracovného alebo obdobného pomeru).
- Pravidlá odstránenia alebo zmeny prístupových práv poverených osôb a zariadení na spracúvanie informácií pri ukončení zamestnania, zmluvy alebo dohody, alebo prispôbenie zmenám rolí.

5.28.2.4 Spracúvanie osobných údajov

- Pravidlá spracúvania osobných údajov v chránenom priestore.
- Nepretržitá prítomnosť oprávnenej osoby v chránenom priestore, ak sa v ňom nachádzajú aj iné ako oprávnené osoby.
- Režim údržby a upratovania chránených priestorov.
- Pravidlá spracúvania osobných údajov mimo chráneného priestoru, ak sa také spracúvanie predpokladá.
- Pravidlá manipulácie s fyzickými nosičmi osobných údajov (napr. listiny, fotografie) mimo chránených priestorov a vymedzenie zodpovednosti.
- Pravidlá používania automatizovaných prostriedkov spracúvania (napr. notebooky) mimo chránených priestorov a vymedzenie zodpovednosti.
- Pravidlá používania prenosných dátových nosičov mimo chránených priestorov a vymedzenie zodpovednosti.

5.28.2.5 Likvidácia osobných údajov

- Určenie postupov likvidácie osobných údajov s vymedzením súvisiacej zodpovednosti jednotlivých oprávnených osôb (bezpečné vymazanie osobných údajov z dátových nosičov, likvidácia dátových nosičov a fyzických nosičov osobných údajov).

5.28.2.6 Porušenie ochrany osobných údajov

- Postup pri oznamovaní porušenia ochrany osobných údajov úradu a dotknutej osobe na včasné prijatie preventívnych a nápravných opatrení.
- Pravidelné preskúvanie záznamov udalostí, záznamov o aktivitách používateľov, záznamov o výnimkách.
- Evidencia porušení ochrany osobných údajov a použitých riešení.
- Postup identifikácie a riešenia jednotlivých typov porušení ochrany osobných údajov.
- Postup odstraňovania následkov porušení ochrany osobných údajov.
- Postupy zaručenia kontinuity pri havárii alebo inej mimoriadnej udalosti.
- Postup pri poruche, údržbe alebo oprave automatizovaných prostriedkov spracúvania.

5.28.2.7 Kontrolná činnosť

- Kontrolná činnosť zameraná na dodržiavanie prijatých bezpečnostných opatrení s určením spôsobu, formy a periodicity jej realizácie (napr. pravidelné kontroly prístupov k informačnému systému).
- Informovanie oprávnených osôb o kontrolnom mechanizme, ak je u prevádzkovateľa zavedený (rozsah kontroly a spôsoby jej uskutočňovania).
- Postupy monitorovania súladu spracúvania osobných údajov podľa § 42 ods. 7 zákona č. 18/2018 Z. z. o ochrane osobných údajov.

5.28.2.8 Dodávateľské vzťahy

- Postup overenia dostatočných záruk.

- Začlenenie požiadaviek na ochranu osobných údajov do požiadaviek nových systémov a do pravidiel vývoja a nákupu systémov.
- Začlenenie požiadaviek na ochranu osobných údajov do zmluvných vzťahov s dodávateľmi a tretími stranami.
- Testovanie bezpečnostných funkcií počas vývoja systémov.
- Monitorovanie a pravidelné preskúmavanie úrovne bezpečnosti služieb poskytovaných dodávateľmi spolu s vypracovaním a aktualizáciou analýzy rizík dodávateľov.

5.28.2.9 Ďalšie ustanovenia

- Na základe posúdenia vplyvu spracúvania osobných údajov, prevádzkovateľ prijal záruky, bezpečnostné (technické, organizačné a personálne) opatrenia a mechanizmy na zabezpečenie ochrany osobných údajov dotknutých osôb.
- Záruky, bezpečnostné (technické, organizačné a personálne) opatrenia a mechanizmy na zabezpečenie ochrany osobných údajov dotknutých osôb, uvedené v tomto dokumente, nadobúdajú platnosť a účinnosť dňom schválenia tohto dokumentu.

