# Příloha č. 4 - Bezpečnostní požadavky

## Kybernetická bezpečnost

* 1. Objednatel je určen jako subjekt kritické (informační) infrastruktury podle § 2 písm. k)  
     zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (dále jen „**krizový zákon**“) ve spojení s § 2 písm. b) zákona č. 181/ 2014 Sb., o kybernetické bezpečnosti (dále jen „**zákon o kybernetické bezpečnosti**“),
  2. PLC úroveň je vedena jako informační systém kritické informační infrastruktury ve smyslu zákona o kybernetické bezpečnosti,
  3. Dodavatel bude veden jako významný dodavatel Objednatele ve vztahu ke shora uvedenému informačnímu systému kritické informační infrastruktury a významným způsobem se bude podílet na zabezpečení jeho provozu,
  4. Dodavatel je povinen plnit veškeré povinnosti uložené provozovateli informačního systému kritické informační infrastruktury zákonem o kybernetické bezpečnosti a příslušné vyhlášky.

## Personální bezpečnost

* 1. Dodavatel je povinen informovat Objednatele o odchodech svých zaměstnanců, pro které byly u Objednatele vytvořeny přístupové účty minimálně v předstihu 5 pracovních dní.
  2. Dodavatel poskytne Objednateli úplný jmenný seznam svých zaměstnanců, popř. externích zaměstnanců Dodavatele, kteří se budou přímo podílet na zajištění předmětu SLA. Dodavatel se zavazuje informovat Objednatele o změnách v personálním zabezpečení SLA v předstihu minimálně 5 pracovních dní. Tento bod je splněn uvedením seznamu pracovníků do přílohy č. 6 SLA – Realizační tým.
  3. Pracovníci Dodavatele, kteří se přímo podílí na plnění předmětu SLA:
     1. musí být seznámeni s bezpečnostními požadavky SLA,
     2. mají dostatečné znalosti a praktické zkušenosti pro plnění přidělených úkolů,
     3. mají veškeré potřebné zkoušky a atestace, které vyplývají ze zákona nebo požadavků regulátora na druh práce, kterou mají v prostředí Objednatele vykonávat,
     4. jsou Dodavatelem pravidelně školeni v oblastech (informační) bezpečnosti a právních a regulatorních požadavků relevantních pro naplnění předmětu SLA.
  4. Personál Dodavatele není oprávněn do prostředí Objednatele přinést zbraně, výbušniny, hořlaviny, bojové prostředky, jedy, radioaktivní a toxické látky, popř. jakékoli jiné látky ohrožující lidský život a/ nebo zdraví.
  5. Personál Dodavatele není oprávněn vstupovat do prostor Objednatele a/ nebo přistupovat k informačním aktivům Objednatele pod vlivem návykových, omamných či psychotropních látek.

## Fyzická bezpečnost

* 1. Přístup zaměstnanců Dodavatele do prostor Objednatele je povolen, pouze pokud je jejich přítomnost nezbytná pro plnění pracovních povinností a na dobu nezbytně nutnou pro plnění pracovních povinností vyplývajících z  SLA.
  2. Zaměstnanci Dodavatele se v prostorách Objednatele vždy pohybuje v doprovodu odpovědného zaměstnance Objednatele.
  3. Volný pohyb zaměstnanců Dodavatele v prostorách Objednatele je povolen pouze v případě, že dané osobě byla vystavena osobní přístupová karta. Zaměstnanec Dodavatele není oprávněn přístupovou kartu dále zapůjčit třetím osobám a/ nebo umožnit přístup třetích osob do prostor Objednatele.
  4. Přístup zaměstnanců Dodavatele do prostor Objednatele se zvýšeným stupněm bezpečnosti – chráněných zón (jako jsou serverové místnosti, datové místnosti, technické místnosti, trezor, pokladna apod.) je povolen pouze v doprovodu oprávněného zaměstnance Objednatele. Doprovod je nezbytný po celou dobu fyzické přítomnosti zaměstnanců Dodavatele v těchto prostorách.
  5. V případě ztráty přístupové karty nebo v případě podezření ze ztráty přístupové karty je Dodavatel povinen bezodkladně zajistit blokaci přístupové karty.
  6. Bez předchozího písemného souhlasu Objednatele není Dodavatel oprávněn z prostor Objednatele odnést žádné paměťové médium (CD/DVD/Blu-ray disk, flash disk/ paměťové karty, hard disk, zálohovací pásky apod.) Objednatele, pořizovat jeho kopie, nebo je připojovat k zařízením, které nejsou ve správě a majetku Objednatele.
  7. Před vrácením zapůjčených paměťových médií Dodavateli musí být veškerá data Objednatele vymazána způsobem, který znemožňuje jejich opětovné obnovení. O tomto je sepsán protokol.

