1. ÚČEL A ROZSAH

Dokument „**Politiky kybernetickej a informačnej bezpečnosti pre dodávateľov a tretie strany**“ napĺňa požiadavky zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov 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 dodávateľov a tretích strán MH Teplárenský holding, a.s.

Cieľom je minimalizovať bezpečnostné riziká spojené s pôsobením dodávateľa (ďalej aj ako tretia strana) v prostredí spoločnosti MH Teplárenský holding, a.s., a preniesť na ňu zodpovednosť za možné následky nedodržiavania týchto bezpečnostných požiadaviek.

Dodávateľ sa zaväzuje, že tieto predpisy budú predstavené zamestnancom dodávateľa, príp. subdodávateľom a ich dodržiavanie bude kontrolované.

Záväznosť pre: Dodávatelia a tretie strany MH Teplárenský holding, a.s.

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

1.1 ZMENOVÝ LIST

Dátum	Vydanie	Popis zmeny	Meno zamestnanca vykonávajúceho zmenu
05/2025	1	nový dokument	Róbert Mramúch
10/2025	2	aktualizácia legislatívnych zmien	Róbert Mramúch
21/2026	3	úprava príloh a doplnenie textu	Tomáš Baksa

2. DEFINÍCIE POJMOV A SKRATKY

ANSI	American National Standard Institute
BSI	Federal Ofiice for Information Security
IB	Informačná Bezpečnosť
KB	Kybernetická Bezpečnosť
NIST	National Institute of Standards and Technology
SW	Software (programové vybavenie)
TK	Tenký klient
V227	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
VPN	Virtual Private Network, Virtuálna privátna sieť
Workaround	Náhradné riešenie alebo opatrenie
ZoKB	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
ZoBOaNP	Zmluva o bezp. opatreniach a notifikačných povinnostiach, podľa požiadaviek ZoKB 69/2018 Z. z.
ZS	Základná služba (výroba a distribúcia tepla, výroba elektriny)
PKZS	Prevádzkovanie kritickej základnej služby (výroba a distribúcia tepla, výroba elektriny)
MHTH	MH Teplárenský holding, a.s.
PKIB	Politika kybernetickej a informačnej bezpečnosti
RIS	Riadiace informačné systémy
Dodávateľ	Subjekt, s ktorým je uzatvorený priamy zmluvný vzťah.
Tretia strana	Subjekt bez priameho zmluvného vzťahu. Príklad: subdodávateľ dodávateľa, banka, regulátor, externý audítor.

3. ÚVOD

Cieľom tejto politiky je informovať Dodávateľa o bezpečnostných požiadavkách, na základe čoho dodávateľ svojím podpisom deklaruje súhlas a vôľu splniť tieto požiadavky.
Dodávateľ sa svojím podpisom zaväzuje tieto požiadavky dodržiavať v prehlásení tretej strany. Vzor prehlásenia je uvedený na konci tohto dokumentu.
Tieto zásady platia pre každú tretiu stranu, ktorá má zmluvný vzťah so spoločnosťou MH Teplárenský holding, a.s. (MHTH), na základe ktorého sa stáva súčasťou vnútorného prostredia spoločnosti počas doby nevyhnutnej na realizáciu dohodnutého diela či projektu.

4. APLIKOVATEĽNOSŤ

Uvedené kapitoly tejto politiky sú predmetom poučenia dodávateľa/tretej strany, vzťahujúce sa na osoby tretích strán v závislosti od ich prístupu a náplne práce na pridelenej úlohe alebo projekte v spoločnosti MH Teplárenský holding, a.s.
Politika ustanovuje základné úlohy a princípy spolupráce zmluvných strán s cieľom zabezpečiť kybernetickú bezpečnosť, bezpečnosť sietí a informačných systémov MHTH, ako prevádzkovateľa základnej služby počas ich životného cyklu, predchádzať kybernetickým bezpečnostným incidentom, ktoré by sa mohli dotknúť sietí a informačných systémov MHTH, a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania kritických základných služieb (PKZS).

5. ZODPOVEDNOSTI A PRÁVOMOCI

Zamestnanci tretích strán 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 neprišlo k ich poškodeniu alebo zneužitiu,
    - zachovávať mlčanlivosť, nezverejňovať, neposkytovať alebo nesprístupňovať údaje iným osobám, ak to priamo nevyplýva z ich pracovných pokynov alebo úloh,
    - pravidelne sa vzdelávať v oblasti informačnej bezpečnosti,
- zamestnanci tretích strán 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,
- zamestnanci tretích strán sú povinní dodržiavať pokyny MHTH a bez zbytočného odkladu upozorniť MHTH na nevhodnú povahu vydaných pokynov, vrátane pokynov a opatrení obsiahnutých v bezpečnostných smerniciach prevádzkovateľa základnej služby.

