 Ministerstvo ivestícií, regionálneho rozvoja a informatizácie Slovenskej Republiky

**** 

Európska únia

Bezpečnostný manuál pre koncových používateľov a administrátorov ITMS2014+

Verzia č. 1.2

Dátum *účinnosti* od: 30. 09. 2020

****

**Predkladá**: Mgr. Roman Miškovič

odbor informačných systémov európskych štrukturálnych a investičných fondov

Dátum:

Podpis:

**Schválil**: Mgr. Marcela Zubriczká

generálna riaditeľka sekcie financovania fondov

Dátum

Podpis:

Obsah

1 Úvod 3

1.1 Ciele 3

1.2 Základné pojmy a skratky 3

2 Základné zásady a pravidlá spracovania OÚ 6

2.1 Zásady spracovania OÚ 6

2.2 Pravidlá spracovania OÚ 7

2.2.1 Spracúvanie osobných údajov 7

2.2.2 Súhlas dotknutej osoby 7

2.2.3 Získavanie osobných údajov 8

2.2.4 Kopírovanie/skenovanie úradných dokladov 8

2.2.5 Poskytovanie, sprístupňovanie a zverejňovanie osobných údajov 8

2.2.6 Spracovanie osobných údajov sprostredkovateľom 9

2.2.7 Cezhraničný prenos osobných údajov 10

2.2.8 Kvalita spracúvania osobných údajov 10

2.2.9 Likvidácia osobných údajov 10

2.2.10 Poučenie oprávnených osôb a zabezpečenie mlčanlivosti 11

2.2.11 Ochrana práv dotknutých osôb 11

2.2.12 Zabezpečenie vedenia záznamov 12

2.2.13 Incidenty týkajúce sa spracovania OÚ 12

2.2.14 Dohľad nad ochranou osobných údajov – zodpovedná osoba 14

3 Základné princípy a pravidlá informačnej bezpečnosti 15

3.1 Princípy informačnej bezpečnosti 15

3.2 Pravidlá informačnej bezpečnosti 16

3.2.1 Riadenie prístupových práv 16

3.2.2 Politika hesiel 16

3.2.3 Politika čistej obrazovky 17

3.2.4 Spracovanie údajov 17

3.2.5 Antivírusová ochrana 18

3.2.6 Riešenie incidentov a porúch 18

3.2.7 Povedomie o informačnej bezpečnosti 18

3.2.8 Aktualizácia používateľských údajov 19

3.3 Vybrané pravidlá informačnej bezpečnosti pre administrátorov IS 19

3.3.1 Riadenie prevádzkových záznamov 19

3.3.2 Riadenie incidentov 20

# Úvod

## Ciele

Cieľom dokumentu je definovať základné bezpečnostné pravidlá pre koncových používateľov, manažérov ITMS2014+ CKO/CO/OA, manažérov ITMS2014+ RO/SO, manažérov ITMS2014+ DC a administrátorov IS.

Všetky bezpečnostné pravidlá sú prijaté s ohľadom na ochranu osobných údajov spracovaných v informačnom systéme osobných údajov ITMS2014+ v súlade so zákonom:

* č.18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov,
* č. 292/2014 Z. z. o príspevku poskytovanom z európskych štrukturálnych a investičných fondov.

## Základné pojmy a skratky

| **Termín** | **Popis** |
| --- | --- |
| MIRRI  Manažér ITMS2014+ CKO/CO/OA | Ministerstvo ivestícií, regionálneho rozvoja a informatizácie Slovenskej republiky  manažér ITMS2014+ na CKO (MIRRI) a manažér ITMS2014+ na CO/OA (MF SR). |
| Manažér ITMS2014+ DC | manažér ITMS2014+ v DataCentre zodpovedný za vytváranie, zmenu a rušenie používateľských účtov. |
| Administrátor IS | databázový, systémový a aplikačný administrátor, zodpovedný za chod aplikácie, udržiavanie databázy, vykonávanie administrátorských zásahov a podporu pri riešení problémov používateľov. |
| Manažér ITMS2014+ RO/SO | manažér ITMS2014+ na RO/SO (rezorty zapojené do čerpania EŠIF a ich sprostredkovateľské orgány). |
| Blokovanie OÚ | je dočasné alebo trvalé pozastavenie spracúvania osobných údajov, počas ktorého možno vykonávať len tie operácie s osobnými údajmi, ktoré sú nevyhnutné na splnenie povinnosti uloženej ZOOÚ. |
| CPU | Centrum podpory používateľov v DataCentre. |
| Dotknutá osoba | je každá fyzická osoba, ktorej sa osobné údaje týkajú. |
| IKT | Informačno-komunikačné technológie. |
| Informačný systém osobných údajov (ďalej aj „IS OÚ“) | je 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 osobných údajov sa na účely ZOOÚ rozumie aj súbor osobných údajov, ktoré sú spracúvané alebo pripravené na spracúvanie čiastočne automatizovanými alebo inými ako automatizovanými prostriedkami spracúvania.  *Poznámka: IS OÚ je osobitne definovaný pojem na účely ZOOÚ, ktorý nie je možné stotožňovať s pojmom informačný systém používaný v oblasti IT. t.j. IS OÚ nemožno stotožňovať s prostriedkami na spracúvanie osobných údajov (hardvér, softvér), ale pri jeho identifikácii je potrebné upriamiť pozornosť na účel spracúvania osobných údajov. Každý účel spracúvania determinuje (určuje) samostatný IS OÚ.*  *IS OÚ nemusí byť nevyhnutne automatizovaný, t.j. prevádzkovaný pomocou technických a programových prostriedkov (hardvér, softvér), ale môže existovať len v papierovej (listinnej) forme. Príkladom IS OÚ je napríklad kartotéka, kniha návštev, agenda riadenia ľudských* *zdrojov.* |
| Koncový používateľ / používateľ | osoby s aktívnym používateľským účtom v systéme ITMS2014+. |
| Oprávnená osoba | je každá fyzická osoba, ktorá prichádza do styku s osobnými údajmi v rámci svojho pracovného pomeru, na základe pokynu/poverenia. |
| Osobné údaje (OÚ) | údaje týkajúce sa identifikovanej fyzickej osoby alebo identifikovateľnej fyzickej osoby, ktorú možno identifikovať priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora, iného identifikátora,ako je napríklad meno, priezvisko, identifikačné číslo, lokalizačné údaje, alebo online identifikátor, alebo na základe jednej alebo viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú identitu, fyziologickú identitu, genetickú identitu, psychickú identitu, mentálnu identitu, ekonomickú identitu, kultúrnu identitu alebo sociálnu identitu. |
| Poskytovanie OÚ | je odovzdávanie osobných údajov tretej strane, ktorá ich ďalej spracúva. |
| Používateľ ITMS2014+ | žiadatelia o prístup a používatelia neverejnej časti ITMS2014+. |
| Prevádzkovateľ | prevádzkovateľom každý, kto sám alebo spoločne s inými vymedzí účel a prostriedky spracúvania osobných údajov a spracúva osobné údaje vo vlastnom mene; prevádzkovateľ alebo konkrétne požiadavky na jeho určenie môžu byť ustanovené v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná, ak takýto predpis alebo táto zmluva ustanovuje účel a prostriedky spracúvania osobných údajov (§ 5 písm. o) ZOOÚ). |
| Spracúvanie OÚ | spracovateľská operácia alebo súbor spracovateľských operácií s osobnými údajmi alebo so súbormi osobných údajov, najmä získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie, bez ohľadu na to, či sa vykonáva automatizovanými prostriedkami alebo neautomatizovanými prostriedkami. |
| Sprístupňovanie OÚ | je oznámenie osobných údajov alebo umožnenie prístupu k nim príjemcovi, ktorý ich ďalej nespracúva. |
| Tretia strana | je každý, kto nie je dotknutou osobou, prevádzkovateľom poskytujúcim osobné údaje, sprostredkovateľom alebo oprávnenou osobou. |
| Účel spracúvania OÚ | je vopred jednoznačne vymedzený alebo ustanovený zámer spracúvania osobných údajov, ktorý sa viaže na určitú činnosť. |
| ZOOÚ | Zákon č.18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov. |
| Zverejňovanie OÚ | je publikovanie, uverejnenie alebo vystavenie osobných údajov na verejnosti prostredníctvom masovo-komunikačných 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. |

