Univerzitná nemocnica Bratislava
Pažítková 1835/4
82101 Bratislava

UNIVERZITNÁ NEMOCNICA BRATISLAVA

OS 8/2021

Bezpečnostné podmienky pre dodávateľov a iné tretie strany UNB

	Funkcia	Titul, meno, priezvisko	Dátum	Podpis
Schvaľovateľ	Riaditeľ	MUDr. Alexander Mayer, PhD., MPH, MHA		
Overovateľ	Vedúci odboru informačno - komunikačných služieb	Bc. Martin Lukáč		
Spracovateľ	Manažér Kybernetickej bezpečnosti	Bc. Adam Lojkó		
Gestor	Referát GDPR a kybernetickej bezpečnosti			
Verzia	1.1			

OBSAH

1 ÚVODNÉ USTANOVENIA

1) Tento dokument **OS 8/2021 Bezpečnostné podmienky pre dodávateľov a iné tretie strany UNB** (ďalej len „**Politika**“) patrí do súboru dokumentov tvoriacich bezpečnostnú dokumentáciu príspevkovej organizácie Univerzitná nemocnica Bratislava, IČO: 31813861, so sídlom Pažítková 1835/4, 821 01 Bratislava (ďalej len „UNB“), ktorú UNB prijala v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej len „**Bezpečnostná dokumentácia**“).

2) Vychádzajúc z dokumentu Bezpečnostná stratégia kybernetickej bezpečnosti UNB (ďalej len „Bezpečnostná stratégia“), táto Politika systematicky a obsahovo nadväzuje na dokument OS 1/2021 – Politika IT bezpečnosti UNB.

1.1 Účel, rozsah a oblasť platnosti

1) Účelom tejto Politiky je záväzne upraviť podmienky uzatvárania zmlúv medzi dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov (ďalej len „Tretia strana“) a UNB.

2) Táto Politika sa vzťahuje na všetky zmluvy na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov, ktoré UNB uzatvára s Treťou stranou, ak táto Politika neustanovuje inak.

3) Na riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov sa pri uzatvorení zmluvy s Treťou stranou analyzujú riziká dodávateľských služieb, akvizície, vývoja a údržby informačných systémov spôsobom uvedeným v bezpečnostnej politike **OS 1/2021 – Politika IT bezpečnosti UNB.**

4) Vývoj a akvizícia siete a informačného systému UNB sa uskutočňuje s ohľadom na zaistenie kompatibility s existujúcimi sieťami a informačnými systémami a zachovanie úrovne bezpečnosti ustanovenej v Bezpečnostnej stratégií kybernetickej bezpečnosti UNB.

5) UNB je povinná pri uzatvorení zmluvy s dodávateľom na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti (ďalej len „**ZoKB**“), počas celej doby platnosti zmluvy. V tomto prípade je evidencia zmlúv o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností uzatvorených s Tretími stranami súčasťou Bezpečnostnej dokumentácie. Za evidenciu všetkých zmlúv uzatvorených s Tretími stranami zodpovedá manažérovi kybernetickej bezpečnosti.

6) Stanovené pravidlá sa vzťahujú na všetky zariadenia, IKT prostriedky a informačné aktíva, ktoré UNB vlastní, alebo sú prenajímané.