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 MHTH,
b) vytvárať a zvyšovať bezpečnostné povedomie svojich zamestnancov, ktorí sa budú podieľať na plnení diela/služby, alebo budú mať prístup k informáciám MHTH,

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

d) sledovať hrozby dotýkajúce sa dodávateľa, ktoré by mohli mať potenciálny nepriaznivý vplyv na základné služby MHTH,

e) predchádzať vzniku incidentov,

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

g) prijímať od MHTH varovania pred incidentmi a vykonávať preventívne opatrenia potrebné na odvrátenie hrozieb, ktoré by mohli mať potenciálny nepriaznivý vplyv na základné služby MHTH,

h) zasielať MHTH včasné varovania pred incidentmi, o ktorých sa dozvie z vlastnej činnosti alebo inak, a

i) spolupracovať s MHTH pri zabezpečovaní kybernetickej bezpečnosti sietí a informačných systémov MHTH.

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

Dodávateľ je povinný doručiť a podľa skutočného stavu priebežne aktualizovať MHTH úplný zoznam zamestnancov a pracovných rolí dodávateľa a všetkých subdodávateľov a ich zamestnancov, ktorí sa budú podieľať na plnení diela/služby alebo budú mať prístup k informáciám MHTH, ktorý sa jeho doručením prevádzkovateľovi základnej služby stane súčasťou tejto bezpečnostnej dokumentácie, ako samostatná príloha.

Dodávateľ je povinný prijať a dodržiavať bezpečnostné opatrenia v oblastiach podľa § 20 ZoKB.

Dodávateľ je povinný bezodkladne hlásiť kontaktnej osobe MHTH, alebo cez HelpDesk MHTH každý incident, spôsobom určeným MHTH 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.

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. Pri riešení incidentov je dodávateľ povinný na žiadosť MHTH spolupracovať s MHTH, Národným bezpečnostným úradom a Ministerstvom hospodárstva Slovenskej republiky, prípadne ďalšími orgánmi verejnej správy a na tento účel im poskytnúť potrebnú súčinnosť a všetky informácie, ktoré by mohli byť dôležité pre riešenie incidentu.

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

Dodávateľ je povinný oznámiť MHTH skutočnosti, že v súvislosti s incidentom mohlo dôjsť k spáchaniu trestného činu.

Dodávateľ je povinný bezodkladne oznámiť a preukázať MHTH vykonanie reaktívneho opatrenia a jeho výsledok.

Po vyriešení incidentu je dodávateľ na výzvu MHTH v určenej lehote povinný predložiť návrh opatrení na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu incidentu na

schválenie. Ak dodávateľ nenavrhne bezpečnostné opatrenie v určenej lehote, alebo ak je navrhované opatrenie zjavne neúspešné, je dodávateľ povinný spolupracovať s MHTH na jeho návrhu.

Po schválení bezpečnostného opatrenia MHTH je dodávateľ povinný ochranné opatrenie bez zbytočného odkladu vykonať.

Po vykonaní bezpečnostného opatrenia dodávateľom je dodávateľ povinný preveriť jeho účinnosť a s protokolom oboznámiť MHTH

6. DODRŽIAVANIE ZMLÚV A NORIEM

6.1 HODNOTENIE BEZPEČNOSTI PREDMETU DODÁVKY

Na požiadanie MHTH tretia strana poskytne bezodkladne všetky informácie potrebné na posúdenie bezpečnosti predmetu dodávky (napr. test/auditné správy, skeny zraniteľností a analýzy robustnosti kódov a pod.).

6.2 BEZPEČNOSTNÉ ZÁSADY

Dodávateľ sa zaväzuje použiť odporúčané postupy, ktoré sú v súlade s aktuálnymi všeobecne akceptovanými bezpečnostnými štandardmi (ISO/IEC 27001 a pod.).
Ak je dodávateľ certifikovaný, poskytne spoločnosti MHTH svoj bezpečnostný certifikát a bude ho informovať o obnovení alebo zrušení svojich certifikátov.
Ak si MHTH vybral dodávateľa na základe certifikácie (napr. ISO/IEC 27001), dodávateľ musí udržiavať takúto certifikáciu počas celého trvania jeho zmluvných povinností.

6.3 AUDIT

MHTH má právo vykonávať audity na kontrolu, či dodávateľ dodržiava bezpečnostné požiadavky definované v tejto politike a predmete dodávaného produktu/diela/služby podľa zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností (ZoBOaNP) podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ZoKB).

