**Kybernetická bezpečnost**

**Požadavky na zajištění kybernetické bezpečnosti**

Elektronický systém spisové služby (dále jen „eSSL“) dodavatele významného informačního systému (dále jen „Dodavatel“), je v souladu s § 2 odst. 1 písm. d) vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, určen Úřadem vlády České republiky jakožto provozovatelem a správcem (dále jen „Provozovatel“), jako významný informační systém (dále jen „VIS“) a Dodavatel se tímto stává významným dodavatelem dle § 2 písm. n) vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „VoKB“).

Za účelem plnění povinností stanovených Poskytovatelem, jakožto povinnou osobou ve smyslu zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZoKB“) a jeho prováděcího předpisu VoKB je Dodavatel povinen nad rámec povinností stanovených smlouvou plnit níže uvedené povinnosti, a to zejména součinnostního a bezpečnostního charakteru dle této přílohy.

Dodavatel je povinen plnit relevantní povinnosti v rozsahu a způsobem tak, aby byl naplněn účel právní úpravy v oblasti bezpečnostních opatření, kybernetických bezpečnostních incidentů, reaktivních opatření, náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat ve vztahu k povinnostem, které tato právní úprava stanovuje Poskytovateli jakožto povinné osobě dle předpisů z oblasti kybernetické bezpečnosti, a to i v případě změny příslušné právní úpravy. V takovém případě je Poskytovatel oprávněn požadovat od Dodavatele přiměřenou součinnost i nad rámec povinností stanovených v této příloze, avšak vždy pouze za účelem zajištění plnění povinnosti Dodavatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

