***Príloha č. 3 k Zmluve o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností***

Logovací štandard

Obsah

[Úvod 1](#_Toc184295821)

[Cieľ dokumentu 2](#_Toc184295822)

[Obmedzenia 2](#_Toc184295823)

[Definícia významu kľúčových slov 3](#_Toc184295824)

[Štandardy pre logovanie 4](#_Toc184295825)

[Obsah logov 4](#_Toc184295826)

[Aktívne logovanie 4](#_Toc184295827)

[Sumarizácia 5](#_Toc184295828)

[Zdroje / kategórie logov 6](#_Toc184295829)

[POZNÁMKY 7](#_Toc184295830)

[Metóda MoSCoW: 7](#_Toc184295831)

[Dodatky 8](#_Toc184295832)

[Zdroje a Legislatívne východiská 8](#_Toc184295833)

[Klasifikačné stupne informačných aktív 11](#_Toc184295834)

# Úvod

Každé vyšetrovanie je založené na dôkazoch, pre informačné systémy sú dôkazy záznamy o aktivitách ktoré aplikácia vykonala. Podobne ako pri vyšetrovaniach v fyzickom svete, lupič v digitálnom svete zanecháva digitálny odtlačok – pripojenie k serveru, autentifikácia do operačného systému, spustenie aplikácie vytvárajú záznam. Tieto záznamy o aktivite sa vytvárajú štandardne pre software zakúpený od osvedčeného výrobcu, pre aplikácie vyvíjané na zákazku alebo interne treba na logovanie , ktoré umožní vyšetrovanie v prípade incidentu zakomponovať do vývoja.

Pre ex-post analýzu KB je nevyhnutné disponovať prevádzkovými záznamami z doby jej výskytu. Zariadení či systémov, ktoré takéto záznamy generujú je veľa, jedná sa všeobecne o bezpečnostné nástroje (antivírus, IDS/IPS, proxy, router, switch, firewall,…), operačné systémy (autentizácia, privilegované spustenie, systémové udalosti,…) a aplikácie (komunikácia medzi klientom a serverom, užívateľské udalosti, prístupy,…).

# Cieľ dokumentu

Tento dokument sumarizuje požiadavky na logovanie, v dokumente sa používajú kľúčové slová „***musí***“, „***malo by byť***“, „***odporúča sa***“. Tieto sú ohodnotením dôležitosti daného opatrenia s ohľadom na jeho implementačnú náročnosť.

Na konci kapitoly je sumárna tabuľka zásad a opatrení s ohodnotením podľa metódy **MoSCoW**, ktorá sa používa pri manažmente, pri analýzach, pri riadení projektov a vývoji softvéru a je v súlade s definíciou významu kľúčových slov uvedenú nižšie.

**Dokument vznikol na základe podkladov z originálu Metodiky zabezpečenia IKT verejnej správy v oblasti informačnej bezpečnosti, ktorého autorom je CSIRT.SK (**[**MetodikaZabezpeceniaIKT\_v2.1.pdf (gov.sk)**](https://www.csirt.gov.sk/wp-content/uploads/2021/08/MetodikaZabezpeceniaIKT_v2.1.pdf?csrt=13636563756532688724)**) a zároveň z dokumentu NIST800-92**

**(**[**SP 800-92, Guide to Computer Security Log Management | CSRC (nist.gov)**](https://csrc.nist.gov/publications/detail/sp/800-92/final)**)**

Pre nasadenie log manažmentu je kľúčové:

* Správne nastavené časové značky na všetkých zdrojoch
* Zaistenie dostatočnej kapacity pre logovanie, pravidelné odosielanie logov do centrálneho log manažmentu a ich uchovávanie po určenú dobu
* Pravidelná analýza logov v log manažmente, najlepšie automatizované upozornenia na výskyt abnormalít
* Zaistenie bezpečnosti a integrity log záznamov (ochrana pred zneužitím, zmenením alebo vymazaním) naprieč celým log manažment systémom
* Dostupnosť logov aj v prípade poruchy systému (zálohovanie)

Dokument neobsahuje podrobné implementačné detaily jednotlivých opatrení. Podrobné implementačné detaily budú musieť byť vypracované v  projektovej dokumentácii, zmenovej dokumentácii a ostatných podkladových materiálov, ktoré spracujú zadávatelia projektov spolu s IT analytikmi, IT architektami, PM a internými či externými dodávateľmi a následne ich predložia odboru BIS na validáciu.

