Smernica
Bezpečnostná politika

pre

Centrum sociálnych služieb LETOKRUHY
Karpatská 3117/9, 010 08 Žilina

Vypracovaná v zmysle Výnosu Ministerstva financií Slovenskej republiky č. 55/2014 Z.z.
o štandardoch pre informačné systémy verejnej správy, ktorá je zosúladená s

Nariadením Európskeho parlamentu a Rady (EÚ) č. 2016/679 (GDPR) a Zákonom č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov pri prevádzke informačných systémov

Obsah:

1. Všeobecné ustanovenia

Článok 1

Účel

Smernica upravuje niektoré práva a povinnosti všetkých zamestnancov ako aj niektorých zmluvných partnerov v oblasti ochrany informačných aktív – hlavne spracúvaných osobných a iných citlivých údajov v informačných systémoch (ďalej len „IS"), ďalej ochrany a bezpečnosti majetku, informácií a ďalších hodnôt, ktoré prevádzkovateľ vlastní.
Bezpečnostná politika vychádza z výsledkov Analýzy bezpečnosti informačných aktív v IS a posúdenia rizík v Dokumentácií bezpečnostných opatrení na ochranu osobných údajov, ktoré rozširuje a dopĺňa tak, aby zodpovedali aj požiadavkám Výnosu Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy.

Článok 2

Základné pojmy a skutočnosti

Osobné údaje – sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby (ďalej len „dotknutá osoba"); identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby;
V podmienkach prevádzkovateľa sú to: všetky údaje o fyzických osobách, ktoré sú spracovávané v IS prevádzkovateľa.

Citlivé údaje – sú obchodné údaje, údaje o ekonomickej a finančnej situácii prevádzkovateľa, know-how a všetky dokumenty týkajúce sa riadenia jeho bezpečnosti a ochrany.
V podmienkach prevádzkovateľa sú to: údaje o pracovných rolách a prístupových oprávneniach používateľov IS.

Poverená osoba – každá fyzická osoba, ktorú prevádzkovateľ poveril spracovaním osobných údajov v jeho mene, pričom vykonal záznam o poverení v ktorom dokladuje, že súčasťou poverenia je oboznámenie poverenej osoby s Dokumentáciou bezpečnostných opatrení na ochranu osobných údajov prevádzkovateľa a Bezpečnostnou politikou prevádzkovateľa. Poverená osoba je prevzatím poverenia zaviazaná riadiť sa týmito dokumentami prevádzkovateľa ako aj príslušnými právnymi predpismi. Poverená osoba prichádza pri výkone svojej funkcie do styku s osobnými údajmi v rámci svojho pracovného pomeru, štátnozamestnaneckého pomeru, služobného pomeru, členského vzťahu, na základe poverenia, zvolenia alebo vymenovania, alebo v rámci výkonu verejnej funkcie a ktorá spracúva osobné údaje v rozsahu a spôsobom pri dodržaní zásad spracúvania osobných údajov v zmysle Nariadenia GDPR a Zák. č. 18/2018 Z.z.
V podmienkach prevádzkovateľa sú to: okrem štatutára prevádzkovateľa najmä jeho zamestnanci. Pre účely prevádzkovateľa sa poverené osoby definujú ako „poverené oprávnené osoby", nakoľko prevádzkovateľ v poverení vymedzuje poverenej osobe okrem práv a povinností aj spracovateľské oprávnenia.

Zodpovedná osoba – je fyzická, alebo právnická osoba určená prevádzkovateľom alebo sprostredkovateľom v zmysle čl.37 GDPR, s postavením podľa čl.38 a úlohami podľa čl. 39 GDPR.
V podmienkach prevádzkovateľa:

Ak prevádzkovateľ dobrovoľne alebo z dôvodov vymedzených v zákone, určil zodpovednú osobu, ktorá je uvedená v Záznamoch o spracovateľských činnostiach prevádzkovateľa, potom o tomto:

- oboznámil cestou tejto Bezpečnostnej politiky o určení zodpovednej osoby všetkých svojich zamestnancov, ktorí sú poverenými osobami, tiež ostatné osoby podľa potreby,
- zverejnil informáciu o určení zodpovednej osoby na svojom webovom sídle.
- nahlásil určenú zodpovednú osobu dozornému orgánu - Úrad na ochranu osobných údajov.

Dotknutá osoba – je identifikovaná alebo identifikovateľná fyzická osoba, ktorej sa osobné údaje týkajú. Identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.
V podmienkach prevádzkovateľa sú to: osoby, ktorých osobné údaje sa spracovávajú v evidenciách jednotlivých IS.

Súhlas dotknutej osoby – súhlasom dotknutej osoby je akýkoľvek vážny a slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby vo forme vyhlásenia alebo jednoznačného potvrdzujúceho úkonu, ktorým dotknutá osoba vyjadruje súhlas so spracúvaním svojich osobných údajov.
V podmienkach prevádzkovateľa: Pri plnení úloh prevádzkovateľa sa súhlas dotknutej osoby pri spracúvaní údajov dotknutých osôb nevyžaduje ak prevádzkovateľ vykonáva spracúvanie osobných údajov v IS na základe iného právneho základu.

Spracúvanie osobných údajov – vykonávanie operácií alebo súboru operácií s osobnými údajmi, najmä ich získavanie, zhromažďovanie, šírenie, zaznamenávanie, usporadúvanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, preskupovanie, kombinovanie, premiestňovanie, využívanie, uchovávanie, blokovanie, likvidácia, ich cezhraničný prenos, poskytovanie, sprístupňovanie alebo zverejňovanie.
V podmienkach prevádzkovateľa: spracúvanie vykonávajú poverené oprávnené osoby – používatelia IS podľa svojej pracovnej náplne (role) a svojich prístupových oprávnení.

Sprístupňovanie osobných údajov – sprístupňovaním osobných údajov oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva.
V podmienkach prevádzkovateľa: sa údaje sprístupňujú oprávneným subjektom za účelom kontroly.

Poskytovanie osobných údajov – poskytovaním osobných údajov odovzdávanie osobných údajov oprávneným prijímateľom, ktorí ich ďalej spracúvajú.
V podmienkach prevádzkovateľa: napr. Daňový úrad, Sociálna poisťovňa, zdravotné poisťovne, a pod.

Likvidácia osobných údajov – zrušenie osobných údajov rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať.
V podmienkach prevádzkovateľa: sa na likvidáciu listín a fyzických nosičov údajov využíva skartovač.

Zverejňovanie osobných údajov – publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovokomunikačných prostriedkov, verejne prístupných

počítačových sietí, verejným vykonaním alebo vystavením diela, verejným vyhlásením, uvedením vo verejnom zozname, v registri alebo v operáte, ich umiestnením na úradnej tabuli alebo na inom verejne prístupnom mieste.
V podmienkach prevádzkovateľa: sa podľa potreby a na základe súhlasu dotknutých osôb zverejňujú audio-vizuálne záznamy z rôznych kultúrno-spoločenských podujatí a iných aktivít na internetovej stránke prevádzkovateľa.

Účel spracúvania osobných údajov – účel spracúvania osobných údajov vopred určuje prevádzkovateľ v súvislosti s plnením svojich úloh.