1. **Systém řízení bezpečnosti informací**
   1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 3 VoKB, které musí Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB plnit.
   2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména:
2. Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení informačních aktiv Poskytovatele, které jsou zpracovávány na straně Dodavatele při poskytování předmětu plnění.
3. Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je a vyhodnocovat jejich účinnost.
4. Vést záznamy o zpracování informačních aktiv Poskytovatele v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto aktiv a na vyžádání tyto záznamy Poskytovateli zpřístupnit.
5. Stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení informačních aktiv Poskytovatele, při poskytování předmětu plnění, přičemž bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.
6. Stanovit a udržovat aktuální bezpečnostní opatření ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.
7. **Řízení aktiv**
   1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 4 VoKB, které musí splnit Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
   2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména stanovit a udržovat rozsah a seznam aktiv využívaných pro plnění Servisní smlouvy (aktivy se rozumí např. data a informace k předmětu plnění dle Servisní smlouvy, systémy ICT, SW moduly, HW prvky - infrastruktura, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač, mobilní koncová zařízení – přenosná zařízení typu notebook, tablet, chytrý mobilní telefon, apod.), a tato aktiva strukturovaně popsat a Poskytovateli předložit kdykoliv na jeho vyžádání, a to po celou dobu trvání Servisní smlouvy.
8. **Řízení rizik**
   1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 5 VoKB, které musí splnit Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
   2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména:
9. Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.
10. Vytvářet a každých 6 měsíců, počínaje dnem účinnosti Servisní smlouvy Poskytovateli předkládat zprávu o řízení kybernetických bezpečnostních rizik, která bude minimálně pokrývat:
11. Vyhodnocení aktuálního stavu kybernetické bezpečnosti s vazbou na předmět plnění.
12. Identifikaci a hodnocení rizik s vazbou na předmět plnění.
13. Realizovaná bezpečnostní opatření.
14. Nepokrytá bezpečnostní rizika a návrh opatření.
15. Vyhodnocení bezpečnostních událostí a incidentů.
16. Aktuální stav souladu Dodavatele s těmito požadavky v oblasti kybernetické bezpečnosti.
17. **Organizační bezpečnost**
    1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 6 VoKB, které musí splnit Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
    2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména:
18. Jmenovat nejpozději do 30 dnů od uzavření této Servisní smlouvy odpovědnou kontaktní osobu (dále jen „Kontaktní osoba“), pro potřeby zajištění plnění KB požadavků a související komunikace mezi smluvními stranami či mezi Dodavatelem a Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“). Kontaktní osobu sdělí v téže lhůtě Dodavatel písemně Poskytovateli a stejně tak i NÚKIB, a to spolu s ostatními kontaktními údaji dle § 34 VoKB.
19. Využívat pro poskytování předmětu plnění pouze oprávněných osob, které byly řádně seznámeny s příslušnými ustanoveními interních řídících aktů Poskytovatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění.
20. **Bezpečnostní role**
    1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 7 VoKB, které musí splnit Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
    2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména:
21. Určit roli manažera kybernetické bezpečnosti.
22. Určit roli garanta aktiv využívaných pro plnění Servisní smlouvy.
23. **Řízení dodavatelů**
    1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 8 VoKB, které musí splnit Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
    2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména:
24. Využívá-li při poskytování předmětu plnění poddodavatele, zajistit adekvátní dodržování požadavků v oblasti kybernetické bezpečnosti rovněž ve smluvních vztazích se svými poddodavateli.
25. Pokud při poskytování předmětu plnění dochází ke zpracování osobních údajů, zajistit uzavření samostatných smluv (tj. smluv se svými poddodavateli, zaměstnanci a případnými dalšími osobami podílejícími se na poskytování plnění ze Servisní smlouvy) ve smyslu příslušných ustanovení Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.
26. **Bezpečnost lidských zdrojů**
    1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 9 VoKB, které musí splnit Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
    2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména:
27. Zajistit, aby Kontaktní osoba nejpozději do 30 dnů od uzavření Servisní smlouvy potvrdila písemně Poskytovateli, že všechny osoby podílející se na poskytování předmětu plnění za stranu Dodavatele byly prokazatelně seznámeny s požadavky v oblasti kybernetické bezpečnosti a příslušnými ustanoveními interních řídících aktů Poskytovatele, byly-li takové Dodavateli zpřístupněny.
