Príloha ____ k zmluve č. _____

Z M L U V A

o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov uzatvorená medzi

MH Teplárenský holding, a.s.
so sídlom Turbínová 3, 831 04 Bratislava – mestská časť Nové Mesto
IČO 36 211 541 | DIČ 2020048580 | IČ DPH SK2020048580 | IBAN SK17 1100 0000 0026 2706 4293
zapísaná v Obchodnom registri Okresného súdu Bratislava I, oddiel Sa, vložka č. 7386/B
v mene spoločnosti konajú Ing. Marcel Vrátný, predseda predstavenstva, a Ing. Lenka Smreková, FCCA, členka predstavenstva
(ďalej len „**prevádzkovateľ základnej služby**“)

a

_____
so sídlom _____
IČO _____ | DIČ _____ | IČ DPH _____ | IBAN _____
zapísaná v Obchodnom registri Okresného súdu _____, oddiel _____, vložka č. _____
v mene spoločnosti koná _____
(ďalej len „**dodávateľ**“)

(prevádzkovateľ základnej služby a dodávateľ spoločne ďalej len „**zmluvné strany**“)

vzhľadom k tomu, že

- spoločnosť MH Teplárenský holding, a.s. je prevádzkovateľom základnej služby podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**zákon o kybernetickej bezpečnosti**“),

- základnou službou prevádzkovateľa základnej služby je: výroba tepla, dodávka tepla a výroba elektriny,

- dodávateľ uzatvára s prevádzkovateľom základnej služby zmluvu č. _____ (ďalej len „**hlavná zmluva**“), ktorej predmet priamo súvisí s prevádzkou sietí a informačných systémov, ako sú definované v zákone o kybernetickej bezpečnosti, pre prevádzkovateľa základnej služby,

- prevádzkovateľ základnej služby je povinný uzatvoriť s dodávateľom zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona o kybernetickej bezpečnosti, ktorú týmto s dodávateľom uzatvára (ďalej len „**bezpečnostná zmluva**“),

- táto bezpečnostná zmluva ustanovuje základné úlohy a princípy spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov prevádzkovateľa základnej služby, a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby zo strany prevádzkovateľa základnej služby (ďalej len „**ciele**“) v súvislosti s plnením hlavnej zmluvy zo strany dodávateľa,

- táto bezpečnostná zmluva ustanovuje požiadavky na plnenie hlavnej zmluvy zo strany dodávateľa, ktoré sú dôležité pre dosahovanie cieľov tejto bezpečnostnej zmluvy,

- plnenie povinností dodávateľa podľa tejto bezpečnostnej zmluvy sa vyžaduje počas celej doby trvania hlavnej zmluvy a tvorí integrálnu súčasť plnenia záväzkov dodávateľa podľa hlavnej zmluvy,

takto:

1. PREDMET DOHODY

1.1 Pojmy používané v tejto bezpečnostnej zmluve majú význam im priradený v zákone o kybernetickej bezpečnosti a jeho vykonávacích predpisoch.

1.2 Dodávateľ je povinný prijímať a dodržiavať opatrenia minimálne v rozsahu uvedenom v tejto bezpečnostnej zmluve tak, aby boli naplnené ciele tejto bezpečnostnej zmluvy. Dodávateľ vyhlasuje, že súhlasí s opatreniami podľa tejto bezpečnostnej zmluvy.

1.3 Dodávateľ je povinný dodržiavať bezpečnostné smernice prevádzkovateľa základnej služby, s ktorými ho prevádzkovateľ základnej služby oboznámi. Bezpečnostné smernice prevádzkovateľa základnej služby detailne rozpracúvajú požiadavky vyplývajúce z tejto bezpečnostnej zmluvy a z dokumentov špecifikovaných v článku 6 ods. 6.1 tejto bezpečnostnej zmluvy na podmienky prevádzkovateľa základnej služby a upravujú konkrétne postupy potrebné na dosahovanie cieľov tejto bezpečnostnej zmluvy. Plnenie bezpečnostných smerníc prevádzkovateľa základnej služby nevyžaduje od dodávateľa dodatočné náklady oproti tomu, čo vyžaduje plnenie najlepšej bezpečnostnej praxe a dokumentov špecifikovaných v článku 6 ods. 6.1 tejto bezpečnostnej zmluvy.

1.4 Dodávateľ berie na vedomie, že opatrenia vyžadované bezpečnostnými smernicami prevádzkovateľa základnej služby sa môžu počas doby trvania hlavnej zmluvy meniť tak, aby reagovali na novo identifikované kybernetické hrozby, ktoré by sa mohli týkať plnenia podľa hlavnej zmluvy vrátane dodávaných tovarov, poskytovaných služieb a/alebo vykonávaných procesov (ďalej len „**produkt**“). Dodávateľ bude na takéto zmeny v bezpečnostných smerniciach prevádzkovateľa základnej služby upozornený, pričom s ním môže dohodnúť podrobnosti týkajúce sa ich implementácie.

1.5 Dodávateľ je povinný dodržiavať pokyny prevádzkovateľa základnej služby. Dodávateľ je povinný bez zbytočného odkladu upozorniť prevádzkovateľa základnej služby na nevhodnú povahu pokynov daných mu prevádzkovateľom základnej služby vrátane pokynov a opatrení obsiahnutých v bezpečnostných smerniciach prevádzkovateľa základnej služby.

1.6 Dodávateľ je povinný plniť notifikačné povinnosti podľa požiadaviek zákona o kybernetickej bezpečnosti tak, aby boli naplnené ciele tejto bezpečnostnej zmluvy.

