Projekt je financován z prostředků Evropského sociálního fondu prostřednictvím
Operačního programu Lidské zdroje a zaměstnanost a jiných národních veřejných finančních prostředků

Projekt: Koordinační centrum pro zavádění e-GOV v územní veřejné správě **Reg. č.: CZ.1.04/4.1.00/62.00011**

Koncepční dokument pro oblast řízení a koordinaci e-GOV:

Koncepce bezpečnosti dat a informací

05. 09. 2013

OBSAH

SEZNAM ZKRATEK

Níže uvedený seznam je výčet zkratek, které jsou použity v dokumentu **Koncepce bezpečnosti dat a informací**. Uvedené zkratky jsou řazeny abecedně.

Zkratka	Vysvětlení zkratky
apod.	a podobně
atd.	a tak dále
COBIT	Control Objectives for Information and Related Technology
e-GOV	Elektronizace služeb veřejné správy
HW	Hardware
ICT	Informační a telekomunikační technologie
ID	Identifikátor
IP	Internetový protokol
IS	Informační systém
ISO	International Organization for Standardization
např.	například
PC	Osobní počítač
Sb.	Sbírka zákonů
SW	Software

POUŽITÉ POJMY

Níže uvedený seznam je výčet pojmů, které jsou použity v dokumentu **Koncepce bezpečnosti dat a informací**. Uvedené pojmy jsou řazeny abecedně.

Pojem	Vysvětlení/význam pojmu
Business Continuity	Kontinuita činností organizace je chápána jako strategická a taktická způsobilost organizace být připraven a reagovat na incidenty a narušení činností organizace za účelem pokračování v činnosti po vypořádání incidentu na předem stanovené přijatelné úrovni.
Disaster Recovery	Proces obnovy stavu organizace po katastrofické ztrátě dat a informací.
Hrozba	Jakýkoli fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné organizací.
Identita	Jednoznačné určení jedinečného subjektu (objektu).
Informační aktivum	Zpracované informace a data, které organizace využívá ke své činnosti.
Kontingenční opatření	Plánované opatření, které vede k nápravě nebo zmírnění důsledků rizikové události, jež skutečně nastala.
Oprávnění	Systém pověření, pod kterými může uživatel pracovat.
Preventivní opatření	Soustava opatření, která mají předcházet nějakému nežádoucímu jevu.
Riziko	Neurčitá událost nebo podmínka, která pokud nastane, má negativní vliv na dosažení cílů organizace (riziko znamená určité nebezpečí a pravděpodobnost nezdaru).
Zranitelnost	Míra tolerance vůči hrozbám.

1 ÚVODNÍ INFORMACE

Předmětem tohoto koncepčního dokumentu jsou doporučení v oblasti bezpečnosti dat a informací informačních systémů e-GOV, pokud již není oblast bezpečnosti dat a informací v organizaci uchopena jinak.

Hlavní cíle opatření v oblasti bezpečnosti dat a informací lze rozdělit do oblastí:

- Zabezpečení infrastruktury a přístupu do ní:
  - řízení přístupů interních uživatelů,
  - řízení přístupu externistů (dodavatelů),
  - pravidla pro přístup mobilních zařízení,
  - pravidla vzdáleného přístupu.
- Základní a zvýšená ochrana dat:
  - dostupnost dat v IS e-GOV - data v IS e-GOV jsou k dispozici vždy, když jsou oprávněně autorizovaným uživatelem vyžadována,
  - důvěrnost dat v IS e-GOV - data v IS e-GOV jsou chráněna před neautorizovaným přístupem, rozšiřováním, modifikací a před ztrátou či zničením dle principu identifikace, autentizace a autorizace uživatele,
  - integrita dat v IS e-GOV - data v IS e-GOV jsou autentická, přesná a úplná,
  - garance původu dat v IS e-GOV – data v IS e-GOV mají svého vlastníka (autora), který je za ně odpovědný, a kterého lze vždy dohledat,
  - ochrana proti neoprávněné manipulaci s daty,
  - šifrování dat,
  - ukládání, zálohování a archivace dat.
- Prvky pasivní bezpečnosti:
  - ochrana proti škodlivým programům,
  - ochrana proti nežádoucí komunikaci,
  - pravidla užívání internetu,
  - pravidla užívání elektronické pošty.
- Řešení bezpečnostních incidentů.
- Přístup do serverovny.
- Role, zodpovědnost, kompetence, kontrola, metodiky.