6.4 TRETIE STRANY DODÁVATEĽA - SUPPLY CHAIN

V prípade, že dodávateľ na poskytovanie predmetu dodávky spoločnosti MHTH využíva tretie strany, dodávateľ zabezpečí, aby tieto tretie strany spĺňali bezpečnostné opatrenia dohodnuté v tejto politike a v zmysle vyhlášky 227/2025 Z.z.

6.5 NEDODRŽIAVANIE PKIB

V prípade, že sa dodávateľ dozvie o nedodržaní bezpečnostných opatrení v predmete dodávky, bezodkladne poskytne spoločnosti MHTH analýzu situácie a plán nápravy. Ak spoločnosť MHTH akceptovala plán nápravy, dodávateľ ho zrealizuje bez nákladov pre MHTH a dodávateľ poskytne dôkaz o účinnosti plánu nápravy.

7. FYZICKÁ BEZPEČNOSŤ

7.1 ZÁKLADNÉ ZÁSADY FYZICKEJ BEZPEČNOSTI

Pod fyzickými priestormi, ktorých sa týkajú pravidlá uvedené v tomto dokumente, sa myslia administratívne a technologické priestory vrátane príslušenstva, ktoré spoločnosť MHTH dočasne alebo trvale užíva pre výkon svojich podnikateľských činností. Zároveň ide o

priestory, v rámci ktorých spoločnosť MHTH vykonáva elektronickú alebo fyzickú kontrolu vstupu, príp. pohybu v týchto priestoroch.

Všeobecne platí pravidlo, že vstup každej osoby do priestorov spoločnosti MHTH je kontrolovaný a monitorovaný. Spoločnosť MHTH môže na základe uzatvorenia zmluvy s dodávateľom poskytnúť zamestnancom dodávateľa pre vstup do priestorov spoločnosti MHTH prístupové identifikačné prvky (smart card prístupová karta).

Akákoľvek osoba tretej strany môže vstupovať iba do tých priestorov, do ktorých získala povolenie na vstup a iba na čas nevyhnutne potrebný na výkon činností tejto osoby, ktorými bola poverená a zároveň je povinná pri vstupe (aj viacerých osôb) vykonať identifikáciu prostredníctvom prístupovej karty. Vstup do serverovní a dátových centier spoločnosti MHTH je povolený len osobám v sprievode zamestnanca spoločnosti, ktorý je na tento účel poverený. Do priestorov spoločnosti MHTH je povolené vnášať iba veci nevyhnutné na výkon činnosti tretej strany, s výnimkou bežných osobných vecí.
Je prísne zakázané z priestorov spoločnosti MHTH vynášať akékoľvek technické zariadenia, počítače, riadiace prvky, nosiče informácií, dokumenty a iné veci patriace spoločnosti MHTH, pokiaľ to nie je nevyhnutné na výkon činností tretej strany v súlade s príslušnou zmluvou.

Tento dokument neupravuje bezpečnosť a ochranu zdravia pri práci a protipožiarnu ochranu v rámci priestorov spoločnosti MHTH.

8. KYBERNETICKÁ (LOGICKÁ / DIGITÁLNA) BEZPEČNOSŤ

Pod logickým/digitálnym/kybernetickým prostredím, na ktoré sa vzťahujú pravidlá uvedené v tomto dokumente, sa myslia informačné systémy v prostredí spoločnosti MHTH, ktoré spoločnosť MHTH dočasne alebo trvale užíva pre výkon svojich podnikateľských činností.
Pre logické prostredie všeobecne platí, že prístupy tretích strán do informačných systémov spoločnosti MHTH sú riadené a realizované výhradne cez centrálny VPN koncentrátor (v prípade prístupu do OT systémov MHTH, navyše cez bezpečný vzdialený prístup SRA - Secure Remote Access). Iný spôsob vzdialeného prístupu nie je možný. Prístupy do informačných systémov pre zamestnancov tretích strán riadia výhradne interní zamestnanci MHTH, ktorí sú zodpovední za tretiu stranu. Akákoľvek osoba tretej strany môže pristupovať iba do tých informačných systémov, do ktorých získala oprávnenie, v ostatných prípadoch je povinná upovedomiť MHTH o tejto skutočnosti. V prípade práce onsite v priestoroch MHTH s prístupom tretích strán do informačných systémov spoločnosti MHTH, je takýmto osobám poskytnuté na prácu zariadenie. V prípade použitia vlastného zariadenia, tretia strana súhlasí s inštaláciou SW agenta/agentov (napríklad XDR, Vulnerability Management - VM) pre riadenie stavu bezpečnosti na fyzickom ako aj virtuálnych zariadeniach.