1.7 Plnenie povinností podľa tejto bezpečnostnej zmluvy tvorí integrálnu súčasť plnenia zo strany dodávateľa pre prevádzkovateľa základnej služby podľa hlavnej zmluvy. Dodávateľ je povinný plniť povinnosti vyplývajúce z tejto bezpečnostnej zmluvy po celú dobu trvania hlavnej zmluvy.

1.8 Odplata za plnenie povinností dodávateľa podľa tejto bezpečnostnej zmluvy a náhrada všetkých nákladov vynaložených dodávateľom v súvislosti s plnením povinností dodávateľa podľa tejto bezpečnostnej zmluvy sú v plnom rozsahu zahrnuté v peňažnom plnení poskytovanom prevádzkovateľom základnej služby dodávateľovi podľa hlavnej zmluvy a na žiadne ďalšie peňažné plnenia dodávateľ za plnenie povinností podľa tejto bezpečnostnej zmluvy od prevádzkovateľa základnej služby nemá nárok.

2. ZÁKLADNÉ POVINNOSTI DODÁVATEĽA

2.1 Základným princípom, ktorý musí dodávateľ vziať na vedomie a akceptovať, je jeho zodpovednosť za bezpečnosť ním dodávaného produktu do tej miery, aby produkt a jeho komponenty pre prevádzkovateľa základnej služby nepredstavovali riziko z pohľadu dostupnosti, integrity a dôvernosti jednak pre produkt samotný, jednak pre ostatné systémy a vnútorné prostredie prevádzkovateľa základnej služby, s ktorými musí koexistovať. Plnenie týchto požiadaviek je dodávateľ povinný kedykoľvek prevádzkovateľovi základnej služby nepopierateľným spôsobom preukázať (auditovateľnosť). V prípadoch stanovených touto bezpečnostnou zmluvou je dodávateľ povinný zabezpečiť plnenie povinností podľa tejto kybernetickej zmluvy aj u všetkých svojich priamych a nepriamych subdodávateľov v akomkoľvek stupni, ktorých plnenie vrátane dodávaných tovarov, poskytovaných služieb a/alebo vykonávaných procesov bude tvoriť súčasť produktu podľa hlavnej zmluvy (ďalej len „**subdodávateľ**“).

2.2 Dodávateľ má povinnosť po celú dobu trvania hlavnej zmluvy

a) dodržiavať a plniť bezpečnostné smernice prevádzkovateľa základnej služby primerane povahe ním dodávaného produktu tak, aby boli naplnené ciele tejto bezpečnostnej zmluvy,

b) zabezpečiť, aby plnenie hlavnej zmluvy vrátane akýchkoľvek zásahov alebo zmien v produkte počas nasadzovania, prevádzky a technickej podpory vykonávali len dodávateľom autorizované, odborne zdatné a na základy informačnej a kybernetickej bezpečnosti dostatočne poučené osoby,

c) plniť základné bezpečnostné požiadavky a rozšírené bezpečnostné požiadavky,

d) v prípade plnenia hlavnej zmluvy prostredníctvom subdodávateľov zabezpečiť plnenie povinností, ktoré vyplývajú z tejto bezpečnostnej zmluvy dodávateľovi, aj zo strany subdodávateľov uložením písomného záväzku subdodávateľom plniť a dodržiavať povinnosti, ktoré vyplývajú z tejto bezpečnostnej zmluvy dodávateľovi, v primeranom rozsahu tak, aby boli naplnené ciele tejto bezpečnostnej zmluvy. Dodávateľ je povinný zabezpečiť, aby prevádzkovateľ základnej služby mohol vykonať audit v súlade s ustanoveniami tejto bezpečnostnej zmluvy aj u týchto subdodávateľov. Dodávateľ tak nemusí postupovať, ak pred prípadným zapojením subdodávateľa na plnení hlavnej zmluvy dodávateľ poskytne prevádzkovateľovi základnej služby podrobné, pravdivé a úplné informácie o rozsahu a povahe plánovaného využitia subdodávateľa na plnení hlavnej zmluvy s osobitným dôrazom na informácie o tom, nakoľko plnenie poskytované subdodávateľom súvisí s prevádzkou sietí a informačných systémov prevádzkovateľa základnej služby, a prevádzkovateľ základnej služby vzhľadom na to, že plánované využitie subdodávateľa na plnení hlavnej zmluvy nesúvisí s prevádzkou sietí a informačných systémov prevádzkovateľa základnej služby, rozhodne, že uloženie záväzkov tomuto subdodávateľovi podľa tohto ustanovenia sa nevyžaduje; v takom prípade dodávateľ daného subdodávateľa na plnenie hlavnej zmluvy, ktoré súvisí s prevádzkou sietí a informačných systémov prevádzkovateľa základnej služby, využiť nesmie a prípadné porušenie tejto povinnosti sa považuje za podstatné porušenie tejto bezpečnostnej zmluvy.

