Směrnice Trio service group s.r.o.

Detailní bezpečnostní směrnice informačních technologií

	Detailní bezpečnostní směrnice informačních technologií			
Zpracoval: **Bc.Marek Kiša**	**Přezkoumal:**	**Schválil:** **Bc.Marek Kiša**	**Datum:** **22.05.2024**	**Revize č.:**

Obsah

1. Bezpečnost lidských zdrojů

1.1. Před vznikem pracovního vztahu

Cíl: Zajistit, aby zaměstnanci, smluvní a třetí strany byli srozuměni se svými povinnostmi, aby pro jednotlivé role byli vybíráni vhodní kandidáti a snížit riziko lidské chyby, krádeže podvodu nebo zneužití prostředků organizace.

Odpovědnosti za bezpečnost by měly být zohledněny v rámci přijímacího řízení, měly by být zahrnuty v pracovních smlouvách a popisech práce.

Potenciální uchazeči by měli být náležitě prověřeni, zejména v případě citlivých pracovních míst.

Všichni zaměstnanci, smluvní a třetí strany, využívající prostředky organizace pro zpracování informací, by měli podepsat dohodu odpovídající jejich rolím a povinnostem.

1.1.1.Role a odpovědnosti

K doložení pracovní náplně a odpovědnosti v oblasti bezpečnosti informací je možné využívat popisy pracovních míst. Osoby, které nejsou zaměstnanci Trio service group s.r.o. (dále jen Společnost) musí mít svoji odpovědnost zakotvenou v rámci smlouvy, na jejímž základě pro Společnost svou činnost vykonávají. Z hlediska bezpečnosti IT musí být v uvedených dokumentech uvedeny zejména požadavky na:

- Dodržování zásad stanovených schválenou bezpečnostní politikou uplatňovanou ve společnosti
- Určení odpovědnosti za provedenou činnost.
- Hlášení bezpečnostních událostí nebo jiných bezpečnostních rizik.

Odpovědnost za uplatnění těchto požadavků v rámci pracovních vztahů uvedených v této kapitole je určena přímým nadřízeným, resp. objednatelem služby v případě externích pracovníků.

1.1.2.Prověrka

Součástí přijímacího řízení uchazeče o zaměstnání (pracovní příležitost) je prověrka prováděná na těchto základech:

- Dostupnost profesních a osobních referencí.
- Ověření vzdělání a odborné kvalifikace.
- Detailnějšího prověření (např. výpis trestního rejstříku).

Prověrky v tomto smyslu musí být uplatněny i pro organizace, které se v rámci výběrových řízení ucházejí o zakázky v oblasti IT. Za zařazení těchto prověrek do podmínek účasti ve výběrovém řízení je zodpovědný jeho zadavatel.

1.1.3. Podmínky výkonu pracovní činnosti

Společnost smluvně zajišťuje souhlas uživatelů s tím, že budou dodržovat bezpečnost informací přiměřenou rozsahu jejich přístupu k aktivům Společnost. Děje se tak v rámci uzavírání pracovní smlouvy,
která musí obsahovat tato témata:

- Ochrana informací a zachování mlčenlivosti.
- Odpovědnost za nakládání s aktivy spojenými s informačními systémy ve Společnosti
- Odpovědnost při nakládání s osobními údaji zpracovávanými v rámci informačních systémů.
- Popis kroků následujících při nedodržení bezpečnostních požadavků ze strany uživatelů.

2. Během pracovního vztahu

Cíl: Zajistit, aby si pracovníci, smluvní a třetí strany byli vědomi bezpečnostních hrozeb a problémů s nimi spjatých, svých odpovědností a povinností a byli připraveni podílet se na dodržování politiky bezpečnosti informací během své běžné práce a na snižování rizika lidské chyby.

Měly by být jasně definovány odpovědnosti vedoucích pracovníků, aby se zajistilo dodržování bezpečnosti ze strany jednotlivců během doby trvání pracovního vztahu.

Pracovníci, smluvní a třetí strany by měli být proškoleni v bezpečnostních postupech a ve správném používání prostředků pro zpracování informací, aby byla minimalizována bezpečnostní rizika. Měla by být vytvořena formalizovaná pravidla pro disciplinární řízení v případě narušení bezpečnosti.

2.1. Odpovědnosti vedoucích pracovníků

Vedoucí pracovníci musí po uživatelích ve společnosti požadovat dodržování bezpečnosti v souladu s platnou bezpečnostní politikou a dalšími vnitropodnikovými normami (dále jen VPN). Odpovědností vedoucích pracovníků je zajistit:

- Dostatečnou informovanost o rolích a odpovědnostech za bezpečnost informací.
- Seznámení s VPN týkající se oblasti zpracování a užívání dat.
- Jednání svých podřízených v mezích bezpečnostní politiky a návazných vnitropodnikových předpisů.

2.2. Povědomí, vzdělávání a školení v oblasti bezpečnosti informací

V rámci zaškolovacího programu absolvují noví pracovníci elektronický kurz Bezpečnost IT. Aby se jim absolvováním tohoto kurzu dostaly do povědomí informace obsažené v BP IT, je třeba obsah kurzu pravidelně aktualizovat. Všichni pracovníci Společnosti mají povinnost tento kurz absolvovat při nástupu a následně každé dva roky.

Za aktualizaci elektronického kurzu Bezpečnost IT v souladu s obsahem a zněním BP IT odpovídá IT Společnosti

2.3. Disciplinární řízení

Disciplinární řízení musí zajistit korektní a spravedlivé zacházení s uživateli podezřelými z narušení bezpečnosti a nesmí být zahájeno bez předchozího ověření, že se opravdu jedná o narušení bezpečnosti. V závažných případech by měl být narušitel okamžitě zbaven přístupových práv a výsad.

