Bezpečnostní pravidla pro významné dodavatele

Cílem těchto bezpečnostních pravidel je snižování rizik informačního a komunikačního systému a zohlednění požadavků vyplývajících z bezpečnostních opatření chránících aktiva Univerzity Tomáše Bati ve Zlíně (dále jen „UTB“), ke kterým mají přístup dodavatelé ve smyslu ustanovení § 4 odst. 4 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), v platném znění (dále jen „zákon o kybernetické bezpečnosti“), ve spojení v přílohou č. 7 k vyhlášce č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), v platném znění (dále jen „vyhláška o kybernetické bezpečnosti“).

Přitom významným dodavatelem ve smyslu § 2 písm. n) vyhlášky o kybernetické bezpečnosti je každý provozovatel informačního nebo komunikačního systému a každý, kdo s UTB vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému.

Základní odpovědnosti významného dodavatele

S významným dodavatelem musí být uzavřena smlouva o mlčenlivosti (NDA, Non-Disclosure Agreement) zavazující dodržování důvěrnosti a zabezpečení poskytnutých informací, dokumentů a zařízení. V případě porušení této smlouvy je dodavatel povinen nést důsledky vyplývající z této smlouvy (smluvní pokuta, náhrada škody).

S významným dodavatelem musí být uzavřena servisní smlouva (SLA, Service Level Agreement) zavazující dodržování úrovně poskytovaných služeb. V případě porušení této smlouvy je dodavatel povinen nést důsledky vyplývající z této smlouvy (smluvní pokuta, náhrada škody).

S významným dodavatelem musí být upravena pravidla pro zajištění integrity informací. V nich je třeba stanovit požadavky na šifrování dat při jejich výměně; použití elektronického podpisu, aby bylo možné jednoznačně určit, kdo provedl úpravu dat; omezení práv zápisu a úpravy dat na vybrané role; řízení přístupu k datům apod.

Významný dodavatel musí mít zavedený systém řízení bezpečnosti informací (certifikace není vyžadována).

Významný dodavatel

1. Je povinen postupovat v souladu s platnými a účinnými právními předpisy, zejména pak v souladu s požadavky vyplývajícími pro UTB, jakožto správce a provozovatele významného informačního systému (dále jen „VIS“), ze zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti a reflektovat případné novely uvedených právních předpisů či novou právní úpravu;

2. Odpovídá za své řešení/dodávku/správu (dále též jen „řešení“) tak, aby respektovalo požadavky na bezpečnost UTB, zabránilo bezpečnostním incidentům a krizovým situacím;

3. Odpovídá za dodávku a implementaci řešení v požadované kvalitě s ohledem na bezpečnost informací, zejména za správnou implementaci bezpečnostních postupů vyplývajících z těchto bezpečnostních pravidel.

4. Je povinen zajistit, aby předmět plnění neobsahoval technologie/klíčové prvky, vůči jejichž výrobcům příslušný správní orgán vydal opatření v souladu se zákonem o kybernetické bezpečnosti nebo které dle analýzy rizik představují vysoké riziko;

5. Je povinen vytvořit a schválit bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, které mohou být vytvářeny a zpracovávány na straně dodavatele při poskytování předmětu plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.

6. Je povinen provádět analýzu a hodnocení rizik informační infrastruktury, která mohou ovlivnit poskytování předmětu plnění smlouvy (dodávaného řešení) a na základě bezpečnostních potřeb a výsledků navrhovat a předkládat UTB ke schválení příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění na minimalizaci nebo odstranění zjištěných rizik, opatření monitorovat, vyhodnocovat jejich účinnost.

7. Je povinen pravidelně provádět také vlastní analýzu a hodnocení rizik a kontrolu zavedených bezpečnostních opatření. Tato kontrola probíhá v pravidelných intervalech stanovených dodavatelem, na žádost UTB. O výsledku kontroly podá dodavatel UTB bez zbytečného odkladu písemnou kontrolní zprávu.

8. Má povinnost informovat UTB o způsobu řízení rizik, jakož i o zbytkových rizicích souvisejících s plněním předmětu smlouvy.