2.3 Základné bezpečnostné požiadavky (aplikovateľné bez ohľadu na typ produktu) sú:

a) povinnosť poskytnúť úplný a pravdivý zoznam všetkých komponentov použitých pri riešení a implementácii v rámci produktu na úrovní výrobcov a verzií a bezodkladne ho aktualizovať,

b) povinnosť dodávať produkt vo výrobcom alebo výrobcami jeho jednotlivých komponentov podporovaných verziách,

c) povinnosť včas upozorňovať prevádzkovateľa bezpečnostnej služby na zistené bezpečnostné (technické) zraniteľnosti dodávaného produktu vrátane všetkých jeho komponentov, ktoré dodávateľ zistil sám alebo o ktorých sa dozvedel,

d) povinnosť pravidelne aktualizovať dodávaný produkt na bezpečnostné záplaty – buď priamo dodávateľom alebo nepriamo prostredníctvom aktualizácií poskytovaných výrobcom alebo výrobcami jeho jednotlivých komponentov,

e) povinnosť pravidelne aktualizovať návod na používanie produktu z hľadiska jeho kybernetickej bezpečnosti,

f) povinnosť bezodkladne upozorňovať prevádzkovateľa základnej služby na všetky okolnosti alebo zmeny v ním dodávanom produkte, ktoré môžu viesť alebo by mohli viesť k bezpečnostnému incidentu (nesprávna konfigurácia, neoprávnený prístup alebo pokus o neoprávnený prístup, zneužitie prístupov oprávnenou osobou, chýbajúce bezpečnostné záplaty, výsledok scanu na technické zraniteľnosti a pod.),

g) povinnosť dodávať produkt v potrebnej a zabezpečenej konfigurácii.

2.4 Rozšírené bezpečnostné požiadavky (s osobitným vzťahom k produktu a plneniu hlavnej zmluvy) sú požiadavky pre OT prostredie vyplývajúce z IEC 62443 a požiadavky pre IT prostredie vyplývajúce z IEC ISO 27001 a IEC ISO 27002; sú špecifikované v bezpečnostnej smernici prevádzkovateľa základnej služby „Technický a bezpečnostný štandard IT/OT systémov“. Rozšírené bezpečnostné požiadavky sa uplatňujú:

a) na dodávku alebo integrovanie IT/OT technológií a ich komponentov,

b) na implementáciu, zmeny, upgrade alebo inovácie pre OT (ICS/DCS) systémy,

c) na implementáciu, zmeny, upgrade alebo inovácie pre IT systémy a

d) na nové pripojenia a integrácie pre IT alebo OT systémy.

2.5 Dodávateľ je povinný preukázať prevádzkovateľovi základnej služby, do akej miery zabezpečil produkt a jeho komponenty z pohľadu základných bezpečnostných požiadaviek a rozšírených bezpečnostných požiadaviek a že produkt a jeho komponenty, ako aj ich architektúra, dizajn, konfigurácia a prevádzka zohľadňujú a spĺňajú základné bezpečnostné požiadavky a rozšírené bezpečnostné požiadavky, požiadavky dobrej praxe, ako i štandardy priemyselného odvetvia.

2.6 Pri uzatvorení zmluvy dodávateľ preukazuje prevádzkovateľovi základnej služby pripravenosť zabezpečiť súlad s odsekom 2.5 tohto článku predložením minimálne jedného alebo viacerých nasledovných dokumentov:

a) všeobecného formálneho vyhlásenia dodávateľa o bezpečnosti produktu alebo o bezpečnostných vlastnostiach produktu (dôvernosť, integrita, dostupnosť, nepopierateľnosť vykonaných aktivít) obsahujúceho zoznam všetkých opatrení, ktoré boli

pri produkte (komponente), jeho architektúre, dizajne, konfigurácii a plánovanej prevádzke nasadené alebo brané do úvahy, v ktorom budú uvedené aj akékoľvek všeobecne známe a overiteľné postupy riadenia kvality a získané nezávislé potvrdenia o aplikovaných postupoch,

b) vyhlásenia dodávateľa o aplikovaní všeobecne známych zásad najlepšej praxe zabezpečujúcej bezpečnosť produktu (napr. štandardy, checklisty alebo odporúčania, ako sú ISO/IEC 62443, ISO/IEC 27001:2013, ISO/IEC 27019:2017, OWASP, CIS, PCI DSS, NIST SP alebo dokumentácia k bezpečnému nasadzovaniu, konfigurácii alebo prevádzke od výrobcov jednotlivých komponentov produktu), v ktorom treba vždy podrobnejšie vysvetliť, ktorá časť tejto praxe a v akom rozsahu bola pre daný produkt aplikovaná (napr. pri odkazovaní na certifikáciu podľa ISO/IEC 27001 je treba uviesť, aký bol skutočný rozsah certifikácie a ako tento súvisí s daným produktom; pri odkazovaní na dokumentáciu od výrobcu niektorého z komponentov produktu napr. pri Oracle databáze treba spomenúť konkrétny dokument výrobcu, podľa ktorého dodávateľ postupoval, napr. Oracle® Database Security Guide 19c, E96299-10; podobne, ak bol produkt posúdený z pohľadu napr. požiadaviek štandardu NIST SP 800-82 alebo ISO/IEC 27019:2017, dodávateľ poskytne zoznam všetkých bezpečnostných opatrení, ktoré boli posudzované),

c) výsledkov formálnej analýzy rizík, ktorú môže vykonať sám dodávateľ alebo akákoľvek odborne spôsobilá a nezávislá osoba, pokiaľ z analýzy bude zrejmé, ktoré hrozby relevantné z hľadiska konkrétneho používania produktu boli posudzované, akými opatreniami boli príslušné zraniteľnosti minimalizované a aká známa metodika bola pri tom použitá (OCTAVE, CORAS, CRAMM, EBIOS, COBRA, IRAM/ISF, RA2 atď.).