5.29 FYZICKÁ BEZPEČNOSŤ

5.29.1 ÚČEL

Účelom tejto politiky je definovať bezpečnostné zóny vo všetkých nehnuteľnostiach/budovách podľa bezpečnostných požiadaviek. Lokácia bude používať tento štandard na poskytnutie definície zóny fyzickej bezpečnosti a na správnu klasifikáciu a ochranu fyzických oblastí v rámci lokality a na zaistenie správnej úrovne bezpečnosti, aby sa zabránilo neoprávnenému fyzickému prístupu, krádeži, poškodeniu, znehodnoteniu a strate informačných aktív.

5.29.2 ZODPOVEDNOSŤ

MHTH zodpovedá za to, že všetky definované priestory sú zabezpečené, organizačné požiadavky na manipuláciu a prístup sú splnené a všetky aktíva sú chránené.

Všetci zamestnanci spoločnosti musia dodržiavať požiadavky zónovania definované smernicami (interní, externí, návštevy).

Pred začatím nového projektu projektový manažér definuje a preškolí celý projektový tím, v zmysle požiadaviek zákazníka, o čom vykoná zápis, minimálne v rozsahu:

5.29.2.1 Organizačné bezpečnostné opatrenia

- Menovanie projektového tímu;
- Preškolenie tímu na požiadavky zákazníka pre projekt;
- Definovanie prístupovej matice k projektovým údajom;
- Skladovanie materiálu/hardware;
- Prenášanie/manipulácia s materiálom/hardware;
- Označovanie štítkom;
- Obmedzenie fotenia a vyhotovovania videozáznamov;
- Opatrenia na vytvorenie chránenej zóny vo výrobných priestoroch.

5.29.2.2 Technické opatrenia

- Definovanie dátového úložného priestoru;
- Nastavenie a kontrola prístupových práv;
- Definovanie retenčnej doby (prístupových údajov, dokumentácie,...);
- Definovanie požiadavky na kryptovanie pri ukladaní údajov
- Definovanie požiadavky na kryptovanie pri prenose údajov;
- Definovanie na kryptovanie pri použití prenosných médií;
- Označovanie dokumentov klasifikačným stupňom;
- Likvidácia papierových dokumentov výhradne skartovačkou;
- Požiadavky na bezpečnosť cloudových služieb;

- Požiadavky na ukladanie papierových dokumentov (segregácia);
- Vymazanie údajov po ukončení retenčnej doby.

5.29.3 ZÓNOVÝ KONCEPT

Každé oddelenie/úsek zdefinuje bezpečnostnú zónu a požiadavky pre svoje oblasti v rámci lokality alebo potvrdiť zónovanie, ktoré pre nich určí (špecialista FOB).

Zóny fyzickej bezpečnosti sú definované ako oblasti vo fyzickom priestore budovy, lokality alebo fyzickej oblasti, ktoré majú spoločné bezpečnostné požiadavky a ktoré majú jasne definované fyzické alebo logické hranice. To umožňuje, aby boli fyzické oblasti správne klasifikované a zabezpečené na základe kritickosti a vplyvu informačných aktív vo fyzickom priestore.

Zvyčajne by sa zóny nemali preskakovať. Namiesto toho by sa mali implementovať postupne reštriktívnym spôsobom od najmenej obmedzujúcej (verejná zóna) po najvyššiu požadovanú zónu. Realita však diktuje, že existujú prípady, kedy je ťažké alebo nepraktické implementovať celý rozsah zón. V týchto obmedzených prípadoch je možné preskočiť jednu zónu za predpokladu, že bezpečnostné opatrenia tejto zóny sú kompenzované v nasledujúcej zóne.

