Příloha č. 2 ke směrnici Politika řízení dodavatelů SME-PIS-BEZ-175

Bezpečnostní pravidla pro dodavatele

OBSAH

1. ÚČEL

Bezpečnostní politika (dále jen **„BP“**) stanovená v tomto dokumentu platí pro všechny dodavatele, obchodní partnery, poskytovatele IT služeb a další spolupracující subjekty Nemocnice Třebíč (dále jen **„Nemocnice“**), uváděné pod souhrnným označením **„třetí strany“**, kteří mají na základě smluvního vztahu, pracovně právního nebo obdobného vztahu nebo právních předpisů **oprávnění přistupovat zevnitř nebo zvenčí k počítačové síti, IS, prostředkům ICT Nemocnice a ke zpracovávaným informacím v jakékoliv podobě a formě.**

2. DEFINICE POJMŮ A ZKRATEK

2.1. POUŽITÉ ZKRATKY

SLA – Service-level agreement (SLA), smlouvu sjednaná mezi poskytovatelem služby a jejím uživatelem
NDA – dohoda o mlčenlivosti
VyKB – Vyhláška 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)
ICT – oddělení komunikačních technologií
BP – bezpečnostní politika
IS – informační systém
ISZS – informační systém základní služby dle VyKB

3. CÍLE

Nemocnice si v zájmu zajištění bezpečnosti informací stanovila tzv. bezpečnostní cíle:

a) chránit informace v souladu s jejich hodnotou, citlivostí a určením,
b) podporovat vytváření bezpečného prostředí, procesů a způsobů zpracování informací vedoucích k zajištění bezpečnosti informací, jak interně, tak externě,
c) poskytovat bezpečnou infrastrukturu, informační a komunikační technologie a prostředky zpracování informací obsahující potřebné bezpečnostní funkce,
d) vzdělávat zaměstnance a pracovníky Nemocnice, včetně externích subjektů, v kybernetické bezpečnosti a neustále zvyšovat jejich bezpečnostní povědomí,
e) efektivně řídit a zvládat mimořádné situace a bezpečnostní incidenty a minimalizovat negativní dopady na informace a provoz Nemocnice.

4. PRINCIPY

Nemocnice je povinna zajistit, aby informace a informační technologie, se kterými pracuje, splňovaly požadavky na dostupnost, důvěrnost a integritu. Z uvedeného důvodu Nemocnice zavádí bezpečnostní opatření k zajištění základních principů bezpečnosti informací:

1. **důvěrnosti** – zpřístupnění informací jen těm, které mají řádné oprávnění s informacemi nakládat,
2. **integrity** – zabezpečení přesnosti a kompletnosti informace a metod jejího zpracování,
3. **dostupnosti** – zajištění, aby informace a s nimi spojené aktivity (služby) byly uživatelům přístupné v době, kdy je požadují.

5. MINIMÁLNÍ BEZPEČNOSTNÍ POŽADAVKY NA TŘETÍ STRANY

5.1. POŽADOVANÁ BEZPEČNOSTNÍ DOKUMENTACE

Řízení bezpečnosti informací a zajištění kontinuity Nemocnice zajišťuje prostřednictvím **bezpečnostní dokumentace.** Třetí strana poskytne Nemocnici bezpečnostní dokumentaci jí dodávaného nebo spravovaného IS nebo ISZS.
Požadavky na bezpečnostní dokumentaci stanoví smluvní ujednání mezi Nemocnicí a třetí stranou. Splnění požadavků na bezpečnost informací v bezpečnostní dokumentaci může být také prokázáno certifikátem systému řízení bezpečnosti informací (např. dle ISO 27001), který zahrnuje oblast dodávky či správy IS nebo ISZS třetí stranou.

5.2. POŽADAVKY VE SMLUVNÍCH VZTAZÍCH SE TŘETÍMI STRANAMI

Přístup třetích stran k ICT a informacím Nemocnice, včetně vzdáleného přístupu, lze umožnit pouze jako časově omezený přístup servisních pracovníků třetích stran k ICT a informacím nemocnice za účelem náhledu, popřípadě změny informací a/nebo fungování ICT, který je upraven:
- smluvně,
- v souladu s touto BP,
- tak, aby byla zajištěna bezpečnost ICT a informací uvnitř i vně Nemocnice.

Požadavky na ochranu ICT a informací podle této BP (tj. primárním nebo podpůrným aktivům) musí být zakotveny ve smluvních ujednáních s třetími stranami:
- předtím, než bude povolen a aktivován schválený přístup,
- pouze v rozsahu nezbytně nutném pro výkon smluvních závazků,
- a součástí musí být ustanovení o povinné mlčenlivosti (tzv. NDA), případně i požadavek adresnosti, tzn. jmenovité uvedení fyzických osob, kterým má být přidělen přístup a oprávnění.