28. Dodržovat příslušná ustanovení interních řídících aktů Poskytovatele v rozsahu, v jakém byl s těmito akty seznámen. Za prokazatelné seznámení se považuje protokolární či elektronické předání příslušné dokumentace nebo Poskytovatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní akty řízení. Současně s tím se Dodavatel zavazuje k mlčenlivosti o informacích, které se v souvislosti s dokumentací poskytnutou Poskytovatelem dozvěděl.
29. V případě, že je součástí předmětu plnění služba dohledu nad předmětem plnění, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu plnění.
30. Zajistit, aby osoby podílející se na poskytování plnění Poskytovateli v prostředí nebo s prostředky Poskytovatele, a to i tehdy, pokud jsou prostředky Poskytovatele používány mimo jeho prostředí:
31. Pro uložení a sdílení dat a informací Poskytovatele využívali pouze k tomu schválené prostředky.
32. V souvislosti s předmětem plnění neukládali ani nesdíleli data a informace eticky nevhodného obsahu, odporující dobrým mravům nebo jinak poškozující jméno Poskytovatele.
33. Nestahovali, nesdíleli, neukládali, nearchivovali ani neinstalovali datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem.
34. Nerealizovali pokusy o neautorizovaný přístup ke zdrojům Poskytovatele ani ke zdrojům jiných subjektů.
35. Nerealizovali pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků Poskytovatele, a to ani v případě, kdy jim byl prostředek Poskytovatele svěřen do správy.
36. Nepodíleli se v souvislosti s předmětem plnění nebo prostředky Poskytovatele na šíření spamu ani škodlivého softwaru.
    1. Dodavatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům (informačním / technickým) Poskytovatele je na straně Poskytovatele zpracování osobních údajů pracovníků Dodavatele, kteří se podílejí na zajištění předmětu plnění. Pokud nebude Poskytovateli umožněno osobní údaje dotčených pracovníků Dodavatele zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům Poskytovatele.
37. **Řízení provozu a komunikací**
    1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 10 VoKB, které musí splnit Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
    2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména:
38. Zajistit bezpečný provoz aplikačního vybavení a podpůrné infrastruktury využívané pro poskytování předmětu plnění.
39. Na vyžádání poskytnout Poskytovateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených v souvislosti s předmětem plnění.
40. Zajistit, že pro poskytování předmětu plnění bude využíváno pouze aplikační vybavení a technologie, které jsou v souladu s platnými právními předpisy České republiky a Evropské unie, především s ohledem na licenční podmínky a autorský zákon.
41. **Řízení změn**
    1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 11 VoKB, které musí splnit Poskytovatel jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
    2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména:
42. Přiměřeně reagovat na změny na straně Poskytovatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.
43. Oznamovat významné změny Poskytovateli a aktivně spolupracovat při jejich testování.
44. **Řízení přístupu**
    1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 12 VoKB, které musí splnit Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
    2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména:
45. Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k informačním aktivům Poskytovatele.
46. Zajistit, aby udělený přístup nebyl sdílen více osobami za strany Dodavatele. V takovém případě musí Dodavatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit Poskytovateli kdykoli v průběhu trvání účinnosti Servisní smlouvy.
47. Stanovit v požadavku na přístup rozsah dat/informací, služby a účely, pro které je přístup k informačním aktivům Poskytovatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou / 1 rok / 1 měsíc / 1 den).
48. Zajistit, aby osoby podílející se na poskytování předmětu plnění a mající přístup k informačním aktivům Poskytovatele chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.
49. Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně Dodavatele, které přistupují k informačním aktivům Poskytovatele.
    1. Dodavatel bere na vědomí, že přístup k informačním aktivům Poskytovatele je možné povolit pouze fyzické identitě zaměstnance Dodavatele resp. poddodavatele Dodavatele, a to na základě požadavku Dodavatele na přístup.
    2. Dodavatel bere na vědomí, že přidělení oprávnění zaměstnanci Dodavatele musí být realizováno na základě zásady nejnižšího oprávnění a principu need-to-know.
    3. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu Dodavatele) může být příslušný účet zablokován a řešen jako bezpečnostní incident a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům Poskytovatele).