3. Ukončení nebo změna pracovního vztahu

Cíl: Zajistit, aby ukončení nebo změna pracovního vztahu zaměstnanců, smluvních a třetích stran proběhla řádným způsobem.

Měly by být určeny jednoznačné odpovědnosti za řádný průběh ukončení pracovního vztahu zaměstnanců, smluvních a třetích stran, za odevzdání přiděleného vybavení a odejmutí přístupových práv.

Změna odpovědností a pracovního vztahu v rámci organizace by měla probíhat jako by se jednalo o odebrání odpovědností nebo ukončení pracovního vztahu, tedy tak, jak je popsáno v této kapitole. Při uzavření nového pracovního vztahu by se mělo postupovat tak, jak je popsáno v kapitole 1.1.

3.1. Odpovědnosti za ukončení pracovního vztahu

Odpovědnosti a povinnosti platné i po ukončení pracovního vztahu musí být obsaženy již ve smlouvách uzavřených s uživateli v jejich přijímacím řízení.

3.2. Navrácení zapůjčených předmětů

V rámci procesu ukončení pracovního vztahu musí uživatelé odevzdat jim svěřené prostředky zpracování dat, dokumentů a vybavení, jež jsou majetkem Sem je řazena veškerá výpočetní technika, mobilní telefon, přístupový čip, případná dokumentace a informace uložené na datových médiích.

V případě, že uživatelé mají znalosti důležité z hlediska provozování informačních systémů a tyto informace nejsou dosud zdokumentované, je třeba toto učinit před odchodem pracovníka.

3.3. Odebrání přístupových práv

Při ukončení pracovního vztahu musí být uživatelům odejmuta přístupová práva k informacím a prostředkům pro zpracování informací. Při změně pracovního vztahu musí být odebrána ta práva, která nejsou schválena jako součást nově vzniklého pracovního vztahu.

O zrušení či změnu přístupových práv žádá nadřízený pracovník u IT oddělení a to nejlépe přes helpdesk.

V případě ukončení pracovního poměru z důvodu porušení pracovní kázně a existuje-li nebezpečí poškození zájmů Společnosti, žádá nadřízený pracovník odebrání přístupových práv ještě před předáním

výpovědi a to emailem vedoucímu pracovníkovi IT oddělení.

Zároveň se zrušením přístupových práv musí být příslušnými administrátory provedeno zrušení uživatelských nastavení, díky nimž by mohly být prováděny automatické akce (přesměrování pošty, spuštění úloh apod.).

2. Fyzická bezpečnost a bezpečnost prostředí

1. Bezpečnost zařízení

Cíl: Předcházet ztrátě, poškození nebo kompromitaci aktiv a přerušení činnosti organizace.

Zařízení by měla být fyzicky chráněna proti bezpečnostním hrozbám a působení vnějších vlivů.

Ochrana zařízení (včetně těch, která se používají mimo hlavní lokalitu) je nezbytná jak pro snížení rizika neautorizovaného přístupu k datům, tak k zajištění ochrany proti ztrátě nebo poškození. Pozornost by měla být věnována také jejich umístění a likvidaci. Na ochranu proti možnému ohrožení nebo neautorizovanému přístupu a na ochranu podpůrných prostředků, jako například dodávky elektrické energie a struktury kabelových rozvodů, mohou být požadována zvláštní opatření.

1.1. Bezpečnost zařízení mimo prostory

Zařízení pro zpracování dat Společnosti zahrnují všechny druhy osobních počítačů, mobilníchtelefonů, nosičů dat a ostatních zařízení používaných pro práci mimo prostory Společnosti (kanceláře a pracovní prostory), nebo vynášených mimo normální pracovní prostory Společnosti. Při vynášení uvedených zařízení mimo pracovní prostory je potřeba dodržovat následující pravidla:

- Mobilnímu zařízení využívanému uživatelem mimo objekty musí být věnována zvýšená pozornost z hlediska jeho ochrany (např. v autech a jiných dopravních prostředcích a veřejně přístupných místech). V takovém prostředí nesmí být přenosné zařízení ponecháno bez dohledu. Pokud je to možné, je nutné zajistit vhodné umístění např. do uzamykatelné skříňky.
- Veškeré mobilní zařízení Společnosti je nezbytné přenášet v taškách, pouzdrech a podobných a tím jej chránit před mechanickýmpoškozením.
- Uživatel musí dané zařízení Společnosti chránit před silným elektromagnetickým polem a dodržovat další bezpečnostní opatření doporučená výrobcem.
- Uživatel je povinen chránit bezpečnost všech autentizačních a autorizačních informací tj. přihlašovacích jmen, hesel a kódů, kterými je chráněn přístup k uloženým informacím Společnosti. V případě důvodné obavy z prozrazení je uživatel povinen své heslo či kód neprodleně změnit.

1.2. Přemístění majetku

Síťové a serverové zařízení nesmí být bez písemného schválení IT oddělení přemísťováno a ani sním, nesmí být nijak manipulováno. Pokud má dojít ke stěhování je nutné tuto informaci sdělit IT oddělení nejméně 30 dní předem a domluvit si následný postup přesunu zařízení.

Za vynesené technické zařízení Společnosti nese po celou dobu odpovědnost příslušný pracovník, který byl IT oddělením pověřen. O přesunu musí být pořízen záznam.

2. Řízení komunikací a řízení provozu

2.1. Ochrana proti škodlivým programům a mobilním kódům

Cíl: Chránit integritu programů a dat.

Pro prevenci a detekování škodlivých programů a nepovolených mobilních kódů jsou vyžadována patřičná opatření.