Základním požadavkem z hlediska řízení informační bezpečnosti je:

- identifikace aktiv (všech dat a informací v jakékoliv formě, HW, SW, prostory organizace – fyzická bezpečnost);
- jejich ohodnocení;

- analýza nežádoucích stavů a rizik s nimi spojených.

Rizikům je nutné nastavit bezpečnostní protiopatření, a poté rizika prokazatelně řídit – eliminovat jejich příčiny a vznik.

Zajištění bezpečnosti dat a informací je vhodné řídit interními dokumenty, směrnicemi a nařízeními na jednotlivých krajích, pokud tomu již tak není. Doporučením je řízení zahrnout do organizačního řádu a tímto stanovit jednoznačnou odpovědnost vedoucích zaměstnanců za bezpečnost a ochranu dat a informací. Současně dokumentované postupy slouží jako nástroj ověřování shody skutečné činnosti organizace s očekáváním.

Politika informační bezpečnosti je potom nezbytným předpokladem pro účinnost řízení bezpečnosti dat a informací. Aby mohla plnit svůj účel, musí:

- mít písemnou formu,
- být závazná v celé organizaci, platit pro všechny odbory, zaměstnance a vedoucí pracovníky,
- být známá všem, koho se týká (např. i externím pracovníkům a společnostem),
- být schválena na úrovni vrcholového vedení organizace.

Dalším doporučením je seznámit se s mezinárodními standardy v oblasti řízení bezpečnosti, např. ISO normami řady 27000 nebo souborem praktik COBIT, a individuálně implementovat vhodná opatření, pokud již nejsou implementována.

2 VYMEZENÍ ROZSAHU

Hlavní směr koncepce bezpečnosti dat a informací je tedy vytvářen:

- Zpracováním dokumentace k bezpečnosti informací – **stanovení cílů a politik, základních rámcových pravidel** a **postupů bezpečnosti informací**. Takto dokumentovaná pravidla musí odpovídat potřebám organizace a musí být ve shodě se strategickými záměry.
- **Identifikací aktiv, hrozeb a zranitelností** – identifikace všech aktiv, hrozeb a zranitelností vztahující se k předmětné organizaci. Jedná se o "inventuru" **všech aktiv, které mají nějaký vliv na činnost organizace.**
- **Ohodnocením aktiv** – určování **významu aktiv pro organizaci** z hlediska potřebnosti (podmínka realizovatelnosti procesů) a přínosů (podpora rozhodování). Hodnota aktiva odráží míru důležitosti pro fungování organizace.
- **Ohodnocením hrozeb** – určení **možnosti výskytu u jednotlivých identifikovaných hrozeb**. Hrozby lze rozdělit na personální, organizační, technické, přírodní, společenské apod. Hodnota hrozeb vychází například z počtu výskytů za období.
- **Ohodnocením zranitelností** – určení míry dopadu na činnosti organizace. Dělí se stejně jako hrozby do skupin, hodnota se určuje podle míry dopadu splnění hrozby.
- **Stanovením míry rizika** – určení rizik a míry hodnot rizika k jednotlivým aktivům, hrozbám a zranitelnostem. Míra rizika se určuje jako číselná hodnota z důvodu objektivnosti a měřitelnosti.
- **Definicí protiopatření k rizikům** dle míry hodnot rizika – cílem je stanovení takového protiopatření, které eliminuje dané riziko.
- **Řízením rizik v reálném čase** – stanovení postupů k eliminaci vysokých měr hodnoty rizika. V praxi probíhá prostřednictvím plánu zvládání rizik, ve kterém jsou všechna rizika s protiopatřeními, mírami rizika, termíny, odpovědností a ověřením účinnosti.
- **Měřením účinnosti** – průběžné měření účinnosti nastavených procesů a protiopatření. Jde o pravidelné kontroly, které prokazují, zda zavedená pravidla fungují správně. Pokud ne, kontroly zjistí důvod, a poté jsou stanovena opatření k nápravě tak, aby došlo k navrácení plánované úrovně bezpečnosti informací.