Informačný systém – v ktorom sa na vopred vymedzený alebo ustanovený účel systematicky spracúva alebo má spracúvať akýkoľvek usporiadaný súbor osobných údajov prístupných podľa určených kritérií bez ohľadu na to, či ide o informačný systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe; informačným systémom sa na účely tejto smernice rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania.
V podmienkach prevádzkovateľa: je na základe určených účelov, rozsahu spracovaných osobných údajov a právneho základu spracúvania osobných údajov (osobitné zákony) prevádzkovateľom vymedzený zoznam informačných systémov (IS), ktoré môže prevádzkovateľ meniť podľa zmien v plnení svojich povinností, alebo zmien v účeloch.
O spracúvaní osobných údajov v jednotlivých IS a podľa jednotlivých účelov spracúvania vedie prevádzkovateľ záznamy o spracovateľských činnostiach.

Záznam o spracovateľských činnostiach prevádzkovateľa / zástupcu prevádzkovateľa
Tento záznam musí obsahovať najmenej tieto údaje:

Prevádzkovateľ / zástupca prevádzkovateľa
a) identifikačné údaje a kontaktné údaje prevádzkovateľa, spoločného prevádzkovateľa, zástupcu prevádzkovateľa, ak bol poverený, a zodpovednej osoby,
b) účel spracúvania osobných údajov,
c) opis kategórií dotknutých osôb a kategórií osobných údajov,
d) kategórie príjemcov vrátane príjemcu v tretej krajine alebo medzinárodnej organizácii,
e) označenie tretej krajiny alebo medzinárodnej organizácie, ak prevádzkovateľ zamýšľa prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii a dokumentáciu o primeraných zárukách, ak prevádzkovateľ zamýšľa prenos podľa § 51ods.1a 2, Zák. č.18 /2018 Z.z.
f) predpokladané lehoty na vymazanie rôznych kategórií osobných údajov,
g) všeobecný opis technických a organizačných bezpečnostných opatrení podľa § 39ods.1. Zák. č.18 /2018 Z.z.

Sprostredkovateľ
a) identifikačné údaje a kontaktné údaje sprostredkovateľa a prevádzkovateľa v mene ktorého sprostredkovateľ koná, zástupcu prevádzkovateľa alebo sprostredkovateľa, ak bol poverený, a zodpovednej osoby,
b) kategórie spracúvania osobných údajov vykonávaného v mene každého prevádzkovateľa,
c) označenie tretej krajiny alebo medzinárodnej organizácie, ak prevádzkovateľ zamýšľa prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácii, a dokumentáciu o primeraných zárukách, ak prevádzkovateľ zamýšľa prenos podľa § 51ods.1a 2,
d) všeobecný opis technických a organizačných bezpečnostných opatrení podľa § 39ods.1.
V podmienkach prevádzkovateľa: prevádzkovateľ vedie záznamy o spracovateľských činnostiach pre všetky účely spracúvania osobných údajov a všetky informačné systémy,

zoradené podľa informačných systémov. Tieto záznamy sa vedú elektronicky aj listinne, pričom v listinnej podobe sú priložené k Dokumentácií bezpečnostných opatrení a k tejto smernici.

Aktíva - sú všetky hmotné i nehmotné hodnoty, ktoré prevádzkovateľ vlastní, alebo využíva a slúžia najmä na plnenie jeho povinností.
Medzi hmotné aktíva patria najmä administratívne priestory, počítače, počítačová sieť, komunikačné zariadenia a ďalšie hmotné predmety vo vlastníctve prevádzkovateľa.
Medzi nehmotné aktíva patria pracovné postupy, know-how, údaje o zamestnancoch, ekonomické a finančné údaje, majetkové práva a ďalší nehmotný majetok. Medzi aktíva patria tiež osoby, ktoré sú v zamestnaneckom, obchodnom a majetkovom vzťahu k prevádzkovateľovi.
V podmienkach prevádzkovateľa sú to najmä: všetky hmotné aj nehmotné kľúčové komponenty informačných systémov so spracúvanými údajmi, bez ktorých by nebolo možné prevádzku IS spustiť a ďalej plynulo realizovať. Sú to napríklad: hardware (pracovná stanica, tlačiareň, switch, router, pamäťové média, záložné zdroje ...atď.),
software: (inštalačné média k SW OS, aplikačnému, antivírusovému, zálohovaciemu, atď.), inštalačné kľúče, SW licencie, rôzne oprávnenia a podobne. Aktívami sú aj jednotliví pracovníci prevádzkovateľa a ich know-how, teda vzdelanie, schopnosti a zručnosti, potrebné pre správnu a bezproblémovú prevádzku IS.
Ďalej sú to informačné aktíva:

- osobné údaje, uchovávané a spracovávané v IS, v zmysle zachovania ich dôležitých atribútov ako je správnosť, aktuálnosť, integrita, autenticita a dôvernosť,
- schopnosť poskytovať bez zbytočného odkladu a v náležitej kvalite a presnosti služby nevyhnutné pre plnenie svojich úloh a úloh organizačných jednotiek v jej pôsobnosti,
- schopnosť poskytovať vybrané osobné údaje v náležitej kvalite (aktuálnosť, neporušenosť, autenticita) vybraným externým subjektom, predovšetkým určeným orgánom verejnej správy.

Hrozby – sú vplyvy okolia, iných osôb, zariadení a prostriedkov, ktoré úmyselne alebo neúmyselne vplývajú na aktíva tak, že ich prevádzkovateľ nemôže využívať alebo inak ohrozujú oprávnené záujmy prevádzkovateľa.
Katalóg hrozieb podľa ISO27005 uvádza hrozby:

- fyzické poškodenie
- prírodné udalosti
- strata dôležitých služieb
- narušenie spôsobené žiarením
- kompromitácia informácii
- technické zlyhanie
- nepovolené aktivity
- kompromitácia funkcií

V podmienkach prevádzkovateľa sú to hlavne hrozby:

- **možnosť úniku a zneužitia osobných údajov** nachádzajúcich sa v IS (ISO27005: kompromitácia informácii),
- **možnosť neoprávnenej manipulácie** s osobnými údajmi v IS (ISO27005: nepovolené aktivity)
- **nenávratné zničenie alebo poškodenie** osobných údajov v IS (ISO27005: fyzické poškodenie, prírodné udalosti, technické zlyhanie),
- **cielené úmyselné zmeny, alebo vnášanie nepravých, neautentických údajov** do IS. (ISO27005: nepovolené aktivity)

Bezpečnostné opatrenia – sú činnosti, nariadenia a postupy, ktoré vykonáva prevádzkovateľ na ochranu aktív pred hrozbami. Rozlišujú sa na proaktívne (realizované preventívne pred možným uskutočnením hrozby s cieľom znemožniť hrozbe na aktíva pôsobiť – napr. antivírusové opatrenia) a reaktívne (realizované ako reakcia na už uskutočnenú hrozbu s cieľom zamedziť pôsobeniu hrozby a eliminovať dôsledky jej pôsobenia – teda uviesť aktíva do stavu pred začatím pôsobenia hrozby).
V podmienkach prevádzkovateľa: Prevádzkovateľ má svoje technické a organizačné bezpečnostné opatrenia popísané v Dokumentácií bezpečnostných opatrení.

Bezpečnostný incident – je také pôsobenie hrozby na aktívum, pri ktorom prevádzkovateľovi na aktíve vzniká škoda.
V podmienkach prevádzkovateľa má bezpečnostné incidenty najmä tieto dopady:

- porušenie povinností stanovených nariadením č. **2016/679 EP a Rady EÚ a** zákonom č. 18/2018 Z. z. o ochrane osobných údajov a možné súvisiace sankcie,
- porušenie práv dotknutých osôb pri nezákonnom spracúvaní ich osobných údajov, alebo pri nedostatočnej ochrane ich osobných údajov v zmysle narušenia ich osobnej integrity, dôstojnosti, dobrého mena a podobne, ktorého dôsledkom môžu byť nielen sankcie regulačného orgánu, ale aj súdne spory s dotknutými osobami,
- možnosť výskytu úmyselných aktivít zameraných k zneužitiu osobných údajov,
- v prípade súčasného poškodenia alebo zničenia záložných kópií prácna rekonštrukcia údajov (so zvýšenou pravdepodobnosťou chýb),
- v prípade poškodenia, zlyhania, alebo odcudzenia výpočtovej techniky omeškanie spracovania osobných údajov a nadväzujúcich činností,
- narušenie práce pracoviska, v prípade niektorých aplikácií prácna rekonštrukcia údajov (nedostatočné, resp. žiadne údaje v listinnej forme),
- obmedzenie schopnosti pracoviska včas plniť svoje úlohy.