9. Je povinen stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.

10. Je povinen zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost během poskytování plnění pro UTB.

11. Je povinen vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat všechny podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na požádání tyto záznamy zpřístupnit UTB.

12. Odpovídá za trvalé zachování mlčenlivosti všech svých pracovníků podílejících se na řešení o poskytnutých informacích, dokumentech a zařízeních i po ukončení smluvního vztahu se UTB.

13. Je povinen předat UTB kontaktní údaje dohledového centra (helpdesku) se zaznamenanou činností/kontaktní údaje všech svých pracovníků podílejících se na řešení.

14. Využívá-li při poskytování předmětu plnění subdodavatele (významného dodavatele), zajistit adekvátní dodržování těchto bezpečnostních pravidel i ve smluvních vztazích se svými subdodavateli.

Subdodavatelé

1. Dodavatel nezapojí do poskytování plnění dle této smlouvy žádného dalšího subdodavatele bez předchozího konkrétního nebo obecného povolení UTB.

2. Dodavatel je povinen předat UTB kontaktní údaje všech osob subdodavatele podílejících se na řešení, zejména osob dodávajících systémovou a technickou podporu pro řešení.

3. Dodavatel má povinnost zajistit, že subdodavatel bude v souladu s požadavky těchto Bezpečnostních pravidel.

4. Dodavatel odpovídá za to, že jeho subdodavatelé nebudou jednat v rozporu s bezpečnostními opatřeními vyplývajícími z těchto bezpečnostních pravidel. V případě, že dojde k nedodržení těchto požadavků ze strany subdodavatele dodavatele, považuje se každé takové nedodržení požadavků za porušení povinnosti dodavatele dle smlouvy.

1 ŘÍZENÍ INFORMAČNÍ A KYBERNETICKÉ BEZPEČNOSTI

1.1 Významný dodavatel má, včetně jeho případných subdodavatelů povinnost ve svých interních procesech realizovat následující opatření:

1.1.1 mít stanoven plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí v následující formě, obsahu a rozsahu:
a) poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů, včetně jeho subdodavatelů o jejich povinnostech a o bezpečnostní politice;
b) potřebná teoretická i praktická školení uživatelů, administrátorů a osob zastávajících bezpečnostní role;

1.1.2 mít určeny osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny;

1.1.3 v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů (subdodavatelů) o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení;

1.1.4 pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pravidelná odborná školení, přičemž musí vycházet z aktuálních potřeb v oblasti kybernetické bezpečnosti;

1.1.5 v souladu s plánem rozvoje bezpečnostního povědomí zajišťovat pravidelná školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní;

1.1.6 zajišťovat kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a mít nastaven proces pracovněprávního postihu pro své zaměstnance;

1.1.7 v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajišťovat předání odpovědností;

1.1.8 hodnotit účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí;

1.1.9 určovat pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;

1.1.10 vést o provedených školeních přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

1.1.11 alespoň jedenkrát ročně předat UTB informace, týkající se osob souvisejících s poskytovaným předmětem plnění smlouvy, o provedených školeních a jejich obsahu.

1.2 Dodavatel má stanoveny všechny podstatné požadavky na bezpečnost informací s každým svým dodavatelem, který může k jeho informacím a k informacím jeho zákazníků přistupovat, zpracovávat je, ukládat, přenášet je nebo pro ně poskytovat komponenty ICT infrastruktury.

1.3 UTB si vyhrazuje právo vést záznamy a prověřovat činnosti dodavatele, vést záznamy o incidentech a nestandardních činnostech zaměstnanců a dalších osob působících ve prospěch dodavatele (dále jen „zaměstnanci dodavatele“). Na základě těchto záznamů má oprávnění vyhodnocovat důvěryhodnost a spolehlivost zaměstnanců dodavatele. V případě identifikovaného rizika oznámí UTB nesoulad dodavateli a obě strany vejdou v jednání za účelem řešení této situace.

2 ŘÍZENÍ LIDSKÝCH ZDROJŮ

2.1 Dodavatel zajistí, že všechny osoby, účastnící se plnění dle uzavřené smlouvy s UTB, jsou seznámeny s těmito bezpečnostními pravidly a dalšími upřesňujícími bezpečnostními informacemi prokazatelně předanými ze strany UTB. Tyto osoby stvrdí seznámení s pravidly písemně.