# Základné zásady a pravidlá spracovania OÚ

Prevádzkovateľom IS OÚ v zmysle ZOOÚ sa rozumie každý orgán definovaný zákonom č. 292/2014 Z. z. o príspevku poskytovanom z európskych štrukturálnych a investičných fondov (najmä CKO, CO, OA, RO a SO).

Táto kapitola sumarizuje princípy a pravidlá ochrany osobných údajov aplikovateľné pre prevádzkovateľov a oprávnené osoby prevádzkovateľov v rámci informačného systému ITMS2014+.

Každé závažné narušenie princípov alebo pravidiel spracovania OÚ môže viesť k disciplinárnemu konaniu, resp. k rozviazaniu pracovného pomeru a/alebo k začatiu priestupkového alebo trestného konania.

## Zásady spracovania OÚ

##### Zásada zákonnosti (§ 6 ZOOÚ)

Osobné údaje možno spracúvať len zákonným spôsobom a tak, aby nedošlo k porušeniu základných práv dotknutej osoby.

##### Zásada obmedzenia účelu (§ 7 ZOOÚ)

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 § 78 ods. 8, sa nepovažuje za nezlučiteľné s pôvodným účelom.

*Zásada minimalizácie osobných údajov (§ 8 ZOOÚ)*

Spracúvané osobné údaje musia byť primerané, relevantné a obmedzené na nevyhnutný rozsah daný účelom, na ktorý sa spracúvajú.

*Zásada správnosti (§ 9 ZOOÚ)*

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 (§ 10 ZOOÚ)*

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 § 78 ods. 8.

*Zásada integrity a dôvernosti (§ 11 ZOOÚ)*

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 (§ 12 ZOOÚ)*

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 úradu preukázať.

##### Dodržiavanie uvedených zásad sa zabezpečuje ich zapracovaním do príslušných procesov, ktoré má organizácia na spracovávanie osobných údajov vypracované.

## Pravidlá spracovania OÚ

Každý kto spracúva osobné údaje v systéme ITMS2014+ sa riadi a dodržiava zásady ochrany osobných údajov, chráni osobné údaje pred možným zneužitím, poškodením alebo stratou a bráni prípadnému úniku osobných údajov.

### Spracúvanie osobných údajov

Spracúvať osobné údaje môže len oprávnená osoba a len v rozsahu pridelených oprávnení. V rámci vykonávanej činnosti zodpovedá za dodržiavanie pravidiel spracúvania osobných údajov určených týmto predpisom ako aj ostatnými predpismi vydanými CKO alebo prevádzkovateľom, ktorý oprávnenú osobu poveril.

Spracúvať možno len také osobné údaje, ktoré svojim rozsahom a obsahom zodpovedajú účelu ich spracúvania: „***poskytovanie príspevku z európskych štrukturálnych a investičných fondov, kontrola a súvisiace činnosti***“ (porovnaj § 47 ods. 1 zákona č. 292/2014 Z. z.).

### Súhlas dotknutej osoby

Osobné údaje je možné spracúvať iba s jednozančným vyjadrením súhlasu dotknutej osoby s výnimkou situácií uvedených nižšie.

Bez súhlasu dotknutej osoby je možné spracúvať osobné údaje len v prípadoch ak:

* spracúvanie osobných údajov je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo na vykonanie opatrenia pred uzatvorením zmluvy na základe žiadosti dotknutej osoby,
* spracúvanie osobných údajov je nevyhnutné podľa osobitného predpisu alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná,
* spracúvanie osobných údajov je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, alebo
* 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 osobu dieťa; tento právny základ sa nevzťahuje na spracúvanie osobných údajov orgánmi verejnej moci pri plnení ich úloh.

### Získavanie osobných údajov

Osobné údaje je možné od dotknutej osoby získavať iba spôsobom a postupom schváleným prevádzkovateľom a v súlade s jeho internými predpismi. Spravidla sú osobné údaje získavané prostredníctvom formulárov webovej aplikácie ITMS2014+.

Na požiadanie dotknutej osoby je oprávnená osoba zabezpečujúca získavanie osobných údajov povinná preukázať príslušnosť k prevádzkovateľovi.

