1 Všeobecné ustanovenia

1.1 Všeobecné bezpečnostné štandardy spoločnosti Slovenské elektrárne, a.s. (ďalej len „**VBŠ**") v oblasti kybernetickej bezpečnosti sú neoddeliteľnou súčasťou Zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných opatrení alebo inej zmluvy, ktorej predmetom je dodávka sietí a informačných systémov (ďalej len „**Zmluva**").

1.2 Odchylné dojednania v Zmluve majú prednosť pred znením týchto VBŠ.

1.3 Bez ohľadu na pomenovanie v Zmluve sa Slovenské elektrárne, a.s. označujú ako „**SE**".

1.4 SE sú prevádzkovateľom základných služieb 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 KB**"), a v rámci SE sú prevádzkované siete a informačné systémy, ktoré majú vplyv na poskytovanie základnej služby zo strany SE v nasledovných lokalitách:

- Atómové elektrárne Mochovce (EMO),
- Atómové elektrárne Bohunice (EBO),
- Elektrárne Nováky (ENO),
- Elektrárne Vojany (EVO),
- Riaditeľstvo SE, a.s, Mlynské nivy 47, Bratislava (R-SE)
- Vodné elektrárne (VET).

1.5 Za „**Dodávateľa**" podľa týchto VBŠ sa považuje zhotoviteľ diela, vykonávateľ opravy, údržby, opravy, alebo úpravy veci, vykonávateľ prác, poskytovateľ služby, vrátane dodávky tovarov. Za Dodávateľa sa považuje samotný Dodávateľ označený v záhlaví Zmluvy, ako aj jeho subdodávatelia a ich právni nástupcovia. Ustanovenia, v ktorých sa nachádza označenie „Dodávateľ", sa vzťahujú na tuzemského aj zahraničného dodávateľa. Za pracovníkov Dodávateľa sa považujú zamestnanci Dodávateľa a zamestnanci jeho subdodávateľov a subdodávatelia (ďalej len „**pracovníci Dodávateľa**").

1.6 „**Hlavnou zmluvou**" sa rozumie zmluva, ktorá je takto označená priamo v Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných opatrení alebo iná zmluva, ktorej predmetom je dodávka sietí a informačných systémov, ktorej prílohou sú tieto VBŠ.

1.7 SE svoje práva a povinnosti uplatňuje cez oprávnenú osobu Dodávateľa, ktorá musí byť k dispozícii počas realizácie zmluvných výkonov, a ktorá bude partnerom oprávnenej osobe SE pri organizovaní zmluvného plnenia a riešení problémov v súvislosti s realizáciou zmluvných výkonov podľa Hlavnej zmluvy, a ktorá je uvedená v Hlavnej zmluve ako „**Manažér zmluvy za Dodávateľa**".

1.8 Dodávateľ svoje práva a povinnosti uplatňuje cez oprávnenú osobu SE, ktorá je uvedená v Hlavnej zmluve ako Manažér zmluvy za SE, prípadne oprávnený zamestnanec, v prípade, že je to uvedené v týchto VBŠ.

1.9 Zmluvnými výkonmi a zmluvným plnením na účely tohto VBŠ a Hlavnej zmluvy sa rozumejú všetky zmluvne dohodnuté poskytované plnenia, služby, výkon prác, vrátane dodávky tovarov a výkony činností Dodávateľa, ako aj zhotovenie diela (ďalej len „**Plnenie**").

1.10 Za „**pracovisko**" podľa týchto VBŠ sa považuje miesto zhotovovania diela, sieť alebo informačný systém, miesto vykonávania prác, stavenisko, miesto vykonávania opravy, údržby, opravy alebo úpravy veci, poskytovania služby v zmysle Hlavnej zmluvy alebo inej písomnej požiadavky SE, ktoré je Dodávateľom zápisnične prevzaté od SE.

1.11 Prílohou VBŠ je zoznam, ktorý obsahuje špecifikáciu legislatívnych požiadaviek podľa 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 v platnom znení pre jednotlivé kategórie sietí a informačných systémov.