# Obmedzenia

Dokument sa v tejto verzií nezaoberá špecifickými požiadavkami na: fyzickú bezpečnosť infraštruktúry, bezpečnosť mobilných zariadení, bezpečnosť Internetu vecí (IoT – Internet of Things), bezpečnosť ICS systémov (Industrial Control Systems), zabezpečenie služieb využívajúcich IPv4 multicast, zabezpečenie webových služieb (web services)

# Definícia významu kľúčových slov

V tomto dokumente sú použité nasledujúce kľúčové slová podľa uvedeného významu:

**„*musí*“** – špecifikuje povinnú požiadavku (platí aj pre „**je nutné**“)

**„*nesmie*“** – špecifikuje povinný zákaz

**„*malo* by [byť]”** – špecifikuje požiadavku, ktorá je povinná pokiaľ neexistuje pádny dôvod prečo nemôže byť splnená. Ak existuje takýto dôvod, ***musí*** byť zdokumentovaný a schválený.

**“*nemalo by [byť]*”** - špecifikuje zákaz, ktorý je povinný pokiaľ neexistuje pádny dôvod prečo nie je ***možné*** ho splniť. Ak existuje takýto dôvod, ***musí*** byť zdokumentovaný a schválený.

**“*odporúča sa*”** – špecifikuje odporúčanú požiadavku (platí aj pre “***je možné***”)

Ak je rozdiel medzi operátorom (***musí*** / ***malo by byť*** / ***odporúča sa***) v konkrétnom opatrení a jeho nadradeným číslovaných bodom, tak platí operátor v konkrétnej odrážke (to znamená posledný špecifikovaný). *V nasledujúcom príklade pre bod b) platí operátor „****malo*** *by byť“:*

 *1.1 V organizácii* ***musí*** *byť vykonávané pravidelné monitorovanie a preskúmavanie bezpečnosti IS v rozsahu:*

* 1. *Pravidelné preskúmavanie plnenia cieľov bezpečnostnej politiky aspoň raz za 12 mesiacov vedením organizácie.*
	2. ***Malo*** *by byť vykonávané pravidelné testovanie záloh dôležitých systémov na kontrolu funkčnosti.*

# Štandardy pre logovanie

## Obsah logov

1. **Musí** byť implementované logovanie a logy by ***mali*** zaznamenávať minimálne:
2. (Úspešné aj neúspešné) Prihlásenie a odhlásenie
3. (Úspešné aj neúspešné) Vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny
4. (Úspešné aj neúspešné) Pokusy pristúpiť k citlivým údajom (údaje klasifikované hornými dvomi klasifikačnými stupňami v rámci organizácie)
5. (Úspešné aj neúspešné) Pokusy o kritické operácie
6. (Úspešné aj neúspešné) Spustenie procesu alebo služby
7. (Úspešné aj neúspešné) Pokusy o prihlásenie prostredníctvom RDP, SSH, VPN
8. Logy **musia** byť centrálne ukladané a archivované minimálne 6 mesiacov
9. Riešenie **musí** podporovať aj logovanie **minimálne** vo formáte syslog a **musí** podporovať preposielanie týchto logov na externý syslog server.