Pri získavaní a spracúvaní osobných údajov dotknutých osôb sú osoby oprávnené spracúvať osobné údaje povinné dodržiavať nasledovné pravidlá:

* zabezpečiť dodržiavanie diskrétnosti v mieste získavania osobných údajov,
* zabezpečiť, aby do písomností, ktoré obsahujú osobné údaje, nemali možnosť nahliadnuť osoby, ktoré nie sú oprávnené spracúvať osobné údaje,
* overiť správnosť osobných údajov v súlade s definovanými pracovnými postupmi,
* telefonický prenos osobných údajov minimalizovať iba na nevyhnutné prípady a v minimálnom rozsahu,
* osoby oprávnené spracúvať osobné údaje nesmú získavať osobné údaje dotknutých osôb pod zámienkou iného účelu alebo inej činnosti.

### Kopírovanie/skenovanie úradných dokladov

Kopírovanie/skenovanie úradných dokladov je možné iba po splnení niektorej z nižšie uvedených podmienok, iba s písomným súhlasom dotknutej osoby, alebo ak to osobitný zákon výslovne umožňuje bez súhlasu dotknutej osoby (napríklad v zmysle § 47 ods. 6 zákona č. 292/2014 Z. z.).

Ak je to nevyhnutné, za získanie písomného súhlasu dotknutých osôb s kopírovaním/skenovaním úradného dokladu zodpovedá oprávnená osoba. Súhlas dotknutej osoby nesmie byť podmieňovaný hrozbou odmietnutia zmluvného vzťahu, služby, tovaru alebo povinnosti ustanovenej právnym prepisom.

Pri získavaní osobných údajov kopírovaním/skenovaním úradných dokladov je nevyhnutné zabezpečiť, aby boli získavané osobné údaje len v rozsahu zlučiteľnom s účelom spracúvania (to znamená, že všetky nepotrebné osobné údaje musia byť pred kopírovaním/skenovaním prekryté alebo po kopírovaní musí byť zabezpečené ich vymazanie/začiernenie tak, aby neboli čitateľné).

### Poskytovanie, sprístupňovanie a zverejňovanie osobných údajov

Zverejňovanie osobných údajov spracúvaných prevádzkovateľom je zakázané s výnimkou, ak je zverejňovanie osobných údajov vykonané v súlade s ustanoveniami zákona, ktorý ukladá povinnosť prevádzkovateľovi na ich zverejnenie (napríklad § 47 ods. 5 alebo § 48 ods. 1 zákona č. 292/2014 Z. z.).

Poskytovanie a sprístupňovanie osobných údajov tretím stranám môže byť realizované len na základe písomnej zmluvy alebo platného právneho predpisu (napríklad § 47 ods. 5 zákona č. 292/2014 Z. z.).

Spracúvané osobné údaje na základe osobitného zákona možno z informačného systému poskytnúť, preniesť alebo zverejniť len vtedy, ak osobitný zákon ustanovuje účel poskytovania alebo účel zverejňovania, zoznam spracúvaných osobných údajov alebo rozsah spracúvaných osobných údajov, ktoré možno poskytnúť alebo zverejniť, prípadne príjemcov, ktorým sa osobné údaje poskytnú (napr. Sociálna poisťovňa, miestne príslušný Daňový úrad, zdravotná poisťovňa a pod.).

Poskytovanie alebo zverejnenie osobných údajov nesmie narušiť vážnosť, dôstojnosť a bezpečnosť dotknutej osoby.

### Spracovanie osobných údajov sprostredkovateľom

Spracúvanie osobných údajov v mene prevádzkovateľa môže zabezpečovať aj sprostredkovateľ za nasledujúcich podmienok:

* Sprostredkovateľ poskytuje dostatočné záruky na prijatie primeraných technických a organizačných opatrení tak, aby spracúvanie osobných údajov spĺňalo požiadavky ZOOÚ a aby sa zabezpečila ochrana práv dotknutej osoby. Na poverenie sprostredkovateľa spracúvaním osobnýchú dajov sa v tomto prípade súhlas dotknutej osoby nevyžaduje.
* Sprostredkovateľ nesmie poveriť spracúvaním osobných údajov ďalšieho sprostredkovateľa bez predchádzajúceho osobitného písomného súhlasu prevádzkovateľa alebo všeobecného písomného súhlasu prevádzkovateľa. Sprostredkovateľ je povinný vopred informovať prevádzkovateľa o poverení ďalšieho sprostredkovateľa, ak sa poverenie vykonalo na základe všeobecného písomného súhlasu.
* Spracúvanie osobných údajov sprostredkovateľom sa riadi zmluvou alebo iným právnym úkonom, ktorý zaväzuje sprostredkovateľa voči prevádzkovateľovi a v ktorom je ustanovený predmet a doba spracúvania, povaha a účel spracúvania, zoznam alebo rozsah osobných údajov, kategórie dotknutých osôb a povinnosti a práva prevádzkovateľa; zmluva alebo iný právny úkon musí byť uzatvorený v listinnej alebo elektronickej podobe. V zmluve alebo inom právnom úkone musia byť ustanovenené povinnosti sprostredkovateľa minimálne v zmysle § 34 ods. 3 písmeno a) až i) ZOOÚ.
* Ak sprostredkovateľ zapojí do vykonávania osobitných spracovateľských činností v mene prevádzkovateľa ďalšieho sprostredkovateľa, tomuto ďalšiemu sprostredkovateľovi v zmluve alebo inom právnom úkone je povinný uložiť rovnaké povinnosti týkajúce sa ochrany osobných údajov, ako sú ustanovené v zmluve alebo v inom právnom úkone medzi prevádzkovateľom a sprostredkovateľom podľa § 34 ods. 3 ZOOÚ, a to najmä poskytnutie dostatočných záruk na prijatie primeraných technických a organizačných opatrení tak, aby spracúvanie osobných údajov spĺňalo požiadavky ZOOÚ. Zodpovednosť voči prevádzkovateľovi nesie pôvodný sprostredkovateľ, ak ďalší sprostredkovateľ nesplní svoje povinnosti týkajúce sa ochrany osobných údajov.

Dohľad pri výbere sprostredkovateľa a vypracovanie návrhu zmluvy alebo písomného poverenia zabezpečí štatutár prevádzkovateľa, alebo ním poverený zamestnanec.

Každá zmluva, v ktorej je súčasťou plnenia aj spracúvanie osobných údajov inou zmluvnou stranou, musí byť pred podpisom odsúhlasená štatutárom prevádzkovateľa alebo ním splnomocnenou osobou (napr. zabezpečenie technickej prevádzky informačného systému obsahujúceho osobné údaje).