Existence, trvání a plnění povinností vyplývajících ze smluv pro dodavatele (vč. NDA, SLA) musí být pravidelně (min. 1x ročně) kontrolována.

5.3. KATEGORIZACE DODAVATELŮ

Nemocnice stanovuje minimální bezpečnostní požadavky na třetí strany v závislosti na zařazení dodavatele do některé z níže uvedených skupin:

a) Dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti IS, kteří nespadají do skupiny b):
   - dohoda o mlčenlivosti (NDA Nemocnice),
   - smluvní podmínky kybernetické bezpečnosti,

b) Významní dodavatelé - provozovatel IS a každý, kdo vstupuje do právního vztahu, který je významný z hlediska bezpečnosti IS:
   - dohoda o mlčenlivosti (NDA Nemocnice),
   - podmínky kybernetické bezpečnosti dle přílohy č. 7 VyKB.

5.4. DOHODA O MLČENLIVOSTI (NDA)

S dodavateli IT služeb, kteří pro výkon smluvních povinností potřebují přístup k aktivům Nemocnice, musí být povinně ještě před povolením přístupu uzavřena písemná Dohoda o mlčenlivosti (NDA) obsahující zejména:
- identifikaci správce nebo provozovatele,
- identifikaci informačního a komunikačního systému,
- identifikaci významného dodavatele,
- vyrozumění o skutečnosti, že dodavatel je pro správce významným dodavatelem, a popřípadě také o tom, že významný dodavatel je zároveň provozovatelem,
- je-li relevantní, pravidla obsahují:
  - Politika přístupových práv,
  - Monitoring,
  - Ochrana duševního vlastnictví,
  - Způsob předání / výmazu informací při ukončení smlouvy.
  - Sankce v případě porušení

Seznam dodavatelů, se kterými byla podepsána „NDA“, případně mají povolen přístup k primárním či podpůrným aktivům Nemocnice, eviduje vždy garant aktiva (případně po dohodě s garantem Manažer kybernetické bezpečnosti).

5.5. VÝZNAMNÍ DODAVATELÉ

Smluvní ujednání se třetími stranami, které byly zařazeny na seznam „Významných dodavatelů“ Nemocnice a informovány o tom, že se staly „Významným dodavatelem“ a provozovatelem ISZS, musí obsahovat minimálně následující body (v souladu s přílohou č. 7 k VyKB):
- definice „chráněné informace“,
- vzájemná odpovědnost,
- doba trvání smlouvy,
- vymezení pojmů,

- sankce v případě porušení,
- zmínění akcí, které budou následovat v případě porušení smlouvy,
- úprava pravidel o předávání informací třetím stranám, případně také (dle relevance):
- instrukce o nakládání s osobními údaji,
- opatření pro nakládání s majetkem,
- školení osob, které budou nakládat s chráněnými informacemi,
- revize a ukončení smlouvy.

5.6. POŽADOVANÁ OCHRANA KLASIFIKOVANÝCH INFORMACÍ

Informace Nemocnice mají přiděleny stupně ochrany podle jejich citlivosti. Jednotlivé stupně klasifikace informací mají současně stanoveno povolené zacházení s nimi, a to jak v elektronické, tak v písemné (tištěné) a jiné podobě, tj.:

- v průběhu jejich vstupu do IS, ukládání, přepravy či přenosu, např. e-mailem, poštou, internetem,
- ve všech formách výstupu, tisku, kopírování, ústního sdělení, zálohování, archivace a likvidace.

Pokud třetí strany v rámci smluvně dohodnuté činnosti získají přístup k informacím střední a vyšší úrovně klasifikace, musí dodržovat požadovaná opatření na ochranu a způsob zacházení s nimi podle klasifikace aktiv.