2 Poučenia pracovníkov Dodávateľa

2.1 Dodávateľ je povinný zabezpečiť, aby všetci jeho pracovníci podieľajúci sa na poskytovaní Plnenia v sieťach a informačných systémoch SE, boli pred ich začatím zo strany Dodávateľa preukázateľne:

2.1.1 poučení o kybernetickej bezpečnosti, minimálne oboznámení s pravidlami používania informačných aktív SE a

2.1.2 poučení podľa požiadaviek príslušných všeobecne záväzných právnych predpisov ako osoby, ktoré vykonávajú činnosti alebo sa oboznamujú s informáciami podľa osobitného predpisu (napr. osobné údaje, citlivé informácie o kritickej infraštruktúre) (ďalej len „**Poučenie**"). Dodávateľ berie na vedomie, že Poučenie je podmienkou pre povolenie prístupu a narábania s týmito informáciami zo strany SE pre pracovníkov Dodávateľa.

3 Riadenie prístupu

3.1 Dodávateľ sa zaväzuje, že pri riadení prístupu používateľov do sietí a informačných systémov, bude dodržiavať nasledovné zásady:

3.1.1 **zásada najnižších privilégií**, podľa ktorej sú každému používateľovi obmedzené privilégiá v maximálnom rozsahu potrebnom na splnenie pridelených úloh (**least privilege**),

3.1.2 **zásada**, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa (**need-to-know, need-to-do**),

3.1.3 **zásada oddelenia zodpovedností**, podľa ktorej žiaden používateľ nemá oprávnenie pristupovať, upravovať alebo používať aktíva prevádzkovateľa základnej služby bez autorizácie alebo overenia identity (**segregation of duties**).

3.2 Dodávateľ berie na vedomie, že pri riadení prístupu do sietí a informačných systémov musí byť vždy používateľovi priradený **jedinečný identifikátor používateľa**, určený na jeho osobné a výhradné použitie, vytvorený na základe zo strany SE vopred

definovaných pravidiel pre tvorbu používateľských účtov (identifikátorov).

3.3 Dodávateľ berie na vedomie, že pri riadení prístupu do sietí a informačných systémov musia byť vždy zo strany SE používateľom priradené **jednoznačné prístupové oprávnenia**.

3.4 Dodávateľ je povinný zabezpečiť, aby autentizačné informácie (heslo, PIN a pod.) boli chránené pred zneužitím, prezradením alebo náhodným odhalením a jeho pracovníci dodržiavali dôvernosť pridelených autentizačných informácií. Ak je predmetom Plnenia dodávka sietí a informačných systémov Dodávateľ je ďalej povinný zabezpečiť, aby:

3.4.1 v riešení neboli používané výrobcom preddefinované autentizačné informácie,

3.4.2 autentizačné informácie neboli ukladané v čitateľnej forme ("plaintext"),

3.4.3 prihlasovacie údaje v skriptoch neboli uvádzané v čitateľnej forme ("plaintext"),

3.4.4 prihlasovanie používateľa mohlo byť vykonané cez zabezpečené komunikačné kanály, ktoré nemôžu byť odchytené.

3.5 Dodávateľ sa zaväzuje, že pri riadení prístupu do sietí a informačných systémov bude používať nástroj na správu a overovanie identity používateľa (**autentizácia**) pred začiatkom jeho aktivity v rámci siete a informačného systému a nástroj na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom (**autorizácia**), ako aj prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy) (**audit**).

3.6 Dodávateľ berie na vedomie, že pri riadení prístupu do sietí a informačných systémov musí byť zaznamenaný každý prístup, ako aj neúspešné pokusy o prístup do siete a informačného systému.

3.7 Dodávateľ berie na vedomie, že pri riadení prístupu do sietí a informačných systémov musia byť všetky zmeny prístupových oprávnení zaznamenané.

3.8 Dodávateľ berie na vedomie, že pravidlá podľa predchádzajúcich bodov musia byť aplikované na riadenie:

3.8.1 prístupu používateľov,

3.8.2 prístupu k sieťam,

3.8.3 prístupu k operačnému systému a jeho službám,

3.8.4 prístupu k aplikáciám,

3.8.5 vzdialeného prístupu.