Bezpečnostná požiadavka v danej zóne závisí od dôvernosti, kritickosti a vplyvov objektov alebo informácií spracovaných v danej fyzickej oblasti.

Potrebné bezpečnostné opatrenia sa musia zodpovedajúcim spôsobom prispôbiť. Konštrukčné riešenie stien, okien a dverí musí zodpovedať príslušnej bezpečnostnej požiadavke; tieto musia byť podľa potreby vybavené ďalšími funkciami, ako je napríklad bezpečnostná a monitorovacia technológia.

Z hľadiska riadenia pohybu osôb a ochrany majetku, sú bezpečnostné zóny definované pre všetky lokality spoločnosti.

Zónové ovládanie prístupu, ako napríklad ovládanie systému prístupových dverí s čipovou kartou (minimálny fyzický kľúč), je potrebný na prechod medzi oblasťami medzi zónami.

Vonkajšie priestory by mali byť monitorované pomocou inteligentného CCTV systému.

Fyzické prístupové cesty by mali byť zabezpečené vhodnými bránami, ktoré umožnia fyzický prístup do priestorov len oprávneným osobám; uplatnenie tejto kontroly môže závisieť od prenajímateľa, ak objekt nevlastní alebo nespravuje MHTH.

Každá definovaná bezpečnostná zóna musí mať implementované bezpečnostné požiadavky a definované opatrenia.

5.29.4 OBVODOVÁ BEZPEČNOSŤ

Musí sa zabrániť tomu, aby neoprávnené osoby mali prístup do chránených budov. Preto je zavedená kontrola prístupu.

Okolité prostredie je chránené a zabezpečené (napr. oplotením, stenami, kontrolou prístupu, atď.). Ak to nie je možné z dôvodu rôznych okolností, musí byť vonkajšia strana všetkých chránených budov bezpečná.

5.29.5 STABILITA VONKAJŠIEHO POVRCHU

Vonkajší plášť všetkých chránených budov vrátane oplotenia, vstupov a okien, musia byť konštruované tak, aby ich nebolo možné prekonať bez pomoci nástrojov v zmysle smernice [MHTH S46 Fyzická a objektová bezpečnosť](#), príloha č.1. Štandardy pre fyzickú a objektovú bezpečnosť. Všetky dvere a brány musia byť trvalo zatvorené a každá oblasť musí byť vybavená kontrolou prístupu.

5.29.6 PREDCHÁDZANIE NEOPRÁVNENÉMU PRÍSTUPU A KONTROLA PRÍSTUPU

Všetky chránené oblasti musia byť zabezpečené kontrolou prístupu.

Zamestnanci, vrátane dodávateľov (ktorí podpísali dohodu NDA - dohoda o mlčanlivosti) a ktorí pracujú vo vnútri chránených zón, dostanú prístup k príslušným chráneným zónam počas bežnej pracovnej doby. Po normálnom pracovnom čase bude prístup obmedzený iba na zamestnancov, ktorí vykonávajú činnosti vo vnútri týchto chránených zón.

Na kontrolu a zabezpečenie osobitných potrieb (napr. núdzové situácie, zabezpečenie bezpečnosti, atď.) je vytvorený schválený zoznam externých pracovníkov, ktorí budú mať z hadiska chránených zón rovnaké prístupové práva ako kmeňoví zamestnanci spoločnosti. Tento osobitný prístup je potrebné vopred vyžiadať.

Osobitné potreby môžu byť tieto (príklady):

- Poskytovatelia prvej pomoci - všeobecný prístup k chráneným zónam, ale iba v prípade núdze (prístupové obmedzenia)
- Bezpečnostný personál - všeobecný prístup k chráneným zónam, ale iba v prípade núdze (prístupové obmedzenia)
- Zamestnanci správy budov - všeobecný prístup k chráneným zónam, ale iba v prípade núdze (obmedzenia prístupu)

Pre získanie kontroly prístupu do rôznych zón je potrebné ustanoviť proces žiadosti o prístup. Zoznam zamestnancov, ktorí majú prístup do chránených zón (bude pravidelne preverovať vedúci oddelenia a HR).