Úroveň		Označení úrovně	Popis	Požadovaná opatření
1	Nízká	Veřejné	Informace jsou veřejně přístupné, jsou určeny ke zveřejnění nebo byly oprávněně zpřístupněny či poskytnuty neurčitému okruhu osob (např. na základě zákona č. 106/1999 Sb. o svobodném přístupu k informacím, ve znění pozdějších předpisů, zveřejňované informace na webových stránkách Nemocnice Třebíč, tiskové zprávy apod.). Narušení důvěrnosti informací neohrožuje oprávněné zájmy Nemocnice Třebíč.	Není vyžadovaná ochrana
2	Střední	Interní	Informace nejsou veřejně přístupné. Jsou určené pro interní potřeby zaměstnanců Nemocnice Třebíč, případně i třetích stran. S těmito informacemi se musí seznamovat všichni zaměstnanci Nemocnice Třebíč a zainteresovaní pracovníci třetích stran. Jedná se zejména o informace typu řády, směrnice, příkazy, metodické pokyny a další závazné vnitřní předpisy Nemocnice Třebíč, které jsou standardně zpřístupněné prostřednictvím intranetu, rozesílané zaměstnancům mailem, či distribuované tištěnou formou.	Pro ochranu důvěrnosti musí být využívány prostředky pro řízení přístupu.
3	Vysoká	Citlivé	Informace nejsou veřejně přístupné a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (např. občanský zákoník, osobní údaje podle zákona č. 110/2019 Sb., o zpracování osobních údajů, nařízení evropského parlamentu a rady (EU) 2016/679 (GDPR) s výjimkou zvláštní kategorie osobních údajů). Jedná se rovněž o informace, jejichž ochrana není výslovně vyžadována právním	Pro ochranu důvěrnosti musí být využívány prostředky, které zajistí řízení a zaznamenávání přístupů. Přenosy informací po komunikační síti musí být chráněny pomocí schválených kryptografických prostředků.

			předpisem, avšak u kterých narušení bezpečnosti může významně zvýšit rizika poškození oprávněných zájmů Nemocnice Třebíč. S těmito informacemi se seznamuje pouze omezený okruh zaměstnanců, v souladu s jejich pracovní náplní a pracovním zařazením a plněním pracovních povinností. Třetím osobám mohou být tyto informace poskytnuty pouze na základě právního předpisu. Jedná se zejména o informace obsahující jakékoliv osobní údaje, chráněné interní obchodní informace Nemocnice Třebíč, obchodní tajemství dodavatelů, dále interní materiály typu zpráv z auditů a kontrol, finanční a mzdové, dokumenty k občanskoprávním či trestněprávním řízením apod.	
4	Kritická	Vysoce citlivé	Informace nejsou veřejně přístupné a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (zejména zvláštní kategorie osobních údajů a data chráněná podle zvláštních předpisů vztahujících se k ochraně utajovaných informací). Jedná se rovněž o informace, jejichž ochrana není výslovně vyžadována právním předpisem, avšak u kterých narušení bezpečnosti může významně zvýšit rizika poškození oprávněných zájmů Nemocnice Třebíč (zejména informace související se zajišťováním kybernetické bezpečnosti Nemocnice Třebíč, tj. informace o informační a komunikační infrastruktuře Nemocnice Třebíč včetně bezpečnosti zdravotnických prostředků, dále informace o systému krizového řízení, informace o energetické, komunikační, vodohospodářské a další kritické infrastruktuře Nemocnice Třebíč). S těmito informacemi se seznamuje pouze omezený okruh zaměstnanců, v souladu s jejich pracovní náplní a pracovním zařazením a plněním pracovních povinností. Třetím osobám mohou být tyto informace poskytnuty pouze na základě právního předpisu. Informace se strategickým obsahem pro Nemocnice Třebíč, jejichž vyzrazení či zneužití je způsobilé poškodit nebo ohrozit zájmy Nemocnice Třebíč např.: • zamezení naplnění klíčových cílů zdravotní péče, • porušení zákona (např. na ochranu hospodářské soutěže), • ztráta dobrého jména a kreditu Nemocnice Třebíč na národní či mezinárodní úrovni.	Pro ochranu důvěrnosti musí být využívány prostředky, které zajistí řízení a zaznamenávání přístupů. Dále musí být nasazena odpovídající bezpečnostní opatření zabraňující zneužití aktiv ze strany osob s privilegovanými oprávněními. Přenosy informací po komunikační síti musí být chráněny pomocí schválených kryptografických prostředků.

5.7. POŽADOVANÁ PERSONÁLNÍ OPATŘENÍ

Je-li pro plnění smluvních povinností třetí strany nezbytné přidělení přístupu k ICT a informacím Nemocnice (dále také „přístup“), je třetí strana povinna dodržovat procesy a postupy stanovené touto politikou.

Podmínky udělení přístupu:
- Platná a účinná smlouva mezi třetí stranou a Nemocnicí.
- Nezbytnost přístupu k realizaci smlouvy.
- Žádost o přístup.
- Schválení přístupu Manažerem kybernetické bezpečnosti.

O přístup je možné požádat po uzavření smlouvy nebo schválení objednávky o provedení služeb. O přístup žádá písemně správce systému dodavatele. Žádost musí schválit Manažer kybernetické bezpečnosti. Požadavek (Žádost o přístup) je následně zpracován automatizovaně (v případě RDP), nebo předáván administrátorovi Nemocnice, který:
- zřizuje, mění nebo ruší uživatelský účet externího uživatele,
- přiděluje či odebírá příslušná oprávnění externího uživatele.