2.7 Pri plnení hlavnej zmluvy a nasadzovaní produktu pred jeho uvedením do prevádzky a odovzdaním prevádzkovateľovi základnej služby dodávateľ preukazuje prevádzkovateľovi základnej služby súlad s odsekom 2.5 tohto článku predložením minimálne jedného alebo viacerých nasledovných dokumentov:

a) výsledkov štandardizovaných testov technických zraniteľností získaných prostredníctvom procesu identifikácie, kvantifikácie a prioritizácie zraniteľností v systéme a produkte aplikovaním vhodných testovacích nástrojov v rôznej fáze životného cyklu produktu, napríklad:

- vo fáze vývoja statickou analýzou zdrojového kódu (SAST – Static Application Security Testing) nástrojmi ako Checkmarx, Kiuwan,
- vo fáze testovania interaktívnou analýzou zdrojového kódu (IAST – Interactive Application Security Testing) nástrojmi ako Seeker (Synopsis),
- vo fáze prevádzky dynamickou analýzou zdrojového kódu (DAST – Dynamic Application Security Testing) nástrojmi ako Netsparker, Acunetix, AppScan, alebo sieťovými scannermi ako nmap, OpenVAS, Nessus,

vrátane predloženia najnovšej dostupnej správy o stave technických zraniteľností produktu (napr. scan na technické zraniteľnosti) a dokumentácie o spôsobe nasadzovania bezpečnostných záplat, pričom ak produkt využíva komponenty od iných výrobcov, musí správa o technických zraniteľnostiach a dokumentácia o nasadzovaní záplat zahŕňať aj tieto komponenty,

b) bezpečnostného auditu alebo penetračného testu vykonaných nezávislou treťou stranou, pričom bezpečnostný audit musí byť zameraný na tie relevantné bezpečnostné vlastnosti,

ktoré by v podmienkach nasadenia produktu u prevádzkovateľa základnej služby mali minimalizovať bezpečnostné riziká ohrozujúce základnú službu prevádzkovateľa základnej služby, a z penetračného testu musí byť zrejmé, ktoré bezpečnostné scenáre alebo možné zlyhania boli overované a ktoré špecifické prípady neboli predmetom testu (napr. získanie neoprávneného prístupu, vykonanie aktivity pod identitou iného používateľa, zahladenie stôp po vykonanej operácii alebo zničenie kritických dát),

c) výsledkov modelovania kybernetických hrozieb, ktorým sa posudzujú možné hrozby, pri ktorých sa predpokladá veľký až katastrofický dopad, s uvedením zoznamu všetkých možností založených na príležitosti, motivácii alebo technických prostriedkoch, ktoré má potenciálny útočník k dispozícii (model umožňuje určiť profil ohrozenia systému z pohľadu útočníka).

2.8 Výsledky testov, auditov alebo modelovania podľa odseku 2.7 tohto článku sa musia zameriavať na tie oblasti funkcionality a opatrenia, ktoré boli identifikované ako relevantné pre daný produkt z pohľadu zaručenia jeho kybernetickej bezpečnosti a dosiahnutia cieľov tejto bezpečnostnej zmluvy. Tieto výsledky sú následne jedným z podkladov pre rozhodnutie prevádzkovateľa základnej služby o akceptovaní produktu a o jeho uvedení do prevádzky.

2.9 Prevádzkovateľ základnej služby môže akceptovať aj iné dôkazy predložené dodávateľom, ktoré potvrdzujú súlad s odsekom 2.5 tohto článku (štandardy priemyselného odvetvia SANS, NIST, ISO štandardy a pod.).

2.10 Všetky základné bezpečnostné požiadavky a rozšírené bezpečnostné požiadavky prevádzkovateľ základnej služby overí vždy pri akceptácii produktu pred uvedením do prevádzky. Prevádzkovateľ základnej služby ich môže overiť aj kedykoľvek priebežne, náhodne alebo pri každej významnej zmene, napr. pri aktualizácii alebo upgrade na vyššiu alebo inak rozšírenú verziu produktu.

2.11 Dodávateľ je povinný písomne informovať prevádzkovateľa základnej služby o každej zmene, ktorá má významný vplyv na opatrenia realizované dodávateľom.

3. PREVENCIA KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV

3.1 Pre účely tejto bezpečnostnej zmluvy sa za kybernetický bezpečnostný incident považuje udalosť, ktorá reálne alebo potenciálne ohrozila alebo narušila dôvernosť, integritu alebo dostupnosť informačných aktív priamo alebo nepriamo súvisiacich s poskytovaním základnej služby.

3.2 Dodávateľ je povinný v rámci prevencie kybernetických bezpečnostných incidentov, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu prevádzkovateľa základnej služby, alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby, (ďalej len „**incidenty**“):

a) zabezpečiť vlastnú kybernetickú bezpečnosť, aby cez dodávateľa nebolo možné zasiahnuť siete a informačné systémy prevádzkovateľa základnej služby,

b) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení hlavnej zmluvy a tejto bezpečnostnej zmluvy alebo budú mať prístup k informáciám prevádzkovateľa základnej služby opísaným v článku 5 a článku 6 ods. 6.3 tejto bezpečnostnej zmluvy,

c) sledovať výstrahy a varovania a ďalšie informácie slúžiace na minimalizovanie, odvrátenie alebo nápravu následkov incidentov všeobecne,

d) sledovať hrozby dotýkajúce sa dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu prevádzkovateľa základnej služby,

e) predchádzať vzniku incidentov,

f) systematicky získavať (monitorovať a detegovať), sústreďovať (evidovať), analyzovať a vyhodnocovať informácie o incidentoch,

g) prijímať od prevádzkovateľa základnej služby varovania pred incidentami a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základnú službu prevádzkovateľa základnej služby,

h) zasielať prevádzkovateľovi základnej služby včasné varovania pred incidentami, o ktorých sa dozvie z vlastnej činnosti podľa tejto bezpečnostnej zmluvy alebo inak, a

i) spolupracovať s prevádzkovateľom základnej služby pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby.