## Identifikace a autentizace

* 1. Zaměstnancům Dodavatele jsou přiděleny pouze účty, které nezbytně potřebuje pro plnění pracovních povinností vyplývajících z této SLA.
  2. Účtům Dodavatele jsou přidělena pouze oprávnění nezbytná k plnění pracovních povinností dle této SLA.
  3. Dodavatel pracuje v prostředí Objednatele pouze s účty umožňující jednoznačnou identifikaci uživatele. Objednatel se zavazuje vytvořit účty v produkčních i testovacích systémech pro všechny uvedené pracovníky v příloze č. 10 přílohy č. 8 SLA (SLA) – Realizační tým ve všech podporovaných aplikacích, uvedených v příloze č. 7 přílohy č. 8 SLA (SLA) – Katalog aplikací a v produkčním a testovacím systému.
  4. Neaktivní účty Dodavatele v prostředí Objednatele jsou proaktivně Dodavatelem reportovány.

## Nakládání s certifikáty

* 1. Přístup k certifikátům (logický i fyzický) bude umožněn pouze těm zaměstnancům Dodavatele, u kterých je tento přístup nezbytný pro plnění jejich pracovních povinností.
  2. Certifikáty nebudou poskytnuty/ zpřístupněny třetím stranám bez písemného souhlasu Objednatele.
  3. Certifikáty budou po instalaci uloženy pouze v bezpečném úložišti na produkčních serverech, na kterých je jejich uložení nezbytné pro zajištění poskytované Služby, a veškeré další kopie budou odstraněny/ zničeny způsobem, který znemožňuje jejich opětovnou obnovu.
  4. Pakliže je to možné, Dodavatel nastaví privátní klíč jako neexportovatelný z bezpečného úložiště certifikátů.
  5. Certifikát musí být vždy chráněn silným heslem a nesmí být uložen v nešifrované podobě.
  6. Dodavatel se zavazuje neprodleně informovat Objednatele o ztrátě a/ nebo podezření ze ztráty důvěrnosti privátního klíče.
  7. Dodavatel se zavazuje zničit veškeré záložní kopie předaných certifikátů způsobem, který znemožňuje jejich opětovnou obnovu.
  8. Přístup k záložním kopiím (logický i fyzický), na kterých je kopie certifikátu uložena, bude umožněn pouze těm zaměstnanců dodavatele, u kterých je tento přístup nezbytný pro plnění pracovních povinností.
  9. Šifrovací hesla k předaným certifikátům budou bezpečně uložena a přístup k nim bude poskytnut pouze těm zaměstnanců Dodavatele, u kterých je tento přístup nezbytný pro plnění pracovních povinností.