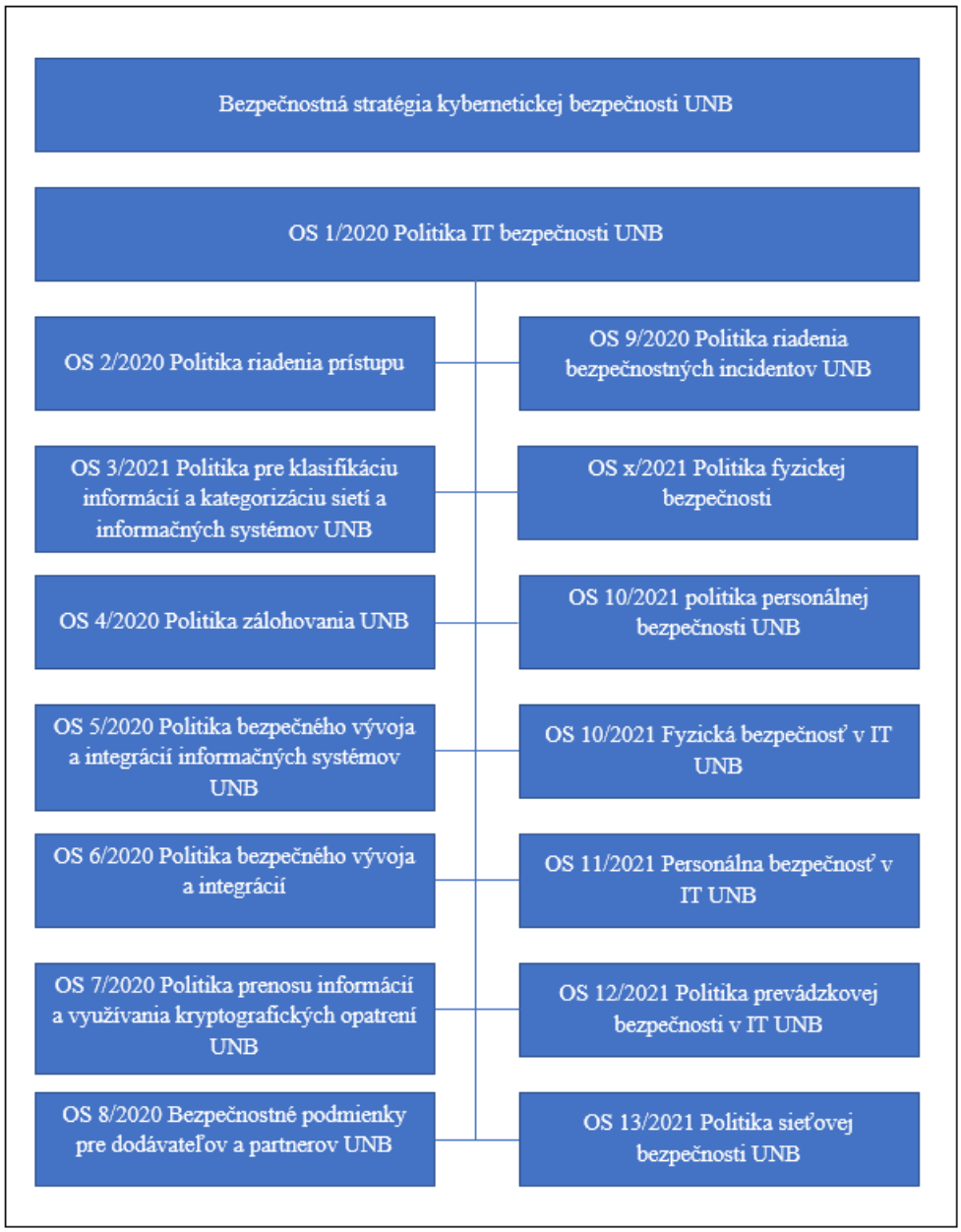
7) Jednotlivé ustanovenia môžu slúžiť ako podklad pri zostavovaní zmluvnej dokumentácie s dodávateľom alebo partnerom. Právne znenie zmluvy musí byť pripravené, resp. odkonzultované osobou zodpovednou za právne záležitosti UNB.

2 VŠEOBECNÉ USTANOVENIA

Nasledujúca časť upravuje zaradenie tejto Politiky v rámci Bezpečnostnej dokumentácie, definície používaných pojmov, používané skratky a referenčné dokumenty použité pre tvorbe tejto Politiky.

2.1 Zaradenie tejto Politiky v rámci Bezpečnostnej dokumentácie

Zaradenie tejto Politiky v rámci Bezpečnostnej dokumentácie možno znázorniť nasledovne:



2.2 Definície pojmov

Pojmy uvedené v tejto Politike majú význam podľa jednotného výkladového slovníka, ktorý je upravený v Bezpečnostnej stratégii, ibaže táto Politika ustanovuje inak.

2.3 Skratky

Skratky uvedené v tejto Politike majú význam podľa jednotného zoznamu skratiek, ktorý je upravený v Bezpečnostnej stratégií kybernetickej bezpečnosti UNB, ibaže táto Politika ustanovuje inak.