5.29.7 POPLACHOVÝ SYSTÉM NARUŠENIA

Vo všetkých budovách, v ktorých sa nachádzajú aktíva/ich komponenty, je nainštalovaný funkčný systém narušenia. Alarm musí byť vyvedený k bezpečnostnej službe alebo do pultu centralizovanej ochrany. Musí byť zavedený miestny relevantný reakčný plán poplachov (poplachové smernice).

5.29.8 ZDOKUMENTOVANÁ SPRÁVA NÁVŠTEVNÍKOV

Všetci návštevníci sú povinní sa zaregistrovať s príchodom na recepciu a musia byť preukázateľne oboznámení s bezpečnostnými usmerneniami a získať kartu návštevníka.

Návštevník nemá dovolené chodiť sám v chránených oblastiach a musí byť sprevádzaný zamestnancom spoločnosti.

5.29.9 ORGANIZAČNÉ POŽIADAVKY

Musia byť splnené nasledujúce požiadavky, aby sa zabezpečilo, že všetci zamestnanci, dodávatelia, partneri a poskytovatelia služieb majú spoľahlivý rámec na to, aby mohli konať a predchádzať porušeniam dôvernosti alebo neverejných informácií.

Celková zodpovednosť za ochranu vo výrobných častiach je v spoločnosti na manažérovi výroby.

5.29.10 POVINNOSTI MLČANLIVOSTI

Medzi spoločnosťou a zákazníkom musí existovať dohoda o mlčanlivosti, ktorá je platná podľa zmluvného dojednaní.

Všetci zamestnanci spoločnosti a všetci externí pracovníci, ktorí sú zapojení do projektov, musia podpísať NDA. Zoznam všetkých zamestnancov, ktorí pracujú v rámci projektov a ktorí podpísali NDA, musí byť aktuálny.

5.29.11 SUBDODÁVATELIA

Musí existovať písomný súhlas zákazníka o poskytnutí dôverných informácií subdodávateľovi.

Všetci subdodávatelia musia podpísať NDA. Dodržiavanie bezpečnostných požiadaviek musí byť zabezpečené a preukázané. NDA musia podpísať všetci externí pracovníci.

5.29.12 PREŠKOLENIE

Pravidelné školenie (minimálne raz ročne) sa musí vykonávať pre všetkých zamestnancov pracujúcich v chránených územiach a pre všetkých zamestnancov, ktorí sa podieľajú na výrobných projektoch. Obsahom školenia musí byť obsah tejto politiky, zaobchádzania s utajovanými údajmi a bezpečnosti priestorov (napr. všetky dvere a brány musia byť trvalo zatvorené, všetky okná musia byť chránené proti pohľadu, atď.).

5.29.13 BEZPEČNOSTNÁ KLASIFIKÁCIA

Bezpečnostná klasifikácia musí byť zavedená v súlade s politikou klasifikácie informácií a zamestnanci musia byť minimálne raz ročne preškolení.

5.29.14 FOTOGRAFOVANIE A NATÁČANIE

Fotografovanie a nahrávanie je vo všeobecnosti zakázané. Fotografovanie a filmovanie pre špeciálnej potreby je povolené iba pre zamestnancov pracujúcich v chránených oblastiach (a ak je to pre danú úlohu relevantné (dokumentácia o skúškach, dokumentácia k otázkam kvality atď.)). Pre tieto účely budú definované a poskytované firemné zariadenia. Súbor s fotografiami budú uložené na centrálnom sieťovom úložisku s obmedzeným prístupom zamestnancov. Tieto údaje sa musia po definovanej retenčnej dobe uchovávaní vymazať v súlade s plánom uchovávaní záznamov.