2.2 Osoby, účastnící se plnění dle uzavřené smlouvy s UTB, musí mít prokazatelné potřebné kvalifikační předpoklady, zkušenosti a znalosti.

2.3 Dodavatel musí zajistit, aby osoby, které se účastní plnění dle uzavřené smlouvy s UTB, prošly procesem prověřování a byly jim stanoveny pro jejich činnosti podmínky a odpovědnosti.

3 BEZPEČNOST A OCHRANA ZDRAVÍ PŘI PRÁCI A POŽÁRNÍ OCHRANA (BOZP A PO), FYZICKÁ BEZPEČNOST

3.1 Dodavatel jako zaměstnavatel při vykonávání prací při plnění předmětu plnění zodpovídá za:
a) dodržování předpisů BOZP a PO svými zaměstnanci, příp. jinými fyzickými osobami vykonávajícími práci v jeho prospěch,
b) zamezení neoprávněného přístupu do objektů UTB, ve kterých poskytuje službu (nebo plní závazek z uzavřené smlouvy),
c) zamezení poškození a neoprávněné zásahy v objektech UTB.

4 ŘÍZENÍ PROVOZU

4.1 Dodavatel se zavazuje:

4.1.1 zajistit bezpečný provoz informačního systému a infrastruktury, pokud zajišťuje její provoz, využívané pro poskytování předmětu plnění v souladu s požadavky vyhlášky o kybernetické bezpečnosti a doporučeními standardů informační bezpečnosti, např. technických norem řady ISO/IEC 27000;

4.1.2 na vyžádání poskytnout UTB přehled o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře, kterými plní předmět smlouvy.

4.1.3 zabezpečit, že pro poskytování předmětu plnění budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky, autorská práva a práva související s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů.

5 ŘÍZENÍ PŘÍSTUPU

5.1 Identifikace

5.1.1 Každý zaměstnanec dodavatele podílející se na plnění smlouvy výpočetními prostředky dodavatele, musí mít v rámci své infrastruktury evidován a veden svůj vlastní jedinečný uživatelský účet, kterému jsou v jednotlivých systémech, modulech nebo aplikacích přiřazeny specifické role. Každý zaměstnanec dodavatele musí být veden s platnými identifikačními a aktuálními kontaktními údaji.

5.1.2 Každý zaměstnanec dodavatele, pokud přistupuje k interním informačním systémům UTB, má u UTB veden a evidován jedinečný uživatelský účet, kterému jsou v jednotlivých systémech, modulech nebo aplikacích přiřazeny specifické role související výhradně s plněním předmětu smlouvy.

5.2 Autentizace (ověření identity)

5.2.1 Podmínky pro autentizaci uživatelů, administrátorů a aplikací při využití informační infrastruktury UTB:

a) využívá se dvou faktorová autentizace, tj. identifikátor účtu a dva faktory z trojice <autentizační předmět, heslo, biometrický údaj>;
b) do doby splnění požadavku podle bodu a) se musí používat autentizace pomocí identifikátoru účtu a kryptografického klíče se zaručením obdobné úrovně bezpečnosti;
c) do doby splnění požadavku podle bodu a) nebo b) se musí používat autentizace pomocí identifikátoru účtu a hesla s definovanými pravidly, která musí být technologicky vynucována.

5.2.2 Pro vzdálený přístup zaměstnanců dodavatele předkládá dodavatel podklady pro vyplnění žádosti o vzdálený přístup, podle které jsou pak nastaveny parametry bezpečného vzdáleného přístupu, vč. časového období trvání přístupu.
a) za dodavatele žádost interně ve UTB vyplňuje odpovědná osoba příslušného určeného systému UTB (na základě podkladů od kontaktní osoby dodavatele).
b) po zpracování žádosti je zaměstnanec dodavatele individuálně obeznámen s podrobnostmi pravidel vzdáleného přístupu a jsou mu předány autentizační údaje.