2.4 Legislatívne východiská

Táto Politika je vytvorená s ohľadom na nasledovné všeobecne záväzné právne predpisy:

- Zákon NR SR č. 215/2004 Z. z. o ochrane utajovaných skutočností
- Vyhláška NBÚ SR. č. 336/2004 o fyzickej bezpečnosti a objektovej bezpečnosti
- Vyhláška NBÚ SR č. 339/2004 o bezpečnosti technických prostriedkov
- Zákon č. 45/2011 Z. z. o kritickej infraštruktúre
- Zákon č. 179/2011 Z. z. o hospodárskej mobilizácii
- Nariadenie EP a Rady o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov
- Smernica EP a Rady o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
- Zákon NR SR č. 18/2018 Z. z. o ochrane osobných údajov
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov
- Vyhláška NBÚ SR č. 164/2018 Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)
- Vyhláška NBÚ SR č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov
- Vyhláška NBÚ SR č. 362/2018 Z. z., ktorou sa stanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení
- STN ISO/IEC 27001 – Návod pre manažérstvo informačnej bezpečnosti
- STN ISO/IEC 27002 – Kódex praxe manažérstva informačnej bezpečnosti

3 Základné bezpečnostné princípy s Tretími stranami podľa Bezpečnostnej dokumentácie

Dokument stanovuje základné bezpečnostné princípy, ktoré sa Tretia strana počas trvania kontraktu zaväzuje plniť a dodržiavať. UNB má právo počas trvania zmluvného vzťahu kontrolovať správne dodržiavanie a vykonávanie prijatých opatrení, čím je zaistený súlad s bezpečnostnými opatreniami UNB a vysoká úroveň bezpečnosti prostredia.

3.1 Základné bezpečnostné princípy s Tretími stranami – začiatok zmluvného vzťahu

1) UNB uzatvorením zmluvného vzťahu udelí súhlas Tretej strane na zbieranie, spracovávanie, využívanie a uchovávanie informačných aktív UNB, s ktorými Tretia strana pracuje v rozsahu nevyhnutnom na realizáciu zmluvného plnenia.

2) UNB po uzatvorení zmluvného vzťahu oboznámi zainteresované osoby Tretej strany, ako aj jej prípadných subdodávateľov, sú povinné sa s nimi oboznámiť a dodržiavať ich. Tretia strana zodpovedá za porušenie povinností subdodávateľmi v celom rozsahu.

3) Pri narábaní s informačnými aktívami UNB sa Tretia strana zaväzuje používať rovnakú klasifikačnú schému ako platí v UNB, aby bola zachovaná minimálne podobná alebo rovnaká úroveň bezpečnosti týchto aktív.

4) K informačným aktívam UNB majú prístup len vybrané osoby Tretej strany v závislosti od príslušného klasifikačného stupňa daného aktíva.

5) Tretia strana je povinná oznámiť UNB akýkoľvek nepovolený a neoprávnený prístup k informačným aktívam, bez ohľadu na ich klasifikačný stupeň, porušenie ich dôvernosti alebo integrity, alebo akúkoľvek inú bezpečnostnú udalosť, ktorá môže byť relevantná pre UNB.

6) V prípade, že Tretia strana využíva k práci zariadenia IKT patriace UNB, je povinná ustanoviť zodpovedné osoby za prácu so zverenými zariadeniami, a tento zoznam odovzdať do rúk Manažérovi kybernetickej bezpečnosti UNB. Zoznam musí byť pravdivý a aktuálny.

7) Pre prácu s informačnými systémami UNB je zodpovedným osobám Tretej strany vytvorený prístup, ktorý schvaľuje Manažér kybernetickej bezpečnosti UNB. Prístupové práva sú prideľované iba v nevyhnutnom rozsahu pre plnenie zmluvných záväzkov a sú termínované. Tretia strana si je vedomá skutočnosti, že prístupy sú evidované a monitorované.

8) Je vytvorený zoznam zodpovedných osôb Tretej strany, ktorým boli pridelené prístupové práva. Zoznam je k dispozícii u Manažéra kybernetickej bezpečnosti UNB. Zoznam musí byť pravdivý a pri každej zmene aktualizovaný.