## Aktívne logovanie

1. ***Malo*** by byť použité kombinované logovanie na ukladanie Transfer logov (formát podporujúci prispôsobenie formátu logu). Ak takýto formát nie je dostupný, je potrebné zabezpečiť aby bolo logované aj hlavičky Referer a User-Agent.
2. Pre každý virtuálny host na fyzickom webserveri by ***mal*** existovať separátny log.
3. V logoch **musia** byť uvedené: timestamp, kedy udalosť nastala, vrátane určenia časovej zóny, verejná IP adresa používateľa, dopytovaná stránka/URL, HTTP kód odpovede servera, veľkosť odpovede servera v bytoch, obsahy hlavičiek User-Agent a Referer. V prípade záznamov o udalostiach súvisiacich s autentifikáciou alebo s činnosťou autentifikovaného používateľa je **nutné** zaznamenať účet a akciu, aká bola vykonaná.
4. Logy **musia** byť uchovávané na separátnom zariadení, resp. na separátnej logickej partícii.
5. Na uchovávanie logov **musí** byť vyhradená dostatočná kapacita.
6. Logy by ***mali*** byť archivované po dobu stanovenú pravidlami organizácie, minimálne však počas 6 mesiacov.
7. Logy **musia** byť prezerané v pravidelných intervaloch v závislosti od politiky organizácie, minimálne však raz týždenne. V prípade služieb, ktoré spracúvajú citlivé údaje alebo ich správna činnosť ovplyvňuje kritické aktíva organizácie, by ***mali*** byť logy kontrolované denne.
8. Logy **musia** obsahovať korektné informácie o dátume, čase a použitej časovej zóne. Pre korektné nastavenie času sa ***odporúča*** nastaviť synchornizáciu s dôveryhodným NTP serverom. ***Odporúča*** sa využiť autentifikovanú NTP synchronizáciu.
9. Všetky servery a syslog servery **musia** byť synchronizované s dôveryhodným NTP serverom.
10. Logovanie **musí** byť nastavené tak, aby prípadné zaplnenie logovacieho miesta neovplyvnilo stabilitu OS. ***Možné*** opatrenia: samostatná disková partícia, rotovanie logov a maximálna veľkosť logov.
11. Logy z kritických služieb a serverov **musia** byť synchronizované na samostatné logovacie zariadenie.
12. Logovacie súbory by ***mali*** byť zabezpečené aspoň takýmto spôsobom:
13. ***Mali*** by byť čitateľné len administrátorom.
14. ***Nemali*** by byť prepisovateľné a vymazateľné (***mal*** by byť možný len zápis na koniec súboru)
15. ***Odporúča*** sa komprimovať a šifrovať archivované logovacie súbory. Pri ručnej archivácii sa ***odporúča*** aj podpisovať logovacie súbory.
16. Granularita logovania **musí** zodpovedať požiadavkám danej služby alebo zariadenia a jeho kritickosti.

## Sumarizácia

Tabuľka 1

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **Požiadavka** | **MoSCoW** | **Komentár**  |
| SR 21 | Implementované logovanie | **M** |   |
| SR 22 | (Úspešné aj neúspešné) Prihlásenie a odhlásenie | **S** |   |
| SR 23 | (Úspešné aj neúspešné) Vytvorenie, modifikáciu alebo zmazanie používateľa alebo skupiny  | **S** |   |
| SR 24 | (Úspešné aj neúspešné) Pokusy pristúpiť k citlivým údajom (údaje klasifikované hornými dvomi klasifikačnými stupňami v rámci organizácie) | **S** |   |
| SR 25 | (Úspešné aj neúspešné) Pokusy o kritické operácie | **S** |  |
| SR 26 | (Úspešné aj neúspešné) Spustenie procesu alebo služby | **S** |  |
| SR 27 | (Úspešné aj neúspešné) Pokusy o prihlásenie prostredníctvom RDP, SSH  | **S** |  |
| SR 28 | Logy musia byť centrálne ukladané a archivované minimálne 6 mesiacov | **M** |   |
| SR 29 | Riešenie musí podporovať aj logovanie vo formáte syslog a musí podporovať preposielanie týchto logov na externý syslog server | **M** |  |

Tabuľka 2

|  |  |  |  |
| --- | --- | --- | --- |
| **Ref** | **Požiadavka** | **MoSCoW** | **Komentár**  |
| SR 30 | Použitie kombinácie logovanie na ukladanie Transfer logov (formát podporujúci prispôsobenie formátu logu). Ak takýto formát nie je dostupný, je potrebné zabezpečiť aby bolo logované aj hlavičky Referer a User-Agent. | **S** |   |
| SR 31 | Pre každý virtuál host na fyzickom webserveri by mal existovať separátny log. | **S** |   |
| SR 32 | Obsah logu: timestamp, kedy udalosť nastala, vrátane určenia časovej zóny, verejná IP adresa používateľa, dopytovaná stránka/URL, HTTP kód odpovede servera, veľkosť odpovede servera v bytoch, obsahy hlavičiek User-Agent a Referer. V prípade záznamov o udalostiach súvisiacich s autentifikáciou alebo s činnosťou autentifikovaného používateľa je nutné zaznamenať účet a akciu, aká bola vykonaná. | **M** |   |
| SR 33 | Logy musia byť uchovávané na separátnom zariadení, resp. na separátnej logickej partícii. | **M** |   |
| SR 34 | Na uchovávanie logov musí byť vyhradená dostatočná kapacita. | **M** |  |
| SR 35 | Logy by mali byť archivované po dobu stanovenú pravidlami organizácie, minimálne však počas 6 mesiacov. | **S** |  |
| SR 36 | Logy musia byť prezerané v pravidelných intervaloch v závislosti od politiky organizácie, minimálne však raz týždenne. | **M** |  |
| SR 37 | V prípade služieb, ktoré spracúvajú citlivé údaje alebo ich správna činnosť ovplyvňuje kritické aktíva organizácie, by mali byť logy kontrolované denne. | **M** |   |
| SR 38 | Logy musia obsahovať korektné informácie o dátume, čase a použitej časovej zóne. | **M** |  |
| SR 39 | Pre korektné nastavenie času sa odporúča nastaviť synchornizáciu s dôveryhodným NTP serverom. Odporúča sa využiť autentifikovanú NTP synchronizáciu. | **C** |  |
| SR 40 | Všetky servery a syslog servery musia byť synchronizované s dôveryhodným NTP serverom. | **M** |  |
| SR 41 | Logovanie musí byť nastavené tak, aby prípadné zaplnenie logovacieho miesta neovplyvnilo stabilitu OS.  | **M** |  |
| SR 42 | Možné opatrenia: samostatná disková partícia, rotovanie logov a maximálna veľkosť logov. | **C** |  |
| SR 43 | Logy z kritických služieb a serverov musia byť synchronizované na samostatné logovacie zariadenie. | **M** |  |
| SR 44 | Logovacie súbory by mali byť čitateľné len administrátorom. | **S** |  |
| SR 45 | Logovacie súbory by nemali byť prepisovateľné a vymazateľné (mal by byť možný len zápis na koniec súboru). | **S** |  |
| SR 46 | Odporúča sa komprimovať a šifrovať archivované logovacie súbory. Pri ručnej archivácii sa odporúča aj podpisovať logovacie súbory. | **C** |  |
| SR 47 | Granularita logovania musí zodpovedať požiadavkám danej služby alebo zariadenia a jeho kritickosti. | **M** |  |

## Zdroje / kategórie logov

* **Skupinou SEC** je myslený bezpečnostný softvér a nástroje, ako sú *AV* antivírusový/antimalware softvér, *IPS a IDS* systémy, *VPN* Vzdialený prístup, *Web proxy*, *Vulnerability management* software, *firewally a routery*, *autentizačné servery* a pod.
* **Skupina OS** zahŕňa servery, pracovné stanice a sieťové prvky (routery a switche).

Ide prevažne o dva typy logov:

* *systémové udalosti* (spustenie/zastavenie služby, vypnutie/zapnutie stanice, zlyhanie služieb, závažné chyby a pod.)
* *udalosti auditu* (pokusy o ne/úspešné prihlásenie, prístupy k súborom, zmeny nastavenie, využitie oprávnenia a pod.)
* **Skupina APP** označuje logovanie chodu aplikácií.

Ide predovšetkým o:

* Komunikácia klienta so serverom (*C<>S*) - klientske požiadavky prijaté serverom a ich odpovede.
* Využitie účtov (*ACC* = Account info.) - Informácie o prihlásení k aplikácii/službe (aj neúspešné pokusy), zmeny v účtoch, zmeny oprávnenia a pod.
* Údaje o aktivite užívateľov (*Aktivita*) – napr. počty transakcií a ich objem.
* Významné prevádzkové akcie (*Akcie*) ako spustenie alebo ukončenie aplikácie, pády aplikácie alebo jej významné zmeny.

Tabuľka 3

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **SEC =>** | ***AV*** | ***IDS/IPS*** | ***Vzdialený prístup*** | ***Web Proxy*** | ***Autentizačný server*** | ***Vulnerability management*** | ***FW /Routery*** | ***Switche*** | ***Radius*** |
| **Počet dní** | 30 | 30 | 30 | 30 | 30 | 30 | 30 | 30 | 30 |
| **OS =>** | ***Systém*** | ***Audit*** |  |
| **Počet dní** | 30 | 30 |  |
| **APP =>** | ***C<>S*** | ***ACC*** | ***Aktivita*** | ***Akcie*** |  |
| **Počet dní** | 7 | 7 | 1 | 30 |  |

Tabuľka 3 špecifikuje jednotlivé skupiny logov a stanovuje koeficient (počet dní) pre jednotlivé skupiny na uchovávanie logov

Tabuľka 4

|  |  |  |  |
| --- | --- | --- | --- |
| **Kategória IT podľa vplyvu na chod SP** | **Nízky** | **Stredný** | **Vysoký** |
| Retencie dát SEC | Min 1 \* počet dní | Min 3 \* počet dní | Min 6 \* počet dní |
| Retencie dát OS | Min 1 \* počet dní | Min 3 \* počet dní | Min 6 \* počet dní |
| Retencie dát APP | Min 1 \* počet dní | Min 3 \* počet dní | Min 6 \* počet dní |
| Rotácie logov | Každý týždeň alebo každých 25MB | Každých 6 – 24 hodín alebo každých 2 až 5MB | Každých 15-60 minút alebo každých 0,5 až 1MB |
| Odosielanie do agregátora logov (managementu logov) | Každé 3-24 hodín | Každých 15 – 60 minút | Aspoň každých 5 minút |
| Kontrola integrity (pri rotácii) | Voliteľná | Áno | Áno |
| Šifrovanie logov | Voliteľné | Áno | Áno |
| Šifrovaný prenos logov do agregátora logov (managementu logov) | Voliteľný | Áno | Áno |

Tabuľka 4 určuje odporučenia pre kategórie informačných technológií v zmysle uvedenej doby uchovávania logov podľa Tabuľky 3.

# POZNÁMKY

## Metóda MoSCoW:

* **M**– MUSÍ BYŤ (**Must have**) – špecifikuje povinnú požiadavku (platí aj pre „**je nutné**“ ako aj pre povinný zákaz „**nesmie**“).
* **S**– MALO BY BYŤ (**Should have**) - špecifikuje požiadavku, ktorá je povinná pokiaľ neexistuje pádny dôvod prečo nemôže byť splnená.

Ak existuje takýto dôvod, ***musí*** byť zdokumentovaný a schválený.

Platí aj pre zákaz “**nemalo by byť**”, ktorý je povinný pokiaľ neexistuje pádny dôvod prečo nie je ***možné*** ho splniť.

Ak existuje takýto dôvod, ***musí*** byť zdokumentovaný a schválený.

* **C**- MOHLI BY BYŤ (**Could have**) - špecifikuje odporúčanú požiadavku (platí aj pre “***je možné***”).
* **W**– NATERAZ NEBUDE, ale v budúcnosti možno (**Won't have (this time)**).

# Dodatky

## Zdroje a Legislatívne východiská

* [Slov-lex](https://www.slov-lex.sk/domov)
* [Eur-lex](https://eur-lex.europa.eu/homepage.html)
* [Sémantický znalostný strom vedomostí Knowww EU portál](https://knowww.eu)
* [Vláda SR](https://www.vlada.gov.sk/)
* [Ústredný portál verejnej správy](https://www.slovensko.sk/sk/titulna-stranka)
* [Rokovania legislatívnej rady vlády SR](https://hsr.rokovania.sk/rokovania-legislativnej-rady-vlady-sr/)
* [Zoznam uznesení vlády SR](https://rokovania.gov.sk/RVL/Resolution)
* [Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky](https://www.mirri.gov.sk/)
* [CSIRT](https://csirt.gov.sk)
* [NASES](https://www.nases.gov.sk/index.html)
* [NBÚ](https://www.nbu.gov.sk/)
* [Interné normy SP](http://intranet/Stranky/DMS/dms.aspx)
* [NIST](http://www.nist.gov)
* [NSA](https://www.nsa.gov/)
* [OWASP](https://owasp.org/)
* [IETF](https://trustee.ietf.org/)
* [IAB](https://www.iab.org/)
* [RFC](https://www.rfc-editor.org/)
* Zákon č. **395/2002** Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov v znení neskorších predpisov
* Zákon č. **461/2003** Z. z. o sociálnom poistení v znení neskorších predpisov
* Zákon č. **215/2004** Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
* Trestný zákon č. **300/2005** Z. z. (trestné činy páchané pomocou elektronických prostriedkov a v elektronickom prostredí) v znení neskorších predpisov
* Zákon č. **45/2011** Z. z. o kritickej infraštruktúre v znení neskorších predpisov
* Zákon č. **305/2013** Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov
* Zákon č. **272/2016** Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách) v znení neskorších predpisov
* Zákon č. **18/2018** Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a odporúčacích opatrení (zákon o ochrane osobných údajov)
* Zákon č. **69/2018** Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
* Zákon č. **95/2019** Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov
* Zákon č. **452/2021** Z. z. o elektronických komunikáciách v znení neskorších predpisov (ochrana súkromia a osobných údajov, ochrana sietí a zariadení)
* Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. **401/2023** Z. z. o riadení projektov a zmenových požiadaviek v prevádzke informačných technológií verejnej správy
* Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. **179/2020** Z. z.ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
* Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. **78/2020** Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov
* Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **85/2018** Z. z., ktorou sa ustanovujú podrobnosti o spôsobe vyhotovenia a náležitostiach listinného rovnopisu elektronického úradného dokumentu
* Vyhláška Ministerstva investícií, regionálnej rozvoja a informatizácie Slovenskej republiky č. **335/2023** Z. z., ktorou sa vykonávajú niektoré ustanovenia zákona o e-Governmente
* Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **70/2021** Z. z. o zaručenej konverzii v znení neskorších predpisov
* Vyhláška Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. **547/2021** Z. z. o elektronizácii agendy verejnej správy
* Vyhláška Národného bezpečnostného úradu č. **164/2018** Z. z., ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby)
* Vyhláška Národného bezpečnostného úradu č. **165/2018** Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov
* Vyhláška Národného bezpečnostného úradu č. **166/2018** Z. z. o podrobnostiach o technickom, technologickom a personálnom vybavení jednotky pre riešenie kybernetických bezpečnostných incidentov
* Vyhláška Národného bezpečnostného úradu č. **362/2018** Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v znení neskorších predpisov
* Vyhláška Národného bezpečnostného úradu č. **48/2019** Z. z., ktorou sa ustanovujú podrobnosti o administratívnej bezpečnosti utajovaných skutočností
* Nariadenie GDPR - Nariadenia Európskeho parlamentu a Rady (EÚ) **2016/679** z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
* Nariadenie Európskeho parlamentu a Rady (EÚ) **2018/1725** z 23. októbra 2018 o ochrane fyzických osôb pri spracúvaní osobných údajov inštitúciami, orgánmi, úradmi a agentúrami Únie a o voľnom pohybe takýchto údajov, ktorým sa zrušuje nariadenie (ES) č. 45/2001 a rozhodnutie č. 1247/2002/ES
* Nariadenie Európskeho parlamentu a Rady (EÚ) **2019/881** zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti)
* Smernica Európskeho parlamentu a Rady (EÚ) **2016/1148** zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
* Smernica Európskeho parlamentu a Rady (EÚ) **2016/2102** z 26. októbra 2016 o prístupnosti webových sídel a mobilných aplikácií subjektov verejného sektora
* Smernica Európskeho parlamentu a Rady (EÚ) **2019/1024** z 20. júna 2019 o otvorených dátach a opakovanom použití informácií verejného sektora
* Smernica č. **7/2019** o riešení Bezpečnostných incidentov Vládnou jednotkou CSIRT
* Metodika Jednotný́ dizajn manuál elektronických služieb verejnej správy - Metodické usmernenie UVSR č. 002089/2018/oLŠISVS-7 zo dňa 11.05.2018 <https://www.mirri.gov.sk/wp-content/uploads/2018/10/Metodicke-usmernenie-ID-SK-publikovat.pdf>
* Metodické usmernenie pre tvorbu používateľsky kvalitných elektronických služieb verejnej správy (Číslo spisu v DKS: 004307/2019/oBI) <https://www.mirri.gov.sk/wp-content/uploads/2019/04/Metodicke-usmernenie-pre-tvorbu-pouzivatelsky-kvalitnych-elektronickych-sluzieb-verejnej-spravy.pdf>
* Metodika riadenia QAMPR