**¨**

1. **Akvizice, vývoj a údržba**
   1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 13 VoKB, které musí splnit Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
   2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména:
2. Zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění.
3. Předat Poskytovateli dokumentaci předmětu plnění minimálně v následujícím rozsahu:
4. Dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů.
5. Dokumentaci obsahující popis autorizačního konceptu a oprávnění.
6. Dokumentaci obsahující instalační a konfigurační postupy.
   1. V případě, že předmět plnění zahrnuje též vývoj softwaru, zavazuje se Dodavatel:
7. Dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru v rámci celého jeho životního cyklu.
8. Na vyžádání umožnit Poskytovateli realizaci auditu prováděného nebo provedeného plnění a na vyžádání předložit Poskytovateli relevantní část zdrojového kódu k softwaru na provedení codereview, a to zejména za účelem ověření skutečnosti, zda Dodavatel postupuje či postupoval při poskytování plnění v souladu se Servisní smlouvou a těmito požadavky v oblasti kybernetické bezpečnosti.
9. Poskytnout Poskytovateli v jím stanoveném termínu, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru či kdykoli po jeho dokončení.
10. Zajistit, že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování softwaru a/nebo které jsou specifikovány výslovně v Servisní smlouvě (zejména, že software nebude obsahovat žádné nepotřebné či z pohledu Poskytovatele nežádoucí komponenty).
11. Pokud je součástí plnění též instalace softwaru třetích stran, zajistit že budou použity aktuální, podporované a kompatibilní verze těchto softwarových produktů.
12. Zajistit bezpečnost testovacího prostředí a ochranu Poskytovatelem poskytnutých testovacích dat.
13. Zajistit, že do produkčního prostředí Poskytovatele bude dodán jen předmětem smlouvy specifikovaný kompilovaný, resp. spustitelný kód a další nezbytná data pro provozování předmětu plnění.
14. Zajistit, že v rámci poskytovaného plnění bude dodávaný software/služba
15. v souladu s bezpečnostními politikami a standardy Poskytovatele;
16. otestován na soulad s bezpečnostními politikami Poskytovatele (platí pro Dodavatele, pokud byl s takovými bezpečnostními politikami seznámen)
17. Zajistit řízení verzí zdrojového kódu.
18. Zajistit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí.
19. Nevyvíjet, nekompilovat a nešířit v prostředí Poskytovatele programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.
20. **Zvládání kybernetických bezpečnostních událostí a incidentů**
    1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 14 VoKB, které musí splnit Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
    2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména:
21. Stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání kybernetických bezpečnostních incidentů.
22. Bez zbytečného odkladu hlásit Poskytovateli všechny kybernetické bezpečnostní události a incidenty s potenciálním negativním dopadem na informační aktiva Poskytovatele, a to stanoveným komunikačním kanálem nebo prostřednictvím Kontaktní osoby.
23. Vyhodnocovat informace o kybernetických bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platných právních předpisů České republiky a Evropské unie.
24. V případě vzniku kybernetické bezpečnostní události či incidentu a jeho následného zvládání a vyhodnocování a/nebo v případě podezření na kybernetický bezpečnostní incident poskytnout Poskytovateli bezodkladnou aktivní součinnost a veškeré relevantní informace.
25. Bez zbytečného odkladu a po dohodě s Poskytovatelem realizovat bezpečnostní opatření požadovaná Poskytovatelem v dohodnutých termínech, ke snížení dopadu kybernetického bezpečnostního incidentu nebo zamezení jeho pokračování.
26. Spolupracovat při analýze příčin vzniku kybernetického bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že Dodavatel kybernetický bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.
    1. Dodavatel bere na vědomí, že postup zvládání kybernetického bezpečnostního incidentu či jiný důsledek porušení požadavků v oblasti kybernetické bezpečnosti, jehož příčina je na straně Dodavatele, nebude posuzován jako okolnost vylučující odpovědnost Dodavatele.
27. **Řízení kontinuity činností**
    1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 15 VoKB, které musí splnit Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
    2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména:
28. Zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění.
29. Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zajistit dle požadované úrovně služeb.
30. **Kontrola a audit**
    1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 8 a § 16 VoKB, které musí splnit Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
    2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění poskytnout adekvátní součinnost při výkonu kontroly Poskytovatele ze strany NÚKIB dle § 23 ZoKB.
31. **Fyzická bezpečnost**
    1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 17 VoKB, které musí splnit Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
    2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména:
32. Dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny aktiva systémů ICT nebo datové nosiče.
33. V rozsahu předmětu plnění zajistit fyzické zabezpečení, označení, uchování a likvidaci informačních aktiv Poskytovatele, instalačních, záložních nebo archivních médií a dokumentace v souladu s Přílohou č. 1 VoKB a klasifikací informačních aktiv Poskytovatele, pokud s ní byl Dodavatel seznámen.
34. **Bezpečnostní nástroje**
    1. Dodavatel se v rozsahu předmětu plnění aktivně podílí na splnění povinností uvedených v § 18 až § 27 VoKB, které musí splnit Poskytovatel, jakožto provozovatel a správce VIS a povinná osoba dle ZoKB.
    2. Krom jiného se Dodavatel v tomto kontextu zavazuje v rozsahu předmětu plnění na své straně zejména:
35. Realizovat opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity a bezpečnosti komunikační sítě.
36. Realizovat přístup z mobilního zařízení do prostředí Poskytovatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN), pokud mu takový přístup byl udělen.
37. Nepřipojovat do infrastruktury, která je součástí dodaného řešení technické prostředky potenciálně rizikových výrobců, které jsou předmětem varování NÚKIB.
38. Na technická aktiva, která jsou součástí dodaného řešení bez písemného souhlasu Poskytovatele neinstalovat a nepoužívat v prostředí dodaného řešení tyto typy nástrojů, pokud nejsou součástí předmětu plnění:
39. Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.
40. Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.
41. Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT.
42. Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí dodaného řešení.
43. Připojovat do prostředí dodaného řešení pouze technická aktiva, která jsou chráněna proti malware a jinému škodlivému softwaru a která jsou v souladu s interními bezpečnostními předpisy Poskytovatele nebo jím schválená.
44. Průběžně zaznamenávat a uchovávat data o provozu technických aktiv (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platných právních předpisů České republiky a Evrospké unie.
45. Na vyžádání poskytnout Poskytovateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění, a to po celou dobu trvání Servisní smlouvy.
46. Zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.
47. Pro on-line transakce realizované prostřednictvím webových technologií implementovat na aktuálně bezpečných kryptografických algoritmech založené TLS/SSL certifikáty, s cílem zajistit jejich důvěrnost, integritu a identitu komunikujících protistran.
48. Veškeré neveřejné informace poskytnuté Poskytovatelem chránit proti neautorizovanému přístupu aktuálně bezpečnými kryptografickými nástroji.