Programy a prostředky pro zpracování informací jsou zranitelné škodlivými programy, jako jsou například počítačové viry, síťoví červi, trojští koně a logické bomby. Uživatelé by měli být upozorňováni na nebezpečí neschválených a škodlivých programů.

2.1.1.Opatření na ochranu proti škodlivým programům

Pro uživatele využívající techniku společnosti platí přísný zákaz svévolné instalace, stahování a používání neschváleného programového vybavení. Veškeré programové vybavení nad rámec základní instalace (OS, kancelářské aplikace) může být nainstalováno pouze po žádosti o instalaci prostřednictvím aplikace
„Helpdesk“. Tuto žádost schvaluje oddělení IT.

IT oddělení musí vést přehled použitých licencí a v případě schválené žádosti o instalaci nad licenční rámec musí neprodleně objednat další licence v adekvátní rezervě.

Pokud je požadována instalace SW, který není ve standardní nabídce, musí být schválena instalace vedoucím IT oddělení.

Na jednotlivých pracovních stanicích musí být aplikován antivirový program v poslední verzi a nastaven následující režim kontrol:

- 1x za měsíc obsah lokálních disků.
- Při každém stahování z internetu nebo otevírání příloh emailů (kontrola příchozích dat z Internetu).
- Kontrola příloh elektronické pošty.
- Kontrola spouštěných a ukládaných souborů v reálném čase.

V případě nalezení škodlivého programu musí být antivirový program nastaven tak, aby se nejdříve pokusil infikovaný soubor vyléčit a v případě neúspěchu jej následně přesunul do tzv. karantény. Všechny antivirové programy musí být pravidelně aktualizovány v intervalech ne větších než:

- Klientské instalace (PC, notebook) 1x za den.
- Servery 1x za den.

Podmínkou pro přístup z pracovní stanice na internet je aktivovaný antivirový program.

Všichni uživatelé mají povinnost nahlásit všechny „poplašné správy“ a emaily, které varují před konkrétním virem a nejsou odeslány z IT oddělení prostřednictvím aplikace „Helpdesk“ anebo emailem.

2.2. Bezpečnost při zacházení s médii

Cíl: Předcházet neoprávněnému prozrazení, modifikaci, ztrátě nebo poškození aktiv a přerušení činnosti organizace.

Média by měla být kontrolována a fyzicky zabezpečena.

Měly by být stanoveny náležité provozní postupy týkající se zabezpečení dokumentů, počítačových médií (např. pásky, disky), vstupních/výstupních dat a systémové dokumentace před neoprávněným prozrazením, modifikací, odstraněním nebo poškozením.

2.2.1.Správa vyměnitelných počítačových médií

Jako vyměnitelná média jsou rozuměna všechna přenosná média, na která lze data ukládat - CD, DVD, flashdisky, přenosné disky, atd. Při práci s těmito médii je nutné dodržovat následující zásady:

- Všechna média musí být ukládána v prostředí dle specifikace výrobce.
- Pokud jsou znovupoužitelná média vyřazována, musí být jejich obsah bezpečně vymazán (v souladu s pravidly dle klasifikace důvěrnosti obsažených dat) ještě před jejich předáním k fyzické likvidaci. O odstranění záznamu dat a následném vyřazení z provozu musí být prováděny záznamy.
- Data, jejichž požadavek dostupnosti přesahuje životnost médií (dle výrobce) na kterých jsou uloženy, musí být včas přemístěna na úložiště splňující podmínku jejich dostupnosti.

Za nakládání s vyměnitelnými médii nenese Společnost žádnou zodpovědnost a plně za ně zodpovídá jejich uživatel.

2.2.2.Likvidace médií

Nosiče dat dále provozně neupotřebitelné musí být likvidovány s ohledem na klasifikaci důvěrnosti uložených dat. Při likvidaci musí být dodržena následující opatření:

- Bezpečnou likvidaci umožňuje přesná identifikace médií a jejich obsahu. Veškerá likvidace musí být zaznamenávána.
- V případě komplikací při vyčlenění „důvěrných“ dat musí být použita pravidla pro bezpečný sběr a likvidaci u všech médií.
- Média musí být likvidována průběžně, nejpozději při nahromadění 10 kusů k likvidaci.
- V případě, že se pro likvidaci médií využívá služeb smluvní strany, odpovídá vedoucí IT oddělení za pravidelné kontroly dodržování uvedených pravidel na straně Společnost

Za bezpečnou likvidaci ve smyslu tohoto dokumentu zodpovídá uživatel těchto nosičů dat.

2.4. Výměny informací

Cíl: zajistit bezpečnost informací a programů při jejich výměně s externími subjekty.
Výměna informací a programů mezi organizacemi by měla být založena na formální politice, prováděna v souladu s platnými dohodami a měla by být ve shodě s platnou legislativou.

Měly by být stanoveny postupy a normy pro ochranu informací a jejich nosičů při přepravě.

2.4.1.Postupy při výměně informací a programů

Informace mohou být ohroženy díky nedostatku bezpečnostního povědomí, neznalostí pravidel a postupů používání odpovídající techniky. Výměnu informací lze rozdělit do dvou kategorií:

a) Interně, kde platí, že pracovníci Společnost nesmí:
   - Vynášet přenosná zařízení z prostor Společnosti (výjimka je služební notebook).
   - Ukládat firemní informace na soukromá zařízení.

b) Mezi Společnost a externími subjekty:
   Veškeré výměny informací mezi Společnost a externími subjekty musí být dodrženy následující zásady:
   - Data musí být při přenosu nedůvěryhodnou sítí šifrována.
   - Přístup k přenášeným datům musí být řízen (např. username + heslo)Za bezpečné odesílání, resp. příjem dat zodpovídá odesilatel, resp. příjemce.