5.8. POŽADAVKY NA ŽÁDOST O PŘÍSTUP

Formální požadavek na přidělení, změnu či odebrání uživatelských účtů a přístupů k primárním a podpůrným aktivům (ICT a informacím) Nemocnice musí obsahovat minimálně:
- identifikaci žadatele (název, sídlo, IČO), a kontaktní údaje (osoba, telefon, e-mail),
- zdůvodnění požadavku na přístup a identifikace smlouvy (datum uzavření, číslo)
- rozsah přístupu (tj. ke kterým systémům / aplikacím / informacím může žadatel přistupovat),
- oprávněnou osobu (konkrétní pracovník třetí strany s požadovaným přístupem),
- email a telefonní číslo oprávněné osoby (konkrétní pracovník třetí strany s požadovaným přístupem)

Každému externímu uživateli je na základě schváleného požadavku přidělován přístup, jehož rozsah určuje garant aktiva. Nadstandardní rozšíření přístupu a výjimky jsou řešeny individuálně:
- podle specifických potřeb určovaných garantem aktiv,
- v souladu s interní klasifikací informací.

Pracovníci třetích stran s přidělenou možností hlásit se k IS zvenčí musí používat zabezpečený způsob přístupu a autentizace dle aktuálně používaných metod přístupu pro dodavatele.

5.9. POŽADAVKY NA DETEKCI A HLÁŠENÍ BEZPEČNOSTNÍCH UDÁLOSTÍ

Třetí strany musí být schopny v závislosti na zařazení do kategorie dodavatelů detekovat kybernetické bezpečnostní události a identifikovat kybernetické bezpečnostní incidenty a v případě, že nastanou detekovat bezpečnostní události a identifikovat kybernetické bezpečnostní incidenty.

Třetí strany s přístupem k ICT a informacím Nemocnice jsou povinny dohodnutým způsobem hlásit zjištěné závady, poruchy, incidenty, podezřelé aktivity, případně odhalené slabiny administrátorovi Nemocnice nebo Manažerovi kybernetické bezpečnosti Nemocnice.

6. TECHNICKÁ OPATŘENÍ

Vzdálený přístup je s třetími stranami řešen individuálně podle technických podmínek smlouvy. Náklady na technická opatření u třetí strany na zajištění jejího vzdálenému přístupu k zařízením nebo informacím Nemocnice nese třetí strana.

6.1. POŽADAVKY NA BEZPEČNOST OBJEKTŮ

- V případě fyzického přístupu pracovníků třetích stran do objektů Nemocnice třetí strany zajistí, aby tito pracovníci dodržovali požadavky na objektovou bezpečnost ve fyzických zabezpečených oblastech, kam mají v rámci plnění smluvních závazků a schválené žádosti oprávněn fyzický vstup.
- V případě ICT a informací umístěných, spravovaných nebo poskytovaných mimo objekty Nemocnice, tzn. u třetích stran, jsou třetí strany povinny zajistit naplnění požadavků objektové bezpečnosti tak, aby nemohlo dojít k neoprávněnému fyzickému přístupu k ICT a informacím Nemocnice.

6.2. POŽADAVKY NA BEZPEČNOST ZAŘÍZENÍ

Zařízení a vybavení, které slouží k zajištění provozu podpůrných aktiv (ICT nebo podpůrných služeb), musí být chráněno před fyzickými hrozbami, jako jsou přírodní události (oheň, voda, mráz, vítr) nebo působení lidského činitele, jejichž výsledkem může být havárie, porucha, poškození, zničení, krádež apod. Mezi zařízení a vybavení, která musí být chráněna v objektech Nemocnice i třetích stran, a na kterých je závislá provozuschopnost ICT, patří:

- výpočetní technika, switch/router, přístupové zařízení (AP), kabeláž, tiskárna, skener, kopírka,
- zdroje energie, jističe, UPS, agregáty,
- klimatizace, dodávky tepla, vody.

Třetí strany jsou prostřednictvím svých pracovníků povinny zabezpečit fyzický přístup k zařízení a vybavení ve všech lokalitách, kde jsou umístěny ICT, IS nebo jejich komponenty (v elektronické i tištěné podobě), před výše uvedenými fyzickými hrozbami jak v mimopracovní době, tak i v případě krátkodobého opuštění pracoviště, zejména těmito opatřeními:

- dodržování zásady „čistého stolu“, tzn. bezpečné ukládání dokumentů v listinné podobě a nosičů dat a médií podle citlivosti obsažených informací (v souladu s klasifikací informací) – do uzamykatelných schránek (zásuvka, skříň, trezor),
- uzamčení kanceláře při jejím i krátkodobém opuštění,
- fyzická ochrana klíčů, vstupních / čipových karet apod. včetně znemožnění přístupu k nim nebo jejich zneužití neoprávněnou osobou,
- zákaz kouření a nakládání s nebezpečnými látkami na pracovišti.