5.2.3 Dodavatel odpovídá za činnosti svých zaměstnanců, případně dalších fyzických osob zaměstnaných v jeho prospěch, které musí být v souladu s bezpečnostními pravidly a dalšími upřesňujícími bezpečnostními informacemi prokazatelně předanými ze strany UTB na základě vyžádání ze strany dodavatele. Veškeré škody, které vzniknou porušením těchto a dalších upřesňujících bezpečnostních informací zaměstnanci dodavatele nebo dalšími osobami vykonávajícími práci v jeho prospěch, jdou k tíži dodavatele, který je povinen tyto škody v plném rozsahu UTB nahradit.

5.3 Autorizace

5.3.1 Zaměstnanci dodavatele jsou povinni v informační infrastruktuře UTB využívat privilegovaná oprávnění jen v přiměřené míře a jen po dobu nezbytně nutnou pro vykonání činností v souladu s plněním předmětu smlouvy. Uživatelé ani administrátoři nesmějí používat účty s privilegovanými oprávněními pro běžnou práci nesouvisející se správou příslušného informačního systému.

5.3.2 Zaměstnanci dodavatele jsou informováni UTB, které informace UTB považuje za chráněné, ke kterým chráněným informacím UTB mají přístup a jak s nimi mohou nakládat. Jakékoliv manipulace a další operace s chráněnými informacemi UTB, které nebyly výslovně v instrukcích uvedeny, nemá dodavatel povoleny.

5.4 Vzdálený přístup

5.4.1 Pro přístup k informačním systémům UTB může dodavatel používat své vlastní prostředky (HW, SW).

5.4.2 Pracovní stanice dodavatele přistupující k infrastruktuře UTB prostřednictvím VPN (Virtual Private Network) musí mít:
a) pokročilou funkční antivirovou ochranu (se zapnutou ochranou v reálném čase (real time protection mode)), včetně komponenty pro aktivní sběr logů a kybernetických

bezpečnostních incidentů (např. SIEM) v souladu s požadavky zákona o kybernetické bezpečnosti;
b) funkční osobní firewall;
c) plně aktualizovaný operační systém a nastavené automatické aktualizace operačního systému;
d) operační systém, který není mimo servisní podporu výrobce (pokud není smluvním ujednáním výslovně stanoveno jinak);
g) aktualizované aplikace třetích stran bez porušování autorských práv třetích stran;
h) zajištěno šifrování všech paměťových médií, na kterých jsou uložena chráněná data a informace UTB. Přístup k paměťovým médiím a k dešifrování chráněných dat a informací UTB musí být umožněno jen oprávněným osobám dodavatele;
i) nainstalovaného VPN klienta dle pokynu UTB;
j) druhý autentizační faktor, pokud UTB vyžaduje, případně je-li dostupný (např. HW, mobile app nebo SMS token) pro přístup k VPN, který bude poskytnut určeným zaměstnancem UTB proti podpisu předávacího protokolu.

6 ŘÍZENÍ ZMĚN

6.1 Změny na straně dodavatele musí být řízeny s ohledem na kritičnost informací, systémů, procesů a opětovným posuzováním rizik.

6.2 Dodavatel se zavazuje:

6.2.1 řídit a evidovat smluvní změny;

6.2.2 řídit a evidovat změny v poskytovaných službách v souladu s požadavky vyhlášky o kybernetické bezpečnosti a doporučeními standardů informační bezpečnosti, např. technických norem řady ISO/IEC 27000;

6.2.3 poskytnout UTB veškerou nezbytnou součinnost při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu;

6.2.4 v případě realizace penetračního testování nebo testování zranitelnosti řešení poskytnout UTB veškerou potřebnou součinnost a přijmout dodatečná, účinná nápravná opatření k odstranění zranitelností, které byly zjištěny v průběhu penetračního testování.

7 AKVIZICE, VÝVOJ A ÚDRŽBA

7.1 Dodavatel se zavazuje:

7.1.1 zajistit bezpečnou implementaci, inovaci, aktualizaci, testování technologií, které jsou předmětem plnění;

7.1.2 předat UTB dokumentaci předmětu plnění minimálně v následujícím rozsahu:
a) dokumentaci skutečného provedení;

b) dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;
c) dokumentaci obsahující popis autorizačního konceptu a oprávnění;
d) dokumentaci obsahující zálohovací a archivační postupy;
e) dokumentaci obsahující instalační a konfigurační postupy;
f) dokumentaci zahrnující testy zranitelností a soulad s bezpečnostními požadavky UTB;
g) dokumentaci pro zajištění kontinuity provozu a obnovy po havárii.