Riziko – Riziko je odhadom pravdepodobnosti možného pôsobenia konkrétnej hrozby na konkrétne aktívum vo vzťahu k predpokladanému dopadu na aktívum. Posudzuje sa veľkosť rizika pre každú identifikovanú hrozbu a každý IS samostatne s následným zhrnutím a identifikovaním najväčších rizík.

V podmienkach prevádzkovateľa: prevádzkovateľ má vykonané posúdenie úrovne rizík naplnenia jednotlivých hrozieb spracované v Dokumentácií bezpečnostných opatrení v časti Analýza bezpečnosti informačných aktív v IS a posúdenie rizík.

Prevádzkový záznam – je záznam o chode a činnosti technického prostriedku, organizačnej súčasti a pod., a to najmä ak sú tieto považované za aktíva.
V podmienkach prevádzkovateľa: sa prevádzkové záznamy realizujú formou evidencie do prevádzkového denníka.
Externá organizácia – právnická, alebo fyzická osoba - externý špecialista vstupujúca do informačného systému za účelom jeho údržby alebo obnovy na základe zmluvného vzťahu.
V podmienkach prevádzkovateľa: tieto externé organizácie vstupujú podľa potreby prevádzkovateľa a na zmluvnom základe obsahujúcom náležitosti podľa čl.28 nariadenia GDPR do IS za účelom údržby a opráv aktív – kľúčových komponentov IS. Externé organizácie sú zaevidované v zozname sprostredkovateľov.

Článok 3
Zásady spracúvania osobných údajov

Zásada zákonnosti - osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby.

Zásada obmedzenia účelu - osobné údaje sa môžu získavať len na konkrétne určený, výslovne uvedený a oprávnený účel a nesmú sa ďalej spracúvať spôsobom, ktorý nie je zlučiteľný s týmto účelom. Ďalšie spracúvanie osobných údajov na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel, ak je v súlade s osobitným predpisom a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa §78ods.8, Zák.č.18/2018 Z. z. sa nepovažuje za nezlučiteľné s pôvodným účelom.

Zásada minimalizácie osobných údajov - spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.

Zásada správnosti - spracúvané osobné údaje musia byť správne a podľa potreby aktualizované. Musia sa prijať primerané a účinné opatrenia na zabezpečenie toho, aby sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bez zbytočného odkladu vymazali alebo opravili.

Zásada minimalizácie uchovávania – osobné údaje musia byť uchovávané vo forme, ktorá umožňuje identifikáciu dotknutej osoby najneskôr dovtedy, kým je to potrebné na účel, na ktorý sa osobné údaje spracúvajú. Osobné údaje sa môžu uchovávať dlhšie, ak sa majú spracúvať výlučne na účel archivácie, na vedecký účel, na účel historického výskumu alebo na štatistický účel na základe osobitného predpisu a ak sú dodržané primerané záruky ochrany práv dotknutej osoby podľa § 78ods.8.

Zásada integrity a dôvernosti - osobné údaje musia byť spracúvané spôsobom, ktorý prostredníctvom primeraných technických a organizačných opatrení zaručuje primeranú bezpečnosť osobných údajov vrátane ochrany pred neoprávneným spracúvaním osobných údajov, nezákonným spracúvaním osobných údajov, náhodnou stratou osobných údajov, výmazom osobných údajov alebo poškodením osobných údajov.
Zásada zodpovednosti - prevádzkovateľ je zodpovedný za dodržiavanie základných zásad spracúvania osobných údajov, za súlad spracúvania osobných údajov so zásadami spracúvania osobných údajov a je povinný tento súlad so zásadami spracúvania osobných údajov na požiadanie dozornému orgánu preukázať.

Zákonnosť spracúvania - spracúvanie osobných údajov je zákonné, ak sa vykonáva na základe aspoň jedného z týchto právnych základov:

a) dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov aspoň na jeden konkrétny účel,

b) spracúvanie osobných údajov je nevyhnutné naplnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,

c) spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,

d) spracúvanie osobných údajov je nevyhnutné na ochranu života, zdravia alebo majetku

dotknutej osoby alebo inej fyzickej osoby,

e) spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi,

f) spracúvanie osobných údajov je nevyhnutné na účel oprávnených záujmov prevádzkovateľa alebo tretej strany okrem prípadov, keď nad týmito záujmami prevažujú záujmy alebo práva dotknutej osoby vyžadujúce si ochranu osobných údajov, najmä ak je dotknutou osobou dieťa.

2. Zodpovednosť za bezpečnosť a ochranu

Článok 4

Bezpečnostný správca

Za organizáciu bezpečnosti a ochrany všetkých aktív prevádzkovateľa je zodpovedný **Bezpečnostný správca**, (ďalej tiež „BS“) ktorého určí prevádzkovateľ.

Bezpečnostný správca zodpovedá za:

- bezpečnú, plynulú a spoľahlivú prevádzku IS z pohľadu informačnej bezpečnosti.
- pridelenie aktív do správy správcom aktív – vybraným zamestnancom, ktorí potom zodpovedajú za ich ochranu a bezpečnosť. O pridelení aktív je povinný viesť si inventár, v ktorom je vymedzený účel používania aktíva.
- Prehodnotenie odhadov rizík vykonáva najmenej jedenkrát za rok v spolupráci s určenou Zodpovednou osobou.
- proces získavania osobných a citlivých údajov, ich poskytovanie, sprístupňovanie, prípadne zverejňovanie,
- posúdenie pred začatím spracúvania osobných a citlivých údajov v informačnom systéme, či ich spracúvaním nevzniká nebezpečenstvo narušenia práv a slobôd dotknutých osôb,
- zisťovanie narušenia práv a slobôd dotknutých osôb pred začatím spracúvania alebo porušenia zákonných ustanovení v priebehu spracúvania osobných údajov,
- posudzovanie, či osobné údaje svojím obsahom a rozsahom zodpovedajú účelu spracúvania, resp., či sú s daným účelom zlučiteľné,
- zabezpečovanie aktuálnosti spracúvaných osobných údajov a za ich likvidáciu (ak bol splnený účel spracúvania alebo sa nedajú opraviť alebo doplniť tak, aby boli správne a aktuálne),
- rozhodnutia, či daným spracúvaním môže byť poverený sprostredkovateľ, ak je záujem na tom, aby spracúvanie vykonával,
- preverenie, či možno vykonávať cezhraničný tok osobných údajov, ak sa požaduje,
- zabezpečenie a organizáciu školení zamestnancov ohľadom informačnej bezpečnosti v spolupráci s určenou Zodpovednou osobou.
- vykonávanie kontrolnej činnosti na základe plánu kontrolnej činnosti, ktorý vypracuje a predloží štatutárovi prevádzkovateľa na schválenie. V pláne uvedie pre každú plánovanú kontrolu predmet kontroly, kontrolovaný IS a obdobie, kedy sa má kontrola vykonať. Plán kontrol BS spracúva na obdobie jedného kalendárneho roka.