Povinnosti fyzické ochrany (tj. zvýšená opatrnost a používání prostředků fyzické bezpečnosti) se vztahují i na mobilní zařízení, jako jsou např. přenosné počítače, notebooky, tablety, nosiče dat a média, pokud fyzicky opouštějí zabezpečené oblasti Nemocnice a jsou používány v nezabezpečených objektech nebo místech.

6.3. POŽADAVKY NA KONTROLU FYZICKÉHO PŘÍSTUPU

Fyzický vstup do zabezpečených oblastí objektů Nemocnice je kontrolován. K prostředkům ICT, které jsou umístěny v zabezpečených oblastech Nemocnice nebo třetích stran, je fyzický přístup vyhrazen pouze oprávněným osobám, kterými mohou být:

- zaměstnanci Nemocnice na základě přidělených oprávnění,
- pracovníci třetích stran na základě smluvních ujednání a přidělených oprávnění,
- zaměstnanci orgánů veřejné moci na základě právních předpisů.

Osobám, které nemají příslušné oprávnění, je fyzický přístup a používání ICT Nemocnice zakázán.

6.4. POŽADAVKY NA ŘÍZENÍ PŘÍSTUPU K INFORMACÍM

Základními požadavky (principy udělení) na řízený přístup třetí osoby s přihlašováním se k uživatelskému účtu k informacím zpracovávaným v ICT jsou:

- zákaz nebo maximální omezení všech práv, přičemž postupné rozšiřování a přidělování práv je možné pouze se souhlasem garanta informací, potažmo Manažera kybernetické bezpečnosti Nemocnice, který posuzuje oprávněnost přístupu, a na základě písemného požadavku třetí osoby, posuzuje potřebnost přístupu třetí strany;
- přístup je v souladu s interní klasifikací informací;
- třetí strana má přidělen svůj vlastní (jmenovitý) externí uživatelský účet pro každou fyzickou osobu třetí strany;
- zákaz sdílení jednoho administrátorského přístupu (účtu) více fyzickými osobami;
- každý pracovník třetí strany dbá na ochranu jemu přidělených přihlašovacích údajů (jméno, heslo, PIN, další autentizační údaje).

6.5. POUŽÍVÁNÍ PRIVILEGOVANÉHO PŘÍSTUPU

Za **privilegovaný přístup** (nebo také privilegovaný přístupový účet) je považován takový přístup (administrátorský a podobné povahy), který umožňuje uživateli spravovat systém, zejména zasahovat do jeho konfigurace, provádět změny, vytvářet či rušit účty a přístupy dalším uživatelům. Privilegovaný přístup přidělený třetím stranám je dovoleno používat pouze pro správu systémů, nikoliv k běžné činnosti třetí osoby. Jeden účet nesmí být sdílen více administrátory, pokud je to technicky / provozně možné.

Privilegovaný přístup a neprivilegovaný přístup (přístup bez oprávnění role administrátora) třetí strany **musí být udělen a provozován v souladu s následujícími podmínkami:**

- Přidělení privilegovaného přístupu k ICT Nemocnice třetí straně schvaluje Manažer kybernetické bezpečnosti.
- Uživatelé bez oprávnění administrace systému Nemocnice mají systémově odepřen přístup k těmto činnostem a není jim dovoleno vytvářet další účty a přístupy k operačnímu systému počítače, z nějž přistupují k ICT a informacím nemocnice.
- Na všech počítačích s přístupem k ICT a informacím Nemocnice je povolen výskyt pouze administrátorem předem definovaných účtů a jsou zakázány všechny obecné účty vytvářené např. při instalaci OS s přednastaveným přístupem (typu „guest“, „anonymous“ apod.).
- Přihlašování k systému probíhá za použití jedinečného identifikátoru (jménem a heslem) příp. jiným povoleným způsobem identifikace a autentizace při ověření uživatele vůči systému a využití schválených autentizačních prostředků, např. HW tokenů, čipových karet a digitálních certifikátů.
- Pokud aplikace využívají vlastní omezení přístupu k informacím zpracovávaným jejich prostřednictvím, pak tato omezení nesmějí být v rozporu se stanovenou BP přístupových práv a úrovní přístupu (zejména ke klasifikovaným informacím) pro konkrétní externí uživatele či jimi zastávané funkce.