9) Tretia strana do zverených zariadení IKT neinštaluje žiadny softvér. Inštalácia programového vybavenia je v kompetencii UNB.

10) Tretia strana je povinná informovať UNB o poškodení, zničení, strate alebo krádeži zverených zariadení IKT, alebo o akejkoľvek inej udalosti relevantnej pre záujmy UNB.

11) UNB si vyhradzuje právo vyžiadať si potvrdenie o absolvovaní príslušného školenia alebo zaučenia zodpovedných osôb za Tretiu stranu. UNB odmietne sprístupniť svoje informačné alebo iné aktíva zamestnancovi Tretej strany, pokiaľ nie je preukázaná požadovaná vedomosť zamestnanca alebo absolvovanie školenia.

12) Počas trvania zmluvného vzťahu má UNB právo vykonať kontrolu, či Tretia strana dodržiava príslušné bezpečnostné opatrenia. Zároveň má UNB právo vykonať kontrolu aj po ukončení zmluvného vzťahu v stanovenej časovej lehote pre potreby odstránenia alebo likvidácie informačných aktív patriacich UNB.

13) Po ukončení zmluvného vzťahu je Tretia strana povinná odstrániť alebo zlikvidovať zo svojich fyzických priestorov alebo IKT zariadení informačné aktíva UNB,

4 MINIMÁLNE OBSAHOVÉ NÁLEŽITOSTI ZMLÚV S TRETÍMI STRANAMI

1) Tento článok upravuje povinné obsahové náležitosti zmlúv uzatvorených medzi Tretími stranami a UNB.

2) Pri výbere dodávateľa alebo Tretej strany by mali byť okrem ekonomických alebo personálnych faktorov zohľadňované aj bezpečnostné faktory na zachovanie takej úrovne bezpečnosti, ktorá je v maximálnej možnej miere v súlade so štandardom v prostredí UNB.

3) O všetkých bezpečnostných požiadavkách je potrebné Tretiu stranu informovať vopred z dôvodu následného preukázania schopnosti tieto požiadavky zabezpečiť.

4) Pri podpise zmluvy musí byť Tretia strana oboznámená s kľúčovými bezpečnostnými politikami a postupmi. Zároveň musí byť stanovené, ktoré platné dokumenty UNB sú pre Tretiu stranu záväzné.

5) Pri podpise zmluvy sú všetky zúčastnené strany povinné podpísať dohodu o mlčanlivosti platnú počas celého trvania zmluvného vzťahu, aj po jeho ukončení. Táto povinnosť sa považuje za splnenú aj v prípade, ak je povinnosť zachovávať mlčanlivosť obsiahnutá v samotnej zmluve na plnenie.

4.1 Minimálne obsahové náležitosti zmlúv s Tretími stranami podľa ZoKB

1) V prípade, ak ide o výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby, je UNB povinná zmysle ZoKB pri uzatvorení zmluvy s Treťou stranou uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností počas celej doby platnosti zmluvy. Na uvedenú skutočnosť je spracovateľ zmluvy povinný upozorniť pripomienkovateľov zmluvy na plnenie a zároveň v súčinnosti s manažérom kybernetickej bezpečnosti upraviť znenie podľa potreby tak, aby bolo v súlade s platnými právnymi predpismi a potrebami UNB.

2) Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností s Treťou stranou obsahuje najmenej:

   a) obdobie trvania zmluvy;

   b) ustanovenie záväzku Tretej strany dodržiavať bezpečnostné politiky UNB a vyjadrenie súhlasu s nimi;

   c) ustanovenie o povinnosti chrániť všetky informácie poskytnuté UNB Tretej strane;

   d) ustanovenie o povinnosti dodržiavať a prijímať bezpečnostné opatrenia Treťou stranou;

   e) konkrétnu špecifikáciu a rozsah bezpečnostných opatrení, ktoré prijíma Tretia strana a vyjadrenie súhlasu s nimi;

   f) konkrétny rozsah činnosti Tretej strany;

g) zoznam pracovných rolí Tretej strany, ktoré majú mať prístup k informáciám a údajom UNB, s povinnosťou oznámiť UNB každú zmenu v personálnom obsadení; osoba zúčastnená na predmete plnenia podpisuje vyjadrenie o zachovávaní mlčanlivosti podľa § 12 ods. 1 ZoKB;