7.2 V případě vývoje řešení se dodavatel zavazuje:

7.2.1 dodržovat a implementovat osvědčené postupy (best practices) pro bezpečný vývoj softwaru dle doporučení standardů informační bezpečnost, např. technických norem řady ISO/IEC 27000;

7.2.2 pokud jsou softwarové auditní činnosti a předání zdrojového kódu k řešení součástí plnění dle smlouvy, bude umožněn audit prováděného nebo provedeného plnění a na písemnou žádost bude předložen vyvíjený zdrojový kód k řešení na provedení code review (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), a to zejména za účelem ověření skutečnosti, zda bylo postupováno dle plnění v souladu se smlouvou;

7.2.3 zajistit, že plnění bude obsahovat pouze ty součásti, které jsou objektivně potřebné pro řádné provozování řešení a/nebo které jsou specifikovány výslovně ve smlouvě (zejména řešení nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.);

7.2.4 pokud je součástí plnění i instalace operačního systému případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity požadované verze těchto produktů kompatibilní a funkční v prostředí UTB;

7.2.5 zajistit bezpečnost testovacího prostředí u dodavatele a ochranu poskytnutých testovacích dat UTB;

7.2.6 zajistit, že do produkčního prostředí UTB bude implementován pouze předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další potřebné údaje k provozování předmětu plnění;

7.2.7 zajistit, že v rámci poskytovaného plnění bude dodávané řešení v souladu s doporučeními standardů informační bezpečnosti, např. technických norem řady ISO/IEC 27000;

7.2.8 poskytnout UTB potřebnou součinnost v případě, že UTB vyžaduje/realizuje provedení bezpečnostních testů souvisejících s předmětem plnění;

7.2.9 v případě, že UTB požaduje od dodavatele potvrzení o provedení bezpečnostních testů, bude uvedené dohodnuto samostatnou smluvní dohodou;

7.2.10 předat zdrojový kód UTB, je-li tak stanoveno ve smlouvě, bezpečnou formou zajišťující jeho integritu, a v takovém případě:
a) zajistit řízení verzí zdrojového kódu;
b) zajistit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí;
c) zajistit, aby distribuce zdrojových kódů obsahovala soubor z vývojového prostředí na řízenou kompilaci těchto zdrojových kódů;

7.2.11 nevyvíjet, nekompilovat a nešířit v prostředí UTB programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

8 UŽÍVÁNÍ KRYPTOGRAFICKÝCH PROSTŘEDKŮ

8.1 Je-li v rámci předmětu plnění vyžadováno použití kryptografických prostředků, technické podmínky jsou následující:

8.1.1 šifrování symetrickým algoritmem metodou AES využitím délky klíčů 256 bitů, heslo musí být předáno jiným komunikačním kanálem, než jsou přenášena data;

8.1.2 šifrování asymetrickým algoritmem metodou DSA s využitím délky klíčů 3072 bitů a více nebo metodou založenou na eliptických křivkách (EC-DSA, EC-Schnorr) s využitím délky klíčů 256 bitů a více;

8.1.3 použití hašovací funkce metodou SHA-2 anebo SHA3 s využitím délky výstupů 256 bitů a více;

8.1.4 šifrování pomocí digitálních certifikátů vydaných obecně uznávanou CA nebo CA, které explicitně důvěřují obě strany;

8.1.5 šifrování disků módem XTS (délka jednotky dat/sektoru nesmí přesáhnout 2^{20} bloků šifry) nebo EME2;

8.1.6 ochrana integrity módem HMAC (se schválenou hašovací funkcí) nebo EMAC;

9 MONITORING

9.1 Přístup zaměstnanců dodavatele k vybraným chráněným interním informacím a k informačním a komunikačním systémům UTB je nepřetržitě zaznamenáván do logů, monitorován a vyhodnocován. Je-li to z technického a provozního hlediska možné, s systémech UTB jsou zaznamenávány následující události:
a) úspěšné a neúspěšné přihlášení a odhlášení uživatelů;
b) činnosti provedené administrátory;
c) úspěšné a neúspěšné manipulace s účty, oprávněními a právy;
d) neprovedení činností v důsledku nedostatku přístupových oprávnění;
e) činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému;
f) zahájení a ukončení činností technických aktiv;

g) automatická varovná nebo chybová hlášení technických aktiv;
h) přístupy k logům a pokusy o manipulaci s logy;
i) změny nastavení nástroje pro zaznamenávání činností;
j) změny použití mechanismů autentizace včetně změny údajů, které slouží k přihlášení.