Článok 5
Správa aktív

Aktíva prevádzkovateľa sa na účely tejto smernice členia do nasledujúcich skupín:
- aktíva s vysokou ochranou - sú to tie aktíva, ktorých poškodenie alebo strata by ohrozila záujmy prevádzkovateľa v plnom rozsahu,
- aktíva so zvýšenou ochranou – sú tie aktíva, ktorých poškodenie alebo strata by čiastočne ohrozili záujmy prevádzkovateľa,
- aktíva obvyklej ochrany – sú to aktíva, ktorých individuálne poškodenie alebo strata spôsobia ľahko odstrániteľnú škodu alebo neohrozia záujmy prevádzkovateľa.

Zaradenie predmetu alebo skutočnosti medzi aktíva vykonáva BS.
Zamestnanci používajúci aktívum so zvýšenou a vysokou ochranou sú povinní oznámiť správcovi tohto aktíva akúkoľvek skutočnosť, o ktorej sa domnievajú, že by mohla byť hrozbou pre dané aktívum.
Za ochranu a správu aktív obvyklej ochrany sú zodpovední zamestnanci, ktorí za tieto aktíva prevzali hmotnú zodpovednosť alebo im boli zverené do používania.
Aktívum sa môže používať len na ten účel, ktorý je deklarovaný v inventári aktív. Iné dočasné použitie je možné len so súhlasom BS.

Bezpečnostný správca pravidelne, najmenej jedenkrát za rok, zvoláva poradu Správcov aktív.

Článok 6
Kontrolná činnosť

Úlohou kontrolnej činnosti je zisťovanie stavu bezpečnosti a ochrany informačných technológií, stavu pripravenosti a účinnosti opatrení a výkon dozoru nad plnením tejto smernice.

V podmienkach prevádzkovateľa kontrolnú činnosť vykonáva Bezpečnostný správca (BS) nasledovne:

- každý pracovník – poverená oprávnená osoba – používateľ IS je povinný poskytnúť BS všetky informácie o ktoré pri výkone prehliadky, alebo kontroly žiada a sú vo vzťahu k predmetu prehliadky alebo kontroly,

- prehliadkou, ktorú BS vykonáva popri výkone svojich obvyklých pracovných povinností a vedie o jej zisteniach záznam v prevádzkovom denníku,

- kontrolou podľa schváleného plánu kontrol, resp. nenaplánovanou kontrolou, ktorých cieľom je preveriť dodržiavanie tejto smernice u konkrétneho pracovníka – oprávnenej osoby – používateľa IS, alebo viacerých takýchto osôb. O kontrole Bezpečnostný správca vykoná záznam, v ktorom uvedie predmet kontroly, dátum a čas, kedy bola kontrola vykonaná, kto kontrolu vykonal a zistené skutočnosti; ak sa kontrolou zistí porušenie tejto smernice, všeobecne záväzných predpisov, alebo iných interných nariadení prevádzkovateľa, predloží BS správu o kontrole štatutárovi prevádzkovateľa.
  Správa o výsledkoch kontroly musí obsahovať:
  a) chronologický opis priebehu kontrolnej činnosti,
  b) zoznam zistených nedostatkov,
  c) odporúčané opatrenia.

- každý pracovník – poverená oprávnená osoba – používateľ IS je povinný poskytnúť BS všetky informácie o ktoré pri výkone prehliadky, alebo kontroly žiada a sú vo vzťahu k predmetu prehliadky alebo kontroly.
- BS má právo oboznámiť sa s výsledkami iných kontrol s iným predmetom kontroly a ak v ich výsledkoch a záveroch sú skutočnosti, ktoré signalizujú alebo informujú o narušení bezpečnosti a ochrany osobných údajov, je BS povinný uvedené informácie okamžite prešetriť formou ním samostatne vykonanej kontroly.

- BS štatutárovi prevádzkovateľa podá 1x ročne súhrnnú správu o kontrolnej činnosti, v ktorej uvedie prehľad všetkých vykonaných kontrol a zistených nedostatkov.

Článok 7

Bezpečnostné incidenty

- detekcia incidentov je súbor činností a opatrení, vedúci k včasnému zisteniu bezpečnostného incidentu, resp. k včasnému zisteniu, že hrozba pôsobí na niektoré aktívum prevádzkovateľa,

- detekcia sa vykonáva nasledovným spôsobmi:
  a) automatizovanými technickými prostriedkami – sú to napr. prostriedky hlásiace výskyt požiaru, senzory zisťujúce pohyb a pod.,
  b) automatickými informatickými (programovými) prostriedkami - sú to špecializované programy, ktoré vyhodnocujú prevádzkové záznamy, indikujú potenciálny incident,
  c) sústavnou činnosťou zamestnancov–primeraná ostražitosť zamestnancov, najmä Správcov IT a správcov aktív ako aj BS a výkon kontrolnej činnosti,

- ak výstupy z automatizovaných prostriedkov umožňujú záznam týchto výstupov, manipuluje sa s nimi ako s prevádzkovými záznamami,

- pri zistení incidentu musí byť o tomto informovaný BS, Správca IT a všetci správcovia dotknutých aktív. Na základe povahy bezpečnostného incidentu a zasiahnutých aktív rozhodne BS o zmene bezpečnostného režimu v zmysle Článku 8 tejto smernice.

Maximálna prípustná doba výpadku IS pri zmene bezpečnostného režimu je 48 hodín.

- o každom bezpečnostnom incidente musí byť spracovaný záznam. Záznam spracúva BS. Každá oprávnená osoba je povinná poskytnúť BS všetky podklady a údaje, ktoré potrebuje pre spracovanie záznamu o bezpečnostnom incidente,
- záznam o bezpečnostnom incidente musí obsahovať:
  a) dátum a čas, kedy incident bol zistený, kedy skončil, a ak je to možné, zistiť aj kedy incident začal,
  b) opis spôsobu, ako bol incident zistený – uvedie sa najmä meno zamestnanca, ktorý incident ohlásil,
  c) dátum a čas, kedy bol zmenený bezpečnostný režim,
  d) chronologický opis priebehu incidentu, opis hrozieb, ktoré pôsobili a spôsob, akým sa realizovali,
  e) zoznam dotknutých aktív, doklad o škodách a predpokladaná doba zotavenia,
  f) porovnanie s rizikovou analýzou v Dokumentácií bezpečnostných opatrení – posúdenie, či bolo možné incident očakávať, či boli správne odhadnuté úrovne rizík a dopady,
  g) opis prijatých opatrení – doklad, kedy a kým boli prijaté, doklad o ich účinnosti a trvaní,

h) návrh na prijatie opatrení pre zamedzenie recidívy bezpečnostného incidentu, odhad pravdepodobnosti recidívy, záznam o úprave analýzy rizík v Dokumentácii bezpečnostných opatrení, ak takúto úpravu bolo potrebné vykonať,

i) zoznam opatrení a nariadení, ktoré boli porušené a mohli spôsobiť že incident nastal, zoznam osôb ktoré tieto nariadenia porušili,

- ak nastal bezpečnostný incident vedomou alebo nevedomou činnosťou oprávnenej osoby, bude sankcionovaná podľa príslušných ustanovení Zákonníka práce a Pracovného poriadku.

Článok 8
Bezpečnostné režimy

Bezpečnostný režim je stav organizácie činnosti prevádzkovateľa alebo jej časti, ktorý zodpovedá aktuálnemu ohrozeniu jeho aktív.

Stupeň a rozsah bezpečnostného režimu určuje BS alebo Správca IT na základe poznania aktuálneho stavu bezpečnosti a úrovne ohrozenia aktív prevádzkovateľa.