## Požadavky na kvalitu hesel

* 1. Personál Dodavatele je povinen vytvářet hesla k osobním účtům v souladu s následujícími pravidly za předpokladu, že Objednatel zajistí technickou způsobilost podporovaných aplikací k uplatnění požadovaných pravidel:
     1. minimální délka hesla je 12 znaků,
     2. minimální platnost hesla je 5 dnů,
     3. pokud není řečeno jinak, heslo musí být pravidelně měněno každých 90 dnů,
     4. heslo nesmí být zadáváno, pokud existuje riziko odpozorování hesla při zadávání jinou osobou,
     5. Heslo musí splňovat požadavky na komplexitu.
  2. Hesla k účtům, kterým jsou v prostředí Objednatele přidělena administrátorská oprávnění, musí být vytvořena v souladu s následujícími pravidly:
     1. minimální délka hesla je 17 znaků,
     2. minimální platnost hesla je 5 dnů,
     3. pokud není řečeno jinak, heslo musí být pravidelně měněno každých 90 dnů,
     4. Heslo musí splňovat požadavky na komplexitu.
  3. Hesla k technickým nebo servisním účtům musí být vytvořena v souladu s následujícími pravidly:
     1. minimální délka hesla je 30 znaků,
     2. minimální platnost hesla je 5 dnů,
     3. k vytvoření hesla musí být použit pseudo-náhodný generátor hesel,
     4. pokud není řečeno jinak, heslo musí být pravidelně měněno každých 365 dnů.
  4. Veškerá hesla vytvořena Dodavatelem v prostředí Objednatele musí dále splňovat následující požadavky:
     1. heslo musí obsahovat kombinaci velkých a malých písmen, číslic a speciálních znaků,
     2. heslo nesmí být jednoduše uhodnutelné, nesmí obsahovat žádnou část jména, přihlašovacího jména, jména společností Dodavatele a Objednatele apod. a musí být tvořeno tak, aby znemožňovalo úspěšné uhodnutí pomocí slovníkového útoku,
     3. heslo nesmí obsahovat datum ani žádnou jeho část (rok, měsíc, den) a to ani v psaném ani číselném vyjádření,
     4. každé nově zadané heslo musí být vždy odlišné od všech dříve použitých hesel,
     5. hesla nesmí být uživatelem uložena s možností nešifrovaného přístupu
     6. heslo nesmí být uloženo v místě, kde by mohlo být úmyslně či neúmyslně zjištěno jinou osobou,
     7. heslo nesmí být sdíleno s další osobou, pokud k tomuto nebyl v předstihu vydán písemný souhlas Objednatele.
  5. Pokud je prvotní heslo k účtu vytvořeno zaměstnanci Objednatele, je Dodavatel po získání prvotního hesla povinen heslo neprodleně změnit.
  6. Předávání prvotního hesla probíhá vždy způsobem, který vylučuje vyzrazení hesla dalším osobám.
  7. V případě vyzrazení hesla nebo v případě podezření z vyzrazení hesla musí Dodavatel bezodkladně zajistit změnu/ blokaci hesla.

## Nakládání s informačními aktivy Objednatele

* 1. Přístup k informačním aktivům Objednatele je přidělen pouze zaměstnancům Dodavatele, kteří tento přístup potřebují pro plnění pracovních povinností vyplývajících z této SLA.
  2. Dodavatel nesmí zpracovávat nebo ukládat následující typy informačních aktiv mimo prostředí Objednatele a/ nebo informační systémy Objednatele:
     1. informace ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů,
     2. současné i historické informace o klientech Objednatele, jejich majetku, finančních transakcích, využívaných produktech a/ nebo jejich smluvních vztazích,
     3. současné i historické účetní záznamy Objednatele a smluvní dokumentaci Objednatele.
  3. Po ukončení prací vyplývajících z této SLA a/ nebo v případě zrušení/ vypovězení této SLA se Dodavatel bez zbytečného prodlení zavazuje vrátit a/ nebo odstranit veškerá informační aktiva Objednatele uložená v prostředí Dodavatele související s plněním předmětu této SLA, pakliže držení těchto informací není vyžadováno zákony České republiky. Toto se týká elektronické i papírové dokumentace. Odstranění dat musí být provedeno způsobem, který znemožňuje jejich opětovné obnovení.