3 BEZPEČNOSTNÍ POLITIKA

K základním principům náležité správy služeb e-GOV patří zachování jejich požadovaného stavu a ochrana souvisejících aktiv organizace před hrozbami. Proto je zapotřebí nastavit, případně zdokonalit systémy informační bezpečnosti organizace (nejen v oblasti ICT), a poté efektivně řídit identifikovaná informační rizika vzhledem k poskytovaným službám e-GOV (a hlavním procesům organizace).

K tomu slouží dokument Bezpečnostní politika organizace, který by po schválení vrcholovým vedením organizace měl být závazný pro celou organizaci.

3.1 Vymezení rozsahu a oblastí

- **Fyzická bezpečnost** – zajištění bezpečnosti skutečného místa fyzického umístění HW a v něm uložených dat:
  - zajištění proti pohromám a živlům (požár, povodeň,…);
  - zabezpečený fyzický přístup;
  - zajištění proti poruchovosti zařízení pro ukládání dat, aplikací a IS;
  - umístění serverů výhradně do serveroven;
  - vstupní karty, klíče, návštěvy, volný pohyb osob.
- **Úložiště dat**
  - práce s daty, ukládání dat v datové struktuře;
  - u vybraných dat zabezpečený archiv.
- **Zálohování a archivace dat**
  - zálohování je aplikováno pro uchovávání operativních dat umožňujících rychlou obnovu v případě nežádoucího incidentu;
  - archivace uchovává historická data pro požadované či chtěné dohledávání původních dat včetně řízených zápůjček.
- **Řízení pohybu dat** – stanovení řízení pohybu dat, manipulace s nimi, sledování jejich pohybu, autorizace přístupu k nim apod.
- **Zajištění před krádeží dat** – opatření zabraňující neřízenému pohybu (úniku) a zneužití dat.
- **Řízení přístupu** k systémům, aplikacím a datům samotnými uživateli:
  - jednotná identifikace uživatele;
  - hesla;
  - anonymní účty;
  - připojení systémů do vnitřní sítě;
  - zamykání přístupu k počítačům (koncovým zařízením).
- **Identity management** – systém řízení přístupových práv.

- **Konfigurační databáze –** systém správy objektů.
- **Monitoring uživatelů a procesů** – nastavení systému sledujícího pohyb dat uživateli s možností zpětného dohledání a kontroly.
- **Externí přístup k datům** – pravidla pro přístup z externích sítí do infrastruktury a naopak, včetně mobilních zařízení.
- **Přístup externistů** k datům ze zvolených (i mobilních) zařízení:
  - ochrana informací – dohoda o mlčenlivosti;
  - povinnosti třetích osob.
- **Pravidla používání SW**
  - užívání SW oprávněnými uživateli;
  - užívání řádně nabytého SW.
- **Pravidla pro soukromé využití ICT zařízení, prostor a služeb organizace**
  - poštovní služby (e-mail) pro soukromé potřeby;
  - tiskárny, kopírovací stroje, počítače, telefony a další komunikační prostředky;
  - zařazování vlastních prostředků do infrastruktury organizace.
- **Zabezpečení před viry a zákeřným SW** – opatření ochraňující ICT prostředky před útoky zvenčí a před narušením dat.
- **Patch management** – pravidelné aktualizace SW udržujícího informační systémy zabezpečené proti nejnovějším hrozbám,
- **Řízení změn v síťové infrastruktuře**
  - zapojení nových systémů do infrastruktury;
  - řízení dostupnosti oprávnění pro správce systémů zařazených do infrastruktury.
- **Domény**
  - registrace a správa;
  - umístění a dostupnost;
  - editace dat.
- **Periodické kontroly a audit**
- **Školení uživatelů** – informování uživatelů o důvodech existence bezpečnostních pravidel a způsobech jejich dodržování.

3.2 Povinnosti a odpovědnosti rolí

- **Vlastníci IS e-GOV**

Jakýkoliv IS e-GOV musí mít určeného vlastníka – garanta informací a dat (procesů a modulů IS e-GOV).