Návštevníci pri registrácii na recepcii musia byť poučení o zákaze používať zariadenia s funkciami videa a kamery. Toto poučenie musí byť súčasťou súboru bezpečnostného poučenia, ktoré musia návštevníci pred vstupom podpísať.

5.29.15 PREZENTÁCIE

Pre prezentácie a udalosti zahŕňajúce dôverné aktíva (napr. mediálne udalosti, marketingové udalosti) sa musia pripraviť a implementovať vhodné bezpečnostné koncepcie, ktoré sa vzťahujú na organizačné, personálne a technické opatrenia (vhodná klasifikácia a šifrovanie, riadenie prístupu, retencia a pod.).

Všetky požiadavky musia byť definované spolu s marketingovým oddelením spoločnosti.

5.29.16 FYZICKÉ ZABEZPEČENIE SERVEROVÝCH MIESTNOSTÍ

Fyzické zabezpečenie serverovni je realizované súhrnom zavedených opatrení ako:

- Systém kontroly vstupov,
- Monitorovací kamerový systém,
- Systém detekcie narušenia - Elektronický zabezpečovací systém,
- Protipožiarne opatrenia,
- Fyzická ochrana pre príjem a vyhodnocovanie poplachových hlásení.

5.29.16.1 Systém kontroly vstupov

- serverové miestnosti musia mať nainštalované systémy na kontrolu prístupu,
- aplikácie na udelenie povolení fyzického prístupu do serverovne - vstup musí byť schválený IT manažérom,
- Systém kontroly fyzického prístupu musí byť pripojený k neprerušiteľnému zdroju napájania (UPS), aby sa zabránilo automatickému otvoreniu pri strate hlavného napájania. Ak systém kontroly prístupu už nie je funkčný, mali by prístupové systémy umožniť správny výstup a miesto musí byť zabezpečené pomocou používania štandardných uzamykacích systémov na kľúč a/alebo bezpečnostných strážcov.
- Všetky osoby, ktoré nemajú platnú (personalizovanú) prístupovú kartu/kľúč do serverovne sú povinní sa zaregistrovať vrátane záznamu o ich mene, vstupe a výstupe (čas a účel návštevy). Tretie strany musia byť vždy sprevádzané interným personálom a sú povinní dodržiavať všetky ostatné interné predpisy (t. j. kódex správania a pod.).
- Príslušný IT manažér skontroluje zoznam oprávnení a prístupové záznamy personálu, ktorý vchádza do serverovne aspoň raz ročne.

5.29.16.2 Monitorovací kamerový systém

Serverovne musia byť monitorované kamerovým systémom. Záznam z kamerového systému slúži na zdokumentovanie udalostí v prípade bezpečnostného incidentu.

5.29.16.3 Protipožiarne opatrenia v serverovej miestnosti

Lahko horľavé materiály (t.j. papier, kartónové krabice, penový plast), a iné nebezpečné materiály sa nesmú skladovať ani vnášať do serverovej miestnosti.

Na kontrolu environmentálnej bezpečnosti musia byť nainštalované nasledujúce senzory / systémy:

- Požiarne a dymové detektory;
- Vetranie a klimatizácia (HVAC).

Príslušné vybavenie umiestnené v serverovni musí byť vybavené neprerušiteľným zdrojom napájania (UPS). Inštalované systémy UPS musia poskytovať zariadenia s výkonom, ktorý spĺňa aspoň jednu z nasledujúcich definovaných požiadaviek na jednotlivé zariadenia:

- Vhodné pokrytie napájaním na dobu, pokým dokáže núdzový generátor poskytnúť alternatívny zdroj energie z hlavného napájania;
- Pokrytie energie na definovaný počet hodín pri strednom trvaní napájania výpadku;
- Pokrytie napájania pre krátkodobé výpadky prúdu;
- Systémy batériových jednotiek UPS sa musia udržiavať a podľa potreby vymieňať, aby bola zachovaná nepretržitá funkčnosť. Tieto by sa mali testovať minimálne raz ročne. (Poznámka: plánovaná životnosť batérií sa zvyčajne uvádza na päť rokov).

