**Bezpečnostní požadavky v oblasti kybernetické bezpečnosti**

Nemocnice Hodonín (dále jen „Objednatel“) od svých Poskytovatelů (dále jen „Poskytovatel“) vyžaduje dodržování těchto Bezpečnostních požadavků v oblasti kybernetické bezpečnosti

Poskytovatel bere na vědomí, že Objednatel je provozovatelem základní služby s informačním systémem základní služby v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů.

Provozovatel bere na vědomí, že je pro Objednatele v pozici významného Poskytovatele podle §2 odst. n) vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti a musí při plnění smluvního vztahu (dále jen „Předmět plnění“) pro Objednatele dodržovat níže uvedené bezpečnostní požadavky.

1. OBECNÁ PRAVIDLA

1.1. Předmět plnění nesmí být zatížen žádnými faktickými ani právními vadami a musí odpovídat všem technickým požadavkům, technickým a bezpečnostním normám pro daný druh Předmětu plnění, a to jak normám závazným, tak i doporučujícím.

1.2. Zaměstnanci Poskytovatele mohou přistupovat k informačním a komunikačním prostředkům (ICT prostředky) Objednatele výhradně prostřednictvím autentizačních údajů přidělených Objednatelem (např. VPN přístup).

1.3. Poskytovatel se zavazuje dodržovat bezpečnostní opatření a pravidla Objednatele při práci s informacemi a ICT prostředky Objednatele.

1.4. Poskytovatel se zavazuje nakládat s veškerými daty, informacemi a údaji, ke kterým se dostane v rámci Předmětu plnění takovým způsobem, aby nemohlo dojít k jejich ztrátě, vyzrazení, neoprávněné či neodborné manipulaci. Dále se zavazuje používat tato data pouze k danému účelu a neumožnit jejich zpřístupnění nepovolané osobě.

1.5. Poskytovatel se zavazuje dodržovat veškerou platnou legislativu, zejména pak tu v oblasti kybernetické bezpečnosti a ochrany osobních údajů.

2. BEZPEČNOST KOMUNIKACE

2.1. V případě ztráty nebo odcizení hardware, software, dat, informací Objednatele musí Poskytovatel vždy neprodleně nahlásit tuto skutečnost oddělení IT Objednatele, a to i v případě pouhého podezření neoprávněný přístup a manipulaci s daty.

2.2. Při práci na zařízení (například: počítači, notebooku, mobilním telefonu, zdravotnickém prostředku) připojeném do sítě a/nebo k informačním systémům Objednatele musí Poskytovatel dodržovat tyto zásady:

2.2.1. umožnit přístup jen proškolenému zaměstnanci Poskytovatele,

2.2.2. chránit výpočetní techniku a všechna data Objednatele před porušením důvěrnosti, integrity či dostupnosti,

2.2.3. po ukončení práce v síti a/nebo v informačním systému Objednatele provést neprodleně odhlášení uživatele.

2.3. Při práci na serverech Objednatele musí být splněny následující zásady, které se vztahující i na servisní (provozní) smlouvy (s ohledem na specifikace informačních systémů):

2.3.1. server svěřený Poskytovateli do správy musí Poskytovatel pravidelně udržovat a kontrolovat zejména z pohledu bezpečnosti, dostupnosti a integrity dat,

2.3.2. Poskytovatel nesmí měnit jakákoliv oprávnění na serveru nebo informačním a komunikačním systému bez souhlasu oddělení IT,

2.3.3. Poskytovatel nesmí měnit nastavení operačního systému serverů a jeho komponent bez souhlasu oddělení IT,

2.3.4. Poskytovatel musí zajistit bezpečnostní aktualizaci operačního systému a aplikačních částí serverů; bezpečnostní aktualizace kritického charakteru, které mohou ohrozit bezpečnost sítě Objednatele musí aplikovat neprodleně po jejich vydání.

2.4. Při práci v interní sítí Objednatele odpovídají zaměstnanci Poskytovatele, kteří mají přidělen přístup do interní sítě Objednatele, za své činnosti prováděné v rámci této sítě. Zaměstnanci Poskytovatele nesmí, zejména:

2.4.1. zneužívat síťové prostředky pro osobní účely a zatěžovat kapacitu sítě,

2.4.2. šířit či jinak nakládat se škodlivým malwarem,

2.4.3. využívat nástroje sloužící k maskování identity,

2.4.4. provádět bezdůvodné skenování portů či jiných parametrů sítě a síťových zařízení,

2.4.5. provádět jakoukoliv formou monitorování sítě, které může vést k zachycení dat, pokud není Předmětem plnění Smlouvy,

2.4.6. obcházet autentizaci uživatele nebo obcházet zabezpečení jakéhokoliv počítače, sítě nebo uživatelského účtu,

2.4.7. provádět jakékoliv nepracovní aktivity vedoucí k omezování nebo odepírání služeb jiným uživatelům,