Vlastník IS e-GOV musí:

- klasifikovat informace zpracovávané v IS e-GOV,
- určovat přístupová práva jednotlivých uživatelů (dle definovaných pravidel).

Vlastník IS e-GOV je odpovědný za:

- definování zabezpečení,
- seznámení uživatele, který není zaměstnancem Kraje, s bezpečnostními pravidly před udělením přístupových práv,
- provádění pravidelných (obvykle nejméně jednou za půl roku) kontrol přístupových práv,
- odebrání přístupových práv uživatelům, kteří již přístup k dané aplikaci pro výkon své práce nepotřebují.

- **Administrátoři IS e-GOV**

Administrátoři IS e-GOV musí:

- implementovat zabezpečení aplikace,
- před uvedením každého prvku infrastruktury nebo aplikace do ostrého provozu změnit všechny přístupy nastavené dodavateli systému nebo modulu, případně vydat uživatelům pokyn pro jejich změnu při prvním spuštění.

Administrátoři IS e-GOV jsou odpovědni za:

- zabezpečení jimi spravovaných systémů a aplikací.

- **Uživatelé**

Uživatelé musí:

- dodržovat související interní normy a nařízení,
- respektovat pokyny vlastníků IS e-GOV a administrátorů,
- hlásit nepotřebnost přístupů do aplikací jejich vlastníkům (pro zrušení přístupových práv) a bezpečnostnímu manažerovi,
- směřovat jakékoli dotazy týkající se zabezpečení informací nebo modulů na administrátory nebo na vlastníky IS e-GOV (obvykle prostřednictvím odboru informatiky),

- dodržovat stupeň důvěrnosti u klasifikovaných dokumentů, tzn. nešířit nabyté informace mimo okruh lidí, kteří mají právo se s nimi seznamovat. Tato povinnost platí i po skončení pracovního poměru.

Uživatelé jsou odpovědni za:

- ochranu informací.

- **Bezpečnostní manažer**
  - Bezpečnostní manažer vytváří bezpečnostní politiku a vrcholově odpovídá za dodržování.
  - Bezpečnostní manažer je odpovědný za řízení rizik.

- **Auditor bezpečnosti**
  - Auditor bezpečnosti kontroluje dodržování souvisejících interních a externích norem a nařízení.

3.3 Pravidla pro zabezpečení systémů a aplikací

- **Řízení přístupu k systémům a aplikacím**

Přístup k systémům a aplikacím je založen na jejich potřebě pro výkon práce s ohledem na pracovní zařazení uživatele. Toto musí být bráno v úvahu při návrhu, vývoji, nastavování a udržování systémů a aplikací. Přístup k informačním aktivům je potřeba řídit na logické i fyzické úrovni. Doporučený popis logického řízení přístupu je uveden v této podkapitole.

- **Identifikace uživatele**

Všichni uživatelé se musí pro přístup do systémů a aplikací jednoznačně identifikovat.

Každý uživatel se hlásí výhradně svými identifikačními údaji.

Každý uživatel je zodpovědný za operace, které byly provedeny pod jeho identifikačními údaji.

- **Autentizace a hesla**

Hesla zajišťují řádnou autentizaci uživatelů. Autentizace slouží k ověření identity uživatele a opravňuje uživatele k získání požadovaných služeb a přístupu k aplikacím a datům. Uživatelé odpovídají za volbu a ochranu svých hesel.

Hesla musí mít minimální délku 8 znaků, obsahovat kombinaci alfanumerických a zvláštních znaků obsahovat malá i velká písmena (a, b, …, A, …, 1, 2, …, *, @, #, …). Hesla se nesmí vztahovat k práci nebo osobnímu životu (např.

registrační značka vozidla, jméno manželky, manžela, části bydliště atp.) a nesmí používat slova obsažená ve slovníku (vlastní jména, technické výrazy, atd.). Složitost hesla musí odpovídat citlivosti informace (citlivější informace = složitější heslo), ke které je přistupováno. Heslo musí být uchováno v tajnosti, nesmí být vyzrazena dalším uživatelům, nebo zapsaná na papíře.