h) ustanovenie o rozsahu, spôsobu a možnosti vykonávania kontrolných činností a auditu UNB v Tretej strane;

i) vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre UNB namiesto Tretej strany;

j) ustanovenia o povinnosti informovať UNB o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti UNB;

k) ustanovenia o spôsobe a forme hlásenia ďalších informácií požadovaných UNB na plnenie jej povinností vyplývajúcich zo ZoKB a ich vymedzenie;

l) ustanovenie o spôsobe a forme hlásenia všetkých informácií majúcich vplyv na zmluvu;

m) ustanovenie o sankčných mechanizmoch pri porušení zmluvy;

n) ustanovenia o podmienkach a spôsobe ukončenia zmluvy;

o) záväzok Tretej strany po ukončení zmluvného vzťahu vrátiť, previesť alebo aj zničiť všetky informácie patriace UNB, ku ktorým má Tretia strana počas trvania zmluvného vzťahu prístup;

p) záväzok Tretej strany po ukončení zmluvného vzťahu udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity činnosti UNB; tento záväzok Tretej strany ostáva v platnosti aj po ukončení zmluvného vzťahu po dobu dohodnutú zmluvnými stranami, ktorá nesmie byť kratšia ako päť rokov po ukončení zmluvného vzťahu.

3) Zmluva o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností s Treťou stranou obsahuje bezpečnostné opatrenia najmenej pre oblasť:

a) technických zraniteľností systémov a zariadení;

b) riadenia bezpečnosti sietí a informačných systémov;

c) riadenia prístupov;

d) riešenia kybernetických bezpečnostných incidentov;

e) monitorovania, testovania bezpečnosti a bezpečnostných auditov.

4.2 <u>Minimálne obsahové požiadavky na Tretie strany podľa Bezpečnostnej dokumentácie</u>

1) Vychádzajúc z Bezpečnostnej dokumentácie, priamo v zmluvách s Tretím stranami, musia byť príslušným spôsobom upravené zároveň nasledovné oblasti:

a) zodpovednosť Tretej strany v prípade porušenia záväzku mlčanlivosti;

b) zabezpečenie plnenia predmetu zmluvy Treťou stranou vhodným spôsobom;

c) povinnosť Tretej strany poučiť svojich zamestnancov a iné osoby spolupracujúce s Treťou stranou v rozsahu vykonaného poučenia Tretej strany zo strany UNB;

d) zmluvná alebo iná dokumentácia s Tretími stranami musí obsahovať ustanovenie o povinnosti Tretej strany uchovávať informácie UNB v bezpečí;

e) povinnosť Tretej strany bez zbytočného odkladu informovať Špecialistu/Administrátora IT o zmenách, ktoré majú vplyv na rozsah prístupov používateľov IS;

f) prístupy pre Tretie strany sa vytvárajú na dobu určitú, v trvaní najviac na dobu platnosti zmluvy, maximálne však do konca kalendárneho roka, pričom po uplynutí tejto doby môže Tretia strana opätovne požiadať o predĺženie prístupu;

g) v prípade, že vývoj IS a aplikácií je pre UNB realizovaný formou outsourcingu treťou stranou, musia byť jasne stanovené podmienky týkajúce sa najmä autorských práv aplikácií, práv duševného vlastníctva, bezpečnostných parametrov, bezpečnostného a funkčného testovania, legislatívnych a regulačných požiadaviek dokumentácie a pod. Za dané záležitosti zodpovedá vlastník IS;

h) povinnosť dodávateľa IT technológie:

- Určiť, ktoré systémové záplaty je potrebné testovať a následne aplikovať;
- Poskytnúť dokumentáciu popisujúcu politiku opráv softvéru pre tovary a ich systémy, ktoré dodávajú;
- Validovať záplaty z hľadiska uplatniteľnosti a kompatibility prostredníctvom analýzy a overovania opráv vrátane opráv, ktoré vydáva výrobca OS a softvéru Tretej strany používaný produktmi IT;
- Poskytnúť zoznam všetkých opráv a ich stavu validácie vrátane informácií a formátu údajov;
- Informovať vlastníkov aktív a pravidelne aktualizovať zoznam popísaných záplat, a to do 30 dní po vydaní záplaty výrobcom OS alebo softvérom Tretích strán;
- Poskytovať primerané varovanie (najmenej dva roky pred) o IT systémoch, ktoré dosiahnu koniec životného cyklu.