## Bezpečnostní požadavky na Dodavatele

* 1. Bez předchozího písemného souhlasu Objednatele nesmí Dodavatel poskytnout žádným třetím stranám přístup k informačním aktivům Objednatele, včetně externím zaměstnancům Dodavatele, dodavatelům Dodavatele, mateřským či sesterským společnostem Dodavatele, Dodavatelům outsourcingu, Dodavatelů cloudových služeb a/ nebo cloudových úložišť.
  2. Dodavatel je povinen zajistit adekvátní zabezpečení výpočetní techniky, na které jsou uloženy, zpracovávány a/ nebo přes které jsou přenášeny informační aktiva Objednatele. Vhledem k informačním aktivům Objednatele je Dodavatel povinen zajistit splnění minimálně následujících požadavků:
     1. v prostředí Dodavatele jsou používány nástroje pro detekci a odstranění škodlivého kódu s nastavením pravidelné aktualizace databáze signatur škodlivého kódu s frekvencí nepřesahující jeden týden. Tento software je centrálně spravován a jsou nastaveny odpovídající procesy dohledu, logování a reakci na pozitivní nález škodlivého kódu v prostředí Dodavatele,
     2. v prostředí Dodavatele jsou definovány, nastaveny, vykonávány a centrálně monitorovány procesy aktualizace bezpečnostních záplat softwarových komponent (minimálně však operačního systému, nástrojů kancelářského softwaru, webových prohlížečů a jejich doplňků – JAVA, Adobe Flash Player, Adobe Reader a doplňky sady Microsoft Office) v intervalu nepřesahující jeden měsíc od vydání záplat,
     3. vnitřní prostředí Dodavatele je od internetu odděleno Firewallem, který je připojen k centrálnímu dohledu. Zaměstnanci Dodavatele při vzdáleném přístupu do vnitřního prostředí Dodavatele využívají šifrované připojení zamezující neautorizovaný odposlech a změnu přenášené komunikace.
  3. Jsou-li informační aktiva Objednatele přenášena Dodavatelem mimo prostory Objednatele, je Dodavatel povinen důsledně dbát na fyzickou bezpečnost těchto aktiv a mít tato informační aktiva stále pod dohledem. Dodavatel není výslovně oprávněn:
     1. ponechat informační aktiva Objednatele na veřejných místech bez dozoru,
     2. ponechat informační aktiva Objednatele bez dozoru v zaparkovaném vozidle,
     3. ponechat informační aktiva Objednatele bez dozoru v hotelovém pokoji. Informační aktivum musí být uloženo v hotelovém trezoru a/ nebo jinak uzamčeno a adekvátně chráněno proti odcizení,
     4. při přepravě letadlem, ponechat informační aktiva Objednatele v zapsaných zavazadlech uskladněných v přepravním prostoru letadel. Pokud to bezpečnostní pravidla leteckých přepravců nevylučují, musí být informační aktiva Objednatele přepravována na palubě letadel.
  4. Dodavatel je povinen dodržovat bezpečnostní a provozní pokyny výrobce hardwaru, na kterém jsou informační aktiva Objednatele uložena/ zpracovávána.
  5. Hesla Objednatele uložená v prostředí Dodavatele, musí být uložena na úložišti, ke kterému je přístup šifrován. Hesla musí být dále chráněna před neautorizovaným přístupem těch zaměstnanců Dodavatele, kteří tento přístup bezpodmínečně nepotřebují k plnění pracovních povinností vyplývajících z této SLA.
  6. Dodavatel používá pouze řádně licencovaný software a pouze v souladu s licenčními ujednáními jednotlivých dodavatelů licence.