Hesla nesmí být uchovávána v čitelné podobě v dávkových souborech, automatických přihlašovacích skriptech, makrech, zkratkových klávesách, v nechráněných systémech a všude jinde, kde by mohlo dojít k jejich odhalení.

Heslo musí být periodicky, nejméně jednou za 90 dnů, měněno. Pokud existuje jakékoli podezření, že heslo zná někdo jiný než uživatel, je uživatel povinen heslo okamžitě změnit.

Uživatelé musí mít aktivován spořič obrazovky s požadavkem opětného zadání hesla při 30 minutové nečinnosti počítače. Zároveň musí svůj počítač zamykat spořičem obrazovky vyžadujícím heslo při vzdálení se od počítače. Při odchodu domů musí uživatelé počítač vypnout. Spuštění počítače z režimu spánku (apod.) musí vyžadovat obnovení přihlášení.

Hesla musí být předávána prokazatelně, musí o tom být záznam písemný nebo elektronický s označením data, a osoby, které je heslo předáváno. Hesla nesmějí být v žádném případě sdílena s ostatními uživateli.

- **Obecné zásady zabezpečení systémů a aplikací**
  - **Jednoznačná identifikace uživatelů**

Každý uživatel používá jednoznačný identifikátor (uživatelské ID), aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti. Sdílení uživatelských ID není povoleno.

Doporučením je používat globální identity management s cílem jednoznačně identifikovat uživatele napříč informačními systémy, pokud tomu již tak není. V každém systému zabezpečeném způsobem „uživatel/heslo" musí být zajištěno, aby uživatelské jméno a heslo byly jedinečné – a měly jasnou vazbu na globální systém identifikace uživatelů.

  - **Anonymní účty**

Vytváření anonymních účtů, které nemají přímou vazbu na konkrétního uživatele, je zakázáno.

  - **Zamykání přístupu**

Pokud uživatel nemá koncovou stanici pod dohledem je povinen k ní uzamknout přístup. Na všech koncových stanicích je instalován a aktivován spořič

obrazovky, který po definované době nečinnosti tento přístup sám uzamkne. Uživatel nesmí měnit nastavení tohoto spořiče.

- **Komunikace z externích sítí do infrastruktury organizace a naopak**

Všechna připojení, která směřují z/do externích sítí (internet, bezdrátové sítě, atd.) do/z vnitřní sítě organizace, musí odpovídat platným bezpečnostním pravidlům a musí být schválena odborem informatiky.

- **Zapojení nového systému do infrastruktury**

Uživatelé nesmějí zavádět lokální počítačové sítě bez písemného souhlasu odboru informatiky. Zapojení jiného systému do systému Kraje podléhá schválení odborem informatiky.

- **Změny v síťové infrastruktuře**

Změny v počítačové síti zahrnují upgrade komunikačního softwaru (firmware komunikačních prostředků), změny konfigurací IP adres, změny konfigurací routerů a jiných aktivních prvků apod. Veškeré tyto změny musí být zdokumentovány a evidovány a současně schváleny odborem informatiky.

- **Umístění PC a serverů do serveroven**

Každý zaměstnanec má svůj počítač, který je na jeho pracovišti. Ve výjimečných případech může mít zaměstnanec nebo skupina zaměstnanců další PC/server. O umístění PC/serveru do serveroven rozhoduje odbor informatiky na základě žádosti správce daného zařízení. Odpovědnost za provoz zařízení a instalovaný SW dál zůstává na zaměstnanci.

- **Operace s přístupovými právy**
  - **Přístupová práva založena na rolích**

Základním opatřením je definice přístupových práv pomocí rolí. Pro typové uživatele jsou vytvořené jednotlivé role a těmto rolím jsou přidělena jednotlivá práva. Role jsou poté přiřazeny konkrétním uživatelům. Role tedy představují pojmenované skupiny uživatelů seskupené podle stejných práv.

  - **Požadavky na přístupy**

Požadavky na udělení přístupových práv musí být písemně předloženy ke schválení nadřízenému žádajícího uživatele.