6.6. POŽADAVKY NA HESLA

Pro oprávněný přístup třetích stran musí být používána přístupová hesla, která splňují stanovená kvalitativní kritéria:

- vygenerované prvotní heslo musí být uživateli předáváno bezpečným způsobem,
- přidělené heslo k uživatelskému účtu musí být při prvním přihlášení uživatelem změněno,
- musí být uplatňována více faktorová autentizace, nebo:
  - délka hesla je alespoň:
    - 12 znaků u uživatelů a
    - 18 znaků u administrátorů a aplikací,
  - heslo může dosahovat délky až 64 znaků,
  - heslo musí vždy obsahovat znaky alespoň tří ze čtyř následujících kategorií:
    - malá písmena,
    - velká písmena,
    - číslice,
    - speciální znaky (např. @, &, #...),
  - uživatel může měnit heslo nejdříve 5 dnů po poslední změně, ledaže příslušný administrátor stanoví jinak,
  - uživatelé ani administrátoři nesmějí:
    - volit triviální hesla,
    - tvořit hesla na základě mnohonásobně opakujících se znaků, údajů osobního charakteru, přihlašovacího jména, e-mailu, názvu systému nebo obdobným způsobem, ani
    - opětovně použít dříve užité heslo, přičemž paměť předchozích hesel musí obsahovat alespoň 12 předchozích hesel,
  - uživatel musí změnit heslo nejdéle po 18 měsících,
  - administrátor musí změnit heslo nejdéle po 6 měsících, přičemž toto pravidlo se nevztahuje na účty sloužící k obnově systému v případě havárie,
  - po prvním použití výchozího hesla bude vynucena jeho změna,
  - heslo k obnovení přístupu bude zneplatněno po jeho prvním použití nebo marném uplynutí 60 minut od jeho vytvoření,

6.7. POŽADAVEK ČISTÉHO STOLU A OBRAZOVKY

V případě fyzického opuštění pracoviště v Nemocnici nebo v místě, odkud se pracovník třetí strany přihlašuje k ICT Nemocnice, je povinností třetí strany a uživatele zabezpečit pracoviště i pracovní stanici před neoprávněným fyzickým i logickým přístupem jiných osob takovým způsobem, který je přiměřený délce nepřítomnosti, například:

- odhlášení uživatele,
- uzamknutí stanice,
- aktivace spořiče obrazovky chráněného kvalitním heslem,

- bezpečné uložení nosičů dat a výtisků klasifikovaných informací,
- uzavření oken, uzamčení místnosti,
- aktivace zabezpečovacího systému EZS apod.

Jedná-li se o nepřetržitý provoz, při němž se nelze odhlásit ze systému a stanice či konzola serveru musí zůstat v provozu např. i v nočních hodinách, je nezbytné zamezit přístupu k systému neoprávněným osobám jinými vhodnými opatřeními, která stanoví Manažer kybernetické bezpečnosti. Všechny neaktivní stanice či terminály musí být po definovaném čase nečinnosti automaticky zablokovány.

6.8. POŽADAVKY NA OCHRANU MOBILNÍCH PROSTŘEDKŮ A PRÁCI NA DÁLKU

Nemocnice uplatňuje politiku ochrany přístupu k mobilním prostředkům používaným vně (tzn. mimo chráněné prostředí počítačové sítě) Nemocnice, jako jsou např. notebooky, „chytré“ mobilní telefony, SD karty a další zařízení či média fungující jako nosiče dat, kde mohou být potenciálně ohroženy klasifikované informace.
Používá-li třetí strana mobilní prostředky, v nichž se nacházejí chráněné informace Nemocnice klasifikované vyšší než „nízkou“ úrovní (veřejné informace), je povinna takové prostředky zabezpečit některým ze stanovených způsobů:

- ochrana zařízení (dle typu mobilního prostředku),
- ochrana přístupu k informacím v zařízení (dle typu např. PIN, gesto, biometrika, vícefaktorová autentizace),
- šifrování dat (šifrovací nástroj a použití kvalitního hesla),
- příp. fyzická ochrana mobilního prostředku (přenosná schránka chráněná zámkem s kódem).

Dostatečnost zabezpečení mobilních prostředků používaných k práci na dálku s ICT a informacemi v Nemocnici posuzuje, případně vhodné metody ochrany konkrétních mobilních prostředků stanovuje administrátor se souhlasem Manažera kybernetické bezpečnosti.

7. POŽADAVKY NA IT PROCESY

Všechny důležité nebo kritické IT-procesy v rámci podpůrných aktiv (dále jen „podpůrné IT-procesy“) týkající se provozu, zpracování dat a služeb poskytovaných třetími stranami, na kterých jsou závislá primární aktiva, musí být definovány, popsány a spravovány podle potřeby tak, aby:

- bylo možno je zabezpečit,
- bylo možno zajistit zastupitelnost jednotlivých výkonných rolí.