Rozoznávajú sa nasledovné režimy:

1. normálny – normálny stav bežného chodu prevádzkovateľa, kedy nie je bezprostredne ohrozené žiadne aktívum,

2.ohrozenie - činnosť prevádzkovateľa nie je ničím zmenená alebo ovplyvnená, ale úroveň ohrozenia niektorého aktíva je zvýšená (zvýšená je pravdepodobnosť realizácie niektorej hrozby), čo vyžaduje monitorovanie tohto stavu a prijatie ďalších proaktívnych opatrení. Opatrenia sa prijímajú na základe aktuálneho poznania stavu hrozieb, ktorý je indikovaný najmä analýzou obsahu prevádzkových záznamov alebo výskytom bezpečnostných incidentov, ktoré síce bezprostredne nevyžadovali zmenu bezpečnostného režimu, ale dôsledky incidentu mohli spôsobiť zvýšenie pravdepodobnosti výskytu a realizácie niektorej z hrozieb. Po prijatí opatrení sa odhadne ich účinnosť, znovu sa posúdi úroveň rizika a rozhodne sa o prijatí ďalších opatrení, alebo o prechode do režimu **„normálny“**. Ak sa zistí, že aj napriek prijatým opatreniam došlo k realizácii hrozby a dochádza k poškodzovaniu alebo ničeniu aktív prevádzkovateľa, vyhlási sa režim **„kríza“**,

3. kríza - činnosť prevádzkovateľa je zmenená následkom účinku niektorých hrozieb na aktíva prevádzkovateľa. Vyžaduje sa prijatie účinných reaktívnych opatrení na odvrátenie hrozby a minimalizáciu škôd. Tento režim sa vyhlasuje, ak bol zistený výskyt realizujúcej sa niektorej hrozby na aspoň jedno IT aktívum (server alebo informačný systém), na ktorom sa spracovávajú osobné alebo citlivé údaje. Pod pojmom realizujúca sa hrozba, sa rozumie taký stav, kedy je aktívum hrozbou poškodzované alebo ničené, čo má za následok znefunkčnenie aktíva alebo ohrozenie záujmov prevádzkovateľa. Počas tohto režimu je možné odpojiť časť prevádzkovateľa alebo celého prevádzkovateľa od internetu, nariadiť vypnutie počítačov a serverov alebo ich odpojenie od počítačovej siete. Po odvrátení hrozby sa prechádza do režimu **„zotavenie“**.

4. zotavenie - špeciálny režim po **„krízovom“** režime, kedy dochádza ku konsolidácii činnosti prevádzkovateľa, rekonštrukcii a náhrade poškodených aktív. Navrhuje sa vedeniu postup pri odstraňovaní škôd. Postup musí obsahovať stanovenie priorít, časovú postupnosť,

technickú špecifikáciu opatrení na odstránenie škôd a odhad ekonomickej náročnosti. BS v súčinnosti so Správcom IT je povinný dôkladne vyšetriť dôvody príčiny, a teda prečo došlo k realizácii hrozieb a škodám. Prechod do režimu „**normálny**" je možný, ak bol schválený postup odstránenia škôd a ak je možné považovať stav prevádzkovateľa ako celku z bezpečnostného hľadiska za konsolidovaný,

- o zmene Bezpečnostného režimu musia byť ihneď vyrozumení všetci zamestnanci a osoby zodpovedné za výkon ochrany prevádzkovateľa.

Článok 9
Oznámenie porušenia ochrany osobných údajov kontrolnému orgánu (do 72 hodín)

Ak došlo pri vzniku bezpečnostného incidentu k porušeniu ochrany osobných údajov úradu, potom:

a) Prevádzkovateľ je povinný toto porušenie oznámiť Úradu na ochranu osobných údajov SR do 72 hodín po tom, ako sa o ňom dozvedel. To neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby.
V rovnakej lehote musí porušenie oznámiť svojej určenej Zodpovednej osobe, aby bola na možné následné konanie s Úradom na ochranu osobných údajov SR informačne pripravená a mohla poskytnúť v konaní svoju súčinnosť.

b) Ak prevádzkovateľ nesplní oznamovaciu povinnosť podľa odseku a), musí zmeškanie lehoty zdôvodniť.

c) Sprostredkovateľ je povinný oznámiť prevádzkovateľovi porušenie ochrany osobných údajov bez zbytočného odkladu potom, ako sa o ňom dozvedel.

d) Oznámenie podľa odseku a) musí obsahovať najmä:
- opis povahy porušenia ochrany osobných údajov vrátane, ak je to možné, kategórií a približného počtu dotknutých osôb, ktorých sa porušenie týka, a kategórií a približného počtu dotknutých záznamov o osobných údajoch,
- kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,
- opis pravdepodobných následkov / dopadov porušenia ochrany osobných údajov,
- opis opatrení prijatých alebo navrhovaných prevádzkovateľom na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov / dopadov, ak je to potrebné.

e) Prevádzkovateľ je povinný poskytnúť informácie podľa odseku d) v rozsahu, v akom sú mu známe v čase oznámenia podľa odseku a). Ak v čase oznámenia podľa odseku a) nie sú prevádzkovateľovi známe všetky informácie podľa odseku d), poskytne ich bez odkladne potom, čo sa o nich dozvie.

f) Prevádzkovateľ je povinný zdokumentovať každý prípad porušenia ochrany osobných údajov podľa odseku a) vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.

Článok 10
Havarijné plánovanie

Havarijne plánovanie je súbor činností na zabezpečenie čo najvyššej dostupnosti údajov a ich ochrana pre zničením alebo poškodením.

V prípade výpadku pracovnej stanice je Správca IT povinný po identifikácii problému zabezpečiť:
- opravu alebo výmenu chybného dielu PC,
- náhradný PC,
- reinštaláciu alebo inštaláciu OS a konfiguráciu z inštalačných médií,
- inštaláciu klientskych aplikácií z inštalačných médií,
- inštaláciu antivírového programu,
- nastavenie prístupových práv,
- v prípade neodkladnosti prístup k informačným systémom z inej funkčnej pracovnej stanice.

V prípade výpadku servera je Správca IT povinný po identifikácii problému zabezpečiť:
- opravu servera v servisnej organizácii alebo náhradný server,
- inštaláciu hardware a jeho fyzické pripojenie do počítačovej siete,
- inštaláciu príslušného operačného systému servera,
- zo záložných kópií obnovenie systémových a konfiguračných súborov,
- inštaláciu antivírového programu a spustenie aktualizácie,
- inštaláciu IS a obnovenie dát z najmladších záložných médií.

V prípade výpadku sieťového prepojenia je Správca IT povinný po identifikácii problému zabezpečiť:
- opravu alebo výmenu chybného aktívneho alebo pasívneho prvku počítačovej siete,
- obnovenie konfiguračného nastavenia zariadenia,
- otestovanie jednotlivých sieťových prepojení.

S postupmi pri haváriách, poruchách a mimoriadnych situáciách, ktoré sledujú efektívnu obnovu systému, je potrebné oboznámiť všetkých vedúcich zamestnancov.

3. Osobné údaje prevádzkovateľa

Článok 11

Zabezpečenie osobných údajov

Každá poverená oprávnená osoba (pracovník, volený zástupca, používateľ IS), ktorá príde do styku s osobnými údajmi, musí byť v poverení oboznámená s príslušnými právnymi normami (Nariadenie GDPR, Zákon č.18/2018 Z.z.) o ochrane osobných údajov. Toto oboznámenie musí byť v súlade a v rozsahu s jeho pracovnou náplňou, alebo volenou funkciou. Oboznámenie vykonáva BS, určená Zodpovedná osoba, alebo iná prevádzkovateľom poverená osoba. O oboznámení musí byť vykonaný záznam.