  - **Vytváření a rušení uživatelských účtů**

V rámci maximálního rozsahu přístupových oprávnění pro danou procesní roli definuje přístupová práva přímý nadřízený uživatele. Má-li být tento rozsah

překročen a přístupová práva rozšířena i do jiných oblastí, stane se tak jedině na základě písemného souhlasu osoby, která zodpovídá za tuto oblast (oblasti).

Postup registrace je následující: Při nástupu personální oddělení spolu s nadřízeným zaměstnance specifikuje roli a předá ji odboru informatiky, který zavede přístupová práva novému zaměstnanci nebo pracovníkům smluvních třetích stran. Při rozvázání pracovního poměru zaměstnance nebo při ukončení smlouvy s třetí stranou platí podobný postup - odbor informatiky přístupy neprodleně zruší. I v případě změny (úpravy) přístupových práv se postupuje obdobně. V případě zřizování přístupu k úložištím kde jsou uložena data podléhající zvláštnímu režimu, musí být zvláštním podpisem stvrzeno, že přístup k těmto úložištím je požadován.

- **Revize přístupových práv uživatelů**

Přístupová práva uživatelů (včetně privilegovaných přístupových oprávnění) podléhají pravidelné revizi (1 x za půl roku). Zodpovědnost za provádění revize je přirazena bezpečnostnímu manažerovi. Případný nesoulad v přidělených přístupových právech se řeší požadavkem na změnu přístupových oprávnění.

- **Bezpečnostní mechanismy proti neoprávněným přístupům do systémů**

Všechny uživatelské účty, a systémové účty s přístupem k dokumentům s minimálním stupněm důvěrnosti: vysoké, musí mít nastavenou časovou platnost hesel (expirační dobu) maximálně na 90 dní. Pokud v tomto časovém úseku nedojde ke změně hesla, účet se po uplynutí expirační doby automaticky uzamkne. Uzamčený účet nedovolí další přihlášení bez změny hesla.

Ve všech systémech musí být implementována kontrola proti pokusům o uhádnutí uživatelských jmen a hesel prostřednictvím omezeného počtu pokusů o přihlášení. V případě několika neoprávněných přístupů musí dojít k automatickému uzamčení postiženého účtu. Opětovné odemknutí je v kompetenci odboru informatiky.

- **Nepovolené aktivity**

Aktivity, které zahrnují neoprávněné přístupy k systémům, aplikacím, datům, neoprávněné dešifrování, neoprávněné pořizování kopií, zatěžování systémů, zneužití počítačových a síťových systémů, a dále aktivity, které nesouvisí s pracovní činností nebo vedou k porušování interních norem či jsou v rozporu s právním řádem ČR, nejsou povoleny a mohou být posuzovány jako porušení pracovní kázně zvláště hrubým způsobem.

Zrušení přístupu do systémů v případě neoprávněného přístupu k systémům, aplikacím, datům, neoprávněného dešifrování, neoprávněného pořizování kopií,

zatěžování systémů, kompromitace počítačových a síťových systémů, neprodleně vykoná odbor informatiky po zjištění či ohlášení, následně informuje bezpečnostního manažera.

- **Internet – důvěryhodnost a obezřetnost**

Připojení k internetu ze sítě organizace je možné pouze při použití určených Proxy-serverů a/nebo firewallu. Ve veřejných sítích, jako je internet, je relativně jednoduché zaměnit identitu jednotlivých subjektů. Předtím, než uživatelé poskytnou citlivé informace třetí straně (např. obchodním partnerům při využití internetu k realizaci kontraktu), je nutné, aby uživatel nejprve ověřil identitu třetí strany, např. pomocí telefonu. Uživatelé, kteří používají internet pro nákup produktů či služeb, musí využít šifrované komunikace pomocí protokolu HTTPS (https://...).

Uživatelům je striktně zakázáno přenášet prostřednictvím internetu klasifikované informace v otevřené (nešifrované) podobě. Jedná se např. o uživatelská jména a hesla pro vstup do systémů apod.

V souvislosti s limitovaným přístupem k internetu jsou jednotlivé požadavky na webové stránky monitorovány včetně velikosti přenesených dat.