2) Za dodržiavanie obsahových náležitosti zmlúv s Tretími stranami podľa článku 4.1 tejto Politiky zodpovedá Manažér kybernetickej bezpečnosti. Manažér kybernetickej bezpečnosti je oprávnený udeliť Tretej strane výnimku v súvislosti s aplikáciu podmienok podľa tejto Politiky. V prípade udelenia výnimky je potrebné vykonať analýzu rizík.

5 ĎALŠIE OBSAHOVÉ NÁLEŽITOSTI ZMLÚV

1) Manažér kybernetickej bezpečnosti je oprávnený rozhodnúť, že zmluva uzatvorená s Tretími stranami alebo akákoľvek iná zmluva, ktorej plnenie môže vplývať na kybernetickú bezpečnosť UNB, môže obsahovať príslušné ustanovenia upravujúce najmä:

- Podrobnosti o poskytovaných službách.

- Definovanie SLA pre úrovne poskytovaných služieb, ich monitorovanie a vytváranie správ.
- Definovanie zmenového konania poskytovaných služieb, pričom každé odklonenie od zadania sa musí riešiť zmenovým konaním.
- Povinnosti pri ukončení dodávky služieb ako odovzdanie, likvidácia alebo vymazanie dôverných informácií a návrat zariadení.
- Pravidlá ochrany citlivých údajov a osobitne legislatívou vyžadované podmienky ochrany osobných údajov, ktoré musí druhá zmluvná strana dodržiavať.
- Špecifikácia informácií, ktoré budú k dispozícii druhej zmluvnej strane a označenie jej klasifikácie, ak spadá do niektorej z kategórií citlivých informácií, ako napríklad osobné údaje.
- Definovanie prístupových práv druhej zmluvnej strany, povinnosť vedenia evidencie všetkých osôb reprezentujúcich druhú zmluvnú stranu a ich prístupových práv a proces odstraňovania prístupových práv.
- Stanovenie práva na prístup UNB k informáciám uloženým alebo spracovávaným druhou zmluvnou stranou.
- Povinnosť zabezpečenia minimálnej vedomosti zamestnancov druhej zmluvnej strany vo všetkých činnostiach, v ktorých sú zapojení do vzťahu s UNB, vrátane povinného zabezpečenia školenia, ak je ich súčasná vedomosť nedostatočná.
- Vymedzenie podmienok riešenia bezpečnostného incidentu, stanovenie procesu jeho eskalácie a riešenia, vrátane garantovaných reakčných časov.
- Podľa potreby určenie ďalších relevantných povinných kľúčových bezpečnostných opatrení na strane druhej zmluvnej strany odlišných od tých uvedených vyššie, napríklad na zabezpečenie ochrany majetku UNB, vo vzťahu ku kontrole ochrany proti škodlivému kódu, kontrole opatrení na ochranu integrity alebo týkajúcich sa postupov zničenia informačných aktív po ich použití, či neriadeného šírenia údajov.
- Sankcie vyplývajúce z porušenia zmluvy a zodpovednosť druhej zmluvnej strany za nesplnené, nevhodné alebo nesprávne plnenie zmluvy.
- Definovanie zodpovednosti za škodu v prípade porušenia zmluvných povinností, vrátane zodpovednosti za porušenia dôvernosti informácií.

2) Všetky zmluvy s Tretími stranami, ktoré sa spravujú podľa tejto Politiky, musia byť pripravené alebo pred uzatvorením príslušnej zmluvy skontrolované osobou zodpovednou za právne záležitosti UNB v súčinnosti so manažérom kybernetickej bezpečnosti a spracovateľom zmluvy.

6 PRIEBEH ZMLUVNÉHO VZŤAHU

1) UNB podpísaním zmluvy na plnenie udeľuje písomný súhlas Tretej strane pre zbieranie, spracovávanie, využívanie a uchovávanie všetkých informačných aktív UNB, s ktorými Tretia strana pracuje v rozsahu nevyhnutnom na plnenie zmluvy.