9.2 Je-li to z technického a provozního hlediska možné, ke každému záznamu v logu přiřazuje UTB:
a) datum a čas;
b) typ činnosti;
c) název relevantního technického aktiva;
d) identifikaci uživatele;
e) identifikaci síťového zařízení původce;
f) úspěšnost nebo neúspěšnost provedení činnosti;
e) úroveň závažnosti.

9.3 Dodavatel je povinen průběžně monitorovat v rámci své ICT infrastruktury zveřejněné a známé bezpečnostní chyby, které mohou ovlivnit hladký a bezpečný provoz systémů souvisejících s jím poskytovanými službami. Jedná se například o zranitelnosti v operačních systémech, software třetích stran, webové komponenty atd.

10 OCHRANA DATOVÝCH ÚLOŽIŠŤ A PŘENOSNÝCH MÉDIÍ

10.1 Uložení chráněných informací UTB do datových úložišť, na přenosná média a případný transport médií mimo prostory UTB podléhá schválení UTB.

10.2 V případě ukládání chráněných informací UTB do datových úložišť a na přenosná média má dodavatel povinnost ukládat, případně vyžadovat uložení těchto dat v šifrované podobě a vést evidenci těchto médií.

10.3 Dodavatel je povinen zajistit likvidaci operativních dat obsahujících chráněné informace UTB ihned po pominutí účelu jejich zpracování a/nebo uložení. Po likvidaci dat na elektronickém médiu nesmí být možné informaci obnovit. O provedení likvidace dat musí dodavatel vyhotovit protokol.

11 KYBERNETICKÉ BEZPEČNOSTNÍ UDÁLOSTI / INCIDENTY

11.1 Dodavatel má za povinnost hlásit veškerá podezření na všechny nestandardní situace, bezpečnostní zranitelnosti a kybernetické bezpečnostní události / incidenty:

11.1.1 bezprostředně nebo bez zbytečného prodlení po zjištění kybernetické bezpečnostní události / incidentu;

11.1.2 odpovědné kontaktní osobě UTB stanovené v nadřízené smlouvě;

11.1.3 písemně prostřednictvím e-mailu abuse@utb.cz.

11.1.4 s uvedením:
a) data a času zjištění události / incidentu;
b) povahy události / incidentu;
c) zdroje události / incidentu;
d) cíle / oběti události / incidentu;
e) potenciálního dopadu.

11.2 Pokud dojde ke kybernetické bezpečnostní události / incidentu a následnému zvládání a vyhodnocování kybernetického bezpečnostního incidentu na straně UTB, poskytne dodavatel požadovanou součinnost, zejména poskytne logy a identifikační údaje (např. IP adresa, MAC adresa, HW typ, sériové číslo, případně IMEI) dotyčného koncového zařízení nebo mobilního koncového zařízení, k analýze obsahu, případně bez zbytečného odkladu zrealizuje opatření požadovaná UTB.

11.3 Dodavatel má povinnost provést analýzu příčin kybernetické bezpečnostní události / incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

12 AUDIT DODAVATELE (ZÁKAZNICKÝ AUDIT)

12.1 Oprávnění k provedení auditu dodavatele

12.1.1 UTB si vyhrazuje právo provádět audity dodavatele.

12.1.2 Dodavatel se zavazuje poskytnout UTB veškerou potřebnou dokumentaci, zejména výčet technických a organizačních opatření, potřebnou k doložení toho, že byly splněny povinnosti vyplývající z těchto bezpečnostních pravidel, jakož i ze zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti, a za tímto účelem se zavazuje umožnit UTB provedení kontrol, včetně auditů prováděných UTB či auditorem, kterého UTB k auditu pověří, a poskytne k těmto kontrolám a auditům veškerou potřebnou součinnost.