3.3 Dodávateľ je povinný počas trvania tejto bezpečnostnej zmluvy mať technické, technologické a personálne vybavenie na úrovni potrebnej na riadne a včasné plnenie tejto bezpečnostnej zmluvy a mať zavedené úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti na úrovni potrebnej na efektívne napĺňanie cieľov tejto bezpečnostnej zmluvy.

3.4 Dodávateľ je povinný doručiť prevádzkovateľovi základnej služby úplný zoznam zamestnancov a pracovných rolí dodávateľa a všetkých subdodávateľov, ktorí sa budú podieľať na plnení hlavnej zmluvy a tejto bezpečnostnej zmluvy alebo budú mať prístup k informáciám prevádzkovateľa základnej služby opísaným v článku 5 a článku 6 ods. 6.3 tejto bezpečnostnej zmluvy, ktorý sa jeho doručením prevádzkovateľovi základnej služby stane súčasťou tejto bezpečnostnej zmluvy ako príloha č. 1 k tejto bezpečnostnej zmluve.

3.5 Každú zmenu v personálnom obsadení v zozname podľa odseku 3.4 tohto článku je dodávateľ povinný prevádzkovateľovi základnej služby písomne oznámiť, pričom pre oznamovanie zmien sa použijú ustanovenia hlavnej zmluvy o doručovaní.

3.6 Dodávateľ je povinný stanoviť postupy plnenia svojich povinností podľa tejto bezpečnostnej zmluvy v bezpečnostnej dokumentácii, ktorá musí byť aktuálna a musí zodpovedať aktuálnemu stavu; bezpečnostnú dokumentáciu je na požiadanie povinný predložiť prevádzkovateľovi základnej služby na nahliadnutie a zhotovenie kópií.

3.7 Dodávateľ je povinný prijať a dodržiavať všeobecné bezpečnostné opatrenia podľa STN ISO/IEC 27002:2013 (Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti) minimálne v rozsahu špecifikovanom v bezpečnostných smerniciach prevádzkovateľa základnej služby.

3.8 Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia v oblastiach podľa § 20 ods. 3 písm. e) f), h), j) a k) zákona o kybernetickej bezpečnosti v rozsahu podľa § 8, 10, 12, 14 a 15 vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah

všeobecných bezpečnostných opatrení, a v rozsahu špecifikovanom v bezpečnostných smerniciach prevádzkovateľa základnej služby.

4. REAKTIVITA PRI RIEŠENÍ INCIDENTOV

4.1 Dodávateľ je povinný bezodkladne hlásiť každý incident prevádzkovateľovi základnej služby spôsobom určeným prevádzkovateľom základnej služby vrátane určenia stupňa jeho závažnosti, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie incidentov. Ak do okamihu hlásenia incidentu nepominuli jeho účinky, dodávateľ je povinný odoslať neúplné hlásenie incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

4.2 Dodávateľ je povinný riešiť incidenty najmä odozvou alebo inou reakciou na incident, ohraničením incidentu a jeho dopadov, nápravou následkov incidentu, asistenciou pri riešení incidentu na mieste, reakciou na incident a podporou reakcií na incident (ďalej len „**reaktívne opatrenie**“). Pri riešení incidentov je dodávateľ povinný na žiadosť prevádzkovateľa základnej služby spolupracovať s prevádzkovateľom základnej služby, Národným bezpečnostným úradom a Ministerstvom hospodárstva Slovenskej republiky, prípadne ďalšími orgánmi verejnej správy a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie získané z vlastnej činnosti podľa tejto bezpečnostnej zmluvy alebo inak, ktoré by mohli byť dôležité pre riešenie incidentu.

4.3 Dodávateľ je povinný v čase incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní, a poskytnúť ho prevádzkovateľovi základnej služby.

4.4 Dodávateľ je povinný oznámiť prevádzkovateľovi základnej služby skutočnosti, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.

4.5 Dodávateľ je povinný bezodkladne oznámiť a preukázať prevádzkovateľovi základnej služby vykonanie reaktívneho opatrenia a jeho výsledok.

4.6 Po vyriešení incidentu je dodávateľ na výzvu prevádzkovateľa základnej služby v určenej lehote povinný predložiť prevádzkovateľovi základnej služby návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu incidentu (ďalej len „**bezpečnostné opatrenie**“) na schválenie. Ak dodávateľ nenavrhne ochranné opatrenie v určenej lehote, alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je dodávateľ povinný spolupracovať s prevádzkovateľom základnej služby na jeho návrhu.

4.7 Po schválení bezpečnostného opatrenia prevádzkovateľom základnej služby je dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať.

4.8 Po vykonaní bezpečnostného opatrenia dodávateľom je dodávateľ povinný preveriť jeho účinnosť.

5. MLČANLIVOSŤ

5.1 Dodávateľ je povinný zachovávať mlčanlivosť o skutočnostiach, o ktorých sa dozvie v súvislosti s plnením hlavnej zmluvy a tejto bezpečnostnej zmluvy, ktoré nie sú verejne známe a ktoré by mohli uľahčiť kybernetický útok alebo viesť ku kybernetickému incidentu (najmä informácie o IT/OT architektúre, používaných systémoch, ich dodávateľoch a verziách, o topológii sietí, o konfiguráciách a pod.). Rovnako je dodávateľ povinný zachovávať mlčanlivosť o reaktívnych

opatreniach a bezpečnostných opatreniach, ako aj o opatreniach a bezpečnostných smerniciach prevádzkovateľa základnej služby.