8.1 ZÁKLADNÉ ZÁSADY (LOGICKEJ A DIGITÁLNEJ BEZPEČNOSTI)

Dodávateľ alebo zamestnanec dodávateľa:

- nesmie poskytnúť svoje autentifikačné údaje inej osobe - používateľ účtu je v každom prípade zodpovedný za používanie jemu prideleného účtu,
- musí chrániť prístup k svojmu počítaču, ak sa práve nepoužíva, tzn. uzamknúť počítač a odpojiť aktívne pripojenia do systémov MHTH aj v prípade pripojenia v režime vzdialené pripojenie,
- je povinný na zariadeniach cez ktoré pristupuje k informačným aktívam MHTH, používať riadne aktualizovaný antivírusový software a zodpovedá za prípadné následky pre spoločnosť MHTH v prípade infikovania malvérom alebo vírusom, ktorý vznikol pôsobením tretej strany v spoločnosti MHTH. Zariadenie musí prejsť pred pripojením do prostredia

spoločnosti MHTH skenom na zraniteľnosti pomocou technických prostriedkov v správe MHTH,

- ak pracuje mimo územia Slovenskej republiky (prípadne mimo krajiny, kde má dodávateľ ústredie) musí byť táto vzdialená práca vopred autorizovaná MHTH,
- má zakázané priame VPN prístupy do OT siete ako aj inštaláciu takýchto zariadení v technických miestnostiach podniku,
- musí pred a po ukončení práce, informovať príslušného manažéra RIS a riadiaceho pracovníka prevádzky (vedúci zmenový zamestnanec) o svojej činnosti,
- nesmie v režime telepráca vykonávať také zmeny a zásahy do riadiaceho systému, ktoré môžu mať negatívny dopad na bezpečnosť, dostupnosť, kontinuitu procesov a majetok spoločnosti MHTH. Toto neplatí v prípade riešenia porúch P1,
- nesmie svojvoľne inštalovať LTE modemy, ani VPN prestupy z interných sietí spoločnosti MHTH smerom do verejného internetu,
- nesmie svojvoľne inštalovať žiadny SW, ktorého inštalácia mu nebola zo strany MHTH povolená. Taktiež nesmie na zariadeniach patriacich MHTH kopírovať a spúšťať samostatne spustiteľné verzie SW bez predchádzajúceho povolenia zo strany MHTH,
- nesmie svojvoľne meniť konfiguráciu/nastavenia/kmeňové dáta SW, prípadne ho spúšťať, zastavovať jeho beh alebo reštartovať bez predchádzajúceho povolenia zo strany MHTH,
- nesmie svojvoľne meniť konfiguráciu/nastavenia/kmeňové dáta prvkov IT/OT infraštruktúry, prípadne ich spúšťať, zastavovať jeho beh alebo reštartovať bez predchádzajúceho povolenia zo strany MHTH,
- nesmie do IT/OT infraštruktúry svojvoľne pripájať žiadne zariadenia bez predchádzajúceho povolenia zo strany MHTH,
- nesmie sa v prípade lokálneho pripojenia do siete MHTH paralelne pripájať do iných sietí alebo smerom do verejného internetu,
- nesmie v prípade pripojenia do siete MHTH pomocou VPN tunelovať toto pripojenie pomocou inej VPN služby,
- nesmie požívať prenosné médiá v IT/OT prostredí bez predchádzajúceho súhlasu zo strany MHTH. V prípade, že je použitie povolené, tak je povinný predmetné médium pred každým použitím skontrolovať antivírusovým SW a výsledok kontroly zdokladovať písomným, digitálnym protokolom/záznamom,
- nesmie vytvárať kópie/zálohy prvkov IT/OT infraštruktúry, IT/OT zariadení, SW a dokumentácie bez predchádzajúceho súhlasu/poverenia zo strany MHTH,
- nesmie prechovávať kópie/zálohy prvkov IT/OT infraštruktúry, IT/OT zariadení, SW a dokumentácie na vlastných zariadeniach alebo ich vynášať mimo priestorov MHTH bez predchádzajúceho súhlasu/poverenia zo strany MHTH.
- musí podstúpiť a strpieť kontrolu vlastných digitálnych zariadení za účelom validácie plnenia jeho povinností. Táto kontrola sa môže skladať hlavne, ale nielen z kontroly stavu antivírového SW, kontroly antivírovým programom, kontroly za účelom preukázania, že nie sú vynášané žiadne nepovolené dáta patriace MHTH,

- nesmie počas pripojenia do siete MHTH vysielať žiadnu nepovolenú či nevyžiadanú komunikáciu.