4 Bezpečnosť sietí a informačných systémov

4.1 Dodávateľ berie na vedomie, že pri riadení bezpečnosti sietí a informačných systémov:

4.1.1 musia byť dodržiavané zásady riadenia prístupu (podľa článku 3 vyššie),

4.1.2 musí byť zabezpečená **segmentácia sietí**, pričom servery so službami priamo prístupnými z externých sietí sa musia nachádzať v samostatných sieťových segmentoch a v rovnakom segmente môžu byť len servery s rovnakými bezpečnostnými požiadavkami a rovnakej bezpečnostnej triedy a s podobným účelom,

4.1.3 prepojenia medzi jednotlivými segmentmi musia byť chránené firewallom, a musia byť dodržiavané nasledujúce pravidlá:

4.1.3.1 všetky spojenia sú povoľované na princípe zásady najnižších privilégií,

4.1.3.2 zoznam všetkých vstupno-výstupných bodov na hranici siete musí byť udržiavaný v aktuálnom stave,

4.1.3.3 komunikácia a prevádzka aplikácií cez neautorizované porty je blokovaná,

4.1.3.4 musia byť identifikované neoprávnené sieťové spojenia na hranici s vonkajšou sieťou,

4.1.4 spojenia do externých sietí musia byť smerované cez firewall a cez systém detekcie prienikov,

4.1.5 musí byť zabezpečené blokovanie neoprávnených spojení zo známych adries označených ako škodlivé alebo spôsobujúce známe hrozby, ak to nastavenie systému umožňuje,

4.1.6 musí byť zabezpečené smerovanie odchádzajúcej používateľskej sieťovej prevádzky cez autentizovaný server filtrovania obsahu (proxy),

4.1.7 na identifikáciu nezvyčajných mechanizmov útokov alebo proaktívneho blokovania škodlivej sieťovej prevádzky musí byť použitý systém detekcie prienikov alebo systém prevencie prienikov,

4.1.8 servery dostupné z externých sietí musia byť zabezpečené podľa odporúčaní výrobcu,

4.1.9 musí byť použitý systém monitorovania bezpečnosti, nakonfigurovaný tak, že zaznamenáva a vyhodnocuje aj informácie o sieťových paketoch na hranici siete.

4.2 Dodávateľ berie na vedomie, že mobilné pripojenie do siete a informačného systému a vzdialený prístup sa musí vykonať použitím dvojfaktorovej autentizácie alebo kryptografických prostriedkov schválených SE. Ak je predmetom Plnenia dodávka sietí a informačných systémov, Dodávateľ nie je oprávnený v dodávanom riešení vytvoriť iný spôsob (vzdialeného) prístupu do sietí a informačných systémov z externých sietí bez predchádzajúceho súhlasu SE.

4.3 Dodávateľ sa zaväzuje zabezpečiť, že pripojenie do sietí a informačných systémov SE bude realizované len zo zariadení, ktoré majú zabezpečené pravidelné posudzovanie a ošetrenie technických zraniteľností, a zabezpečenú identifikáciu možnej prítomnosti škodlivého kódu. Na požiadanie SE sa Dodávateľ zaväzuje splnenie tejto povinnosti preukázať.

5 Technické zraniteľnosti

5.1 Dodávateľ berie na vedomie, že technické zraniteľnosti sietí a informačných systémov ako celku sa musia identifikovať prostredníctvom:

5.1.1 nástroja určeného na detegovanie existujúcich zraniteľností programových prostriedkov a ich častí,

5.1.2 nástroja určeného na detegovanie existujúcich zraniteľností technických prostriedkov a ich častí,

5.1.3 využitia verejných a výrobcom poskytovaných zoznamov, ktoré opisujú zraniteľnosti programových a technických prostriedkov.

5.2 Dodávateľ je povinný ako súčasť Plnenia poskytnúť SE zoznam známych zraniteľností príp. single-point-of-failure použitých programových prostriedkov a ich častí, a technických prostriedkov a ich častí. Ak sa jedná o špecifické programové prostriedky alebo technické prostriedky, Dodávateľ je povinný, ako súčasť Plnenia, poskytnúť nástroj na detegovanie existujúcich zraniteľností týchto prostriedkov, ak taký existuje.

5.3 Dodávateľ je povinný vopred poskytnúť SE odkaz na stránky výrobcu, prostredníctvom ktorých sú poskytované zoznamy zraniteľností programových prostriedkov a ich častí, a technických prostriedkov a ich častí, alebo priamo informovať SE o identifikovaných zraniteľnostiach programových prostriedkov a ich častí, a technických prostriedkov a ich častí.