5.2 V prípade pochybností o tom, či sa jedná o informácie podľa odseku 5.1 tohto článku, platí pre dodávateľa pravidlo, že sa jedná o informácie, o ktorých je dodávateľ povinný zachovávať mlčanlivosť.

5.3 Povinnosť zachovávať mlčanlivosť podľa tohto článku trvá aj po skončení tejto bezpečnostnej zmluvy.

5.4 Výnimky z povinnosti zachovávať mlčanlivosť podľa tohto článku upravuje zákon o kybernetickej bezpečnosti.

5.5 Dodávateľ je povinný zabezpečiť, aby v rovnakom rozsahu dodržiavali povinnosť mlčanlivosti jeho zamestnanci, subdodávatelia a ich zamestnanci, a to aj po zániku ich pracovnoprávneho vzťahu alebo obchodného vzťahu.

5.6 Po ukončení tejto bezpečnostnej zmluvy je dodávateľ povinný vrátiť alebo previesť na prevádzkovateľa základnej služby všetky informácie, ku ktorým mal počas trvania tejto bezpečnostnej zmluvy prístup, resp. tieto podľa pokynu prevádzkovateľa základnej služby zničiť.

6. SPOLOČNÉ USTANOVENIA

6.1 Dodávateľ je povinný plniť povinnosti podľa tejto bezpečnostnej zmluvy v súlade so zákonom o kybernetickej bezpečnosti a jeho vykonávacími predpismi vrátane všeobecných bezpečnostných opatrení, bezpečnostných štandardov, znalostných štandardov v oblasti kybernetickej bezpečnosti a identifikačných kritérií pre jednotlivé kategórie kybernetických bezpečnostných incidentov, ďalej operačnými postupmi, metodikami, politikami správania sa v kybernetickom priestore, zásadami predchádzania kybernetickým bezpečnostným incidentom a zásadami riešenia kybernetických bezpečnostných incidentov, ktoré vydáva Národný bezpečnostný úrad v oblasti kybernetickej bezpečnosti.

6.2 Dodávateľ je ďalej povinný plniť povinnosti podľa tejto bezpečnostnej zmluvy v súlade so sektorovými bezpečnostnými opatreniami, ktoré vydáva Ministerstvo hospodárstva Slovenskej republiky v spolupráci s Národným bezpečnostným úradom.

6.3 Dodávateľ je povinný spracovávať informácie, ktoré by mohli mať vplyv na základnú službu prevádzkovateľa základnej služby alebo ktoré by sa mohli týkať kybernetickej bezpečnosti sietí a informačných systémov prevádzkovateľa základnej služby tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.

6.4 Dodávateľ je povinný mať umiestnenú svoju dokumentáciu, informačné systémy a ostatné informačno-komunikačné technológie, ktoré sa týkajú plnenia povinností podľa tejto bezpečnostnej zmluvy, v zabezpečenom priestore tak, aby nebola narušená ich dôvernosť, autentickosť a integrita.

6.5 Dodávateľ je povinný dokumentovať svoju činnosť podľa tejto bezpečnostnej zmluvy (vrátane evidovania incidentov a dokumentovania školení svojich zamestnancov) a na žiadosť prevádzkovateľa základnej služby mu predložiť uvedenú dokumentáciu na nahliadnutie a zhotovenie kópií.

6.6 Dodávateľ je povinný plniť povinnosti podľa tejto bezpečnostnej zmluvy bezodkladne.

7. AUDIT KYBERNETICKEJ BEZPEČNOSTI

7.1 Prevádzkovateľ základnej služby je oprávnený vykonať u dodávateľa audit zameraný na overenie plnenia povinností dodávateľa podľa tejto bezpečnostnej zmluvy a efektívnosti ich plnenia, najmä na overenie technického, technologického a personálneho vybavenia dodávateľa na plnenie úloh, ako aj nastavenie procesov, rolí a technológií v organizačnej, personálnej a technickej oblasti u dodávateľa pre plnenie cieľov tejto bezpečnostnej zmluvy.

7.2 Prípadné nedostatky zistené auditom je dodávateľ povinný odstrániť bez zbytočného odkladu, najneskôr však v lehote 60 kalendárnych dní.

7.3 Prevádzkovateľ základnej služby môže audit u dodávateľa realizovať sám alebo prostredníctvom tretej osoby; v takom prípade práva a povinnosti prevádzkovateľa základnej služby pri výkone auditu realizuje prevádzkovateľom základnej služby poverená tretia osoba.

7.4 Dodávateľ je povinný pri audite spolupracovať s prevádzkovateľom základnej služby a sprístupniť mu svoje priestory, dokumentáciu a technické a technologické vybavenie, ktoré súvisia s plnením úloh podľa tejto bezpečnostnej zmluvy.

7.5 Prevádzkovateľ základnej služby je v rámci auditu oprávnený klásť otázky zamestnancom dodávateľa, ktorí sa podieľajú na plnení úloh podľa tejto bezpečnostnej zmluvy.