- **Používání mobilních výpočetních prostředků a práce na dálku**

Uživatel se přihlašuje uživatelským jménem a ověřuje heslem. Vzdálený přístup je umožněn pouze vybraným zaměstnancům v souladu s definovanými pravidly. Možnost využívání vzdáleného přístupu musí podléhat pravidelné revizi.

- **Monitorování přístupu k systému a jeho použití**

Monitorování aktivit uživatelů se provádí z důvodu získání důkazů pro případ výskytu bezpečnostního incidentu. K auditním záznamům má přístup jen jedna definovaná osoba, kterou je auditor bezpečnosti. Auditor bezpečnosti mimo jiné v pravidelných intervalech vyhodnocuje záznamy, vytváří přehledy o událostech a bezpečnostních incidentech. Auditní záznamy musí být uchovávány dostatečně dlouhou dobu a musí, pokud možno, obsahovat: identifikátory uživatelů (uživatelská ID), datum a čas přihlášení a odhlášení, záznam o úspěšných a odmítnutých pokusech o přístup k systému, použití privilegovaných účtů, záznam o úspěšných a odmítnutých pokusech o přístup k datům a jiným zdrojům, změny systémové konfigurace.

- **Počítačové viry**
  - **Antivirový program**

K zajištění ochrany a provozu počítačů a počítačové sítě musí být všechny počítače vybaveny schváleným antivirovým programem. Tento program musí

být použit pro prověřování všech softwarů a dat, které se do počítače dostanou jak od třetích subjektů, tak i z organizace. Uživatel nesmí žádným způsobem bránit procesu prověřování antivirovým programem.

- **Likvidace viru**

Jestliže má uživatel podezření, že byl jeho systém napaden počítačovým virem, musí ihned kontaktovat odbor informatiky. Dále postupuje uživatel podle pokynů (např. neprodleně přestane systém používat, odpojí infikovaný počítač od lokální počítačové sítě, vyčká příchodu pověřeného pracovníka, který zahájí všechny potřebné kroky pro likvidaci virové nákazy apod.).

- **Šifrování**

Šifrování je proces, pomocí něhož se skrývají citlivé informace tak, že jsou přístupné pouze oprávněným osobám. Šifrovací klíče, které se používají pro ochranu informací, jsou vždy považovány za klasifikované informace. Přístup k těmto klíčům musí být striktně omezen pouze pro osoby, které mají „právo vědět". Šifrování musí být použito u informací se stupněm důvěrnosti „*velmi vysoký*", pokud to technické možnosti umožňují.

- **Bezpečnost mobilních zařízení**

Mobilní zařízení je zakázáno půjčovat jiné osobě. Uchovávání informací v mobilních zařízeních je možné pouze v případě zajištění definované ochrany závislé na citlivosti informace. Jiné uchovávání citlivých informací v mobilních zařízeních je zakázáno.

- **Tiskárny**

V případě, že jsou tištěny klasifikované informace, nesmí tiskárny zůstat v okamžiku tisku bez dozoru osoby, která má „právo-vědět". Tisknout takové informace bez dozoru je přípustné pouze za předpokladu, že se tiskárna nachází v prostoru, kde se nemůže nacházet osoba bez „práva vědět".

- **Software**

Z důvodu omezení rizika napadení sítě, zneužití informací apod. není uživatelům dovoleno instalovat žádný software (programy), který může ohrozit funkčnost, bezpečnost či dostupnost sítě a informací. Jedná se zejména o viry, spyware, malware, programy s ad-warem, hackerské nástroje a další zákeřný software který by mohl bez vědomí uživatele odeslat informace ven ze sítě nebo jinak uškodit organizaci. Je dovoleno instalovat pouze takový software, jehož legálnost použití lze doložit.

Uživatele smí užívat software jen způsobem, který není v rozporu s příslušným licenčním ujednáním.

- **Zálohování**

  Organizace si musí být vědoma rizik spojených se ztráty informací a povinností daných zákonem č. 499/2004 Sb., o archivnictví a spisové službě v platném znění. Z tohoto důvodu se pravidelně provádí zálohy dat všech určených systémů, včetně jejich úložišť, dle interních pravidel.