2.4.2.Bezpečnost médií při přepravě

Seznam kurýrů oprávněných přepravovat média musí schválit IT oddělení. Odpovědnost za bezpečnost přepravovaných médií má odesílatel prostřednictvím přijatých opatření.

Opatření k zajištění bezpečnosti médií během přepravy jsou následující:

- Používat se smí jen spolehlivá doprava nebo kurýr (dlouhodobě pracující pracovníci Společnosti s praxí v řízení vozidla, dlouhodobě spolupracující a důvěryhodná smluvní strana s vyhovující bezpečnostní politikou přepravy apod.).
- Obal musí médium dostatečně chránit proti fyzickému poškození (horko, vlhko, elektromagnetické pole atd.) a musí odpovídat specifikacím výrobce médií.
- U důvěrných médií musí být aplikována zvláštní opatření (uzamykatelné přepravní skříňky,

osobní doručování, balení odolné proti vniknutí nebo umožňující odhalit jakýkoliv pokus o přístup,).

2.4.3.Elektronické zasílání zpráv

Pro elektronickou komunikaci platí:

- Komunikace elektronickou poštou („email“) je povolena pouze pro účely spojené s činností společnosti.
- Textový obsah a přílohy mohou být důvěrné a mohou být chráněny právními předpisy. (např.: Obchodní tajemství)
- Pokud je do emailu vkládán podpis, musí být nastaven podle závazné podoby.
- Před odesíláním zprávy musí být zajištěno správné adresování emailu.

Veškeré zprávy zasílané emailem jsou chápány jako služební a proto mohou být monitorovány.

Pokud se při zpracování zpráv z monitoringu zjistí, že se jedná o soukromou korespondenci, musí být další zpracování dané zprávy zastaveno. Obecně musí být veškerá komunikace chráněna proti neoprávněnému přístupu, modifikaci nebo odmítnutí služby. Za bezpečnost elektronické komunikace odpovídá odesílatel.

2.5. Monitorování

Cíl: Detekovat neoprávněné zpracování informací. Systémy by měly být monitorovány a bezpečnostní události zaznamenávány. Pro zajištění včasné identifikace problémů informačních systémů by měl být používán operátorský deník a záznamy předchozích selhání.

Veškeré aktivity související s monitorováním a zaznamenáváním událostí by měly být v souladu s relevantními zákonnými požadavky.

Monitorování systému umožňuje kontrolování účinnosti přijatých opatření a ověření souladu s modelem politiky řízení přístupu.

2.5.1.Zaznamenávání událostí

Pro monitorování řízení přístupu a všech bezpečnostně důležitých stavů/činností musí být pořizovány auditní záznamy. Tyto záznamy jsou využívány při vyšetřování bezpečnostních incidentů. Dobu uchování auditních záznamů stanoví vedoucí oddělení IT.

Za pořizování a archivaci těchto dat odpovídá vedoucí pracovník útvaru spravujícího daný systém/síť/ aplikaci. Pokud je to technicky možné, systémoví administrátoři nesmí mít možnost tyto záznamy modifikovat/mazat a nebo deaktivovat vytváření záznamů.

Standardní auditní záznamy (pokud je to možné) musí obsahovat:

- Identifikátory uživatelů (ID).
- Datum, čas a popis klíčových událostí (přihlášení, odhlášení, atd.).

- Identifikátor místa z něhož byl zásah veden (PC, NTB, atd.).
- Záznam o úspěšných a odmítnutých pokusech o přístup k systému.
- Záznam o úspěšných a odmítnutých pokusech o přístup k datům a zdrojům.
- Změny konfigurace systému.
- Použití systémových aplikací a utilit.
- Soubory, ke kterým bylo přistupováno a typ přístupu.
- Sítě, ke kterým bylo přistupováno a použité protokoly.
- Alarmy vyvolané systémy pro kontrolu přístupu.
- Aktivaci a deaktivaci ochranných systémů jako jsou antivirové systémy a systémy detekce průniků.
-

2.5.2. Monitorování používání systému

Úroveň monitorování stanovuje vedoucí oddělení IT, přičemž musí vycházet z hodnocení rizik. Obecně se musí monitorovat:

- Přihlášení a odhlášení do/z aplikace/systému/sítě.
- Neautorizovaný přístup (včetně informací jako uživatelské ID, datum a čas klíčové události, druh události, soubory dat, ke kterým bylo přistupováno, použité programy/ nástroje, ..).
- Privilegované operace (použití privilegovaných účtů (root, administrator apod.), spuštění a ukončení systému, připojení a odpojení vstupně/výstupních zařízení, ..).
- Pokusy o neoprávněný přístup (neúspěšné/odmítnuté aktivity uživatelů, neúspěšné/ odmítnuté pokusy o přístup, narušení přístupové politiky a upozornění od síťových bran, proxy a firewallů, varování od IDS/IPS, ..).
- Systémová varování nebo chyby (zprávy nebo varování z konzole, výjimky v systémových záznamech, alarmy správy sítě, alarmy spuštěné systémy pro kontrolu přístupu, ..).
- Změny/pokusy o změnu bezpečnostních opatření a nastavení bezpečnosti systému.

Výstupy monitorování musí být pravidelně kontrolovány. Za kontrolní činnost odpovídá vedoucí oddělení IT.

2.5.3. Záznam selhání

U všech systémů, které to umožňují, musí být aktivováno zaznamenávání selhání/poruch. Rozsah zaznamenávání musí být stanoven na základě hodnocení rizik a schválen IT oddělením. Zjistí-li uživatel, že programové vybavení funguje chybně, musí tuto chybu oznámit prostřednictvím aplikace
„Helpdesk“.