7.1. GARANT IT-PROCESU

Podpůrné IT-procesy mají přiřazeného garanta (vlastníka procesu), který je zodpovědný za jejich správné provádění. Administrátor je garantem podpůrných IT-procesů a odpovídá za jejich identifikaci, přidělení priorit a kontrolu výkonu smluvně dohodnutých IT-procesů a souvisejících činností pracovníků třetích stran.
Garant podpůrných IT-procesů odpovídá za jejich dokumentaci, popis postupů, jejich aktuálnost a evidenci. Garantem procesu může být stanoven i zástupce třetí strany, jedná-li se o zajištění podpůrných IT-služeb třetí stranou. V takovém případě může být zpracování dokumentovaných postupů smluvně vyžadováno po dodavateli takové služby.
Manažer kybernetické bezpečnosti zajišťuje nezávislou kontrolu podpůrných IT-procesů – revizi postupů třetí strany z hlediska dostatečnosti IT-procesů, aktuálnosti, schválených přístupů a ochrany dat odpovídající jejich klasifikaci.

7.2. DOKUMENTACE PODPŮRNÝCH IT-PROCESŮ

Dokumentace podpůrných IT-procesů zajišťovaných třetí stranou musí obsahovat minimálně:

- garanta procesu;
- popis způsobu zpracování a nakládání s informacemi Nemocnice;
- požadavky na plánování kapacit, příp. závislost na jiných systémech;
- kontaktní osobu / místo pro hlášení a řešení technických či provozních potíží (např. ServiceDesk);
- zásady pro práci s klasifikovanými informacemi v rámci IT-procesů a jejich zabezpečení;
- postup obnovy IT-procesu po závadě, poruše, mimořádné události nebo havárii.

7.3. HLÁŠENÍ INCIDENTŮ PODPŮRNÝCH IT-PROCESŮ

Definování, popis a určení priority podpůrných IT-procesů slouží pro stanovení odpovídající reakce na pravděpodobné bezpečnostní incidenty v těchto procesech. Řízení incidentů obecně přísluší Manažerovi kybernetické bezpečnosti.
V případě zajišťování podpůrných IT-procesů třetí stranou musí být aplikovány následující kontrolní mechanismy vzájemné komunikace s odpovědnými osobami Nemocnice, zejména pro:

- hlášení závad a selhání podpůrných IT-procesů;
- hlášení bezpečnostních incidentů a zranitelných míst (slabin) systémů;
- kontrolu ztráty nebo porušení důvěrnosti informací v systémech spravovaných třetími stranami;
- pravidelné sledování a vyhodnocování auditních záznamů systémů spravovaných třetími stranami.

7.4. ZAJIŠTĚNÍ ZASTUPITELNOSTI

V případě podpůrných IT-procesů realizovaných třetí stranou je uplatňován požadavek na zachování kontinuity. Třetí strana musí zajistit zastupitelnost pracovníků v době jejich nepřítomnosti. Pro tyto případy musí být v dokumentaci třetí strany uvedena podrobná pravidla (např. pro ukládání, resp. obnovu hesel a přístupových kódů pro mimořádné události, prokazatelné přidělení příslušných oprávnění zastupujícím pracovníkům, požadavky přesměrování komunikace apod.).

7.5. POŽADAVEK NA ODDĚLENÍ PROCESŮ VÝVOJE OD OSTRÉHO PROVOZU

Vývoj programového vybavení je řešen dodavatelsky. Pokud dochází k implementaci SW-nástrojů či k úpravám systémů třetí stranou, musí být zajištěno, aby proces testování nového systému či SW nezasahoval do produkčního prostředí (do „ostrého provozu“), a to zejména v případě, kdy by mohl negativně ovlivnit provozuschopnost podpůrných IT-procesů nebo bezpečnost „ostrých dat“. Migrace do ostrého provozu musí respektovat stanovené bezpečnostní zásady a pravidla Nemocnice zajišťující, že nedojde k neplánovanému přerušení činnosti nebo kompromitaci dat.

7.6. ZMĚNOVÉ ŘÍZENÍ

Implementace významných změn (např. přechod na jiný systém, infrastruktury do cloudu, změna dodavatele systému nebo nový informační systém) v systému realizovaných třetí stranou podléhá formalizovanému procesu změnovému řízení, v jehož rámci jsou změny autorizovány odpovědnými osobami. Požadované změny musí být ještě před implementací technicky přezkoumány administrátorem a schváleny Manažerem kybernetické bezpečnosti.