### Cezhraničný prenos osobných údajov

Pred uskutočnením cezhraničného prenosu osobných údajov je každý iniciátor prenosu povinný nechať odsúhlasiť podmienky cezhraničného prenosu štatutárovi prevádzkovateľa alebo ním poverenej osobe.

### Kvalita spracúvania osobných údajov

Všetky osoby, ktoré vykonávajú spracúvanie osobných údajov sú povinné spracúvať iba správne (presné a aktuálne) osobné údaje. Osobný údaj sa považuje za správny, kým sa nepreukáže opak. V zmysle §22 ZOOÚ má dotknutá osoba právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. So zreteľom na účel spracúvania osobných údajov má dotknutá osoba právo aj na doplnenie neúplných osobných údajov.

Nesprávne a neúplné osobné údaje musia byť blokované a bez zbytočného odkladu opravené alebo doplnené. Nesprávne a neúplné osobné údaje, ktoré nemožno opraviť alebo doplniť tak, aby boli správne a úplné, musia byť zreteľne označené a bez zbytočného odkladu zlikvidované. Všetky tieto kroky oprávnené osoby konzultujú so zodpovednou osobou poverenou dohľadom nad spracovaním osobných údajov a v prípade potreby s administrátorom RO/SO.

Oprávnená osoba súčasne zaistí, aby informácie o zablokovaní, oprave, doplnení alebo likvidácii osobných údajov boli bez zbytočného odkladu odovzdané všetkým príjemcom.

### Likvidácia osobných údajov

Osobné údaje je možné spracúvať iba po dobu, pokiaľ pretrváva účel ich spracovania. Po tejto dobe je každá oprávnená osoba povinná tieto osobné údaje bezodkladne zlikvidovať. Doby uchovávania jednotlivých údajov definujú interné riadiace akty prevádzkovateľa (napr. registratúrny plán), respektíve všeobecne záväzné právne predpisy.

Osobné údaje sa nezlikvidujú iba v prípadoch, ak osobitný zákon ustanovuje lehotu, ktorá neumožňuje osobné údaje zlikvidovať.

Vzhľadom k tomu, že na IS ITMS2014+ sa dajú uplatniť obmedzenia na práva dotknutých osôb, ktoré uvádza §30 ZOOÚ (predovšetkým odsek 1 bod e)), nie je prevádzkovateľ povinný vymazať osobné údaje, ktoré sa týkajú dotknutej osoby, ak by táto chcela uplatniť svoje právo podľa §23 ZOOÚ.

Ak nie sú inými internými predpismi prevádzkovateľa definované prísnejšie pravidlá na likvidáciu, musia byť osobné údaje likvidované minimálne vymazaním (prepísaním) alebo fyzickým zničením informačného média prekračujúcim možnosť obnovy informačného obsahu.

Pred odovzdaním pamäťových médií alebo zariadení obsahujúcich pamäťové médiá na údržbu, servis alebo výmenu externému subjektu, musí byť vykonaná identifikácia, či sa na pamäťovom médiu nenachádzajú osobné údaje. V prípade, ak sa na disku osobné údaje nachádzajú, musí byť pred odovzdaním média externému subjektu zabezpečená bezpečná likvidácia osobných údajov z média alebo musí byť externému subjektu odovzdané zariadenie bez takéhoto média.

### Poučenie oprávnených osôb a zabezpečenie mlčanlivosti

Štatutár prevádzkovateľa, alebo ním poverená osoba (zodpovedná osoba), zodpovedá za oboznámenie dotknutých osôb s právami a povinnosťami ustanovenými ZOOÚ, so zodpovednosťami za ich porušenie a s rozsahom oprávnení, popisom povolených činností a podmienkami spracúvania osobných údajov v podmienkach prevádzkovateľa.

Oprávnené osoby musia byť poučené v zmysle ZOOÚ a poverené na výkon činnosti ešte pred uskutočnením prvej operácie. Oprávnené osoby potvrdia vykonanie poučenia vlastnoručným podpisom na zázname: „Poučenie oprávnených osôb“. Všeobecné úlohy a zodpovednosti oprávnenej osoby sú uvedené v internej smernici MIRRI.

V primeranom rozsahu musia byť s obsahom tohto bezpečnostného manuálu oboznámení aj zamestnanci externých subjektov, ktorí majú prístup k IS OÚ ITMS2014+. Oboznámenie týchto osôb a zmluvné zabezpečenie dodržiavania tejto smernice zaistí zodpovedná osoba a zamestnanci úradu, ktorí spoluprácu s externými subjektmi realizujú.

Oprávnené osoby úradu poverené spracovávaním OÚ sú v rámci poučenia v zmysle ZOOÚ tiež upozornené na povinnosť zachovávať mlčanlivosť), pričom povinnosť mlčanlivosti sa vzťahuje aj na obdobie po skončení pracovnoprávneho vzťahu oprávnenej osoby alebo obdobného pracovného vzťahu oprávnenej osoby.

### Ochrana práv dotknutých osôb

Prevádzkovateľ je povinný pri spracovaní osobných údajov dodržiavať nasledovné práva dotknutej osoby, ktorých naplnenie má dotknutá osoba právo vyžadovať na základe písomnej žiadosti:

* Na poskytovanie informácií dotknutej osobe pri získavaní OÚ od nej (§19)
* Na poskytovanie informácií, ak osobné údaje nie sú získané od dotknutej osoby (§20)
* Na prístup k svojim OÚ (§21)
* Na opravu svojich OÚ (§22)
* Na vymazanie svojich OÚ(§23)
* Na obmedzenie spracúvania svojich OÚ(§24)
* Na dodržiavanie oznamovacej povinností voči dotknutej osobe (§25)
* Na zabezpečenie prenosnosti OÚ (§26)
* Na namietanie spracúvania OÚ (§27)
* Aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní osobných údajov vrátane profilovania a ktoré má právne účinky (§28).

Vzhľadom k tomu, že na IS ITMS2014+ sa dajú uplatniť určité obmedzenia na práva dotknutých osôb v zmysle §30 ZOOÚ (predovšetkým odsek 1 bod e)) ak je to zadefinované v osobitnom predpise alebo medzinárodnej zmluve, ktorou je Slovenská republika viazaná (§30 odsek 2), tak konkrétne uplatňované obmedzenia v IS ITMS2014+ sú nasledovné:

* na základe §47 Zákona č. 292/2014 Z. z.:
  + vymazanie svojich OÚ(§23),
  + obmedzenie spracúvania svojich OÚ(§24),
  + namietanie spracúvania OÚ (§27).