Řešení problému se poté řídí pravidly Helpdesku, který nese odpovědnost za zaznamenání problému a průběhu jeho řešení.

3. Řízení přístupu

3.1. Požadavky na řízení přístupu

Cíl: Řídit přístup k informacím. Přístup k informacím, prostředkům pro zpracování informací a procesům organizace by měl být řízen na základě provozních a bezpečnostních požadavků. V úvahu by se měla brát pravidla organizace pro šíření informací a pravidla, podle nichž probíhá schvalování.

3.1.1.Politika řízení přístupu

Řízení přístupu se obecně odehrává na úrovni přístupu k datům, nebo k systémům, sítím, aplikacím, funkcím aplikací a funkcím aplikací. Přístup k informačním systémům, aplikacím, sítím a datům

Společnosti musí vycházet z definovaných provozních a bezpečnostních rolí, na základě nichž uživatel k datům přistupuje. Popis rolí a jejich oprávnění musí být obsažen v dokumentaci k aplikaci/systému.

Za přidělená práva u svých podřízených odpovídají příslušní vedoucí pracovníci.

Vlastník dat musí s ohledem na bezpečnostní požadavky jednotlivých aplikací jasně stanovit pro uživatele resp. skupinu uživatelů seznam informací a procesů, ke kterým mají povolen přístup a jaká úroveň oprávnění je uživateli přidělena. Při stanovování přístupu je nutné uplatňovat pravidla „nejmenšího nutného oprávnění“ a „všechno, co není výslovně povoleno, je zakázáno“. Dále je nutné striktně reflektovat požadavky vyplývající z klasifikace informačních aktiv, ke kterým má pracovník Společnosti získat přístupová oprávnění.

Standardním procesem je přiřazení rolí, jejichž práva schválil vlastník dat. Přiřazení do role provádí přímý nadřízený uživatele. Pokud role neexistuje, musí být vytvořena, nebo musí být přístup schválen vlastníkem dat. Souhlas vlastníka s takovýmto přístupem musí být zadokumentován.

Pro běžné kategorie činností musí vedoucí pracovníci prosazovat využívání standardizovaných přístupových profilů, t.j. pokud pro roli konkrétního uživatele je dostačující již existující profil, musí mu tento profil být přidělen. Pokud není ani jeden z již existujících profilů vyhovující pro činnost daného uživatele, jeho přímý nadřízený musí specifikovat veškeré dodatečné požadavky nad rámec standardního profilu. Tyto požadavky následně předá prostřednictvím aplikace Helpdesk na oddělení IT. Vedoucí tohoto oddělení po schválení daného přístupu předá žádost k vyřízení konkrétnímu správci.

Provozní požadavky pro přístup, t.j. místa a zařízení, ze kterých mají uživatelé přístup k informačním systémům, aplikacím, sítím a datům Společnosti, jim sdělí jejich přímý nadřízený, případně pracovníci oddělení IT.

Vedoucí pracovníci útvarů spravujících přístupy mají odpovědnost za konzistenci přístupů v jejich správě.

V stanovených intervalech (standardně 1x za 6 měsíců u běžných účtů a 1x za 2 měsíce u privilegovaných účtů) musí vedoucí pracovníci provést kontrolu a následnou aktualizaci přidělených přístupových práv.

3.2. Řízení přístupů uživatelů

Cíl: Zajistit oprávněný přístup uživatelů a předcházet neoprávněnému přístupu k informačním systémům. Měly by existovat formální postupy pro přidělování uživatelských práv k informačním systémům a službám.

1.1.1.1 Postupy by měly pokrývat všechny fáze životního cyklu přístupu uživatele, od prvotní registrace nového uživatele až po konečné zrušení registrace uživatele, který přístup k informačním systémům a službám již dále nepotřebuje. V případě nutnosti by měla být věnována zvláštní pozornost potřebě řídit přidělování privilegovaných přístupových oprávnění, která umožňují uživatelům překonat kontroly v systému.

4.2.1 Registrace uživatele

Registrace uživatele spočívá ve vytvoření identifikátoru uživatele (ID) a založení základních přístupových účtů do IS.
Pro každého uživatele musí existovat unikátní identifikátor – přístupový účet (přihlašovací jméno a heslo) a pokud je to možné, musí být aktivován audit všech úkonů definovaných požadavky na monitoring.

Přístup k dalším informačním systémům a službám je možný pouze na základě schválené žádosti přímého nadřízeného (resp. odpovědné osoby oddělení IT) a pokud je to možné, musí být vázán účet daného uživatele. Přístup je přidělován v rámci uživatelské role, která je v aplikaci definována.

Pokud stanovené role neumožní výkon pracovní funkce, je možné žádat o individuálně nastavený přístup do IS. Žádost s uvedením práv, která uživatel potřebuje zpřístupnit, v tomto případě schvaluje přímý vedoucí a vlastník dat daného systému/aplikace.

Při nástupu pracovníka či změně jeho pracovních činností je mu přímým nadřízeným předán přehled všech přidělených přístupů. Uživatel v té souvislosti podepíše prohlášení, že rozumí jejich rozsahu. Po jednom vyhotovení podepsaného prohlášení obdrží uživatel i jeho nadřízený.

Uživatel se nesmí pokoušet o přístup do systémů/aplikací, které jsou nad rámec tohoto seznamu. Takový čin může být chápán jako narušení pracovní kázně zvlášť hrubým způsobem.

Datum vytvoření, změny nebo zrušení přístupu, jméno uživatele a typ přístupu musí administrátor spravující z hlediska přístupů daný systém/aplikaci evidovat. Při změně potřeb přístupu uživatele (např. změna pracovního zařazení) musí jeho přímý nadřízený coby žadatel nahlásit novou potřebnou úroveň přístupu a den jeho účinnosti v aplikaci Helpdesk.