6 Monitorovanie, testovanie bezpečnosti a bezpečnostné audity

6.1 Dodávateľ berie na vedomie, že monitorovanie bezpečnosti sietí a informačných systémov sa musí vykonávať nástrojom na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov, ktorý musí umožňovať vytvárať prevádzkové záznamy a zaznamenávať najmenej:

6.1.1 aktivity v podobe vytvorenia, čítania, aktualizácie alebo odstránenia chránených a prísne chránených informácií a údajov alebo ďalších informačných aktív s nimi spojených,

6.1.2 iniciáciu pripojenia do siete alebo informačného systému a akceptáciu alebo odmietnutie pripojenia do siete alebo informačného systému zaznamenaním aspoň dátumu a času aktivity, identifikácie technického prostriedku, v rámci ktorého je činnosť zaznamenaná, identifikáciu osoby a zdroja vo forme IP adresy,

6.1.3 pridelenie, úpravu alebo zrušenie prístupových práv používateľa vrátane pridania nového používateľa alebo skupiny používateľov, zmenu úrovne oprávnenia používateľa, zmenu pravidiel firewallu alebo zmenu hesla,

6.1.4 automatické varovné alebo chybové hlásenia systémov,

6.1.5 detegované podozrivé alebo škodlivé aktivity a

6.1.6 ďalšie informácie nevyhnutné na posúdenie závažnosti kybernetického bezpečnostného incidentu v spojení s kritickosťou danej služby alebo zariadenia a korektné informácie o dátume, čase a použitej časovej zóne.

6.2 Dodávateľ berie na vedomie, že prevádzkové záznamy (logy) musia byť zabezpečené najmenej tak, že:

6.2.1 sú čitateľné výlučne osobám povereným ich analýzou,

6.2.2 zamedzujú možnosti prepísania alebo vymazania záznamu,

6.2.3 záznamy prenášané alebo presmerované od pôvodného zdrojového zariadenia do bezpečnostného monitorovacieho systému sú presmerované prostredníctvom zabezpečených kanálov alebo prostredníctvom dedikovanej správcovskej siete,

6.2.4 sú uchovávané po dobu zodpovedajúcu kategórii informačného systému.

6.3 Dodávateľ sa zaväzuje, že na základe požiadavky SE poverí pracovníka zodpovedného za monitorovanie prevádzkových záznamov, ich vyhodnocovanie a vykonanie nahlásenia podozrivej aktivity.

7 Riešenie kybernetických bezpečnostných incidentov

7.1 Dodávateľ berie na vedomie, že riešenie kybernetických bezpečnostných incidentov (ďalej len „**KBI**") pozostáva najmenej z/zo:

7.1.1 prípravy a vypracovania štandardov a postupov riešenia KBI,

7.1.2 monitorovania a analyzovania udalostí v sieťach a informačných systémoch,

7.1.3 detekcie KBI,

7.1.4 zberu relevantných informácií o KBI,

7.1.5 vyhodnocovania KBI,

7.1.6 riešenia zistených KBI a zníženia následkov zistených KBI,

7.1.7 vyhodnocovania spôsobov riešenia KBI po ich vyriešení a prijatia opatrení alebo zavedenie nových postupov s cieľom minimalizovať výskyt obdobných KBI.

7.2 Dodávateľ berie na vedomie, že na riešenie KBI sa v SE vypracúvajú a pravidelne aktualizujú štandardy a postupy riešenia KBI, ktoré obsahujú najmenej:

7.2.1 postup pri internom nahlasovaní KBI,

7.2.2 postup pri riešení jednotlivých typov KBI a spôsob ich vyhodnocovania,

7.2.3 spôsob evidencie KBI a použitých riešení.

7.3 Dodávateľ berie na vedomie, že proces detekcie KBI sa zabezpečuje prostredníctvom nástroja na detekciu KBI, ktorý umožňuje v rámci sietí a informačných systémov a medzi sieťami a informačnými systémami overenie a kontrolu prenášaných dát.

7.4 Dodávateľ berie na vedomie, že proces zberu a vyhodnocovania kybernetických bezpečnostných

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

7.4.1 zber a vyhodnocovanie informácií o kybernetických bezpečnostných udalostiach,

7.4.2 vyhľadávanie a zoskupovanie záznamov súvisiacich s KBI,

7.4.3 vyhodnocovanie bezpečnostných udalostí na ich identifikáciu ako KBI,

7.4.4 revíziu konfigurácie a monitorovacích pravidiel na vyhodnocovanie bezpečnostných udalostí pri nesprávne identifikovaných KBI.