Informácie sú poskytované dotknutej osobe bezplatne najneskôr do 30 dní odo dňa prijatia písomnej žiadosti. Za opakované poskytnutie osobných údajov, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Prevádzkovateľ je povinný poskytnúť osobné údaje dotknutej osobe spôsobom podľa jej požiadavky.

Uplatnenie práv dotknutých osôb vyplývajúcich zo ZOOÚ zabezpečuje zodpovedný zamestnanec.

### Zabezpečenie vedenia záznamov

Povinnosť zabezpečiť vedenie záznamov o spracovateľských činnostiach vyplýva prevádzkovateľovi z §37 ods.1 ZOOÚ, pričom:

* Tento záznam musí obsahovať:
  + identifikačné údaje a kontaktné údaje prevádzkovateľa, spoločného prevádzkovateľa, zástupcu prevádzkovateľa, ak bol poverený a zodpovednej osoby,
  + účel spracúvania osobných údajov,
  + opis kategórií dotknutých osôb a kategórií osobných údajov,
  + kategórie príjemcov vrátane príjemcu v tretej krajine alebo medzinárodnej organizácií,
  + označenie tretej krajiny alebo medzinárodnej organizácie, ak prevádzkovateľ zamýšľa prenos osobných údajov do tretej krajiny alebo medzinárodnej organizácie a dokumentáciu o primeraných zárukách, ak prevádzkovateľ zamýšľa prenos podľa § 51 ods. 1 a 2,
  + predpokladané lehoty na vymazanie rôznych kategórií osobných údajov,
  + všeobecný opis technických a organizačných bezpečnostných opatrení podľa § 39 ods. 1.

Záznamy sa môžu viesť v listinnej podobe alebo elektronickej podobe a vedie ich zodpovedná osoba.

### Incidenty týkajúce sa spracovania OÚ

Oprávnené osoby sú povinné informovať svojho priameho nadriadeného, resp. zodpovednú osobu alebo bezpečnostného zamestnanca, ak zistia porušenie alebo nedodržanie princípov ochrany OÚ.

Zodpovedná osoba (v zastúpení prevádzkovateľa) zabezpečí oznámenie porušenia ochrany osobných údajov úradu, pričom:

* musí tak urobiť do 72 hodín po tom, ako sa o incidente dozvedel; to neplatí, ak nie je pravdepodobné, že porušenie ochrany osobných údajov povedie k riziku pre práva fyzickej osoby; ak nedodrží uvedenú lehotu, musí zmeškanie lehoty zdôvodniť,
* oznámenie 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 porušenia ochrany osobných údajov,
  + opis opatrení prijatých alebo navrhovaných prevádzkovateľom  na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.
* ak v čase oznámenia nie sú prevádzkovateľovi známe všetky požadované informácie, poskytne ich bezodkladne po tom, čo sa o nich dozvie.
* je povinná zdokumentovať každý prípad porušenia ochrany osobných údajov vrátane skutočností spojených s porušením ochrany osobných údajov, jeho následky a prijaté opatrenia na nápravu.

Zodpovedná osoba (v zastúpení prevádzkovateľa) zabezpečí oznámenie porušenia ochrany osobných údajov dotknutej osobe, pričom:

* je povinný tak urobiť bez zbytočného odkladu, ak takéto porušenie ochrany osobných údajov môže viesť k vysokému riziku pre práva fyzickej osoby,
* oznámenie musí obsahovať:
  + jasne a jednoducho formulovaný opis povahy porušenia ochrany osobných údajov,
  + kontaktné údaje zodpovednej osoby alebo iného kontaktného miesta, kde možno získať viac informácií,
  + opis pravdepodobných následkov porušenia ochrany osobných údajov,
  + opis opatrení prijatých alebo navrhovaných prevádzkovateľom  na nápravu porušenia ochrany osobných údajov vrátane opatrení na zmiernenie jeho potenciálnych nepriaznivých dôsledkov, ak je to potrebné.
* toto oznámenie sa nevyžaduje, ak:
  + prevádzkovateľ prijal primerané technické a organizačné ochranné opatrenia a uplatnil ich na osobné údaje, ktorých sa porušenie ochrany osobných údajov týka, a to najmä šifrovanie alebo iné opatrenia, na základe ktorých sú osobné údaje nečitateľné pre osoby, ktoré nie sú oprávnené mať k nim prístup,
  + prevádzkovateľ prijal následné opatrenia na zabezpečenie vysokého rizika porušenia práv dotknutej osoby,
  + by to vyžadovalo neprimerané úsilie; prevádzkovateľ je povinný informovať verejnosť alebo prijať iné opatrenie na zabezpečenie toho, že dotknutá osoba bude informovaná rovnako efektívnym spôsobom.

### Dohľad nad ochranou osobných údajov – zodpovedná osoba

Dohľadom nad ochranou osobných údajov je poverená zodpovedná osoba. Postavenie zodpovednej osoby určuje §45 ZOOÚ a jej úlohy §46 ZOOÚ.

# Základné princípy a pravidlá informačnej bezpečnosti

Táto kapitola sumarizuje princípy a pravidlá informačnej bezpečnosti aplikovateľné pre koncových používateľov, administrátorov IS a manažérov ITMS2014+, platné pre prostredie ITMS2014+.

Každé závažné narušenie princípov alebo pravidiel informačnej bezpečnosti (napr. úmyselné porušenie) môže viesť k disciplinárnemu konaniu a/alebo k začatiu priestupkového alebo trestného konania.

## Princípy informačnej bezpečnosti

V tejto podkapitole sú uvedené všeobecne záväzné princípy informačnej bezpečnosti.

##### Dôvernosť

Pri spracúvaní dát v IS ITMS2014+ sú povinní tí, ktorí prichádzajú s nimi do styku, zachovávať o týchto údajoch mlčanlivosť. Údaje môžu zverejniť, poskytnúť a sprístupniť iba v súlade s internými predpismi, resp. po schválení prevádzkovateľom. Osobné údaje je možné spracúvať len v súlade s § 13 ZOOÚ. Povinnosť mlčanlivosti trvá aj po ukončení spracúvania dát a platí aj po zániku oprávnenia k prístupu k údajom. Zároveň sú aplikované primerané bezpečnostné opatrenia proti náhodnému, resp. úmyselnému neautorizovanému prístupu k údajom.