2.4.8. užívat jakékoliv programy, skripty nebo příkazy, nebo zasílat zprávy v jakékoliv formě s úmyslem omezit nebo znemožnit poskytování služeb nebo terminálových relací lokálně nebo přes síť, internet nebo intranet,

2.4.9. využívat bezpečnostních mezer nebo vytvářet útoky na komunikaci v počítačových sítích (např. přístup k datům, jichž není zaměstnanec zamýšleným příjemce, přihlašování na server nebo účet zaměstnancem, který není k tomuto přístupu výslovně oprávněn, s výjimkou případů, kdy tyto aktivity jsou součástí řádných pracovních úkolů),

2.4.10. předávat informace o konfiguraci a topologii sítě cizím osobám; tyto informace je oprávněn předat pouze odpovědný zaměstnanec Objednatele, pokud jsou takové informace nutné z hlediska přípravy či Předmětu plnění.

3. KYBERNETICKÉ BEZPEČNOSTNÍ UDÁLOSTI A INCIDENTY

3.1. Poskytovatel musí vyvinout maximální úsilí pro odvracení bezpečnostních hrozeb a kybernetických útoků pro informační a komunikační systémy Objednatele.

3.2. Poskytovatel musí zajistit maximální součinnost při analýze kybernetických bezpečnostních událostí a incidentů Objednatele a následně zavádět vhodná nápravná opatření určené Objednatelem.

3.3. V případě podezření či potvrzení vzniku bezpečnostní hrozby pro informační a komunikační systém Objednatele je Poskytovatel povinen neprodleně písemně (e-mailem) či telefonicky (a následně také písemně) informovat o této skutečnosti vedoucího oddělení IT Objednatele.

4. POŽADAVKY NA DODÁVENÉ INFORAMČNÝ SYSTÉMY

4.1. Informační systém musí být vytvářen tak, aby dostatečně chránil data před porušením důvěrnosti, dostupnosti a integrity.

4.2. Informační systém musí být vytvořen tak, aby byla každá operace uložena v provozním záznamu (logu) s jedinečným identifikátorem uživatele, který tuto operaci vykonal. Musí být zajištěno, aby nemohlo dojít k provádění operací pod cizím identifikátorem uživatele.

4.3. Uživatel informačního systému musí být nucen si heslo pravidelně měnit.

4.4. Informační systém musí být vytvořen tak, aby byl počet neúspěšných pokusů o přihlášení omezen. Po deseti neúspěšných pokusech o přihlášení musí být další zadávání dočasně zablokováno nebo spojení rozpojeno.

4.5. V případě, že je povolen přístup do informačního systému, v němž určuje vstupní heslo administrátor, je povinností autora informačního systému vynutit si změnu tohoto inicializačního hesla.

4.6. Poskytovatel nesmí používat jedno přihlašovací jméno pro několik svých zaměstnanců, každý účet musí být jmenný.

4.7. V informačních systémech musí být pořizovány auditní záznamy obsahující alespoň:

4.7.1. identifikaci uživatele;

4.7.2. datum a čas přihlášení a odhlášení;

4.7.3. identifikaci místa, odkud se uživatel přihlašoval (pokud je to možné);

4.7.4. záznamy o přístupu (úspěšném i neúspěšném), případně o prováděných operacích.

4.8. Před umožněním přístupu musí být každý uživatel identifikován a autentizován.

4.9. Informační systém by měl po určité době nečinnosti uživatele (doporučeno 15 minut) tohoto uživatele odhlásit.

4.10. Po určitém množství neúspěšných autentizačních pokusů (doporučeno 10) se musí ukončit přihlašovací proces.

4.11. V případě neúspěšné autentizace nesmí informační systém poskytnout uživateli informaci o tom, která část autentizace je chybná.

4.12. Pro každého uživatele informačního systému musí být možné identifikovat, jaká má přístupová práva.

4.13. Pro každý prostředek musí být možné vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku s rozlišením druhu přístupových práv (čtení, úprava atd.).

4.14. Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo skupině.

4.15. Data vstupující do informačních systémů musí být kontrolována tak, aby byla zajištěna jejich správnost. V informačních systémech se musí evidovat identifikátor uživatele, který změny provedl. Pro kontrolu dat musí Poskytovatel aplikovat opatření:

4.15.1. vstupní kontrola (neplatné znaky, rozsah, přetečení, kompletnost, souvislost...),

4.15.2. kontrola vnitřního zpracování dat,

4.15.3. kontrola oprávněnosti běhu programů,

4.15.4. kontrola integrity dat,

4.15.5. kontrola obsahu generovaných dat.