Osobné údaje môžu byť spracovávané a prenášané len zabezpečeným spôsobom.

Zabezpečenie osobných údajov sa vykonáva technickými a organizačnými opatreniami, ktoré sú popísané v Dokumentácií bezpečnostných opatrení prevádzkovateľa, avšak najmä týmito opatreniami:

- dokumenty na papieri a na pamäťových médiách musia byť ukladané v uzamykateľnej skrini, ktorá je umiestnená v uzamykateľnej miestnosti,

- prenášanie papierových dokumentov s osobnými údajmi je možné len v uzavretých a nepriehľadných schránkach alebo obaloch,

- miestnosti, v ktorých sa spracúvajú osobné údaje musia byť v neprítomnosti oprávnenej osoby uzamknuté,

- miestnosti musia byť vybavené zábranným opatrením (priehradkou) , ktorá zamedzí neoprávneným osobám nahliadať do dokumentov a na obrazovky počítačov alebo odcudziť média a dokumenty. Obrazovky počítačov musia byť umiestnené tak, aby z nich neoprávnené osoby nemohli prečítať zobrazený obsah,

- zakazuje sa zhotovovať (tlačiť) dokumenty s osobnými údajmi na iných zariadeniach, než na zariadeniach, ktoré sú umiestnené v zabezpečených priestoroch prevádzkovateľa IS,

- zakazuje sa sprístupňovať pracovnú plochu pomocou prostriedkov vzdialenej správy „Virtual Network Computing (VNC)“, (napr. pomocou SW aplikácie Team Viewer), komukoľvek bez predchádzajúceho súhlasu BS, ktorý o takomto sprístupnení vykoná záznam v prevádzkovom denníku,

- zakazuje sa zanechávanie dokumentov s osobnými údajmi v tlačových zariadeniach napr. kopírkach, tlačiarňach alebo faxoch bez dozoru,

- nariaďuje sa povinnosť dodržiavať pravidlo čistého stola – nenechávať v neprítomnosti, najmä po skončení pracovnej doby, na stole dokumenty s osobnými údajmi,

- poskytovanie a sprístupňovanie osobných údajov cez telefón je zakázané.

Pri získavaní a spracúvaní osobných údajov sú oprávnené osoby povinné dodržiavať nasledovné záväzné pravidlá:

- pri získavaní osobných údajov do jednotlivých IS môže oprávnená osoba vyžadovať od dotknutej osoby len tie osobné údaje, ktoré sú potrebné pre účel ich spracúvania, zakazuje sa získavanie osobných údajov dotknutých osôb pod zámienkou iného účelu alebo inej činnosti než účelu, ktorý je stanovený,

- získavať osobné údaje môže len poverená oprávnená osoba v súlade so svojou pracovnou náplňou,

- pri získavaní a spracúvaní osobných údajov je poverená oprávnená osoba povinná zabezpečiť ochranu osobných údajov tak, že získavať a spracúvať osobné údaje môže len v neprítomnosti neoprávnených osôb. V prípade, ak v mieste získavania alebo spracúvania osobných údajov sa nachádza neoprávnená osoba, je oprávnená osoba povinná prijať opatrenia k tomu, aby tieto údaje nemohli byť známe tejto neoprávnenej osobe a zabrániť tomu, aby táto neoprávnená osoba mohla prísť do styku s týmito osobnými údajmi,

- oprávnená osoba kontroluje a overuje správnosť a aktuálnosť osobných údajov po ich získaní a zaradení v informačnom systéme osobných údajov,

- poverená oprávnená osoba vykonáva spracovateľské operácie len so správnymi, úplnými a podľa potreby aktualizovanými osobnými údajmi vo vzťahu k účelu spracúvania,

- nesprávne a neúplné osobné údaje je oprávnená osoba povinná bez zbytočného odkladu opraviť alebo doplniť. Nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné je povinná blokovať, kým sa rozhodne o ich likvidácii,

- pred získavaním osobných údajov od dotknutej osoby je oprávnená osoba povinná oboznámiť ju s názvom a sídlom prevádzkovateľa, účelom spracúvania osobných údajov, rozsahom spracúvania osobných údajov, predpokladanom okruhu tretích strán pri poskytovaní osobných údajov alebo príjemcov pri sprístupňovaní osobných údajov, forme zverejnenia, ak sa osobné údaje zverejňujú a tretie krajiny, ak sa predpokladá alebo je zrejmé, že sa do týchto krajín uskutoční cezhraničný prenos osobných údajov,

- poverená oprávnená osoba je povinná poučiť dotknutú osobu o dobrovoľnosti alebo povinnosti poskytnutia osobných údajov a o existencii jej práv,

- poverená oprávnená osoba je povinná zabezpečiť preukázateľný súhlas na spracúvanie osobných údajov dotknutej osoby v IS prevádzkovateľa, ak sa spracúvanie osobných údajov nevykonáva podľa iného právneho základu,

- získavať osobné údaje nevyhnutné na dosiahnutie účelu spracúvania kopírovaním, skenovaním alebo iným zaznamenávaním úradných dokladov na nosič informácií je možné len vtedy, ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby alebo na základe písomného súhlasu dotknutej osoby, ak je to nevyhnutné na dosiahnutie účelu spracúvania,

- poverená oprávnená osoba je povinná chrániť prijaté dokumenty a súbory pred stratou, poškodením, zneužitím, odcudzením, neoprávneným sprístupnením, poskytnutím alebo inými neprípustnými formami spracúvania,

- oprávnená osoba je povinná vykonať likvidáciu osobných údajov, ktoré sú súčasťou už nepotrebných pracovných dokumentov (napr. rôzne pracovné súbory, pracovné verzie dokumentov v listinnej podobe) rozložením, vymazaním alebo fyzickým zničením hmotných nosičov tak, aby sa z nich osobné údaje nedali reprodukovať; to neplatí vo vzťahu k osobným údajom, ktoré sú súčasťou obsahu registratúrnych záznamov.

Každá osoba je zodpovedná za fyzickú bezpečnosť svojho pracoviska, jemu zverených aktív a všetkých pracovných prostriedkov. Pri odchode z pracoviska je povinná uzamknúť pracovisko, uzavrieť okná a prekontrolovať zariadenia, či nemôžu spôsobiť požiar alebo inú haváriu. Ak nemôže túto povinnosť splniť, oznámi to ihneď svojmu nadriadenému alebo BS.

Poverené oprávnené osoby sú povinné zachovávať mlčanlivosť o osobných údajoch, s ktorými prídu do styku. Tie nesmú využiť ani pre osobnú potrebu a bez súhlasu štatutára prevádzkovateľa ich nesmú zverejniť, nikomu poskytnúť a ani sprístupniť. Túto mlčanlivosť sú povinní zachovať aj po skončení spracovávania osobných údajov alebo po skončení pracovného pomeru.

Článok 12

Zabezpečenie citlivých údajov

Citlivými údajmi sú všetky údaje o ekonomike a financiách prevádzkovateľa ako aj obchodných partneroch, ktoré nie sú predmetom povinného zverejňovania. Do skupiny ekonomických údajov sa zaraďujú tiež údaje o know-how a technologické informácie.

Ochrana citlivých údajov sa vykonáva rovnakým spôsobom ako ochrana osobných údajov, okrem šifrovania.
O potrebe zašifrovania citlivých údajov rozhoduje ich BS.