##### Integrita

Údaje sú počas celého životného cyklu uchovávané podľa okolností aktuálne, presne a konzistentne a sú chránené pred neautorizovanou alebo náhodnou zmenou. Sú aplikované primerané bezpečnostné opatrenia proti náhodnému, resp. úmyselnému narušeniu alebo modifikácii dát.

##### Dostupnosť

Používatelia s primeranými prístupovými právami majú prístup k údajom spracúvaných v ITMS2014+, v zmysle interných predpisov. Sú aplikované primerané bezpečnostné opatrenia proti náhodnej, resp. úmyselnej strate alebo zničeniu dát.

##### Nepopierateľnosť

Všetky úkony používateľov musia byť primerane zaznamenávané, aby bolo spätne dohľadateľné kto a kedy zmeny vykonal. Činnosť používateľov v IS je zaznamenávaná prostredníctvom auditných záznamov (logov) a vo vybraných prípadoch aj elektronickým podpisom, prípadne časovou pečiatkou. Použitie elektronického podpisu a časovej pečiatky vyplýva buď priamo z požiadaviek legislatívy (napr. zákon č. 215/2002 Z. z. o elektronickom podpise a o zmene a doplnení niektorých zákonov), alebo je to nevyhnutné pre zaručenie právnych následkov spojených s úkonom používateľa v ITMS2014+.

##### Minimálne právomoci

Rozsah prístupu k údajom musí byť v každom okamihu obmedzený na minimálnu možnú a zároveň plne postačujúcu mieru nevyhnutnú pre plnenie pracovných povinností používateľa.

##### Oddelenie právomocí

Špecifické role v matici prístupových práv (napr. audit a prevádzka) nesmú byť vzájomne kombinované, aby sa zamedzilo možnému vzniku konfliktu záujmov.

## Pravidlá informačnej bezpečnosti

Používateľ sa riadi a dodržiava zásady bezpečnosti pri práci s informačným systémom, chráni informačný systém proti možným útokom, ktoré môžu narušiť jeho funkčnosť a bráni prípadnému úniku dôverných informácií.

Nasledujúce pravidlá sú záväzné najmä pre koncových používateľov, administrátorov IS a manažérov ITMS2014+.

### Riadenie prístupových práv

Táto oblasť je v zodpovednosti manažérov ITMS2014+ DC a je podrobne upravená interným predpisom DataCentra: Manuál pre prístupové práva do ITMS2014+, vrátane procesu riadenia prístupových práv ako aj princípom oddelenia právomocí a procesom previerky prístupových práv.

V prípade straty, resp. zneužitia alebo podozrenia zo zneužitia bezpečnostných prvkov je používateľ povinný bezodkladne informovať o tejto skutočnosti na telefónnom čísle 0850 123 344 alebo elektronicky na adrese [cpu@datacentrum.sk](mailto:cpu@datacentrum.sk), a následne písomne na adresu DataCentrum, Cintorínska 5, 814 88 Bratislava.

### Politika hesiel verejnej časti ITMS2014+

Všetci používatelia musia dodržiavať nasledovné pravidlá politiky hesiel:

* heslá musia udržiavať v tajnosti;
* heslá nesmú byť zaznamenávané (napr. na papieri, v súboroch alebo v prenosných zariadeniach), s výnimkou ich bezpečného uloženia a v prípade, ak bol spôsob ich uloženia schválený;
* heslá sa musia zmeniť v prípade akéhokoľvek náznaku možného kompromitovania systému alebo hesla;
* heslo musí byť kvalitné, a to tak, aby:
* bolo dobre zapamätateľné;
* nebolo založené na informáciách vzťahujúcich sa k osobe, ktoré môže ktokoľvek ďalší ľahko uhádnuť alebo získať, napríklad mená, telefónne čísla, dátumy narodenia a pod.;
* nebolo zraniteľné pri použití slovníkových útokov (nemalo by sa skladať zo slov vyskytujúcich sa v slovníkoch);
* neobsahovalo po sebe idúce rovnaké znaky a neobsahovalo iba číselné alebo iba písmenové skupiny,
* celková dĺžka hesla min. 8 znakov,
* minimálne 1 použité veľké písmeno,
* minimálne 1 použitá číslica,
* maximálny počet opakovaní prihlásenia 5 krát (po 5 neúspešných pokusoch o prihlásenie sa konto zablokuje),
* expirácia hesla 90 dní,
* počet dní pre varovanie o expirácií 15 dní
* používatelia sa musia vyhýbať opakovanému používaniu alebo opakovaniu starých hesiel;
* používatelia musia zmeniť dočasné heslá pri prvom prihlásení;
* používatelia nebudú zahŕňať heslá do žiadneho automatizovaného prihlasovacieho procesu, napríklad uloženie do makra alebo funkčné klávesy;
* používatelia nesmú zdieľať osobné používateľské heslá;
* používatelia nebudú používať rovnaké heslá pre súkromné a pracovné účely;
* používatelia sa môžu prihlasovať do informačného systému len pod svojím prístupovým menom (loginom).

Politika hesiel neverejnej časti ITMS2014+ je v kompetencii DataCentra.

### Politika čistej obrazovky

Používateľ je povinný odhlásiť sa z informačného systému pri prerušení alebo ukončení práce, resp. je povinný uzamknúť svoj počítač (napr. pred opustením pracoviska).

### Spracovanie údajov

Používatelia (žiadatelia a prijímatelia) v zmysle § 49 ods. 3 zákona č. 292/2014 Z. z. zodpovedajú za aktuálnosť, pravdivosť, úplnosť a správnosť nimi vložených údajov do ITMS2014+.

Používateľ je povinný kontrolovať údaje, ktoré vkladá do informačného systému. Kontrolované majú byť transakčné vstupy, vlastné dáta (napr. mená a adresy, telefónne čísla) a číselníky (napr. mestá, mestské časti). V prípade, ak zistí chybu v údajoch vložených do systému, pokiaľ je to možné, údaje zaktualizuje alebo o chybe informuje relevantné osoby (napr. CKO).