2) UNB má právo vykonávať kontrolu, či Tretia strana dodržiava bezpečnostné podmienky stanovené v zmluve.

3) Pri podpise zmluvy je Tretia strana oboznámená s kľúčovými bezpečnostnými politikami a postupmi. Zároveň musí byť stanovené, ktoré platné dokumenty UNB sú pre Tretiu stranu záväzné.

4) Tretia strana musí zaistiť minimálnu vedomosť svojich zamestnancov vo všetkých činnostiach, v ktorých sú zapojení do vzťahu so UNB, vrátane povinného zabezpečenia školenia, ak je ich súčasná vedomosť nedostatočná.

6.1 Narábanie s aktívami UNB

1) UNB špecifikuje všetky aktíva (informačné, hmotné alebo personálne), ktoré bude mať Tretia strana k dispozícii. Zodpovedná osoba v spolupráci s manažérom kybernetickej bezpečnosti UNB vytvorí zoznam všetkých aktív, s ktorými bude Tretia strana pracovať, a tento zoznam bude k dispozícii UNB, aj Tretej strane.

2) UNB definuje klasifikáciu informačných aktív, a túto klasifikáciu musí dodržiavať aj Tretia strana po celú dobu trvania zmluvného vzťahu. Tretia strana sa zaväzuje narábať s informačnými aktívami podľa interných predpisov UNB v súlade s príslušnou klasifikáciou informačných aktív.

3) Tretia strana musí určiť zodpovedné osoby, ktoré budú mať prístup k informáciám s príslušným stupňom klasifikácie, a budú môcť s týmito informáciami UNB narábať. Zoznam zodpovedných osôb musí byť k dispozícii všetkým stranám zmluvného vzťahu.

4) Tretia strana je povinná bezodkladne oznamovať UNB akýkoľvek nepovolený a neoprávnený prístup k informačným aktívam, porušenie ich dôvernosti alebo integrity, alebo akúkoľvek inú bezpečnostnú udalosť relevantnú pre UNB.

5) UNB okrem informačných aktív definuje aj IKT zariadenia alebo informačné systémy, ku ktorým budú mať vybrané zodpovedné osoby Tretej strany prístup. Je vytvorený zoznam zodpovedných osôb, ktorý by mal byť k dispozícii všetkých stranám zmluvného vzťahu.

6) Prístupové práva vytvára a ruší UNB. Prístupy sú prideľované v nevyhnutnom rozsahu pre plnenie zmluvných záväzkov.

7) Všetky prístupy pre Tretiu stranu sú terminované – pri krátkodobých zmluvách na dobu platnosti zmluvy a pri dlhodobých zmluvách maximálne do konca kalendárneho roka. Po uplynutí časovej lehoty musí Tretia strana opätovne požiadať o predĺženie prístupu.

8) Prístupové práva Tretích strán sú prideľované iba v nevyhnutnom rozsahu pre plnenie zmluvných záväzkov. Pridelené prístupové práva sú evidované a monitorované.

9) Pokiaľ UNB poskytla Tretej strane na prácu svoje IKT zariadenia, UNB definuje a inštaluje informačné systémy/programy/aplikácie, ktoré bude pre prácu Tretia strana využívať.

10) Manažér kybernetickej bezpečnosti má k dispozícii zoznam zodpovedných osôb Tretej strany, ktorým bol zverený majetok UNB (IKT zariadenia). Zoznam zodpovedných osôb musí byť aktuálny a pravdivý. Tretia strana nesmie do zariadení bez súhlasu manažéra

kybernetickej bezpečnosti UNB alebo inej určenej zodpovednej osoby UNB inštalovať softvér.

11) UNB musí byť bezodkladne Treťou stranou upovedomená o strate, krádeži, zničení alebo inej relevantnej skutočnosti IKT zariadení.

6.2 Školenie zamestnancov Tretej strany

1) Prístup k aktívam UNB majú len vybraní zamestnanci Tretej strany, pričom títo zamestnanci musia byť oboznámení so stanovenými bezpečnostnými politikami UNB. Oboznámenie preukázateľne zabezpečuje gestor zmluvy v spolupráci s manažérom kybernetickej bezpečnosti.