7.6 V rámci auditu je dodávateľ povinný preukázať prevádzkovateľovi základnej služby súlad s touto bezpečnostnou zmluvou, najmä preukázať svoju pripravenosť plniť úlohy podľa tejto bezpečnostnej zmluvy, aktuálne a vysoké bezpečnostné povedomie svojich zamestnancov, záväzok a poučenie svojich zamestnancov, subdodávateľov a ich zamestnancov o povinnosti mlčanlivosti podľa tejto bezpečnostnej zmluvy a aktuálnosť svojej bezpečnostnej dokumentácie.

7.7 Prevádzkovateľ základnej služby je povinný oznámiť dodávateľovi najmenej tri pracovné dni vopred svoj zámer realizovať u dodávateľa audit.

7.8 Vykonanie alebo nevykonanie auditu prevádzkovateľom základnej služby nezbavuje dodávateľa zodpovednosti za plnenie povinností dodávateľa vyplývajúcich z tejto bezpečnostnej zmluvy.

7.9 Ak dodávateľ neumožní vykonanie auditu, má sa za to, že neplní úlohy podľa tejto bezpečnostnej zmluvy.

7.10 Prevádzkovateľ základnej služby je povinný zachovávať mlčanlivosť o okolnostiach, o ktorých sa dozvie pri výkone auditu a ktoré nie sú verejne známe. Ustanovenia článku 5 ods. 5.3 a 5.4 tejto bezpečnostnej zmluvy platia rovnako a ustanovenie článku 5 ods. 5.5 tejto bezpečnostnej zmluvy platí primerane.

7.11 Za vytvorenie podmienok na zaistenie BOZP a PO a zabezpečenie a vybavenie priestorov dodávateľa na bezpečný výkon auditu zodpovedá v plnom rozsahu a výlučne dodávateľ. Dodávateľ je povinný preukázateľne informovať zamestnancov prevádzkovateľa základnej služby alebo iné ním poverené osoby vykonávajúce audit o nebezpečenstvách a ohrozeniach, ktoré sa pri výkone auditu v priestoroch dodávateľa môžu vyskytnúť, a o výsledkoch posúdenia rizika, o preventívnych opatreniach a ochranných opatreniach, ktoré vykonal dodávateľ na zaistenie BOZP a PO, o opatreniach a postupe v prípade poškodenia zdravia vrátane poskytnutia prvej pomoci, ako aj o opatreniach a postupe v prípade zdolávania požiaru,

záchranných prác a evakuácie, a preukázateľne ich poučiť o pokynoch na zaistenie BOZP a PO platných pre priestory dodávateľa.

8. ZODPOVEDNOSŤ DODÁVATEĽA

8.1 Dodávateľ berie na vedomie, že neplnenie jeho povinností podľa tejto bezpečnostnej zmluvy ohrozuje plnenie cieľov tejto bezpečnostnej zmluvy, pričom za dôsledky incidentov, ktoré by sa pri riadnom a včasnom plnení povinností dodávateľa podľa tejto bezpečnostnej zmluvy neprejavili, alebo by sa prejavili v menšej intenzite, zodpovedá prevádzkovateľovi základnej služby v plnom rozsahu (zodpovednosť za výsledok).

8.2 Za každé porušenie povinnosti dodávateľa vyplývajúcej z tejto bezpečnostnej zmluvy môže prevádzkovateľ základnej služby požadovať od dodávateľa zmluvnú pokutu vo výške 5 000 €. Zaplatením zmluvnej pokuty nie je dotknutý nárok na náhradu škody a náhradu škody môže prevádzkovateľ základnej služby požadovať v plnej výške bez ohľadu na úhradu zmluvnej pokuty.

8.3 Dodávateľ je povinný odstrániť prípadné porušenie svojej povinnosti vyplývajúce z tejto bezpečnostnej zmluvy bezodkladne, najneskôr však do troch (3) dní od doručenia výzvy prevádzkovateľa základnej služby, ak sa zmluvné strany nedohodnú písomne inak, pričom porušenie tohto ustanovenia bude považované za podstatné porušenie tejto bezpečnostnej zmluvy.

8.4 V prípade, ak v dôsledku porušenia povinnosti dodávateľa vyplývajúcej z tejto bezpečnostnej zmluvy vznikne prevádzkovateľovi základnej služby povinnosť hradiť poplatky, pokuty alebo iné peňažné sankcie uplatnené orgánmi verejnej správy voči prevádzkovateľovi základnej služby, bude dodávateľ povinný ich nahradiť prevádzkovateľovi základnej služby ako škodu.

9. KONTAKTNÉ OSOBY PRE OBLASŤ KYBERNETICKEJ BEZPEČNOSTI

9.1 Dodávateľ je povinný komunikovať pri plnení povinností podľa tejto bezpečnostnej zmluvy s prevádzkovateľom základnej služby spôsobom určeným prevádzkovateľom základnej služby, pričom dodávateľ musí mať vytvorené podmienky umožňujúce chránený prenos informácií.

9.2 Prevádzkovateľ základnej služby určuje nasledovnú kontaktnú osobu pre komunikáciu s dodávateľom pre oblasť kybernetickej bezpečnosti: Ing. Róbert Mramúch, tel. +421 915 958461, e-mail: robert.mramuch@mhth.sk.

9.3 Dodávateľ určuje nasledovnú kontaktnú osobu pre komunikáciu s prevádzkovateľom základnej služby pre oblasť kybernetickej bezpečnosti: _____, tel. _____, e-mail: _____.

9.4 Kontaktné osoby podľa odsekov 9.2 alebo 9.3 tohto článku môže príslušná zmluvná strana zmeniť, ak oznámi novú kontaktnú osobu druhej zmluvnej strane v písomnej forme. Pre oznamovanie novej kontaktnej osoby sa použijú ustanovenia hlavnej zmluvy o doručovaní.