Používateľ nesmie bez primeraného dôvodu z IS sťahovať citlivé dáta (napr. osobné údaje) a ukladať ich na lokálnu pracovnú stanicu, ani ich posielať nechráneným kanálom (napr. email) alebo poskytovať/sprístupňovať tretím stranám.

### Antivírusová ochrana

Používateľ je povinný používať na svojej lokálnej stanici aktualizovaný antivírusový systém a nesmie ho bezdôvodne vypínať ani inak znefunkčniť.

Používateľ musí pristupovať k mailovým správam s obozretnosťou; neotvárať neznáme prílohy alebo prílohy od neznámych odosielateľov a nespúšťať internetové odkazy z emailových správ, ale odkaz manuálne skopírovať do prehliadača.

V prípade podozrenia na vírusovú infekciu je povinný bezodkladne kontaktovať svojho správcu IT.

### Riešenie incidentov a porúch

Používatelia informačného systému sú povinní zaznamenať a hlásiť akékoľvek bezpečnostné incidenty a slabiny, alebo podozrenia na bezpečnostné incidenty a slabiny v systémoch alebo službách.

Ak používateľ identifikuje akékoľvek problémy, poruchy alebo odchýlky od štandardnej prevádzky, je povinný bezodkladne o týchto problémoch informovať svojho správcu IT alebo CPU.

Niektoré príklady bezpečnostných udalostí a incidentov sú:

* strata služby, zariadenia alebo vybavenia,
* chybné fungovanie alebo preťaženie systému,
* ľudské chyby,
* nesúlad s politikami alebo smernicami,
* porušenie opatrení fyzickej bezpečnosti,
* nekontrolované zmeny systému,
* chybné fungovanie technického a programového vybavenia,
* porušenie prístupu.

### Povedomie o informačnej bezpečnosti

Používateľ je povinný oboznamovať sa s bezpečnostnými princípmi a pravidlami ITMS2014+ a zúčastňovať sa školení koncových používateľov v oblasti informačnej bezpečnosti.

Používateľ je povinný zúčastňovať sa školení v oblasti informačnej bezpečnosti (o možnostiach sa môže informovať u svojho správcu IT). Používateľ si má udržiavať primerané povedomie o informačnej bezpečnosti a potenciálnych hrozbách. Používateľ by mal poznať:

* aktuálne odporúčania pre kvalitu hesiel (napr. odporúčanú minimálnu dĺžku hesla a komplexnosť hesla, odporúčania ohľadom používania fráz miesto tradičných hesiel a pod.),
* aktuálne pravidlá informačnej bezpečnosti platné v jeho organizácii,
* možné negatívne dopady vyplývajúce z úniku a prezradenia citlivých údajov,
* najčastejšie hrozby spojené s používaním sociálnych sietí (napr. Facebook),
* najčastejšie hrozby v oblasti škodlivého softvéru,
* najčastejšie scenáre sociálneho inžinierstva (napr. nevyžiadané maily/telefonáty požadujúce zadanie autentifikačných prostriedkov, podvodné webstránky navodzujúce dojem legitímnosti),
* stav aktualizácií operačného systému, internetového prehliadača, antivírového softvéru a ďalších kľúčových prvkov (napr. JAVA) lokálnej pracovnej stanice používateľa,
* komu a ako nahlasovať podozrenia na porušenie informačnej bezpečnosti.

### Aktualizácia používateľských údajov

Každý používateľ je povinný bez zbytočného odkladu aktualizovať údaje vo svojom používateľskom účte. Prevádzkovateľ nezodpovedá za aktuálnosť používateľových údajov.

## Vybrané pravidlá informačnej bezpečnosti pre administrátorov IS

Základné pravidlá informačnej bezpečnosti pre administrátorov IS sú uvedené  v internej smernici MIRRI . Nasledujúce pravidlá dopĺňajú tieto smernice a sú záväzné pre administrátorov IS.

### Riadenie prevádzkových záznamov

V systéme ITMS2014+ sa musia vytvárať prevádzkové záznamy s cieľom:

* spojiť udalosti v systéme ITMS2014+ s konaním používateľov a administrátorov IS,
* rekonštruovať udalosti v chronologickom slede,
* detegovať potenciálny prienik do systému,
* monitorovať systémové kapacity a prevádzkové parametre.

Za celý životný cyklus (nastavenie, monitorovanie, vyhodnocovanie, zálohovanie a likvidáciu) prevádzkových záznamov sú zodpovední administrátori IS. Rovnako sú zodpovední aj za nastavenie a konsolidovanie časových informácií (prostredníctvom NTP protokolu) naprieč infraštruktúrou ITMS2014+.

Prevádzkové záznamy musia byť chránené pred náhodnou alebo úmyselnou zmenou a pred zničením. Prístup k prevádzkovým záznamom musí byť obmedzený len pre administrátorov IS a ďalšie relevantné role (napr. audítor, vlastník systému a pod).

Pri nastavení rozsahu prevádzkových záznamov, ako aj doby ich archivácie, je potrebné okrem bezpečnostných požiadaviek prihliadať aj na dostupné kapacity monitorovacieho systému. Všetky systémy vytvárajúce prevádzkové záznamy musia mať primeranú diskovú kapacitu pre uchovávanie záznamov. Vhodné je, aby médium uchovávajúce záznamy neumožňovalo zmenu údajov, ale iba zápis a čítanie.

Prevádzkové záznamy musia byť pravidelne vyhodnocované (minimálne raz mesačne). Na vyhodnocovanie sa môže použiť automatizovaný nástroj (napr. SIEM). Takýto systém by mal vytvárať varovania v prípade neštandardných udalostí.

Prevádzkové záznamy musia byť taktiež pravidelne zálohované do geograficky odlišnej lokality a primerane dlho archivované.

Administrátori IS musia zabezpečiť, že v prípade krátkodobého špičkového zaťaženia systému nedôjde k prerušeniu tvorby záznamov.