9. OCHRANA MAJETKU A INFORMÁCIÍ

Tretím stranám je v priestoroch spoločnosti MHTH zakázané:

- akékoľvek vynášanie a premiestňovanie vecí patriacich spoločnosti MHTH, alebo jej zamestnancom, osobitne počítačov, častí riadiacich systémov, počítačových zariadení, iných technológií a pod.,
- zapínanie, vypínanie, alebo akákoľvek iná manipulácia s technickými zariadeniami umiestnenými v priestoroch spoločnosti MHTH (ak tieto činnosti nie sú súčasťou plnení tretej strany na základe príslušnej zmluvy so spoločnosťou MHTH),
- vnášať do priestorov spoločnosti MHTH osobné počítače, zariadenia na ukladanie elektronických informácií a nosiče elektronických informácií (napr. notebooky, USB disky, prenosné pevné disky, prenosné napaľovačky a pod.), pokiaľ tieto zariadenia neslúžia výlučne na výkon činností tretej strany v priestoroch spoločnosti MHTH,
- z priestorov spoločnosti MHTH vynášať akékoľvek nosiče elektronických informácií, počítače a dokumenty patriace spoločnosti MHTH a akokoľvek inak s týmito vecami manipulovať, pokiaľ to výslovne nie je súčasťou plnenia tretej strany v súlade s príslušnou zmluvou.

Zamestnanci tretej strany, ktorí pri poskytovaní svojich služieb prídu do styku so služobnými/obchodnými informáciami alebo osobnými údajmi patriacimi spoločnosti MHTH, nesmú tieto informácie použiť, zneužiť, zverejniť ani neoprávnene poskytnúť žiadnym ďalším stranám.
Tretia strana sa zaručuje prijať záväzné bezpečnostné opatrenia pre riadenie prístupových prvkov a prístupových práv, ktoré zaručia používanie nástrojov a politík na ochranu dát pred stratou a neoprávneným sprístupnením tretím stranám, vrátane dát na pamäťových nosičoch, a to pre všetky vlastné procesy, ktoré sú priamo alebo nepriamo prepojené s výkonom zmluvných služieb.
Dodávateľ alebo tretia strana, bez toho, aby boli dotknuté predchádzajúce ustanovenia, sa zaručuje prijať záväzné bezpečnostné opatrenia pre bezpečné riadenie prvkov a prístupov, ktoré zaručia:

- povinnú zmenu hesla pri prvom prihlásení,
- zamedzenie používania rovnakých hesiel,
- automatickú kontrolu kvality hesiel,

a to pre všetky vlastné procesy, ktoré sú priamo alebo nepriamo prepojené s výkonom zmluvných služieb.

Vzhľadom k tomu, že spoločnosť MHTH v súvislosti s vykonávaním svojich podnikateľských činností spracúva vo svojich informačných systémoch osobné údaje, je každá oprávnená osoba tretej strany, ktorej má byť povolený vstup do priestorov a/alebo prostredia spoločnosti MHTH, kde dochádza k spracovaniu osobných údajov, povinná podpísať poučenie o svojich povinnostiach pre prípad, že by prišla do styku s osobnými údajmi, v rozsahu uvedenom v Prílohe k tomuto dokumentu.

Tretie strany berú na vedomie, že niektoré priestory spoločnosti MHTH sú pre účely ochrany majetku monitorované kamerovým systémom (CCTV/MKS) alebo elektronickým zabezpečovacím a poplachovým systémom narušenia (EZS).
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).

10. KRYPTOGRAFIA A OVEROVANIE

10.1 ZMENA OVEROVACÍCH ÚDAJOV A ŠIFROVACÍCH KĽÚČOV

Všetky overovacie údaje a kryptografické kľúče (napr. certifikáty, páry kľúčov symetrické kľúče, heslá) v softvérových a hardvérových častiach predmetu dodávky bude MHTH meniť a chrániť podľa najnovších technológií. Pokiaľ ide o overovacie údaje a kryptografické kľúče, ktoré MHTH nemôže meniť, dodávateľ poskytne MHTH zoznam takýchto údajov a ich účel. Pri službách XaaS/Cloud sa táto požiadavka vzťahuje iba na overovacie údaje, ktoré MHTH používa na ochranu svojich údajov.