## Práce v prostředí Objednatele

* 1. Dodavatele je oprávněn (vzdáleně) přistupovat pouze k informačním aktivům Objednatele, které nezbytně potřebuje k plnění pracovních povinností vyplývajících z této SLA.
  2. Dodavatele je oprávněn (vzdáleně) přistupovat pouze prostřednictvím VPN a schválených nástrojů, a to jak na servery, tak klientské stanice, a to hlavně s ohledem na bezpečnost a ochranu osobních údajů GDPR.
  3. Do prostředí Objednatele je oprávněn vzdáleně přistupovat pouze k tomuto účelu autorizovaný personál Dodavatele.
  4. Bez předchozího písemného souhlasu Objednatele, není Dodavatel v prostředí Objednatele oprávněn instalovat a/ nebo spouštět žádný, Objednatelem předem neschválený software.
  5. Bez písemného souhlasu Objednatele není Dodavatel oprávněn v prostředí Objednatele provádět jakékoliv testování fyzické nebo logické bezpečnosti a/ nebo kontrolních mechanismů jakéhokoliv typu.
  6. V prostředí Objednatele jsou používány nástroje pro zaznamenání činností administrátorů a činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému, všechny činnosti provedené Dodavatelem v prostředí Objednatele budou zaznamenány ve formě, logů, metadat či nahrávek.
  7. Dodavatel v prostředí Objednatele není oprávněn:
     1. mazat auditní záznamy,
     2. přistupovat, měnit nebo jinak neoprávněně manipulovat s auditními záznamy,
     3. generovat auditní záznamy s cílem ztížit orientaci v auditní stopě,
     4. generovat auditní záznamy s cílem zajistit vymazání jiného auditního záznamu (např. rotace auditních záznamů z důvodu omezení velikosti úložiště auditní stopy) apod.
  8. Zaměstnanci Dodavatele v prostředí Objednatele nemají oprávnění stahovat nelegální obsah (obsah, pro jehož použití nemají souhlas majitele licence), nesmí navštěvovat stránky, jejichž obsah přímo nesouvisí s plněním pracovních povinností vyplývajících z této SLA.
  9. V prostředí Objednatele pak zaměstnanci Dodavatele výslovně nesmí stahovat obsah nebo navštěvovat stránky:
     1. se sexuální tématikou/ porno stránky,
     2. narušující výchovu mládeže či nabádající k chování, které je v rozporu se společensky přijatelnými normami chování,
     3. propagující diskriminaci jednotlivce či skupiny,
     4. propagující či zobrazující násilí, ať už vůči jednotlivci, skupině, celému národu či demokratickému společenskému zřízení,
     5. propagující terorismus a teroristické organizace a/nebo genocidu národa,
     6. propagující či zobrazující násilí na zvířatech,
     7. navádí ke spáchání trestného činu,
     8. jenž hrubě zasahuje do práv jednotlivce a zobrazuje jej dehonestujícím způsobem apod.
  10. Pracovníci Dodavatele v prostředí Objednatele nesmí provádět jakékoliv aktivity poškozující jiné fyzické nebo právnické osoby, včetně rozesílání nevyžádaných emailů (SPAMu), rozesílání podvodných emailů (PHISHING), distribuci škodlivého kódu nebo podílení se na útocích s cílem vyřadit dostupnost služeb (DoS, resp. DDoS).
  11. Na poskytnutém pracovním místě v prostorách Objednatele je Dodavatel povinen zajistit:
      1. čistotu a pořádek tak, aby pracovní místo mohlo být bezpečně využito po čas fyzické nepřítomnosti zaměstnanců Dodavatele,
      2. adekvátní fyzickou bezpečnost veškerých paměťových médií a tištěných dokumentů po čas fyzické nepřítomnosti zaměstnanců Dodavatele,
      3. logické uzamčení přístupu k informačním aktivům (datům, informačním službám, aplikacím) Objednatele po čas fyzické nepřítomnosti zaměstnanců Dodavatele tak, aby nemohlo dojít k neautorizovanému přístupu k těmto aktivům – např. uzamčení obrazovky počítače, odhlášení uživatele operačního systému, ukončení vzdálených relací a připojení apod.
  12. Zaměstnanci Dodavatele nejsou bez předchozího písemného souhlasu Objednatele oprávněni v prostředí Objednatele instalovat zařízení umožňující vzdálený odposlech a/ nebo pořizovat jakýkoliv audio záznam a/ nebo video záznam.