##### Príklady prevádzkových záznamov a štandardizovaného formátu prevádzkových záznamov

Prevádzkové záznamy by mali zahŕňať transakcie alebo udalosti, ako napríklad:

* neúspešné prihlásenia,
* prihlásenia mimo bežného pracovného času (napr. 07:00 – 19:00),
* zamknutie účtov po presiahnutí povoleného počtu pokusov o prihlásenie,
* neobvyklú sieťovú aktivitu (skenovanie siete, prenos neobvykle veľkého objemu dát apod.),
* zmeny konfigurácie mimo bežnej údržby a bez formálneho záznamu,
* prístupy používateľov,
* eskalácia prístupových práv,
* neautorizované použitie zdrojov,
* neprivilegovaný prístup k súborom,
* prístup k samotným prevádzkovým záznamom,
* neobvyklé čerpanie systémových prostriedkov (napr. pamäť, CPU),
* vytvorenie/spustenie novej služby (procesu) v operačnom systéme,
* pokles kapacity systémových prostriedkov pod kritickú hranicu (napr. diskový priestor, pamäte a pod.),
* zlyhanie systémových procesov,
* vznik systémových chýb,
* atď.

Každý log by mal byť generovaný v štandardizovanom formáte (napr. podľa iniciatívy CEE) a mal by obsahovať:

* dátum a časovú počiatku,
* zdrojovú adresu alebo službu alebo ID používateľa (subjekt),
* cieľovú adresu alebo názov služby prípadne zdroja (objekt),
* ďalšie doplňujúce charakteristiky paketu alebo transakcie alebo udalosti.

### Riadenie incidentov

Incidentom je udalosť, ktorá má alebo potenciálne môže mať negatívny dopad na prevádzku IS ITMS2014+. Administrátori IS v spolupráci s manažérom bezpečnosti sú zodpovední za monitorovanie, analýzu a riešenie incidentov. Preverené musia byť všetky podozrenia na incident.

Fázy riešenia bezpečnostných incidentov:

* kategorizácia identifikovaných alebo nahlásených udalostí,
* detekcia potenciálnych incidentov v prostredí IS ITMS2014+,
* návrh riešenia, odstránenie incidentu a obnova bežnej prevádzky,
* podrobná analýza incidentu a návrh opatrení.

Všetky incidenty musia byť evidované. Evidencia zahŕňa dátum a čas zistenia incidentu, jeho popis, eskaláciu, aktuálny stav a dátum zmeny stavov, riešenie a vyhodnotenie incidentu a návrh opatrení, ako aj dátum a čas uzavretia incidentu. Riadenie incidentov by malo byť podporené automatizovaným nástrojom (napr. Service desk). Každý incident musí mať priradeného vlastníka.

Rovnako musia byť všetky incidenty klasifikované podľa veľkosti možného negatívneho dopadu, respektíve rizík spojených s incidentom na škále:

* **nezávažný** – negatívny dopad na ITMS2014+ a údaje v ňom uložené (je zanedbateľný),
* **závažný** – negatívny dopad má významný vplyv na funkčnosť IS alebo dostupnosť, dôvernosť alebo integritu údajov v ňom,
* **kritický** – negatívny dopad môže spôsobiť úplnú nedostupnosť IS alebo kompromitáciu údajov v IS (prezradenie/zmenu/stratu dát).

Základnú podporu pre používateľov poskytuje Centrum podpory užívateľov. V prípade ak nedokážu príčinu incidentu a jeho následky odstrániť v primeranom čase, musia incident bezodkladne eskalovať na príslušného administrátora (databázový, systémový alebo aplikačný) alebo poskytovateľa podpory IS.

V prípade opakovania incidentu musí byť preklasifikovaný na problém a musí byť prešetrená príčina jeho opakovaného vzniku; ak je to nevyhnutné v spolupráci s poskytovateľom podpory alebo relevantným dodávateľom. Rovnako musí byť priradené vlastníctvo problému.

Minimálne raz za rok by malo dôjsť k revízii postupu identifikácie incidentov v informačnom systéme a jeho okolí, predovšetkým v prípade nízkeho počtu identifikovaných incidentov respektíve ak všetky incidenty sú klasifikované ako nezávažné.

Administrátori IS by mali pravidelne vyhodnocovať štatistické informácia ako napríklad:

* celkový počet incidentov a problémov (z toho otvorených a uzatvorených),
* progres v riešení incidentov a problémov,
* eskalované incidenty a pod.

##### Príklady incidentov, ich realizácie a prejavov v IKT prostredí

Príkladom incidentu je:

* neúspešný pokus o prihlásenie sa do systému (osobitne opakovaný),
* preniknutie útočníka do systému,
* odopretie služby (anglicky Denial of service, DoS), prípadne špeciálny typ distribuovaného odopretia služby, kedy je útok realizovaný z mnohých IP adries (Distributed DoS, DDoS),
* prítomnosť škodlivého kódu,
* poškodenie IKT prírodným živlom,
* zahltenie lokálnej siete spôsobené nesprávne nakonfigurovaným sieťovým zariadením,
* zlyhanie aplikácie kvôli chybe v kóde aplikácie,
* poškodenie/krádež komponentov IKT.

Príklady spôsobu realizácie útoku zahŕňajú:

* napadnutie samotnej aplikácie a zneužitie jej zraniteľností,
* použitie techník sociálneho inžinierstva, alebo nainštalovania škodlivého kódu na konkrétne pracovné stanice (odchytávanie stlačených kláves, odpočúvanie, snímanie obrazu) kvôli získaniu cenných informácií,
* priame zneužitie privilegovaného prístupu iných používateľov systému, operátorov, alebo administrátorov IS,
* použitie slovníkových útokov na slabé heslá v informačnom systéme a následná eskalácia privilégií,
* násilné činy vlámania, vydierania a krádeže pre získanie prístupu k inkriminovanému systému, alebo jeho dátam.

Príklady prejavu incidentov v IKT prostredí sú nasledovné:

* úplnou nefunkčnosťou systému – hardvérový komponent, alebo informačný systém nereaguje, alebo nie je prístupný,
* zmeneným obsahom webovej stránky – pôvodný obsah webovej stránky bol zmenený kvôli chybe v systéme, alebo úmyselne prepísaný útočníkom,
* neobvyklou sieťovou aktivitou – dajú sa pozorovať určité anomálie oproti štandardnej prevádzke, nezodpovedajúca frekvencia činností používateľov, alebo podozrivé druhy činností,
* neobvyklou záťažou systému – veľké preťaženia systému, ktoré vedú k odopretiu dostupnosti služby,
* podozrivými záznamami – ak prevádzkové záznamy nie sú konzistentné so skutočným správaním systému, nedá sa vylúčiť riziko, že systém je skompromitovaný a útočník tieto záznamy pozmenil.