7.5 Dodávateľ berie na vedomie, že proces riešenia KBI sa zabezpečuje prostredníctvom:

7.5.1 pridelenia zodpovednosti a určenia postupov na zvládanie KBI,

7.5.2 zavedenia procesu získavania a uchovávania podkladov potrebných na analýzu kybernetickej bezpečnostnej udalosti a KBI,

7.5.3 prijímania opatrení na odvrátenie alebo zmiernenie dopadu KBI,

7.5.4 zavedenia procesu nahlasovania KBI,

7.5.5 vedenia záznamov o KBI, vrátane použitých riešení,

7.5.6 prešetrovania a určenia príčin vzniku KBI aktualizáciou bezpečnostnej politiky a prijatia primeraných bezpečnostných opatrení zamedzujúcich jeho opakovanému výskytu.

7.6 Dodávateľ berie na vedomie, že súčasťou evidencie KBI na zabezpečenie dôkazu alebo dôkazného prostriedku sa musia byť aj informácie identifikujúce kybernetický bezpečnostný incident ako napríklad lokalita, hostname, MAC adresy, IP adresy, identifikačné údaje všetkých zariadení a zúčastnených osôb a dátum, čas manipulácie s údajmi a vymedzenie miesta ich uloženia.

8 Riadenie aktív, hrozieb a rizík

8.1 Dodávateľ berie na vedomie, že na zabezpečenie riadenia aktív, hrozieb a rizík musia byť všetky aktíva súvisiace so zariadeniami na spracovanie informácií a informačnými prostriedkami identifikované a inventár týchto aktív centrálne zaznamenaný a riadený. Súčasťou Plnenia musí byť inventárny zoznam aktív a používaných technológií sietí a informačných systémov, so závislosťami od iných informačných systémov a služieb dodávateľov, ako aj schéma sieťovej architektúry s uvedením miest prepojení sietí a pripojenia voči externým sieťam.

8.2 Súčasťou Plnenia musia byť podkladové informácie do analýzy rizík kybernetickej bezpečnosti, ktorá určuje pravdepodobnosť vzniku škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnou hrozbou v spojitosti s existujúcimi bezpečnostnými opatreniami a identifikáciou dopadov pri narušení dôvernosti, integrity alebo dostupnosti aktíva, minimálne v rozsahu poskytnutia zoznamu známych zraniteľností a single-point-of-failure použitých programových prostriedkov a ich častí, a technických prostriedkov a ich častí.

9 Riadenie bezpečnosti prevádzky

9.1 Dodávateľ berie na vedomie, že riadenie bezpečnosti prevádzky siete a informačného systému sa zaisťuje prostredníctvom určených pravidiel a postupov na:

9.1.1 riadenie zmien,

9.1.2 riadenie záplat a aktualizácií,

9.1.3 riadenie kapacít,

9.1.4 pravidelné zálohovanie a testovanie obnovy informácií zo záloh,

9.1.5 ochranu pred škodlivým kódom,

9.1.6 inštaláciu softvéru v sieťach a informačných systémoch,

9.1.7 inštaláciu zariadení v sieťach a informačných systémoch,

9.1.8 zaznamenávanie a vyhodnocovanie prevádzkových a bezpečnostných záznamov.

10 Kryptografické opatrenia

10.1 Dodávateľ berie na vedomie, že dôvernosť, integrita, dostupnosť a hodnovernosť údajov v rámci sietí a informačných systémov sa musí zabezpečiť pomocou kryptografických prostriedkov používajúcich dostatočne odolné kryptografické mechanizmy, schválených SE.

10.2 Dodávateľ berie na vedomie, že systémy správy kryptografických kľúčov a certifikátov musia byť zabezpečené počas celého životného cyklu kryptografických kľúčov a certifikátov. Správa kryptografických kľúčov a certifikátov musí zahŕňať najmenej:

10.2.1 bezpečné nakladanie s kryptografickými kľúčmi a certifikátmi,

10.2.2 generovanie pseudonáhodných čísel a kľúčov, zriadenie, distribúciu, vkladanie, zmenu, obmedzenie platnosti, vyberanie, ukladanie a likvidáciu kľúčov a zneplatnenie certifikátov,

10.2.3 umožnenie kontroly a auditu.

10.3 Dodávateľ je povinný zabezpečiť, aby používané kryptografické kľúče boli chránené pred zneužitím, prezradením alebo náhodným odhalením, stratou alebo zničením, a zabezpečiť, aby jeho pracovníci dodržiavali požiadavky na ochranu kryptografických kľúčov.