## Vývoj a testování programového kódu

* 1. Před započetím vývojových prací je Dodavatel povinen seznámit se se softwarovými a hardwarovými technologiemi, které jsou v prostředí Objednatele podporované a používané.  
     Dále je Dodavatel povinen si nechat odsouhlasit požadované zdroje (HW, SW atd.) a design/architekturu a z toho vyplívající případné další požadavky.
  2. Před započetím vývojových prací je Dodavatel povinen seznámit se s bezpečnostními a auditními požadavky Objednatele na vyvíjený software.
  3. Dodavatel je povinen přistupovat k bezpečnosti informací jako k integrální součásti celého vývojového cyklu vývoje softwaru. Požadavky na informační bezpečnost musí být součástí analýzy požadavků na vyvíjený software, fáze plánování a návrhu vyvíjeného softwaru, a to ve vztahu k zamýšlenému nasazení a integraci do existujících procesů Objednatele.
  4. Pro veškeré změny provedené Dodavatelem v produkčním prostředí Objednatele existuje schválený HelpDeskový požadavek Objednatele.
  5. Pokud není řečeno jinak, součástí vývojových prací je i dodání úplné dokumentace, včetně:
     1. dokumentace architektury/ designu – Zahrnuje vztahy k prostředí a stavebním základům, které budou použity v návrhu softwarových komponent,
     2. technická dokumentace – Dokumentace kódu, sestavené dodavatelem popis rozhraní a API,
     3. uživatelská dokumentace – Manuály pro koncového uživatele, systémové administrátory a osazenstvo podpory,
     4. Příručka pro administraci, instalaci a údržbu.
  6. Dodavatel musí Objednatele proaktivně upozornit na všechny jemu známé skutečnosti spojené s vývojem a chováním dodaného kódu, které by po nasazení mohli negativně ovlivnit běh v produkčním prostředí a/ nebo návazné systémy.
  7. Dodavatel odpovídá za životní cyklus ve smyslu, že se včas dozvíme, že z testu je produkce, že něco již nežije a není třeba apod.

## Audit

* 1. Objednatel si vyhrazuje právo auditu, jehož cílem je ověřit soulad plnění bezpečnostních požadavků Objednatele.

## Krizové řízení

* 1. Personál Dodavatele je povinen maximálně předcházet vzniku krizových situací (např. požáru) a situacím, při kterých by mohlo dojít ke zranění osob nebo poškození majetku Objednatele.
  2. V případě vzniku krizové nebo mimořádné situace (např. požár, výbuch, povodeň apod.) je personál Dodavatele, který je fyzicky přítomen v místě události, povinen bez výjimky a odkladu dodržovat předpisy a direktivy platné v dané lokalitě a uposlechnout pokynů k evakuaci a ochraně osob. Toto platí i pro případ cvičení.
  3. V případě krizového řízení je personál Dodavatele povinen bezodkladně uposlechnout pokynů krizového manažera Objednatele, vedoucí k ochraně informačních aktiv dodávaných v souladu s touto Smlouvou.

## Hlášení požadavků a bezpečnostních incidentů

* 1. Veškeré požadavky Dodavatele na součinnost Objednatele související s přístupem, nákupem, provozem, bezpečnostním nastavením, konfiguračními změnami informačními systémů a/ nebo IT infrastruktury Objednatele, jsou evidovány v nástroji HelpDesk Objednatele.
  2. Dodavatel je povinen informovat Objednatele i v případě (podezření ze) ztráty svěřeného informačního aktiva (např. přístupové karty, hesla, certifikátu apod.) a/ nebo (podezření z) narušení bezpečnosti prostředí Objednatele.