Po ukončení potřeby uživatele pracovat se zpřístupněným systémem či službou, musí o této

skutečnosti informovat příslušný nadřízený uživatele prostřednictvím aplikace Helpdesk. Administrátor na základě této informace musí ve lhůtě vyplývající z příslušné normy danému uživateli odebrat přístupová práva a tuto skutečnost zaznamenat.

Po ukončení používání IS uživatelem se účty (se statusem Disable) nesmí ze systému odstranit, ani přiřadit jinému uživateli po dobu 5 let.

1. Řízení privilegovaného přístupu

Privilegiem se rozumí přístup ke speciální funkci nebo prostředku umožňujícímu překonat systémové či aplikační kontroly (například převzetí vlastnictví, přímý a neomezený přístup k informacím/datům).

Administrátor IS (OS, DB, aplikace, služby, ...) musí vést evidenci všech přidělených privilegií pro daný IS.

Přidělení privilegia musí případ od případu schválit na návrh provozovatele vlastník dat a to pouze v případech, kdy je to z provozních či bezpečnostních důvodů nutné. Privilegia nesmí být poskytnuta dokud není jejich přidělení schváleno vlastníkem.

Pokud je to možné, musí být privilegium poskytnuto takovému účtu (ID), který není současně využíván pro běžnou práci uživatele.

2. Správa uživatelských hesel

U všech generovaných hesel (i dočasných) je nutné dbát na jejich bezpečnost a integritu. Uživatel musí prvotní heslo neprodleně změnit.

Nová, dočasná nebo náhradní hesla mohou být uživateli předána pouze po jeho jednoznačné identifikaci – např. telefonicky prostřednictvím přímého nadřízeného nebo jeho asistentkou.

Pokud je nutné ukládání hesel v počítači, musí být tato skutečnost ošetřena nastavením systému provozovatelem s využitím šifrovacích technik.

Přednastavená hesla (např. výrobcem) musí být ihned po instalaci změněna a nevyužívané účty musí být ihned po instalaci zablokovány.

Pro přihlášení se do systému/aplikace (minimálně na úrovni přihlašovací jméno + heslo) je připuštěna i forma autentizace pomocí HW autentizačních prostředků (tokeny, ..).

2. Odpovědnosti uživatelů

Cíl: Předcházet neoprávněnému uživatelskému přístupu, prozrazení nebo krádeži informací a prostředků pro zpracování informací.

Pro účinné zabezpečení je nezbytná spolupráce oprávněných uživatelů.

Uživatelé by si měli být vědomi odpovědnosti za dodržování účinných opatření kontroly přístupu, zejména s ohledem na používání hesel, a bezpečnosti jim přidělených prostředků.

Pro snížení rizika neoprávněného přístupu (nebo poškození) k dokumentům, médiím a prostředkům pro zachování informací, by měla být zavedena zásada prázdného stolu a prázdné obrazovky monitoru.

2.1. Používání hesel

Pokud je to možné, musí být aplikace/systémy IT nastaveny tak, aby sami požadovaly kvalitu hesla charakterizovanou níže uvedenými pravidly. V případech kdy to není možné zajistit, musí uživatel při výběru a sestavování hesel dodržovat následující pravidla:

- Minimální délka hesla je 8 znaků.
- Heslo musí být sestaveno jako kombinace číslic a písmen (měla by být použita malá i velká písmena).
- Jako heslo je zakázáno používat prázdný text, opakující se jedno písmeno nebo číslice, přihlašovací jméno, příjmení nebo křestní jméno v jakékoliv podobě, jméno partnera, dětí nebo lehce zjistitelné osobní údaje, (rodné číslo, telefonní číslo, registrační značka automobilu, ulice bydliště atd.), či běžná slova nacházející se v slovnících.
- Heslo se nesmí opakovat dříve než po jeho páté změně.
- Platnost hesla by neměla přesahovat dobu 3 měsíců, u privilegovaných účtů 1 měsíc. Pokud není IS nastaven tak, aby uvedenou dobu expirace sám vynucoval, je uživatel povinen v těchto intervalech hesla měnit sám.
- Pokud uživatel používá několik různých systémů/služeb/aplikací a potřebuje více hesel, může pro všechny používat jedno silné heslo pouze v případě, že splňuje všechny výše uvedené požadavky.
- Heslo si uživatel musí pamatovat, nesmí ho sdělovat jiným osobám.

2.2. Neobsluhovaná uživatelská zařízení

Všechna IT zařízení umístěná v prostorách s přístupem dalších osob musí být chráněna před neautorizovaným přístupem. V době kdy PC či NTB uživatel nepoužívá, musí být aktivován bezpečnostní mechanizmus (uzamčení klávesnice, spuštění spořiče obrazovky s heslem a pod.).

Při ukončení spojení se systémem/aplikací se uživatel musí předepsaným způsobem korektně odhlásit.

Při ukončení práce (odjezd na jiné pracoviště, odchod domů apod.) musí uživatel ukončit všechna spojení k systémům/aplikacím a pokud počítač nevypíná, musí aktivovat bezpečnostní

mechanizmus.

Za splnění výše uvedených požadavků se považuje využití spořiče obrazovky opatřeného heslem spouštěného automaticky po 10 minutách nečinnosti.

Za dodržování těchto pravidel odpovídá každý uživatel daného zařízení, které mu bylo přiděleno pro výkon pracovních činností.

4.3.3 Zásada prázdného stolu a prázdné obrazovky monitoru

Pracovní dokumenty a materiály nesmí být ponechány volně bez dozoru. V případě že se právě nepoužívají (zejména je-li kancelář prázdná), musí být uloženy v uzamykatelné skříni.