10.2 SILA KRYPTOGRAFICKÝCH ALGORITMOV A KĽÚČOV

Je dovolené zavádzať len štandardizované kryptografické algoritmy odporúčané vládnymi inštitúciami (napríklad BSI, ANSSI a NIST) v čase uzavretia alebo obnovenia zmluvy.

Je dovolené 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). Toto poučenie definuje opatrenia a súvisiace postupy pre rôzne oblasti a domény, kde sa používa šifrovanie a šifrovacie techniky.
Je povolené používať iba silné šifrovanie, špeciálne protokol AES256 pre uložené dáta (data at rest) a TLS1.2 alebo TLS 1.3 pre dáta pri prenose (data in transit).

10.3 ŠIFROVANIE V OT PROSTREDÍ

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, je 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).

11. BEZPEČNOSŤ V DIZAJNE (SECURITY BY DESIGN)

11.1 POSILNENIE OCHRANY (HARDENING)

Dodávateľ použije štandardizované postupy na posilnenie ochrany systému. To zahŕňa obmedzenie prístupu k protokolu, odstránenie alebo deaktiváciu nepotrebného softvéru, sieťových portov a služieb, odstránenie nepotrebných súborov, používateľských účtov, obmedzenie povolení pre súbor, riadenie opráv a protokolovanie.
Dodávateľ poskytne predmet dodávky (vrátane komponentov a služieb tretích strán) bezpečne nakonfigurovaný štandardne podľa postupov konfigurácie v súlade s najnovšími technológiami (napr. https://www.cisecurity.org/).
MHTH vyžaduje použitie zabezpečených protokolov na komunikáciu medzi jednotlivými systémami. Taktiež komunikácia medzi jednotlivými komponentmi systému musí byť zabezpečená. V prípade, že dodávateľ nie je schopný túto požiadavku splniť, musí požiadať o výnimku s tým, že navrhne alternatívne riešenie zabezpečenia komunikácie. V prípade, že daná komunikácia zabezpečuje prenos prihlasovacích údajov alebo informácií s vyššou klasifikáciou ako interné, tak v takom prípade nie je výnimku možné udeliť.
Bez ohľadu na vyššie uvedené dodávateľ poskytne MHTH všetky potrebné informácie na bezpečné konfigurovanie a používanie predmetu dodávky a zabezpečí, že takéto informácie budú vždy aktuálne počas trvania zmluvy.
Okrem toho dodávateľ zabezpečí, aby predmet dodávky neobsahoval žiadne „zadné vrátka“ (Back Doors).

11.2 ZISŤOVANIE BEZPEČNOSTNÝCH CHÝB SOFTVÉRU

Dodávateľ vykoná testy predmetu dodávky, aby sa uistil, že neobsahujú nebezpečné softvérové chyby uvedené v „CWE/SANS Top 25“ (http://cwe.mitre.org) a/alebo „OWASP TOP 10“ (http://www.owasp.org) v čase dodania (napr. odolnosť proti neočakávaným vstupom, ako sú SQL Injection, predvídateľné správanie v situáciách preťaženia, atď.). Dodávateľ overí nielen predmet dodávky, ale aj požadované podporné knižnice, ovládače, komponenty a iné podporné časti potrebné pre životný cyklus predmetu dodávky a zabezpečí bezpečnosť komponentov použitých v predmete dodávky.

11.3 BEZPEČNÁ POČIATOČNÁ KONFIGURÁCIA (SECURE ZERO CONFIGURATION)

Systémy, na ktorých sa prevádzkuje daný produkt alebo služba, vrátane súvisiacich systémových služieb, knižníc, databáz alebo nevyhnutných aplikácií, sú dodané v bezpečnej konfigurácii a v najaktuálnejších, výrobcami podporovaných, stabilných verziách a s bezpečnostnými záplatami, ktoré boli v čase dodávky k dispozícii.

Na systéme nie sú ponechané prípadné pred-definované (default) účty, všeobecné nastavenia v konfiguráciách a všetky nepotrebné/nevyužívané komponenty alebo systémové služby sú odstránené.

Dodávateľ poskytne zoznam všetkých dodávaných komponentov produktu alebo služby, potvrdí ich bezpečnú konfiguráciu, nasadenie najnovších bezpečnostných záplat a zaručí, že ide o verzie podporované príslušnými výrobcami.

11.4 ÚČTY A AUTENTIFIKÁCIA

Dodávateľ prehlasuje, že dodaný produkt alebo služba používa na úrovni systému len také účty (personálne, technické, servisné), ktoré sú nevyhnutné pre ich správne používanie a prevádzku, aplikuje na ne princíp minimálne nevyhnutných práv a privilégií, princíp oddeľovania rolí a používa iba bezpečné autentizačné metódy, protokoly a algoritmy, ktoré

zaručujú dôvernosť autentizačných prvkov (šifrovanie hesiel počas prenosu aj uloženia, viac-faktorová autentizácia a pod.) a nezneužiteľnosť identity, ktorú predstavujú.