4.16. Vývoj software musí probíhat:

4.16.1. legálním softwarem,

4.16.2. autorská a licenční ujednání musí být smluvně řešena před samotným vývojem,

4.16.3. na testovacím prostředí odděleném od prostředí produkčního,

4.16.4. na testovacích datech, která nejsou převzata z provozní databáze; pokud je nutné použít data z provozní databáze, je nutné je anonymizovat,

4.16.5. migrace do provozního prostředí může být provedena až po akceptaci výsledků testů ve vývojovém či testovacím prostředí.

5. PŘEDÁNÍ PŘEDMĚTU PLNĚNÍ

5.1. Je-li informační systém vyvíjen na zakázku, musí splňovat všechny níže uvedené body a jedná-li se o již vyvinutý informační systém, musí být tyto požadavky zohledněny v hlavní smlouvě.

5.2. Dodávka software musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována. Pokud není stanoveno ve smlouvě jinak, je Poskytovatel povinen software dodat se zdrojovými kódy.

5.3. U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený software nebo program podléhající licenční a registrační politice. Pracuje-li počítačový program nebo aplikace s daty, musí být specifikováno s jakými daty a musí být provedena jejich kategorizace.

5.4. Ke každé dodávce musí existovat kromě účetních dokladů I předávací protokol podepsaný Poskytovatelem a Objednatelem. Způsob předání závisí na konkrétním hardware a na smlouvě s Poskytovatelem.

5.5. Způsob předání závisí na konkrétní službě a na smluvních podmínkách dohodnutých ve Smlouvě.

5.6. Poskytovatel zajistí monitorování služby tak, aby bylo možné porovnání jejich parametrů, rozsahu a kvality stanovených Smlouvou.

5.7. Nedílnou součástí dodávky Předmětu plnění je projektová a bezpečnostní dokumentace Předmětu plnění. Rozsah a náplň dokumentace musí být specifikován ve smlouvě s Poskytovatelem. Chybějící, neúplná nebo neaktuální dokumentace je důvodem k reklamaci dodávky.

5.8. Pokud má být měněn Předmět plnění, musí Poskytovatel aktualizovat dokumentaci.

5.9. Každý dodávaný prvek Předmětu plnění musí být plně a široce Poskytovatelem otestován, zda splňuje očekávané a smluvně definované parametry, a zda jeho používání nepředstavuje neočekávaná bezpečnostní rizika (penetrační test, práce s daty).

5.10. Každý prvek Předmětu plnění je předán až podpisem písemného předávacího protokolu oprávněnými zástupci smluvních stran.

6. FYZICKÁ BEZPEČNOST

6.1. Na neveřejných pracovištích a prostorách Objednatele (např. datové centrum) není dovolen pohyb cizích osob bez dozoru zaměstnance Objednatele.

6.2. Zaměstnanci Poskytovatele mohou fyzicky přistupovat k ICT prostředkům Objednatele pouze v doprovodu oprávněné osoby Objednatele.

6.3. V případě práce Poskytovatele v prostorách Objednatele nebo v jím využívaných prostorách v datových centrech musí Poskytovatel dále dodržovat tyto zásady:

6.3.1. připojovat vlastní počítač, notebook pouze se souhlasem odpovědné osoby Nemocnice,

6.3.2. v blízkosti ICT prostředků nejíst, nepít a nekouřit.

6.4. Poskytovatel není oprávněn k výměně a odvozu použitých či vadných technologií bez autorizace Objednatele.

7. POSKYTOVÁNÍ INFORMAČNÍ TŘETÍM STRANÁM

7.1. Poskytovatel je povinen dodržovat mlčenlivost o důvěrných informacích Objednatele, které se dozvěděl při dodávce Předmětu plnění, a to i v následujících čtyřech letech po ukončení smluvního vztahu založeného Smlouvou. Důvěrnou informací Objednatele se rozumí informace obchodní, technická, osobní údaje, zdravotnická dokumentace či jiná, která je významná pro Objednatele a/nebo je konkurenčně významná a není v obchodních kruzích běžně dostupná.

7.2. Pokud Poskytovatel přijde do styku s osobními údaji, musí se řídit platnou legislativou na ochranu osobních údajů, především týkající se zpracování a předávání. Je-li zpracovatelem osobních údajů, podepíše zpracovatelskou smlouvu.

7.3. Poskytovatel může šířit informace o Předmětu plnění či o spolupráci s Objednatelem (web, medializace Poskytovatele, publikace, tisk apod.) jen s předchozím písemným souhlasem Objednatele.

8. PORUŠENÍ BEZPEČNOSTNÍ POŽADAVKŮ

8.1. Porušení těchto bezpečnostních požadavků představuje porušení Předmětu plnění. Za porušení těchto bezpečnostních požadavků může být udělena sankce v souladu s čl. XX Smlouvy.

8.2. Pokud Poskytovatel poruší tyto bezpečnostní požadavky hrubým způsobem nebo opakovaně, je Objednatele oprávněna odstoupit od smluvního vztahu s Poskytovatelem v souladu s čl. XX Smlouvy.