16.3 Dodavatel bere na vědomí, že v případě, kdy technické spojení ze strany Dodavatele narušuje chod služeb Poskytovatele, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud tato Serviní smlouva nestanoví jinak.

1. **Využití cloud computingu**

Dodavatelem se v kontextu využití claud computingu rozumí subjekt, který tuto službu (část dodaného řešení) přímo zajišťuje. Může jím být tedy jak samotný Dodavatel dle Servisní smlouvy, tak některý z jeho poddodavatelů (který tuto část řešení zajišťuje).

* 1. Obecné podmínky v případě využití cloud computingu:

1. Dodavatel zajistí, aby měl Poskytovatel k dispozici dostatek jasných a srozumitelných informací o provozu dané služby cloud computingu, o geografické lokaci zpracování zákaznických dat a rizicích souvisejících se zpracováním zákaznických dat v dané geografické lokaci.
2. Dodavatel zajistí, že zákaznická data a provozní údaje jsou dlouhodobě a nepřetržitě uložena výlučně na území členských států EU/EHP.
3. Dodavatel zajistí, že zákaznická data a provozní údaje jsou zpracovávána výlučně na území členských států EU/EHP.
4. Dodavatel je držitelem platné certifikace ČSN ISO/IEC 27001 nebo ISO/IEC 27001, od certifikačního orgánu, který byl akreditován pro provádění auditů a certifikaci systémů řízení bezpečnosti informací některým z členů IAF, a do jehož rozsahu certifikace náleží poskytovaná služba cloud computingu, provozovaná v souladu s postupy normy ČSN ISO/IEC 27017 nebo ISO/IEC 27017 a ČSN ISO/IEC 27018 nebo ISO/IEC 27018. V případě, že rozsah certifikace není uveden jednoznačně na certifikátu, Dodavatel předloží čestné prohlášení, ve kterém bude uvedeno, na které služby se certifikace vztahuje.
   1. Organizace bezpečnosti informací
5. Dodavatel musí mít zaveden systém řízení bezpečnosti informací (dále jen „ISMS“). Rozsah ISMS zahrnuje organizační jednotky Dodavatele, lokality a procesy k poskytování služby cloud computingu. Opatření jsou dokumentována pro řízení, implementaci, údržbu a neustálé zlepšování ISMS. Dokumentace obsahuje rozsah ISMS, prohlášení o aplikovatelnosti, ve kterém jsou doložena, jaká bezpečnostní opatření byla vybrána pro mitigaci bezpečnostních rizik a výsledky posledního interního či certifikačního auditu Dodavatele.
6. Dodavatel musí disponovat politikou bezpečnosti informací, kterou se řídí a kterou komunikuje interním a externím zaměstnancům a svým dodavatelům. Politika bezpečnosti informací popisuje význam bezpečnosti informací, bezpečnostní cíle, požadovanou bezpečnostní úroveň, nejvýznamnější aspekty bezpečnostní strategie k dosažení stanovených cílů a organizační strukturu Dodavatele v rozsahu ISMS.
7. Dodavatel zavede na základě vlastní politiky bezpečnosti informací přiměřená bezpečnostní opatření.
   1. Politiky
8. Politika bezpečnosti informací Dodavatele musí být v souladu s požadavky Poskytovatele na bezpečnost informací.
9. Politiky Dodavatele musí být v souladu s politikou bezpečnosti informací Dodavatele, dokumentovány v jednotné struktuře a vhodným způsobem sdíleny a komunikovány všem interním i externím zaměstnancům Dodavatele. Politiky musí být verzovány, kontrolovány a schvalovány vrcholovým vedením Dodavatele.
10. Politiky zahrnují alespoň následující oblasti:
11. Cíle.
12. Rozsah.
13. Bezpečnostní role a odpovědnosti, včetně kvalifikačních požadavků a pravidel zastupitelnosti.
14. Role a závislosti na jiných organizacích.
15. Postupy pro implementaci politik v rámci bezpečnostní strategie.
16. Platné právní a regulatorní požadavky.
    1. Fyzická bezpečnost