11 Fyzická bezpečnosť a bezpečnosť prostredia

11.1 Dodávateľ berie na vedomie, že sieť a informačný systém, avšak minimálne ich najdôležitejšie komponenty musia byť umiestnené v tzv. zabezpečenom priestore, aby boli chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej

infraštruktúry a fyzickým prístupom nepovolaných osôb. Zabezpečený priestor musí spĺňať požiadavky podľa § 16 ods. 1 písm. b) a c) 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 v platnom znení.

11.2 Dodávateľ berie na vedomie, že musí byť zabezpečená ochrana pred výpadkom zdroja elektrickej energie tých častí siete a informačného systému, ktoré vyžadujú nepretržitú prevádzku a zabezpečenie, že taký výpadok nenastane.

11.3 Dodávateľ berie na vedomie, že pre prácu v zabezpečenom priestore musia byť spracované a dodržiavané pravidlá na prácu v zabezpečenom priestore.

11.4 Dodávateľ berie na vedomie, **že prevádzka, používanie a manažment siete a informačného systému musí byť vždy v súlade s jeho zmluvnými záväzkami voči SE.**

11.5 Dodávateľ berie na vedomie, že **musí byť dodržiavaná politika, ktorá zakazuje nechávanie fyzických dokumentov bez dozoru a prikazuje uzamykanie počítača pred opustením pracoviska.**

11.6 Dodávateľ berie na vedomie, že **organizačné opatrenia vo fyzickej bezpečnosti sietí a informačných systémov musia zahŕňať pravidlá na:**

11.6.1 údržbu, uchovávanie a evidenciu technických komponentov sietí a informačných systémov a zariadení sietí a informačných systémov,

11.6.2 používanie zariadení sietí a informačných systémov na iné účely, ako sú určené,

11.6.3 používanie sietí a informačných systémov mimo zabezpečených priestorov,

11.6.4 vymazávanie, vyraďovanie a likvidovanie zariadení sietí a informačných systémov a všetkých typov relevantných záloh,

11.6.5 fyzický prenos technických komponentov sietí a informačných systémov alebo zariadení sietí a informačných systémov mimo zabezpečených priestorov,

11.6.6 narábanie s dokumentáciou systému a pamäťovými médiami tak, že sa zabráni ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii,

11.6.7 dimenzovanie a fyzické parametre sietí a hardvéru, ktoré priamo alebo nepriamo ovplyvňujú najväčšiu prípustnú dobu výpadku siete a informačného systému.

11.7 Dodávateľ berie na vedomie, že musia existovať záložné kapacity siete a informačného systému, zabezpečujúce dostupnosť, funkčnosť alebo náhradu siete a informačného systému, umiestnené v zabezpečenom priestore bezpečne vzdialenom zálohovanému zabezpečenému priestoru.

12 Riadenie kontinuity procesov

12.1 Súčasťou Plnenia sú:

12.1.1 krízové plány na zabezpečenie dostupnosti siete a/alebo informačného systému po narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu,

12.1.2 komunikačné plány na plnenie havarijných plánov a plánov obnovy spolu s kontaktnými údajmi, určeniami rolí a zodpovednosti na plnenie havarijných plánov a plánov obnovy po kybernetickom bezpečnostnom incidente,

12.1.3 plány havarijnej obnovy a postupy zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu.

12.2 Dodávateľ berie na vedomie, že riadenie kontinuity procesov pozostáva najmenej z testovania a vyhodnocovania jednotlivých procesov riadenia kontinuity činností a realizácie opatrení na zvýšenie odolnosti sietí a informačných systémov.

12.3 Dodávateľ berie na vedomie, že postupy zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu musia obsahovať najmenej:

12.3.1 frekvenciu a rozsah jej dokumentovania a schvaľovania,

12.3.2 určenie osoby zodpovednej za zálohovanie,

12.3.3 časový interval, identifikáciu rozsahu údajov, dátového média zálohovania a požiadavku zabezpečenia vedenia dokumentácie o zálohovaní,

12.3.4 požiadavku umiestnenia záloh v zabezpečenom prostredí s riadeným prístupom,

12.3.5 požiadavku zabezpečenia šifrovania záloh obsahujúcich aktíva klasifikačného stupňa chránené a prísne chránené,

12.3.6 požiadavku na vykonávanie pravidelného preverenia záloh, testovanie obnovy záloh a precvičovanie zavedených krízových plánov najmenej raz ročne.