12.1.3 UTB s dostatečným předstihem alespoň 14 kalendářních dnů oznámí dodavateli záměr na provedení auditu. Obě strany si dohodnou obsah, potřebnou součinnost a časový plán auditu s tím, že UTB se zavazuje postupovat tak, aby nenarušila provozní potřeby dodavatele.

12.1.4 Dodavatel má povinnost určit svého zástupce (případně své zástupce), který bude po dobu provádění kontroly či auditu přítomen.

12.1.5 UTB si vyhrazuje právo v případě závažných důvodů (např. podezření na rizikové chování dodavatele) v souvislosti s plněním této smlouvy provést neohlášený audit u dodavatele s přihlédnutím k provozní situaci dodavatele.

12.1.6 Při zjištění neshod stanoví auditor / inspektor nápravná opatření a termín jejich zavedení. Dodavatel je povinen nápravná opatření realizovat ve stanoveném rozsahu a v požadovaném termínu.

12.1.7 Dokumentace auditů prováděných UTB je vedena v útvaru odpovědném za provádění auditů. Záznamy týkající se určitého auditu jsou vždy označovány stejným identifikátorem. Jednotlivé záznamy auditů tvoří:
a) plán auditu;
b) oznámení o auditu;
c) dotazník k auditu (seznam otázek auditora, pokud auditor uzná za vhodné);
d) zpráva z auditu;
e) písemné, fotografické nebo jiné záznamy provozu, postupů nebo zařízení, které souvisí s auditem (pokud je nezbytné pro dokumentování nálezů);
f) záznam o zjištění (nápravných opatřeních a následné kontrole).

12.1.8 Auditovaná strana (dodavatel) obdrží k vyjádření závěrečnou zprávu auditu obsahující případná zjištění, na jejichž základě:
a) dodavatel navrhne způsob realizace opatření (včetně závazných termínů) stanovených auditorem a předá jejich seznam UTB k odsouhlasení.
b) UTB následně potvrdí souhlas s navrženými opatřeními nebo je vrátí s připomínkami dodavateli k přepracování.

12.2 Nápravná opatření

12.2.1 Auditovaná strana (dodavatel) má za povinnost v určeném čase zajistit realizaci dohodnutých nápravných opatření.

12.2.2 Zprávu o realizovaných opatřeních dodavatel oznamuje a předává UTB.

13 OCHRANA AKTIV PROTI NEAUTORIZOVANÝM ČINNOSTEM

13.1 Dodavatel na aktiva UTB neinstaluje a nepoužívá nástroje, které nejsou součástí předmětu plnění.

14 ŘÍZENÍ KONTINUITY ČINNOSTÍ

14.1 UTB má oprávnění zapojit dodavatele do řízení kontinuity činností, a to zejména oprávnění zahrnout dodavatele do plánu kontinuity činností, který souvisí s informačním systémem a souvisejícími službami a/nebo zahrnout dodavatele do havarijního plánu UTB.

14.2 Dodavatel předloží UTB metodiku zálohování a obnovy dat ve formě zálohovacího plánu, testovacího scénáře obnovy dat, systému evidence, zajištění integrity a autenticity zálohovacího média. Záloha jako taková musí být šifrována.

15 PODMÍNKY PŘI UKONČENÍ SMLOUVY

15.1 V případě ukončení smluvního vztahu musí být dodavateli a jeho zaměstnancům odebrána veškerá přístupová práva k aktivům UTB (VPN, systémy, informace) nejpozději ke dni ukončení smluvního vztahu.

15.2 Pokud byla zaměstnancům dodavatele poskytnuta aktiva UTB, musí být tato aktiva vrácena nejpozději ke dni ukončení smluvního vztahu.

15.3 Pokud byla dodavateli poskytnuta informační aktiva (data) UTB, musí být nejpozději ke dni ukončení smluvního vztahu vrácena a beze zbytku smazána bez možnosti jejich obnovení ze všech informačních systémů dodavatele a nosičů dodavatele, která taková aktiva obsahují.