- **Řízení fyzického přístupu**

  Dodavatelé, kteří se mohou samostatně pohybovat v prostorách objektů organizace, musí dodržovat definovaná pravidla chování pracovníků 3. stran za účelem zajištění služeb. Do serveroven a řídících místností mají dodavatelé přístup pouze za doprovodu pracovníků odboru informatiky.

- **Používání elektronické pošty**

  Při používání elektronické pošty je nutné být obezřetný k podezřelým zprávám. Může se jednat zejména o nevyžádané zprávy, zprávy v anglickém jazyce, od neznámého odesilatele či zprávy s přílohou, která obsahuje spustitelný kód (např. exe, com, cmd, bat a další spustitelné soubory). Vhodné je takové zprávy neotevírat. V žádném případě neotevírat nebo spouštět přílohy. V případě pochybností lze kontaktovat pracovníka odboru informatiky.

  Elektronická pošta nesmí být zneužívána, tzn. nesmí být používána k hromadnému rozesílání zpráv nesloužících k účelům organizace, používána k výdělečné činnosti ani hromadně zveřejňována.

  Obsah poštovní komunikace může být v případě vážných podezření monitorován, avšak pouze za souhlasu Bezpečnostního manažera.

4 ČINNOSTI V OBLASTI POLITIKY ŘÍZENÍ BEZPEČNOSTI

Možné činnosti v oblasti politiky řízení bezpečnosti dat a informací služeb e-GOV mohou být zejména, pokud již v rámci organizace nejsou stanoveny:

Stanovení cílů bezpečnosti dat a informací:

- provádí bezpečnostní architekt,
- bezpečnostní architekt identifikuje aktiva chráněna bezpečnostní politikou,
- bezpečnostní architekt vymezí obecné cíle bezpečnosti dat a informací, popíše je, přidělí jim příslušné atributy včetně požadovaného termínu naplnění a sestaví katalog cílů bezpečnosti.

Stanovení požadavků na bezpečnost:

- bezpečnostní architekt předá cíle bezpečnostním správcům služby e-GOV,
- bezpečnostní správci služby e-GOV pro každý cíl buď konstatují, že jejich služba e-GOV již cíl splňuje, nebo sestaví požadavky, jejichž postupným splněním bude tento cíl naplněn,
- u požadavků si stanoví dílčí termíny takové, aby byl splněn termín požadovaného naplnění cíle.

Implementace požadavků na bezpečnost:

- implementaci požadavků provádí zřizovatel služby e-GOV, provozovatel služby e-GOV nebo provozovatel počítačové sítě v závislosti na povaze konkrétního požadavku na bezpečnost služby e-GOV a na způsobu budování resp. údržby služby e-GOV,
- za implementaci požadavků zodpovídá zřizovatel služby e-GOV, provozovatel služby e-GOV nebo provozovatel počítačové sítě v závislosti na povaze konkrétního požadavku na bezpečnost služby e-GOV,
- vychází z požadavků na bezpečnost a časového harmonogramu jejich naplnění,
- dokončení implementace požadavku hlásí zřizovatel služby e-GOV, provozovatel služby e-GOV nebo provozovatel počítačové sítě bezpečnostnímu architektovi.

Audit dodržování požadavků na bezpečnost:

- provádí auditor bezpečnosti nebo externí organizace,
- prověřuje se buď konkrétní implementace požadavku na konkrétní služby e-GOV, nebo konkrétní požadavek na všech relevantních službách e-GOV nebo všechny požadavky na vybrané službě e-GOV apod.,
- z auditu se vytváří zpráva o kontrole bezpečnosti a bezpečnostních incidentech, kterou obdrží zřizovatel služby e-GOV a provozovatel služby e-GOV.

Vyhodnocení řízení bezpečnosti:

- provádí pracovník odpovědný za bezpečnost služby e-GOV,
- obvykle se provádí minimálně jednou za rok,
- součástí je vyhodnocení závěrů z provedených prověrek dodržování požadavků na bezpečnost stanovených pro danou službu e-GOV
- obvykle se současně též provede revize dlouhodobých cílů bezpečnosti a jejich aktualizace,
- vyřadí se implementované požadavky na bezpečnost,
- vytvoří se nové požadavky na bezpečnost.