17. Dodavatel zajistí, že bezpečnostní požadavky na budovy a prostory vztahujících se k poskytování služeb cloud computingu jsou založeny na bezpečnostních cílech politiky bezpečnosti informací, identifikovaných bezpečnostních požadavcích a posouzení rizik fyzické a environmentální bezpečnosti. Dodavatel též zajistí, že tyto bezpečnostní požadavky jsou zdokumentovány, komunikovány a poskytovány ve formě bezpečnostních politik.
18. Dodavatel zajistí alespoň jedno záložní datové centrum, které je kapacitně dostatečné k převzetí služby poskytované z primárního datového centra.
19. Dodavatel zajistí, že primární i záložní datové centrum, ze kterého jsou poskytovány služby, jsou v dostatečné vzdálenosti od přírodních zdrojů rizik a zdrojů rizik vyvolaných činností člověka vedoucích k narušení nebo omezení poskytování služby cloud computingu nebo bezpečnosti informací, nebo je přijato adekvátní bezpečnostní opatření, nebo se primární a záložní datové centrum nacházejí ve vzájemné vzdálenosti nejméně 50 km, a jsou umístěna v lokalitách, které svým geografickým charakterem vylučují současné nebo následné škodlivé působení přírodních vlivů nebo jevů vyvolaných činností člověka vedoucích k poškození nebo zničení dat anebo vyžadujících provedení záchranných prací.
20. Dodavatel na vstupu do prostor a budov sloužících k poskytování služby cloud computingu kontroluje fyzický přístup, aby tak zabránil případnému neautorizovanému přístupu osob.
    1. Provoz
21. Dodavatel zajistí, že nebude zákaznický obsah zpracovávat jiným způsobem, než se dohodl dokumentovaným způsobem s Poskytovatelem.
22. Dodavatel vyhodnocuje informace a podklady týkající se zranitelností a hrozeb poskytované služby cloud computingu a přijímá relevantní opatření.
23. Dodavatel bezpečně a striktně odděluje zákaznická data, která jsou uložená a zpracovávaná na sdílených virtuálních a fyzických strojích tak, aby byla zajištěna důvěrnost a integrita těchto dat.
    1. Správa identit a řízení přístupu
24. Dodavatel umožní využívat pro přístup do správy služby cloud computingu vícefaktorovou autentizaci.
25. Dodavatel umožňuje řídit přístupy uživatelů do služby cloud computingu zejména ve smyslu:
26. Přiřazovat jedinečná uživatelská jména.
27. Udělovat a upravovat uživatelské účty a přístupová oprávnění na základě zásady nejnižšího oprávnění a pravidla need-to-know.
28. Pravidelně kontrolovat přidělení uživatelských účtů a přístupových oprávnění, alespoň jednou za 90 dní.
29. Blokovat a odebírat přístupové účty v případě nečinnosti.
30. Odebírat nebo měnit přístupová oprávnění při ukončení nebo změně smluvního vztahu.
31. Dodavatel v rámci své organizace řídí přístupy k informačnímu systému využívaného k poskytování služeb cloud computingu Poskytovateli.
    1. Správa klíčů a šifrování
32. Dodavatel má zavedené a zdokumentované politiky týkající se technických a organizačních opatření pro kryptografické procedury a správu kryptografických klíčů, ve kterých jsou popsány alespoň tyto činnosti a oblasti:
33. Používání aktuálně odolných kryptografických postupů a bezpečných síťových protokolů zohledňujících nejnovější poznatky a postupy v dané oblasti.
34. Šifrování, které je na základě risk-based analýzy přizpůsobeno povaze dat, komunikačním kanálům, typu, síle a kvalitě šifrování.
35. Požadavků na zabezpečení generování, uchovávání, vyzvednutí, distribuci, stažení a výmaz šifrovacích klíčů.
36. Zvážení relevantních právních a regulatorních závazků a požadavků.
37. Dodavatel má zavedeny procesy a technická opatření s aktuálně odolnými kryptografickými nástroji a autentizací pro přenos zákaznických dat po sítích mimo kontrolu Dodavatele.
38. Dodavatel má zavedeny procesy a technická opatření pro šifrování zákaznických dat a uživatelů během uchovávání.