Výpadky alebo prerušenia napájania je potrebné registrovať a oznamovať okamžite.

5.29.16.4 Systém detekcie narušenia – alarm

Elektronické zabezpečovacie systémy (EVS) musia byť nainštalované v serverových miestnostiach, ktoré obsahujú vysoko citlivé informácie a údaje. EVS nám umožňuje:

- detegovať pohyb v priestore,
- detegovať zaplavenie priestoru,
- detegovať požiar v priestore.

Od zamestnancov bezpečnostnej služby sa vyžaduje monitorovanie poplachových systémov v reálnom čase.

Keď sa vyskytnú abnormálne podmienky, systém detekcie narušenia musí okamžite reagovať s akustickým alarmom a automatickým oznamovaním personálu bezpečnostnej služby na požadované osoby (Alarm call tree).

5.29.16.5 Kódex správania sa v serverovni

- V serverovni platia všeobecné zdravotné a bezpečnostné požiadavky;
- V serverovni je zakázané jesť, piť a fajčiť;
- Podlahy v serverovni musia byť čisté a miestnosť musí byť udržiavaná v čistote a bez prachu;
- Personál upratovacích služieb musí byť monitorovaný tímom IT po celú dobu čistenia serverových miestností;
- Neoprávnenému personálu nie je dovolené dotýkať sa, používať alebo obsluhovať ICT zariadenia alebo príbuzné zariadenia infraštruktúry bez predchádzajúceho schválenia.

6. SÚVISIACA DOKUMENTÁCIA

6.1 Interné dokumenty

- [MHTH_S02_Telekomunikačná prevádzka-mobil](#)
- [MHTH_S06_Smernica o ochrane osobných údajov](#)

- [MHTH S09 Správa majetku a budov](#)
- [MHTH S11 Organizačný poriadok](#)
- [MHTH S12 Etický kódex](#)
- [MHTH S30 Interné audity](#)
- [MHTH S35 Smernica o ochrane dôverných informácií a obchodného tajomstva](#)
- [MHTH S39 Dodávateľsko odberateľské vzťahy](#)
- [MHTH S45 Prevádzka monitorovacích kamerových systémov](#)
- [MHTH S46 Fyzická a objektová bezpečnosť](#)
- [MHTH IT S01 Proces riadenia zmien v IT \(Change Management process\)](#)
- [MHTH IT S02 Proces riadenia Problémov \(Problem management process\)](#)
- [MHTH KB S02 PKIB pre dodávateľov a tretie strany](#)
- [MHTH IT S03 Proces riadenia požiadaviek a incidentov \(Request & Incident management process\)](#)

6.2 Externé dokumenty

- Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti v znení neskorších predpisov
- Zákon č. 95/2019 Z.z. informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- Zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
- Vyhláška NBÚ č. 227/2025 Z.z. ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v platnom znení
- Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu (ďalej len „ÚPVII“) č. 179/2020 Z. z. ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy
- Metodika NBU pre analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti v znení neskorších predpisov STN ISO/IEC 27000:2016 Informačné technológie Bezpečnostné metódy Systém riadenia informačnej bezpečnosti - Prehľad a slovník
- ISO/IEC 27001 štandard
- STN ISO/IEC 27005:2012 Informačné technológie - Bezpečnostné metódy - Riadenie rizík informačnej bezpečnosti
- STN ISO 31000 Manažérstvo rizika – Návod
- NIST Special Publication 800-39 Managing Information Security Risk
- NIST Special Publication 800-30 Rev. 1 Guide for Conducting Risk Assessments

6.3 Prílohy a formuláre

- Príloha č.1 – Životný cyklus incidentu a jeho riadenie

7. PLATNOSŤ A ÚČINNOSŤ

Začiatkom platnosti tohto dokumentu je deň elektronického schválenia všetkými schvaľovateľmi a dňom účinnosti publikovanie na intranete (Manažment interných predpisov).

Nahrádza:	MHTH_KB_S01 Politiky kybernetickej a informačnej bezpečnosti, v1
------------------	--

Vypracoval: Ing. Róbert Mramúch – manažér odd. bezpečnosti a krízového riadenia

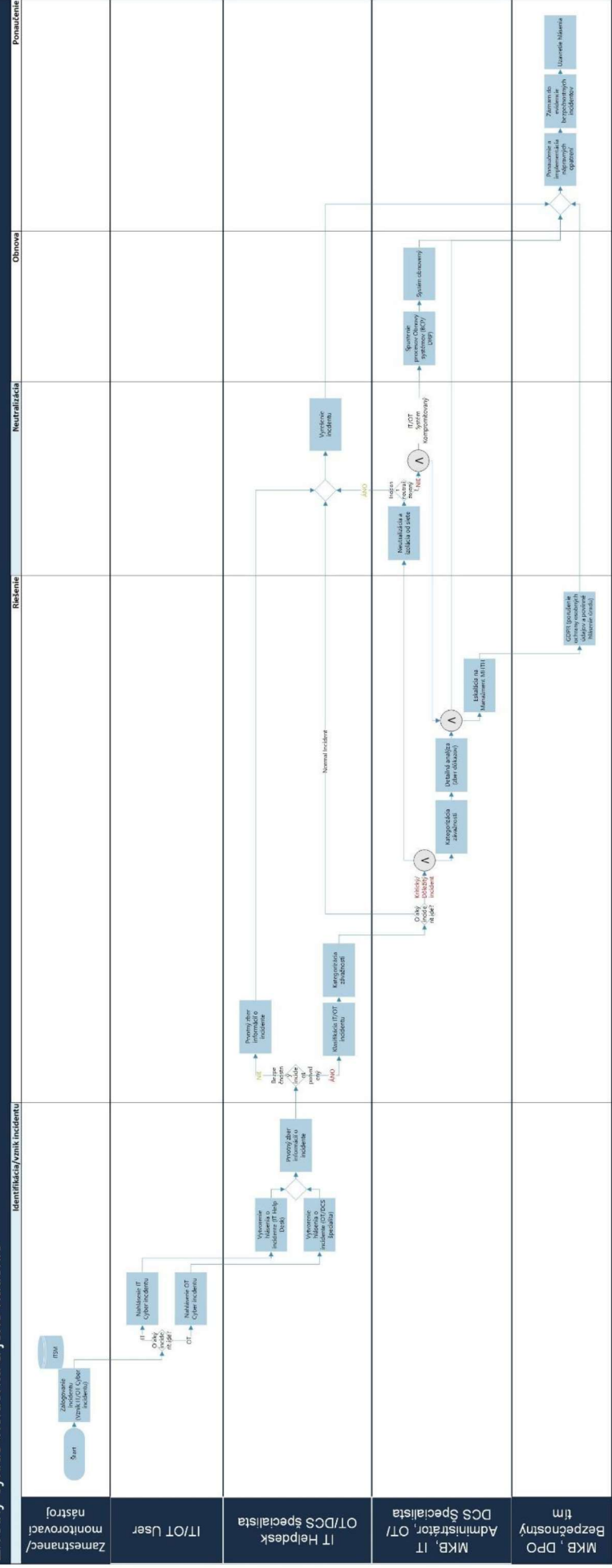
Schválil (elektronické schválenie):

Ing. Adrián Jenčo, LL.M, MBA – generálny riaditeľ

Ing. Peter Kadlec – riaditeľ úseku IT

Príloha č. 1:

Životný cyklus incidentu a jeho riadenie



Obr. č. 6: Proces (workflow) riešenia bezpečnostného incidentu