4. Prostriedky informačných technológií

Článok 13

Správca informačných technológií

Správcom informačných technológií (ďalej tiež „SIT“) a IT aktív je zamestnanec prevádzkovateľa – poverená oprávnená osoba, alebo externý špecialista (pracovník externej organizácie s ktorou má prevádzkovateľ zmluvný vzťah, poverený správou informačných technológií.
Správa informačných technológií musí byť organizovaná tak, aby sa minimalizovala hrozba zneužitia postavenia administrátora.

Za ochranu údajov uložených na prostriedkoch informačných technológií je zodpovedný Správca IT, ktorý k tomuto účelu vykonáva nasledovné činnosti:

- vykonáva kopírovanie údajov na záložné médiá (zálohovanie údajov),

- vykonáva kopírovanie údajov na archívne médiá (archivovanie údajov),

- vykonáva nastavenia prístupových práv k údajom tak, aby k nim mohli pristupovať len oprávnené osoby – oprávnení používatelia IS,

- inštaluje, spravuje a zabezpečuje také služby (aplikácie), ktoré umožnia zvýšenú ochranu údajov,

SIT je zodpovedný za pravidelnú a včasnú aktualizáciu všetkých programových prostriedkov tak, aby boli včas odstraňované chyby v týchto softvérových prostriedkoch, ktorými sú najmä operačné systémy a ich súčasti, databázové systémy, používané aplikácie (najmä ak komunikujú po sieti), systém antivírusovej ochrany a firewally.

SIT je povinný priebežne nainštalovať všetky dostupné nové opravy softvérového vybavenia, pokiaľ sa tým nenaruší bezproblémový chod a činnosť. Najmenej raz za 3 mesiace je SIT povinný overiť, či neboli vydané nové verzie softvéru.

Zakazuje sa používanie neovereného kódu. Pod pojmom neoverený kód sa rozumie taký program, ktorý nemá garanciu výrobcu o jeho spoľahlivosti alebo nebol overený SIT v izolovanom prostredí, či neobsahuje nežiaduce funkcie a chyby. Overenie sa vykonáva tak, aby nemohlo dôjsť k ohrozeniu osobných údajov prevádzkovateľa a musí sa preveriť najmä správanie programu v sieťovom prostredí a vo vzťahu k údajom uloženým na pamäťovom médiu počítača.

Pri konfigurácii prostriedkov, programov a služieb SIT dbá na to, aby sa používali len tie prostriedky, programy a služby, ktoré sú nevyhnutné pre plnenie pracovných úloh a potrieb zamestnancov prevádzkovateľa. Zakazuje sa používanie programov, sieťových služieb a IT prostriedkov, ktoré nie sú potrebné pre výkon práce zamestnancov a plnenie ich úloh. Používané programy, služby a prostriedky musia byť konfigurované tak, aby k nim mali prístup len tí zamestnanci, ktorí tieto programy, služby a prostriedky potrebujú k svojej práci.

Článok 14

Prevádzkové záznamy

Prevádzkové záznamy do prevádzkového denníka vykonáva BS, SIT ako aj poverené oprávnené osoby – používatelia IS. SIT navyše pravidelne vyhodnocuje všetky záznamy v prevádzkovom denníku. Prevádzkovými záznamami v prevádzkovom denníku sú najmä:

- prevádzkové záznamy o chode pracovných staníc (počítačov a ich príslušenstva),

- prevádzkové záznamy o chode aplikačného SW IS a iného programového vybavenia (napr. záznamy o verziách SW, verziách SQL databázy, apod.),

- prevádzkové záznamy o chode komponentov siete LAN / WAN (najmä smerovačov, routerov ,firewall-ov, apod.),

- prevádzkové záznamy o chode z elektronického zabezpečovacieho systému fyzickej ochrany,

Článok 15

Zálohovanie a archivovanie údajov

- SIT aktív je povinný vykonávať zálohovanie a archiváciu podľa metodiky zálohovania a archivácie stanovenej dodávateľmi SW aplikácií IS,

- médiá s archívnymi údajmi musia byť uložené v inej miestnosti, než sa nachádza počítač (pracovná stanica, počítač, server, notebook, tablet...), z ktorého boli záložné údaje vyhotovené a musia byť riadne označené: (druh údajov, verzia, dátum vykonanej zálohy),

- záložné a archivačné médiá sa považujú za médiá obsahujúce digitálne bezpečnostné dokumenty,

- zamestnanci sú povinní na zálohovanie obsahu svojich počítačov, notebookov a tabletov používať primárne centrálne dátové úložisko zriadené v priestoroch prevádzkovateľa. Prístupové práva a nastavenia zálohovania oprávneným osobám určí BS, resp. SIT,

- zakazuje sa na centrálne dátové úložisko prevádzkovateľa ukladať dáta osobného charakteru ako sú napríklad súkromné fotky, súkromné videozáznamy a podobne,

- zakazuje sa používanie externých dátových úložísk (cloud) na ukladanie personálnych a ekonomických údajov a iných dát, bez šifrovania, alebo pseudonymizácie osobných údajov.

V podmienkach prevádzkovateľa: sa údaje zálohujú pomocou softwarových komponentov jednotlivých dodávateľov SW aplikácií najmenej 1 raz za týždeň.
Záložne kópie sa ukladajú do prednastaveného adresára záloh a prednastaveného alternatívneho miesta záloh v rámci záložného média – USB disku, ktorý je uložený mimo miesta prevádzky IS – v uzamykateľnej kovovej skrini.

Článok 16

Riadenie prístupových práv

- SIT pre aktíva ktoré vyžadujú autentizáciu, stanoví autentizačné postupy a mechanizmy,

- pre autentizačné mechanizmy SIT stanoví parametre, a to najmä vlastnosti hesiel: dĺžku, štruktúru a expiračnú dobu,

- SIT nesmie povoliť heslá kratšie ako 8 znakov, heslá musia obsahovať aspoň jeden neabecedný znak a ich expiračná doba nesmie byť dlhšia ako 1 rok.

- zakazuje sa zverejňovať, alebo neoprávnenej osobe akýmkoľvek spôsobom sprístupniť vyzradiť neverejné autentizačné údaje (heslá).

- zakazuje držanie záznamu hesiel (napr. na papieri, v nešifrovanom softvérovom súbore) ak takýto záznam nemôže byť bezpečne uložený. Poverená oprávnená osoba je povinná chrániť autentizačný prostriedok jemu zverený.

- SIT môže prideliť autentizačné údaje a prostriedky len oprávneným osobám prevádzkovateľa, alebo externým špecialistom zmluvnej externej organizácie, ktorá robí údržbu daného aktíva.

- prístupové oprávnenia prideľuje používateľovi IS SIT na základe požiadavky BS, resp. štatutára prevádzkovateľa. Tvoria ich prístupové meno, prístupové heslo a súbor nastavení, ktoré definujú povolené aktivity používateľa (užívateľská rola),

- používateľ IS sa nesmie žiadnymi prostriedkami pokúšať získať prístupové práva alebo privilegovaný stav, ktorý mu nebol pridelený SIT,

- pokiaľ používateľ IS v dôsledku chyby programových alebo technických prostriedkov získa privilegovaný stav, ktorý mu nebol udelený alebo mu prístupové práva neboli pridelené, je povinný túto skutočnosť neodkladne oznámiť SIT,

- po skončení pracovného pomeru oprávnenej osoby - používateľa IS je SIT povinný odobrať odchádzajúcemu zamestnancovi jeho prihlasovacie údaje a zmeniť ich tak, aby sa mu znemožnil ďalší prístup,

- prístupové oprávnenia sú prideľované podľa typu používateľa :
  a) administrátor – prístup k správe a údržbe aktíva, mal by to byť správca aktíva,
  b) používateľ – prístup len k tým modulom aplikácie (aktíva), s ktorými bezprostredne pracuje,
  c) externý používateľ – externý špecialista externej organizácie, ktorá spravuje a udržiava danú aplikáciu (aktívum), prístup je kontrolovaný správcom aktíva alebo administrátorom, ak ho tým poveril SIT,

- SIT je povinný preveriť používateľské prístupové práva minimálne raz za rok,

- nedodržanie zásad používania hesla a autentizácie zamestnancom sa považuje za bezpečnostný incident.