39. Postupy a technická opatření pro bezpečné řízení klíčů a certifikátů v oblasti odpovědnosti Dodavatele zahrnují zejména:
40. Generování klíčů pro různé kryptografické systémy a aplikace.
41. Vydávání a získávání certifikátů veřejného klíče.
42. Poskytování a aktivace klíčů.
43. Bezpečné ukládání klíčů (oddělení systému správy klíčů od úrovně aplikací a middlewaru) včetně popisu toho, jak oprávnění uživatelé získávají přístup.
44. Změna nebo aktualizace kryptografických klíčů včetně politik definujících, za jakých podmínek a jakým způsobem mají být změny nebo aktualizace provedeny.
45. Zacházení s klíči podezřelými z kompromitace.
46. Zneplatnění a vymazání klíčů.
47. Jsou-li použity předem sdílené klíče, specifická ustanovení týkající se bezpečného použití tohoto postupu jsou specifikována samostatně.
    1. Zabezpečení komunikace
48. Dodavatel má zavedeny technické záruky, které jsou vhodné k rychlému odhalení a reakci na síťové útoky na základě nepravidelných vzorců příchozího nebo odchozího provozu a/nebo distribuované útoky typu Denial-of-Service (DDoS).
49. Data Poskytovatele, přenášená do služby cloud computingu jsou chráněna proti neoprávněnému zásahu, kopírování, úpravě, přesměrování nebo vymazání v souladu s jeho požadavky na zajištění bezpečnosti informací.
50. Dodavatel chrání data Poskytovatele přenášená ze služby cloud computingu proti neoprávněnému zásahu, kopírování, úpravě, přesměrování nebo vymazání v souladu se svou politikou bezpečnosti informací.
    1. Přenositelnost, propojení a exit strategie
51. Dodavatel vydá při ukončení využívání služby cloud computingu zákaznická data a provozní údaje, které souvisí s provozem služby cloud computingu Poskytovateli, nebo je zpřístupní přes definovaná rozhraní (formát a rozsah dat odpovídají smluvním dohodám, které byly uzavřeny před používáním služby cloud computingu).
52. Dodavatel má povinnost uhradit Poskytovateli náklady spojené s přenosem dat od Dodavatele do systému určeného Poskytovatelem v případě, že je aktivování exit strategie způsobeno hrubým porušením smluvního vztahu, které nebylo způsobeno Poskytovatelem.
53. Dodavatel zajistí při ukončení využívání služby cloud computingu bezpečnou likvidaci informačních aktiv Poskytovatele (zákaznická data a provozní údaje) po bezprostředně po jejich vydání Poskytovateli, a to v souladu se smluvními ujednáními a relevantními právními a regulatorními požadavky.
    1. Nákup, vývoj a úprava informačních systémů
54. Dodavatel má zaveden proces řízení změn.
55. Produkční prostředí Dodavatele je fyzicky nebo logicky odděleno od testovacích nebo vývojových prostředí, aby se zabránilo neautorizovanému přístupu k zákaznickým datům, šíření malwaru nebo změnám technických aktiv.
56. Data obsažena v produkčních prostředích se nepoužívají v testovacích nebo vývojových prostředích, aby nedošlo k ohrožení jejich důvěrnosti.
    1. Řízení dodavatelů
57. Dodavatel informuje o svých systematických zpracovatelích, a to jak před uzavřením smlouvy, tak vždy s dostatečným předstihem, než dojde k jejich změně.
58. V případě nesouhlasu Poskytovatele se změnou systematického zpracovatele, Dodavatel tuto změnu neprovede.
    1. Správa kybernetických bezpečnostních událostí a incidentů
59. Dodavatel bez zbytečného odkladu informuje Poskytovatele stanoveným způsobem o každém kybernetickém bezpečnostním incidentu, který se týká zákaznických dat Poskytovatele a souvisejících provozních údajů.
60. Dodavatel má zaveden a využívá nástroj na sledování a vyhodnocování kybernetických bezpečnostních událostí.
    1. Řízení kontinuity činností

Dodavatel zajistí, že v jeho pohotovostních plánech je zahrnut případ neočekávaného omezení přístupu k datům Poskytovatele.