10. ZÁVEREČNÉ USTANOVENIA

10.1 Táto bezpečnostná zmluva sa uzatvára na dobu určitú počas trvania hlavnej zmluvy. Prevádzkovateľ základnej služby je oprávnený od tejto bezpečnostnej zmluvy odstúpiť v prípadoch, ak dodávateľ porušuje svoje povinnosti vyplývajúce z tejto bezpečnostnej zmluvy. Odstúpenie od tejto bezpečnostnej zmluvy sa musí urobiť písomne, inak sa na neho neprihliada. Pre doručovanie odstúpenia od tejto bezpečnostnej zmluvy sa použijú

ustanovenia hlavnej zmluvy o doručovaní. Zrušenie tejto bezpečnostnej zmluvy sa netýka tých ustanovení, ktoré vzhľadom na svoju povahu alebo ich výslovné znenie, majú trvať aj po zrušení tejto bezpečnostnej zmluvy, a záväzkov na náhradu škody spôsobenej porušením povinností podľa tejto bezpečnostnej zmluvy.

10.2 Po ukončení tejto bezpečnostnej zmluvy je dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na prevádzkovateľa základnej služby všetky licencie, práva alebo súhlasy potrebné na zabezpečenie kontinuity prevádzkovania základnej služby prevádzkovateľom základnej služby, ktoré musia byť účinné najmenej po dobu piatich rokov po ukončení tejto bezpečnostnej zmluvy.

10.3 Táto bezpečnostná zmluva sa spravuje zákonmi Slovenskej republiky bez prihliadnutia ku kolíznym normám. Právne vzťahy neupravené touto bezpečnostnou zmluvou sa riadia ustanoveniami Obchodného zákonníka č. 513/1991 Zb. v znení neskorších predpisov a súvisiacimi predpismi.

10.4 Súdy Slovenskej republiky majú výlučnú právomoc na rozhodovanie akýchkoľvek sporov týkajúcich sa tejto bezpečnostnej zmluvy. V prípade, ak dodávateľom bude zahraničná osoba, zmluvné strany sa dohodli, že miestne príslušným súdom bude súd, v obvode ktorého má sídlo prevádzkovateľ základnej služby.

10.5 Táto bezpečnostná zmluva sa môže meniť alebo ukončiť dohodou zmluvných strán iba v písomnej forme.

10.6 Ak by sa dôvod neplatnosti vzťahoval len na časť tejto bezpečnostnej zmluvy, bude neplatnou len táto časť.

10.7 Táto bezpečnostná zmluva tvorí úplnú dohodu medzi zmluvnými stranami týkajúcu sa predmetnej záležitosti. Podpisom tejto bezpečnostnej zmluvy zanikajú všetky predchádzajúce písomné a ústne dohody súvisiace s predmetom tejto bezpečnostnej zmluvy a žiadna zo zmluvných strán sa nemôže dovolávať zvláštnych v tejto bezpečnostnej zmluve neuvedených ústnych dojednaní a dohôd.

10.8 Táto bezpečnostná zmluva bola vyhotovená v dvoch rovnopisoch, po jednej pre každú zmluvnú stranu.

10.9 Zmluvné strany berú na vedomie, že prevádzkovateľ základnej služby je v zmysle § 2 ods. 3 zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov povinnou osobou, a preto môže byť táto bezpečnostná zmluva v zmysle § 5a zákona o slobode informácií v spojení s § 47a Občianskeho zákonníka č. 40/1964 Zb. v znení neskorších predpisov povinne zverejňovanou zmluvou.

10.10 Zmluvné strany berú na vedomie, že účinnosť tejto bezpečnostnej zmluvy je v zmysle § 47a Občianskeho zákonníka v nadväznosti na § 5a zákona o slobode informácií podmienená jej zverejnením v Centrálnom registri zmlúv vedenom Úradom vlády Slovenskej republiky.

10.11 Táto bezpečnostná zmluva nadobúda platnosť dňom podpisu oboma zmluvnými stranami a účinnosť dňom nasledujúcim po dni zverejnenia v Centrálnom registri zmlúv.

10.12 Neoddeliteľnú súčasť tejto bezpečnostnej zmluvy tvorí jej príloha č. 1 – zoznam pracovných rolí dodávateľa (podľa článku 3 ods. 3.4 tejto bezpečnostnej zmluvy).

10.13 Zmluvné strany vyhlasujú, že sú plne spôsobilé na právne úkony, že ich zmluvná voľnosť nie je ničím obmedzená, že túto bezpečnostnú zmluvu neuzavreli ani v tiesni, ani za nápadne nevýhodných podmienok, že si obsah tejto bezpečnostnej zmluvy dôkladne prečítali a že tento im je jasný, zrozumiteľný a vyjadrujúci ich slobodnú, vážnu a spoločnú vôľu, a na znak súhlasu ju podpisujú.

Za prevádzkovateľa základnej služby:	**Za dodávateľa:**
V Bratislave dňa _____	V _____ dňa _____
Ing. Marcel Vrátny predseda predstavenstva	_____ _____
Ing. Lenka Smreková, FCCA členka predstavenstva	_____ _____

Príloha ____ k zmluve č. _____

Príloha č. 1 – Zoznam pracovných rolí dodávateľa

Meno zamestnanca	Pracovná rola	Zamestnávateľ (dodávateľ alebo subdodávateľ)