Článok 17

Pracovné stanice

- oprávnená osoba je povinná používať zverené pracovné stanice výhradne na pracovné účely. Porušenie tohto ustanovenia sa považuje za bezpečnostný incident,

- oprávnená osoba môže na pracovných staniciach používať výhradne programové vybavenie nainštalované Správcom IT, resp. nainštalované s jeho preukázateľným súhlasom.

- oprávnená osoba nemôže na pracovnej stanici meniť žiadne programové vybavenie, rovnako nemôže meniť konfiguráciu programového vybavenia s výnimkou zmien, s ktorými sa mení vzhľad pracovného prostredia,

- oprávnená osoba je zodpovedná za dodržiavanie autorských práv a licenčných podmienok, ktoré sa vzťahujú k programovému vybaveniu, súborom, grafike, dokumentom, správam a ostatným materiálom, ktoré má v úmysle inštalovať, sťahovať, zverejňovať alebo kopírovať,

- oprávnená osoba nemôže vytvárať a distribuovať kópie programového vybavenia inštalovaného na pracovnej stanici,

- oprávnená osoba je pred opustením pracoviska povinná ukončiť prácu s aplikačným programovým vybavením, odhlásiť sa zo siete a operačného systému a dohliadnuť na vypnutie pracovnej stanice,

- pri krátkodobej neprítomnosti môže oprávnená osoba nahradiť odhlásenie sa zo systému a vypnutie pracovnej stanice spustením šetriča obrazovky s heslom, resp. jej uzamknutím,

- oprávnená osoba je povinná po inštalácii novej verzie programového vybavenia po dobu minimálne jedného týždňa venovať zvýšenú pozornosť činnosti systému a kontrolovať správnosť výsledkov jeho práce. Prípadne odchýlky od požadovaného stavu je povinný čo najúplnejšie zdokumentovať a bezodkladne ohlásiť SIT,

- zakazuje sa pripájať do siete prevádzkovateľa vlastné zariadenia (napr. notebooky, PDA, tlačiarne a pod.),

- zakazuje sa povoliť neoprávnenej osobe pripojiť sa do siete prevádzkovateľa, alebo priamo k pracovnej stanici bez vedomia BS. Taktiež sa zakazuje používať vlastné USB kľúče a iné pamäťové média. Porušenie tohto bodu sa považuje za bezpečnostný incident.

Článok 18

Antivírusová ochrana

SIT je povinný zabezpečiť inštaláciu a pravidelnú aktualizáciu antivírusových detekčných a nápravných softvérov na prehliadanie počítačov, serverov a médií na rutinnej báze. Vykonávané kontroly musia zahŕňať:

- kontrolu všetkých súborov na elektronických alebo optických médiách, ako aj súborov prijatých prostredníctvom počítačovej siete, z hľadiska prítomnosti škodlivého kódu ešte pred používaním,

- kontrolu príloh elektronickej pošty a stiahnutých súborov z hľadiska výskytu škodlivého kódu ešte pred spustením. Táto kontrola by sa mala vykonávať na rozličných miestach, napr. na elektronických poštových serveroch, pracovných staniciach a pri vstupe do siete prevádzkovanej prevádzkovateľom,

- kontrolu pred nevyžiadanou poštou – „spamom“,

- kontrolu webových stránok z hľadiska výskytu škodlivého kódu,

SIT je povinný venovať zvýšenú pozornosť tomu, aby škodlivý kód nebol zavedený počas výkonu pohotovostných procedúr alebo procedúr údržby.

V prípade, že sa pri práci poverenej oprávnenej osoby – používateľa IS zobrazí na pracovnej ploche varovanie, že sa na disku alebo prenosnom médiu nachádza vírus alebo iný škodlivý kód, oprávnená osoba nesmie toto varovanie ignorovať. V prípade, že vírus obsahujúce prenosné médium patrí inému subjektu, oprávnená osoba toto označí ako „obsahujúce vírus“ a vráti majiteľovi. V prípade infikovania vlastného pevného disku alebo prenosného média, oprávnená osoba túto skutočnosť bezodkladne oznámi SIT.

Článok 19

Prístup do siete internet a mailová komunikácia

Každá oprávnená osoba, ktorej bol umožnený prístup do siete internet, je povinná rešpektovať nasledovné zásady:

- prístup do siete internet využívať predovšetkým v súlade so svojou pracovnou náplňou,

- dodržiavať etické zásady a zdržiavať sa činností, ktoré by mohli viesť k poškodeniu dobrého mena prevádzkovateľa,

- komunikácia v internete spravidla nie je chránená pred “odpočúvaním“. V prípade potreby prenosu osobných údajov je nevyhnutné tieto pred prenosom zabezpečiť šifrovaním. Ak nie je oprávnená osoba schopná prenos takto zabezpečiť, nie je prípustné ho uskutočniť,

- je zakázané zo siete internet preberať nelegálny obsah (softvér, súbory chránené autorskými právami a pod.). Preberanie spustiteľných programov je povolené len po konzultácii so SIT,

- Výber blokovaných stránok bude v kompetencii SIT na základe bezpečnostnej analýzy.

- oprávnená osoba je povinná zabezpečiť správne adresovanie príjemcu mailovej správy a na prenos správ používať všeobecne dané dátové štandardy,

- v prípade posielania citlivých a osobných údajov je povinný použiť kryptovanú komunikáciu za použitia kryptovacieho kľúča, ktorý mu bol na požiadanie vydaný BS,
- poverená oprávnená osoba – používateľ IS je oprávnená používať elektronickú poštu len na legálne účely, obsah dát odosielaných v rámci siete prevádzkovateľa a cez internet nesmie byť

v rozpore s dobrými mravmi, rovnako musí rešpektovať zákaz posielať reťazové a hromadné e-maily, reklamné správy a pod,

- poverená oprávnená osoba je povinná pravidelne vykonávať údržbu vlastnej elektronickej pošty (zálohovanie správ, mazanie, zhutňovanie a pod.),

Porušenie ustanovení tohto článku sa považuje za bezpečnostný incident.

Článok 20
Zamestnanci externej organizácie

Externá organizácia vystupuje vo vzťahu k prevádzkovateľovi ako sprostredkovateľ a má s prevádzkovateľom zmluvný vzťah, kde okrem iných ustanovení garantuje prevádzkovateľovi ochranu osobných údajov, ku ktorým bude mať na základe zmluvného vzťahu prístup.
Prístup zamestnancov – externých špecialistov externej organizácie zriaďuje SIT na základe schválenia BS. BS si vedie zoznam povolených prístupov k jednotlivým aktívam.

SIT vydá zamestnancovi externej organizácie dočasné prístupové heslo a práva pre výkon kontroly, údržby alebo opravy.

5. Záverečné ustanovenia

Článok 21
Účinnosť smernice

Bezpečnostná smernica nadobúda účinnosť dňom 12.11.2020

Na túto smernicu sa nevzťahuje povinnosť zverejnenia v zmysle zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám v znení neskorších predpisov.

Centrum sociálnych služieb

V Žiline dňa: 11.11.2020 .....

Meno, p
(štatutár