Všichni uživatelé jsou povinni zajistit, aby monitory jejich počítačů v době, kdy nejsou používány, byly prázdné (nezobrazovaly žádné informace).

3. Řízení přístupu k síti

Cíl: Předcházet neautorizovanému přístupu k síťovým službám.
Přistup k interním i externím službám by měl být řízen.
Je to nezbytné pro zajištění toho, aby uživatelé mající přístup k sítím nebo síťovým službám neohrožovali bezpečnost těchto služeb. K tomu je potřeba:
a/ vhodné rozhraní sítě organizace se sítěmi jiných organizací nebo veřejnými sítěmi.
b/ odpovídající autentizační mechanizmus pro uživatele a zařízení.
c/ řízení přístupu uživatelů k informačním službám.

3.1. Politika užívání síťových služeb

Uživatelé smí využívat přímý přístup pouze k těm síťovým službám, resp. segmentům sítě společnosti, které jsou pro jejich plnění pracovních povinností nezbytné. O svých oprávněních přístupu k sítím a službám je uživatel informován svým nadřízeným.

Odpovědnost za využití kontrolních prostředků na monitorování přístupů do sítí nese pracovník oddělení IT, který odpovídá za správu síťových služeb. Za ochranu vnitřní sítě Společnosti a její vymezení od veřejných sítí odpovídá vedoucí IT oddělení.

Počítače (PC i notebooky) se musí připojovat do sítě Společnosti pouze prostřednictvím dodaného a schváleného hardware. Uživatel nesmí používat cizí nebo soukromé modemy, přístupové body apod.

Konkrétní nastavení přístupů a úrovně logování služeb je v kompetenci příslušných provozovatelů systémů/aplikací, přičemž musí splňovat standardní požadavky uvedené v politice řízení přístupů

5. Mobilní výpočetní prostředky a práce na dálku

Cíl: Zajistit bezpečnost informací při použití mobilní výpočetní techniky a při využití prostředků pro práci na dálku.

Požadovaná ochrana by měla odpovídat rizikovosti těchto specifických způsobů práce. Při použití mobilních výpočetních prostředků by mělo být zváženo riziko práce v nechráněném prostředí a měla by být zajištěna vhodná ochrana. V případě práce na dálku by měla být zavedena ochrana na místě výkonu práce a měly by být zajištěny vhodné podmínky pro tento způsob práce.

5.1. Mobilní výpočetní prostředky a sdělovací technika

Mobilní zařízení (notebook, mobilní telefon apod.) jsou vydávána uživatelům na základě žádosti příslušného nadřízeného pracovníka……Převzetí tohoto zařízení uživatel potvrdí svým podpisem.

Za bezpečnost mobilního zařízení odpovídá uživatel, kterému bylo zařízení svěřeno k používání. Toto zařízení smí být používáno jen za účelem, za kterým bylo uživateli přiděleno. Krádež nebo ztrátu takového zařízení musí uživatel neprodleně hlásit prostřednictvím aplikace Helpdesk a musí dojít k zablokování přístupových kanálů, jako např. VPNky.

Zvýšená pozornost musí být uživatelem takového zařízení věnována jeho ochraně v nechráněných prostorách mimo Společnost, např. v autech a jiných dopravních prostředcích, hotelích, konferenčních a zasedacích místnostech apod. V takto rizikových prostředích nesmí být přenosný počítač ponecháván bez dohledu. Uživatel je povinen zabránit odpozorování všech autentizačních a autorizačních informací – přihlašovacích jmen a hesel, kterými je chráněn přístup neautorizovaných osob k uloženým informacím.

Připojení přenosného počítače do jiných (neprověřených) než podnikových sítí Společnosti je možné za podmínky instalace personálního firewallu na PC.

Důvěrné informace uchovávané v souborech aplikací typu MS Word, MS Excel apod. musí být na mobilních zařízeních chráněny šifrováním na úrovni HDD.

Uživatel přenosného zařízení je povinen zajistit bezpečné odstranění důvěrných dat, které již nevyužívá jejich vymazáním – soubory nesmí být ponechány v „koši“. Pracovní soubory je uživatel povinen zálohovat (alespoň 1x za týden) do sdílené síťové složky, případně na vyhrazená archivní zařízení a média Společnosti.

5.2. Práce na dálku

Pro práci na dálku (mimo prostory Společnosti) je nutný přístup přes VPNku. Nastavení/instalace VPNky je závislé na splnění odpovídajících bezpečnostních požadavků NTB/PC (poslední aktualizace Windows /jiný operační systém, aktuální antivirové definice.)

Za dodržení všech podmínek práce z domova odpovídá uživatel.

2. Nákup, vývoj a údržba informačního systému

1. Kryptografická opatření

Cíl: Ochránit důvěrnost, autentičnost nebo integritu informací s pomocí kryptografických prostředků.

Měla by být vytvořena pravidla pro použití kryptografických opatření. K podpoře používání kryptografických technik by měl v organizaci existovat systém jejich správy.

1.1. Politika pro použití kryptografických opatření

Kryptografická opatření se standardně používají k ochraně důvěrných informačních aktiv a to i na mobilních počítačových/komunikačních zařízeních, pokud je to technicky možné.

Jejich využití je vhodné i při aktivitách, u kterých je nutné dosáhnout vysoký stupeň důvěrnosti, integrity/autentičnosti nebo nepopiratelnosti.

Každé použití kryptografických prostředků/metod musí být schváleno vedoucí oddělení IT.

Za bezpečnost privátních klíčů a klíčů pro symetrické šifrování mají odpovědnost jejich uživatelé.