11.5 KONFIGUROVANÉ SYSTÉMOVÉ SLUŽBY

Dodávaný produkt alebo služba sú nakonfigurované s minimálnym footprintom, to znamená, že obsahujú len tie systémové služby, knižnice a systémové nástroje (kompilátory, interpretery, debuggery), ktoré sú na ich prevádzku nevyhnutné.

Na požiadanie MHTH sa zmluvné strany môžu vzájomne dohodnúť na doplňujúcich bezpečnostných opatreniach, ktoré musí spĺňať predmet dodávky/služby/diela.

- Dodávateľ musí zaviesť systém riadenia prístupu a zodpovednosti navrhnutý tak, aby zabezpečil, že k systémom majú prístup len schválení zamestnanci pre jednotlivé operácie a podporu. Riadenie prístupu k systému zahŕňa systém overovania, povolenie, schválenie prístupu, poskytovanie a zrušenie pre zamestnancov a iných používateľov, definovaných dodávateľom.
- Dodávateľ musí používať antimalvérový softvér na skenovanie sťahovaných súborov prenášaných do prostredia MHTH. Definície malvéru sa aktualizujú minimálne každý deň.
- Dodávateľ sa zaväzuje vopred informovať MHTH o ukončení podpory IT platforiem a riešení, ktoré sú predmetom dodávky produktu/služby/diela (napr. operačné systémy, knižnice, podporné programy alebo databázy, ktoré už nebudú podporované dodávateľom). Povinnosť dodávateľa udržiavať systémy aktuálne počas celého trvania zmluvy týmto nie je dotknutá.
  Dodávateľ sa zaväzuje, že bude vykonávať pravidelnú aktualizáciu systémov bezpečnostnými záplatami prostredníctvom kontrolovaného procesu, bez zbytočných odkladov, pričom prijateľná doba reakcie závisí od závažnosti zverejnenej zraniteľnosti, najviac však šesť mesiacov a pri kritických zraniteľnostiach by nemala prekročiť pätnásť dní. Nasadenie bezpečnostných aktualizácií musí byť **vopred schválené** MHTH.

11.6 DIZAJN A ARCHITEKTÚRA RIEŠENIA

V nasledujúcich bodoch sú definované základné bezpečnostné požiadavky na SW riešenie, ktoré je potrebné zohľadniť vo funkčnej špecifikácii pre dizajn a architektúru riešenia:

- logovanie všetkých aktivít (admin, events a security logs),
- auditné logy budú uložené takým spôsobom, aby bola zabezpečená ich spoľahlivosť, auditovateľnosť, dôvernosť, integrita a ich dostupnosť na vyžiadanie,
- systém alebo služba je budovaná modulárne tak, aby jej jednotlivé funkčné prvky (napr. šifrovanie, autentifikácia, žurnálovanie) mohli byť podľa potreby vymenené,
- architektúra je postavená na "zero-trust" modeli, t. j. nedovolí komunikovať cez ľubovoľnú sieť a ľubovoľnými (neautorizovanými) komponentmi,
- architektúra nepodporuje zastaralé služby a protokoly, ktoré sú zraniteľné alebo ktoré nie je možné zabezpečiť iným spôsobom (rlogin, telnet, SMB v1, SSL v.3, TLS v.1.1, a pod.),
- autentifikácia (identifikácia a autentizácia) používateľov systému je jednoznačná a povinná, aby na nej mohla byť založená auditovateľnosť,
- k autorizácii musí dôjsť výlučne po identifikácii a autentizácii,
- systém alebo služba podporuje RBAC (role-based access control) a umožňuje oddeľovať role (naplniť princíp segregation of duties),
- systém alebo služba nevyžaduje pre svoju prevádzku trvalé používanie vysokých systémových privilégií,
- systém alebo služba aplikuje princíp úplnej mediácie, to znamená, že overuje identitu používateľa pri každej následnej, kritickej aktivite (opätovné potvrdenie identity napr. pri založení nového účtu),

- systém alebo služba využíva systém navzájom sa prekrývajúcich alebo doplňujúcich bezpečnostných opatrení (napr. nespolieha sa len na šifrovanie autentizačných dát počas prenosu, ale šifruje ich v nevratnej podobe aj pri uložení),
- úplné technické zlyhanie systému nesmie viesť k úplnému zlyhaniu bezpečnosti alebo integrity (napr. nesmie umožniť dump hesiel v pamäti, prístup k iným autorizačným dátam a pod.).