2) Pokiaľ zamestnanci Tretej strany nemajú dostatočnú vedomosť vo vykonávaných činnostiach vo vzťahu k UNB, nie sú oprávnení vykonávať takéto činnosti. Plnenie môže byť poskytované len osobami, ktoré disponujú oprávneniami, vedomosťami a znalosťami potrebnými na poskytovanie príslušného plnenia.

3) UNB má právo vyžiadať si potvrdenie o absolvovaní príslušného školenia/certifikátu zodpovedných osôb Tretej strany a Tretia strana je povinná takýto doklad bezodkladne poskytnúť, inak nie je oprávnená plnenie takouto osobou realizovať.

4) UNB odmietne sprístupniť svoje aktíva zamestnancovi Tretej strany, pokiaľ nie je preukázaná požadovaná vedomosť zamestnanca alebo absolvovanie školenia.

6.3 Kontrola dodržiavania bezpečnostných podmienok

1) Pri uzatvorení zmluvného vzťahu UNB oboznámi Tretiu stranu s relevantnými bezpečnostnými politikami.

2) Počas trvania zmluvného vzťahu má UNB právo vykonávať kontrolu, či Tretia strana dodržiava nariadenia z bezpečnostných politík UNB. Výstupom z kontroly je zápis, ktorý je k dispozícii manažérovi kybernetickej bezpečnosti UNB a zodpovednej osobe Tretej strany.

3) Po ukončení zmluvného vzťahu má UNB v stanovenej lehote právo vykonať kontrolu, či Tretia strana odstránila a zlikvidovala informačné aktíva patriace UNB.

7 UKONČENIE ZMLUVNÉHO VZŤAHU

1) Po ukončení zmluvného vzťahu je Tretia strana povinná odstrániť a zlikvidovať zo svojich IKT zariadení alebo fyzických priestorov informačné aktíva UNB, pokiaľ nebolo zmluvou stanovené inak.

2) V prípade, že Tretia strana využívala na prácu zariadenia patriace UNB, informačné aktíva UNB nadobudnuté počas spolupráce Tretia strana zo zariadenia neodstraňuje, ale odovzdá ich manažérovi kybernetickej bezpečnosti UNB alebo inej zodpovednej osobe na strane UNB.

3) Pokiaľ UNB poskytla Tretej strane na prácu svoje IKT zariadenia, Tretia strana je povinná tieto zariadenia vrátiť v takom stave, v akom ich na začiatku spolupráce od UNB prevzala.

7.1 Porušenie zmluvných podmienok, zmluvná pokuta

1) UNB môže v prípade preukázaného porušenia dohodnutých zmluvných podmienok uplatniť sankcie uvedené v zmluve.
2) V prípade porušenia zmluvných podmienok z Tretej strany, má UNB právo s okamžitou platnosťou zrušiť prístupové práva definovaným osobám Tretej strany.
3) Tretia strana je v prípade porušenia zmluvných podmienok postupovať v zmysle pokynov manažéra kybernetickej bezpečnosti a v prípade hrubého porušenia môže byť na základe pokynu manažéra kybernetickej bezpečnosti povinná s okamžitou platnosťou odovzdať všetky zverené IKT zariadenia. Zariadenia musia byť odovzdané so všetkými dovtedajšími nemodifikovanými informačnými aktívami.

8 SPRÁVA DOKUMENTU A REVÍZIA

Správcom tejto Politiky je manažér kybernetickej bezpečnosti, ktorý je zodpovedný za správnosť tohto dokumentu a ak je to potrebné, aktualizuje dokument pri relevantnej zmene, najmenej však raz za rok.

9 ZÁVEREČNÉ USTANOVENIA

1) Táto Politika platí pre všetky útvary UNB. S obsahom tejto Politiky sú povinní sa oboznámiť všetci Zamestnanci, prípadne Tretie osoby podľa rozhodnutia manažéra kybernetickej bezpečnosti.
2) Za udržiavanie tejto Politiky v aktuálnom stave je zodpovedný manažér kybernetickej bezpečnosti.
3) Táto Politika nadobúda platnosť dňom jej schválenia.