1.2. Správa klíčů

- Pro klíče, které se používají v rámci Společnosti platí:
- Všechny klíče musí být chráněny před modifikací, zničením a prozrazením.
- Prostředky pro generování, ukládání a archivaci klíčů musí být zabezpečeny fyzickou ochranou (v zabezpečené zóně, na zabezpečeném PC apod.).
- Minimální akceptovatelná délka klíče pro asymetrické šifrování je 1024 bitů, prosymetrické šifrování 128 bitů.

Za použití klíčů z externích CA odpovídají jednotliví uživatelé.

6. Zvládání bezpečnostních událostí

6.1. Hlášení bezpečnostních událostí a slabin

Cíl: Zajistit nahlášení bezpečnostních událostí a slabin ve vztahu k informačnímu systému způsobem, který umožní včasné zahájení kroků vedoucích k nápravě.

Měly by být ustaveny formální postupy pro hlášení bezpečnostních událostí a pro zvyšování stupně jejich důležitosti. Všichni zaměstnanci, smluvní strany a uživatelé třetích stran by měli znát postupy hlášení různých typů událostí a slabin, které mohou mít dopad na bezpečnost aktiv organizace. Zjištěné bezpečnostní události a slabiny by měli pracovníci ihned hlásit na určené místo.

6.1.1. Hlášení bezpečnostních událostí

Všichni uživatelé mají povinnost neodkladně ohlásit zjištěnou bezpečnostní událost. Jakékoli chybné, nebo jiné neobvyklé chování systému může být příznakem pokusu o narušení nebo útoku na bezpečnost a mělo by tedy být nahlášeno jako bezpečnostní událost.

Prvotní informaci o této události předá uživatel oddělení IT.

Příklady bezpečnostních událostí a incidentů:

- Ztráta prostředků nebo vybavení.
- Chybné fungování nebo přetížení systému (chování odlišné od popisu v dokumentaci).
- Lidské chyby.
- Nesoulad s politikami nebo směrnicemi.
- Chybné fungování technického a programového vybavení (chování odlišné od popisu v dokumentaci).
- Neautorizovaný přístup nebo jeho pokus do IS nebo k datům.

6.1.2 Hlášení bezpečnostních slabin

Bezpečnostní slabinou se rozumí takové chování systému IT, které dovolí obejít přijaté bezpečnostní nastavení. Všichni uživatelé mají povinnost neprodleně ohlásit jakákoliv zjištěná nebo možná podezření na bezpečnostní slabiny v systémech nebo službách. Neoprávněné testování bezpečnostních slabin bude kvalifikováno jako snaha o zneužití systému.

1. Soulad s požadavky

1.1. Soulad s právními normami

Cíl: Vyvarovat se porušení norem trestního nebo občanského práva, zákonných nebo smluvních povinností a bezpečnostních požadavků.

Návrh, provoz a používání informačních systémů může být předmětem zákonných, podzákonných nebo smluvních bezpečnostních požadavků.

Specifické požadavky vyplývající ze zákona by měly být konzultovány s právními poradci organizace nebo jinými kvalifikovanými právníky. Legislativní požadavky na informace vzniklé v jedné zemi a přenášené do jiné země jsou různé a mění se podle jednotlivých zemí.

1.1.1. Ochrana osobních údajů a soukromí

Veškeré osobní informace o pracovnících Společnosti (včetně údajů z životopisů uchazečů o práci ve Společnosti) mohou být zpřístupněny pouze oprávněným osobám.

Všichni pracovníci Společnosti a smluvní strany jsou povinni chránit tato data před neautorizovaným přístupem a prozrazením.

1.1.2. Prevence zneužití prostředků pro zpracování informací

Přístup k IS nebo datům je řízen na úrovni udělených přístupových oprávnění. Jiné neautorizované přístupy včetně pokusů o ně nejsou dovoleny.

Neautorizovaným uživatelům je zakázáno používat nástroje, s jejichž pomocí je možné provést pokusy o překonání bezpečnostních mechanismů (např. programy pro odhalení hesel, sledování sítě, nástroje pro auditování a pod.).

Užívání výpočetní techniky je povoleno pouze pro výkon pracovních činností.

Porušení výše uvedených pravidel uživatelem může být hodnoceno jako závažný bezpečnostní incident a závažné porušení pracovní kázně.

2. Soulad s bezpečnostními politikami, normami a technická shoda

Cíl: Zajistit shodu systémů s bezpečnostními politikami organizace a normami.

Bezpečnost informačních systémů by měla být pravidelně přezkoumávána.

Tato přezkoumání by měla být prováděna proti příslušným bezpečnostním politikám. Jednotlivé technické platformy a informační systémy by měly být auditovány, zda odpovídají relevantním bezpečnostním normám a opatřením.

2.1. Shoda s bezpečnostními politikami a normami

Vedoucí pracovníci jsou povinni v rozsahu své odpovědnosti:

- Zajistit, aby v jimi řízených oddělení byly požadavky bezpečnostní politiky zavedeny a správně prováděny.
- Pravidelně kontrolovat dodržování těchto požadavků.

Pokud bude v rámci kontroly zjištěno, že stanovené pracovní postupy vedou k nedodržování bezpečnostních požadavků, musí odpovídající vedoucí pracovníci tuto skutečnost neprodleně hlásit prostřednictvím aplikace Helpdesk. Na základě tohoto hlášení bude řešeno nápravné opatření.

V rámci své činnosti oddělení IT vytváří a dále aktualizuje plán kontrol dodržování zásad bezpečnostní politiky ve společnosti. Periodicita prověřování jednotlivých okruhů uvedených v tomto dokumentu je závislá na hodnocení jejich závažnosti.