Třetí strany jsou povinny u programového vybavení, OS a IS, jejichž správu a provoz zajišťují:

- omezit modifikace programových balíků (customizace apod.) na nezbytné minimum,
- kontrolovat opravné „balíčky“ před jejich implementací do ostrého provozu, s ohledem na ochranu před možnými hrozbami, skrytými kanály a trojskými koni,
- v případě vývoje nového SW externím dodavatelem je nutno zajistit příslušné bezpečnostní kontroly a smluvně ošetřit rizika.

7.7. POŽADAVKY NA OCHRANU PŘED ŠKODLIVÝM SW

Informační systémy třetí strany, z nichž se v rámci oprávnění připojují pracovníci k systémům Nemocnice, musí být chráněny před škodlivými kódy pomocí vhodného SW. Antivirová ochrana obecně musí plnit jak detekční funkce, tak podle možností a potřeby i preventivní opatření k zabránění průniku nebo rozšíření škodlivého SW do systémů Nemocnice. Informační systému třetí strany musí naplňovat následující požadavky:

- všechny počítačové stanice, včetně mobilních zařízení, s přístupem k informacím Nemocnice jsou kontrolovány na přítomnost škodlivého kódu a musí mít povinně zapnutou rezidentní AV ochranu;
- na všech počítačových stanicích a mobilních zařízeních musí být zakázáno vypnout či omezit tuto ochranu uživatelem;
- pro všechny pracovníky třetích stran platí zákaz zasahovat do HW a SW konfigurace počítače, k němuž jim byl přidělen přístup, pokud to nevyžaduje plnění smluvních závazků;
- správnost, aktuálnost a účinnost nastavení AV ochrany musí být pravidelně kontrolována a ověřována;
- zveřejněné opravné balíky (záplaty) jsou po nezbytném ověření funkčnosti neprodleně aplikovány na ohrožené systémy či aplikace.

7.8. ZÁLOHOVÁNÍ

Zálohování informací v Nemocnici je řešeno centrálně. Požadavky na zálohování a zálohovací mechanismy jsou na základě dokumentovaných podpůrných IT-procesů definovány jejich garanty.

Třetí strany musí zajistit, aby:
- byla zálohována všechna důležitá data nezbytná pro zajištění kontinuity provozu jimi spravovaných systémů nebo v rámci jimi poskytovaných IT-služeb, a to vhodnou definicí požadavků na zálohy,
- se na lokálních počítačových stanicích nevyskytovaly žádné informace určené ke sdílení a podléhající centrálnímu zálohování. Vyžaduje-li to charakter zpracování, jsou individuální zálohy dat na lokálních PC (např. u specifických lokálních agend) řešeny jednotlivě dle požadavků garantů těchto procesů pověřenými zástupci Nemocnice a třetích stran.

Pokud na straně externích dodavatelů existují záložní kopie důležitých informací, musí být zabezpečeny před neoprávněným přístupem.

7.9. POŽADAVKY NA BEZPEČNOST ELEKTRONICKÉ DOKUMENTACE

Při elektronické komunikaci s Nemocnicí musí třetí strany posuzovat bezpečnostní rizika, která s sebou přináší komunikace prostřednictvím elektronické pošty tak, aby nemohla způsobit přerušení provozu Nemocnice či pád systému nebo služeb, ztrátu nebo kompromitaci neveřejných klasifikovaných informací, infikovat počítačovou síť Nemocnice viry nebo jiným škodlivým SW.

Třetí strany jsou při své činnosti povinny splňovat následující bezpečnostní požadavky:
- obsah elektronické pošty, včetně příloh v různých formátech přijímaných zpráv, musí být chráněn proti škodlivým kódům účinným antivirovým programem;
- neveřejné klasifikované informace Nemocnice musí být při přenosu prostřednictvím elektronické pošty (nebo obdobné formy komunikace prostřednictvím internetu) chráněny, jinak nesmí být v nezabezpečené formě posílány elektronickou poštou.

Vhodným způsobem ochrany je např. šifrování a použití elektronického podpisu.

7.10. POŽADAVKY NA KRYPTOGRAFICKÁ OPATŘENÍ

Neveřejné klasifikované informace Nemocnice v elektronické podobě nesmí opustit chráněné prostředí počítačové sítě v otevřené formě. K jejich zabezpečení a přenosu mezi Nemocnicí a třetí stranou musí být určeny smluvně nebo jinou vzájemně dohodnutou formou stanovené systémy, nástroje nebo kryptografické prostředky.

8. ZÁVĚREČNÁ USTANOVENÍ

Revize externí bezpečnostní politiky probíhá minimálně 1x ročně a zodpovídá za ni Manažer kybernetické bezpečnosti.

9. SOUVISEJÍCÍ DOKUMENTY

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů
- Vyhláška 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)
- Zákon č. 110/2019 Sb., o zpracování osobních údajů
- Nařízení (EU) 2016/679 ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů
- Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů
- Zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů