**Príloha č.1 - Zoznam požadovanej dokumentácie IMS pre NCZI v rozsahu a v obsahu smerníc a politik**

**IMS - Integrovaný manažérsky systém**

**IB - Informačná bezpečnosť**

**Q - Kvalita**

**IT - Informačné technológie**

**1. úroveň riadiacej dokumentácie:**

**Politika IMS pre kvalitu, IB a služby IT**

*Návrh spoločnej politiky IMS pre oblasti kvality, IB a služieb IT*

**Strategické (dlhodobé) ciele pre kvalitu, IB a služby**

*Zoznam a definícia dlhodobých cieľov pre kvalitu, IB a služby IT, vychádzajúcich z prislúchajúcich ustanovení politiky IMS,*

 **Ročné (krátkodobé) ciele na rok 2022**

*Zoznam a definícia krátkodobých cieľov pre kvalitu, IB a služby IT na rok 2022 pomenovanie a prioritizácia cieľov pre daný rok*

**Príručka IMS s prílohami,**

1. Úvodné ustanovenia, organizácia a spôsoby riadenia inštitúcie v oblasti procesov, produktov a služieb

2. Účel a rozsah platnosti príručky a definovanie záväznosti jednotlivých častí

3. Definícia pojmov a skratiek

4. Kontext – súvislosti organizácie

* + História, popis inštitúcie, účel vzniku a jej úloh v kontexte zriaďovacej listiny
	+ Interné a externé súvislosti v kontexte štátnych inštitúcií, orgánov a súkromnej sféry
	+ Zainteresované strany, ich potreby a očakávania
	+ Rozsah IMS, certifikácia a výnimky
	+ Systém IMS a súvisiace procesy. Rizikový prístupriadiacich, hlavných a podporných subsystémov kvality, IB a služieb

5. Líderstvo

* + Líderstvo a zodpovednosť, bezpečnosť, orientácia na občana
	+ Právomoci, zodpovednosti a role, RACI
	+ Politika IMS s odkazmi na špecifické politiky

6. Podpora

* + Spôsobilosti
	+ Zdroje
	+ Povedomie
	+ Interná a externá komunikácia
	+ Manažment znalosti, jeho riadenie a ochrana
	+ Riadenie a klasifikacia dokumentovaných (uchovávaných) informácií

7. Plánovanie

* + Princípy a definovanie rámca pre manažérstvo rizík, metodiky hodnotenia rizík a príležitostí a ich identifikácia
	+ Riadenie rizík a príležitostí
	+ Ciele IMS, programy a plány na ich dosiahnutie *–(väzba na ciele a vybrané rizika)*
	+ Plánovanie systému služieb

8. Prevádzka

* + Plánovanie a riadenie prevádzky
	+ Požiadavky na poskytované produkty a služby
	+ Katalóg služieb
	+ Riadenie dodávateľov, procesov, produktov a služieb
	+ Návrh a vývoj produktov a služieb a riadenie zmien
	+ Release produktov a služieb, ich prechod a nasadzovanie
	+ Prevádzka a poskytovanie interných a externých služieb
	+ Incident management a SLA
	+ Zaistenie behu služieb

9. Hodnotenie výkonnost*i*

* + Interný audit IMS
	+ Monitorovanie, hodnotenie, meranie a analýzy IMS
	+ Preskúmanie a hodnotenie manažmentom IMS *– kvalita, procesy, IB, služby*
	+ Kontinuálne reportovanie *- kvalita, procesy, IB, služby*

10. Zlepšovanie

* + Všeobecne popis procesov zlepšovania
	+ Nesúlad, preventívne a nápravné opatrenia
	+ Trvalé a kontinuálne zlepšovanie

Prílohy

* + Organizačná schéma NCZI
	+ Mapa a karty procesov
	+ Zoznam dokumentácie IMS
	+ Dlhodobé a krátkodobé ciele
	+ Politika IMS
	+ Koncepcia rozvoja ITVS
	+ Integrácia pravidiel pre riadenie dokumentácie
	+ Vybraná metodika a definícia rámcov pre riadenie rizík
	+ Vybrané prehľady

|  |  |  |
| --- | --- | --- |
| Záznamy / Požiadavky na „šablóny“* + Strategické ciele a spôsob ich plnenia
	+ Výstupy z preskúmania manažmentom
	+ Ročné ciele, spôsob ich plnenia a vyhodnotenie cieľov
	+ Zoznam KPI (s väzbami na procesy)
	+ Reporty výkonnosti
	+ Auditné záznamy

 |  |  |

**2. úroveň riadiacej dokumentácie:**

**Mapa procesov**

*Grafické znázornenie procesov s ich rozdelenie na riadiace, hlavné a podporné*

**Karty procesov**

*Manažérsky popis procesov obsahujúci dôležité charakteristiky potrebného pre jeho riadenie v forme excelu*

**Smernice IMS,** (*stručný popis predpokladanej štruktúry):***Riadenie fyzickej bezpečnosti**

* + Fyzická bezpečnosť a bezpečnosť prostredia ( Zabezpečené oblasti, Fyzický bezpečnostný perimeter, Kontroly fyzického vstupu, Zabezpečenie kancelárií, miestnosti a zariadení)
	+ Ochrana proti vonkajším a prírodným hrozbám.
	+ Práca v zabezpečených priestoroch
	+ Dodávka a nakladacie plochy
	+ Zariadenia
	+ Umiestňovanie a ochrana zariadení
	+ Podporné služby
	+ Bezpečnosť káblových rozvodov
	+ Údržba zariadení
	+ Premiestnenie aktív
	+ Bezpečnosť zariadení a aktív mimo prevádzkových priestorov
	+ Neobsluhované zariadenia užívateľa
	+ Zásada prázdneho stola a prázdnej obrazovky monitora
	+ Zoznam príloh:
		- Bezpečnostný perimeter
		- Evidencia zariadení mimo prevádzkových priestorov
		- Záznamy o údržbe zariadení (môže byť identické so záznamami v Help-desku)

**Organizačná a personálna bezpečnosť**

* + Oddelenie povinností
	+ Kontakt s orgánmi a úradmi
	+ Kontakt s záujmovými skupinami
	+ Bezpečnosť ľudských zdrojov pred vznikom pracovného pomeru (Preverovanie, Pravidlá a podmienky zamestnania)
	+ Bezpečnosť ľudských zdrojov počas pracovného pomeru (Zodpovednosť manažmentu, Povedomie o informačnej bezpečnosti, vzdelávania a odborná príprava, Disciplinárny proces)
	+ Ukončenie a zmena zamestnania (Zodpovednosti spojené s ukončením, alebo zmenou pracovného pomeru)
	+ Zoznam príloh:
		- Evidencia a hodnotenie zamestnancov
		- Plán rozvoja bezpečnostného povedomia
		- Zoznam školení a prezenčné listiny o školeniach zamestnancov
		- Určenie členov ISMS tímu (ak takýto tím je vytvorený)
		- Poverenie manažéra ISMS
		- Záznamy z preskúmania manažmentom (patrí súčasne aj ako záznam k Príručke IMS)
* Evidencia dočasných výnimiek oddelenie povinností

**Riadenie prevádzky IT a bezpečnosti a sietí**

* + Riadenie prístupu
	+ Prístup k sieťam a k sieťovým službám
	+ Riadenie prístupu používateľov (Registrácia a de-registrácia užívateľa, Poskytovanie prístupu užívateľom, Riadenie privilegovaných prístupových práv, Riadenie tajných autentizačných informácií o užívateľovi (používateľské heslá), Preskúmanie prístupových práv užívateľov, Odobratie alebo úprava prístupových práv
	+ Zodpovednosti užívateľov ( Používanie tajných autentizačných informácií (heslá))
	+ Riadenie prístupu k systémom a aplikáciám
	+ Obmedzenie prístupu k informáciám
	+ Bezpečné prihlasovacie postupy
	+ Systém správy hesiel
	+ Používanie privilegovaných programov a utilít
	+ Riadenie prístupu k knihovni zdrojového kódu
	+ Kryptografia – šifrovanie ( kryptografické opatrenia, Zásady používania kryptografických opatrení, Správa kľúčov)
	+ Prevádzkové postupy a zodpovednosti
	+ Riadenie kapacít a zmien
	+ Ochrana pred škodlivým softvérom
	+ Zálohovanie a obnova systémových dát
	+ Riadenie prevádzkového softvéru
	+ Riadenie technických zraniteľností
	+ Hľadiska auditu informačných systémov
	+ Riadenie bezpečnosti siete (Sieťové opatrenia, Bezpečnosť sieťových služieb, Segregácia - oddeľovanie v sieťach, Prenos informácií, Zásady a postupy pri prenose informácií, Elektronické správy)
	+ Zoznam príloh:
		- Záznamy v napr. Help desku (identické s požiadavkami riadenia zmien)
		- CMDB databáza (konfiguračná databáza, alebo zoznam zariadení v IT prostredí)
		- Evidencia šifrovacích kľúčov
		- Zoznam bezpečnostných testov a ich výsledky

 **Monitorovanie prevádzky IT a bezpečnosti**

* + Monitorovanie a zaznamenávanie ( Zaznamenávanie udalostí, Záznamy o činnostiach správcov a operátorov)
	+ Ochrana zaznamenaných informácií
	+ Kontroly fyzického vstupu
	+ Vyhodnocovanie monitorovania
	+ Zoznam príloh:
		- Zoznam parametrov, ktoré sa monitorujú a vyhodnocujú (nie je potrebné vytvárať report, stačí evidencia v systéme v ktorom sa robí monitoring)
		- Záznam z hodnotenia monitorovania (napr. týždenný, mesačný ročný report)

**Príprava, nastavenie, riadenie a monitorovanie zmlúv a objednávok, obstarávanie**

* + Kategorizácia dodávateľov
	+ Definícia bezpečnostných požiadaviek v dohodách a zmluvách s dodávateľmi
	+ Definovanie náležitosti zmlúv o úrovniach služieb, spôsoby realizácie bezpečnostných opatrení, a určenie zmluvnej zodpovednosti
	+ Pravidlá pre vykonávanie kontroly zavedenia bezpečnostných opatrení
	+ Zoznam príloh:
		- Zoznam dodávateľov, garantov za dodávateľov a ich zmlúv

**Výber, hodnotenie a riadenie dodávateľov a outsourcing**

* + Pravidlá a princípy pre výber dodávateľov
	+ Monitorovanie a preskúmavanie služieb dodávateľov
	+ Riadenie zmien v službách dodávateľov
	+ Dodávateľský reťazec informačných a komunikačných technológií
	+ Pravidlá pre hodnotenie rizík dodávateľov
	+ Zoznam príloh:
		- Zoznam dodávateľov a ich hodnotenie
		- Záznamy z kontrol dodávateľov

**Riadenie aktív a konfigurácií**

* + Riadenie aktív ( zoznam,  vlastníctvo)
	+ Kategórie aktív
	+ Označovanie aktív a dokumentácie
	+ Prijateľné použitie aktív ( umiestnenie,  externé subjekty,  písomná komunikácia,  elektronická komunikácia,  ústna komunikácia,  telefonická komunikácia)
	+ Vrátenie aktív
	+ Správa vymeniteľných médií
	+ Fyzický prenos médií
	+ Manipulácia s aktívami ( požiadavky na zachovanie dôvernosti, integrity a dostupnosti)
	+ Zoznam príloh:
		- Zoznam primárnych aktív, ich garantov a ich hodnotenie
		- Zoznam podporných aktív, ich garantov
		- Evidencia väzieb medzi primárnymi a podpornými informačnými aktívami (napr. prvky z CMDB databázy)

 **Návrh, vývoj a riadenie produktov a služieb**

* + Analýza a špecifikácia bezpečnostných požiadaviek
	+ Fázy vývoja
	+ Princípy bezpečného vývoja systému
	+ Prostredie na bezpečný vývoj
	+ Vývoj externými zdrojmi
	+ Testovanie bezpečnosti systémov (Akceptačné testy systémov, Ochrana testovacích údajov)
	+ Bezpečnosť v procese vývoja a podporných procesov
	+ Zabezpečenie aplikačných služieb vo verejných sieťach
	+ Ochrana pri transakciách aplikačných služieb
	+ Postupy riadenia systémových zmien
	+ Technické preskúmanie aplikácií po zmene operačného systému
	+ Obmedzenia zmien v softvérových balíkoch
	+ Zoznam príloh:
		- Zoznam vývojových projektov
		- Akceptačné testy ich výsledky
		- Záznamy v napr. Help-desku (identické s požiadavkami riadenia zmien)

**Riadenie dostupnosti, kapacít a kontinuity prevádzky**

* + Princípy riadenia kontinuity
	+ Plánovanie kontinuity bezpečnosti informácií
	+ Implementácia kontinuity bezpečnosti informácií
	+ Kontrola, preskúmavanie a hodnotenie kontinuity z hľadiska informačnej bezpečnosti
	+ Redundancia
	+ Dostupnosť zariadení (zdrojov) na spracovanie informácií
	+ Zoznam príloh:
		- Plány kontinuity
		- Záznamy z testovanie plánov kontinuity a návrhy na zlepšenie

**Riadenie a správa požiadaviek, incidentov a problémov**

* + Riadenie a správa požiadaviek
	+ Princípy zvládania incidentov
	+ Kategórie incidentov a problémov
	+ Postup zvládania incidentov a problémov (Oznamovanie, Evidencia, Vyhodnotenie a návrh postupu zvládania, Okamžitá eliminácia škôd, Realizácia nápravného opatrenia)
	+ Overenie efektívnosti nápravného opatrenia
	+ Ponaučenie sa z incidentov a problémov
	+ Zoznam príloh:
		- Záznamy v napr. Help-desku s evidenciou incidentov, ich aktuálnym stavom a s plánmi ich vyriešenia (môže byť identické s Help-deskom s požiadavkami riadenia zmien)

**Manažérstvo rizík**

* + Rámec pre manažérstvo rizík, princípy
	+ Prístup k rizikám
	+ Hodnotiace parametre, škály a hodnoty
	+ Akceptovateľná úroveň rizika
	+ Identifikácia a hodnotenia rizík
	+ Postupy na minimalizáciu a odstránenie rizika
	+ Overovanie efektívnosti zavedených opatrení
	+ Zoznam príloh:
		- Vybrané metodiky
		- Analýza rizík
		- Plán zvládania rizík

**Riadenie projektov**

* + Prístup k riadeniu projektov
	+ Fázy projektového riadenia
	+ Metodika riadenia projektov
	+ Projektové postupy
	+ Informačná bezpečnosť v oblasti projektového riadenia
	+ Zoznam príloh:
		- Šablóny pre malé, stredné a veľké projekty

**Riadenie zmien**

* + Proces riadenia zmien
	+ Kategórie zmien
	+ Požiadavky na zmenu
	+ Posudzovanie možných dopadov zmien
	+ Schvaľovanie zmien
	+ Implementácia zmien
	+ Dodávatelia v procese zmien
	+ Akceptácia implementácie zmien a zavedenie do prevádzky
	+ Zoznam príloh:
		- Záznamy (napr. v Help-desku s požiadavkami na zmenu a realizáciou zmien)

 **Plnenie právnych a iných požiadaviek**

* + Dodržiavanie zákonných a zmluvných požiadaviek
	+ Identifikácia platných právnych predpisov a zmluvných požiadaviek
	+ Práva duševného vlastníctva
	+ Ochrana záznamov (dokumentovaných informácií)
	+ Ochrana súkromia a o ochrana osobných údajov
	+ Regulácia kryptografických opatrení
	+ Preskúmanie bezpečnosti informácií ( Nezávislé preskúmanie informačnej bezpečnosti, Zhoda s bezpečnostnými politikami a štandardmi , Preskúmanie technickej zhody)
	+ Zoznam príloh:
		- Zoznam platnej legislatívy relevantnej pre organizáciu
		- Záznamy o činnosti spracovania (GDPR)
		- Zoznam bezpečnostných testov
		- Identifikácia a evidencia predmetu činností, na ktoré si organizácia uplatňuje práva duševného vlastníctva, patentové práva a pod

 **Správa architektúry**

* + Príprava a určenie referenčnej architektúry riešení
	+ Voľba riešení a štandardizácie referenčnej architektúry riešení
	+ Realizácia referenčnej architektúry riešení
	+ Služby spojené s referenčnou architektúrou riešení
	+ Zoznam príloh:
		- Základné prvky referenčnej architektúry riešení

 **Riadenie a správa požiadaviek, incidentov a problémov**

* + Riadenie a správa požiadaviek
	+ Princípy zvládania incidentov
	+ Kategórie incidentov a problémov
	+ Postup zvládania incidentov a problémov (Oznamovanie, Evidencia, Vyhodnotenie a návrh postupu zvládania, Okamžitá eliminácia škôd, Realizácia nápravného opatrenia)
	+ Overenie efektívnosti nápravného opatrenia
	+ Ponaučenie sa z incidentov a problémov
	+ Zoznam príloh:
		- Záznamy v napr. Help-desku s evidenciou incidentov, ich aktuálnym stavom a s plánmi ich vyriešenia (môže byť identické s Help-deskom s požiadavkami riadenia zmien)

 **Vyraďovanie IS a likvidácia dát**

* + Spôsoby likvidácie dát a systémov
	+ Likvidácia pamäťových médií
	+ Likvidácia listinnej dokumentácie
	+ Bezpečná likvidácia alebo opätovné použitie zariadení
	+ Zoznam príloh:
		- Záznamy o likvidácií dôležitých dátových nosičov
		- Záznamy o skartácií chránených dokumentov

 **Monitoring a riadenie výkonov a výsledkov**

* Princípy a pravidlá monitoringu výkonov, KPIs
* Frekvencia a rozsah monitoringu
* Procesy, projekty, zákazky a ich monitoring
* Monitoring plnenia požiadaviek na služby
* Monitoring výkonov a spokojnosti zákazníkov
* Zoznam príloh:
	+ - Obsah mesačného reportu výkonnosti služieb
		- Obsah štvrť-ročného reportu výkonnosti procesov
		- Obsah pre preskúmanie IMS vedením