Upresnenia a doplňujúce opatrenia môžu byť vzhľadom k dielu odkomunikované a odsúhlasené v písomnej alebo elektronickej komunikácií oboma stranami.

12. RIADENIE INCIDENTOV

12.1 ODHAĽOVANIE

Dodávatelia a pracovníci tretej strany sú zodpovední za ohlasovanie bezpečnostných incidentov, o ktorých sa pri výkone svojich činností v spoločnosti MHTH dozvedia, alebo ktorých sú bezprostrednými svedkami. Bezpečnostné incidenty zahŕňajú, ale nielen, stratu, zmenu, zverejnenie alebo neoprávnený prístup k údajom alebo informáciám MHTH. Ak dodávateľ zaznamená bezpečnostný incident vo svojom internom prostredí, ktorý môže mať vplyv na predmet dodávky produktu/služby/diela, je povinný ho bezodkladne oznámiť MHTH.

12.2 OZNAMOVANIE

Dodávateľ takéto bezpečnostné incidenty okamžite oznámi MHTH písomne v elektronickej forme pridelenej kontaktnej osobe/gestorovi projektu s patričnou presnosťou.
Ak sa zistí porušenie, kompromitácia alebo zneužitie údajov alebo informácií MHTH, dodávateľ to obratom oznámi MHTH. Akákoľvek udalosť, aj podozrenie je nutné hlásiť podľa platných zákonov, ale najneskôr do 24 hodín.
Podrobnosti o bezpečnostných incidentoch si dodávateľ uchová aspoň do ďalšieho hodnotenia bezpečnosti medzi stranami.

12.3 VYRIEŠENIE

Dodávateľ vynaloží všetko úsilie na okamžité vyriešenie bezpečnostných incidentov a bude informovať MHTH priebežne o postupe až do ukončenia predmetného incidentu.

12.4 POZASTAVENIE PRÍSTUPU DODÁVATEĽA K SYSTÉMU MHTH

V prípade bezpečnostného incidentu týkajúceho sa priamo alebo nepriamo prevádzkovaných základných služieb, MHTH môže až do vyriešenia incidentu pozastaviť prístup dodávateľa k systémom MHTH.

12.5ODOBRATIE PRÍSTUPU ZAMESTNANCA DODÁVATEĽA K SYSTÉMOM MHTH

V prípade porušenia povinností zo strany zamestnanca dodávateľa alebo zamestnancov tretích strán môže MHTH dočasne alebo aj na trvalo odobrať prístup tejto osobe do prostredia MHTH, pričom pri dodávke diela/služby nebude takéto odobratie prístupu brané ako porušenie povinností na strane MHTH a ani ako dôvod na posunutie termínu realizácie diela/dodávky služby.

13. UKONČENIE ZMLUVY

Po ukončení plnenia diela/služby je dodávateľ povinný udeliť, poskytnúť, previesť alebo postúpiť na MHTH všetky licencie, zdrojové kódy, práva alebo súhlasy potrebné na zabezpečenie kontinuity činností MHTH, ak v zmluve nie je dohodnuté inak.

Následne sa dodávateľ písomne zaväzuje vymazať všetky dáta MHTH, ktoré sú uložené v systémoch dodávateľa. Dodávateľ sa zaväzuje vykonať vymazanie dát vhodnými metódami a nástrojmi a proces vymazania riadne zdokumentovať a výsledný protokol o likvidácii zaslať kontaktnej osobe v MHTH. Týmto bodom nie sú dotknuté požiadavky zákona o ochrane osobných údajov.

14. SÚVISIACA DOKUMENTÁCIA

14.1 PRÍLOHY A FORMULÁRE

- Príloha č.1 – Prehlásenia o poučení oprávnenej osoby (pracovníka) tretej strany o politike kybernetickej a informačnej bezpečnosti pre dodávateľov a tretie strany v spoločnosti MH Teplárenský holding a.s.
- Príloha č.2 – Súhlas so spracúvaním osobných údajov

15. 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_S02 Politika KIB pre dodávateľov a tretie strany, vydanie č.2

Vypracoval: Mgr. Tomáš Baksa, špecialista riadenia rizík a biznis kontinuity
Schválili: Ing. Adrián Jenčo, LL.M, MBA, generálny riaditeľ
Ing. Peter Kadlec, riaditeľ úseku IT
Ing. Róbert Mramúch, manažér oddelenia bezpečnosti a krízového riadenia