<https://www.mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/riadenie-kvality-qa/index.html>

* Metodický pokyn k zabezpečeniu centrálneho nákupu produktov a služieb spoločnosti ORACLE v rámci Centrálnej rámcovej dohody na poskytovanie licencií a produktov ORACLE a služieb s nimi súvisiacich <https://www.mirri.gov.sk/wp-content/uploads/2020/02/Metodicky_pokyn_ORACLE_CRD_2019.pdf>
* Metodické usmernenie nariadeniu (GDPR) k spracúvaniu osobných údajov (prostredníctvom web stránok) v súlade s požiadavkami Nariadenia Rady EÚ č. 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov <https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20190901.html>
* Metodika pre Systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti (CSIRT) – aktuálne znenie [MetodikaZabezpeceniaIKT\_v2.1.pdf (gov.sk)](https://www.csirt.gov.sk/wp-content/uploads/2021/08/MetodikaZabezpeceniaIKT_v2.1.pdf?csrt=7605654333627490631)
* Jednotný dizajn manuál elektronických služieb <https://idsk.gov.sk/>
* PGR SP č. **29/2024** Programové, projektové a zmenové riadenie v podmienkach Sociálnej poisťovne
* PGR SP č. **19/2017** Informačná bezpečnosť Bezpečnostná politika
* PGR SP č. **21/2017** Elektronická komunikácia
* PGR SP č. **9/2017** Zásady na zabezpečenie postupu pri poskytovaní údajov z IS SP
* PGR SP č. **9/2016** Prevádzkový poriadok informačného systému Sociálnej poisťovne,

## Klasifikačné stupne informačných aktív

Klasifikačné stupne informačných aktív opisujú citlivosť informácií, údajov alebo ďalších s nimi spojených informačných aktív (ďalej len „informačné aktíva“) z pohľadu narušenia ich dôvernosti, integrity a dostupnosti a odrážajú dôležitosť alebo hodnotu týchto aktív pre procesy prevádzkovateľa základnej služby.

**Dôvernosť**

Z hľadiska dôvernosti sú klasifikačné stupne informačných aktív definované ako

**verejné** informačné aktíva určené pre verejnosť, ktoré sú získateľné z verejných zdrojov alebo z informácií, ktoré sú pripravené na tento účel alebo sú preklasifikované z inej úrovne prostredníctvom vlastníka a zahŕňajú napríklad informácie z médií, povinne publikované informácie alebo všeobecne dostupné informácie,

**interné** informačné aktíva, ktoré sú používané a prístupné pre všetkých používateľov v rámci organizácie prevádzkovateľa základnej služby bez ohľadu na ich pracovnú rolu; na sprístupnenie týchto aktív tretím stranám je potrebné schválenie zo strany vlastníka informácie,

**chránené** informačné aktíva, ktoré sú používané a prístupné len určeným skupinám oprávnených osôb a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať pre prevádzkovateľa základnej služby negatívny vplyv na poskytovanie služby; prístup k údajom klasifikovaným ako „Chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a je vymedzený výhradne vopred definovaným a schváleným útvarom alebo iným jasne vymedzeným skupinám osôb; tretie strany majú k týmto údajom prístup len v nevyhnutných a jednoznačne definovaných prípadoch schválených vlastníkom,

**prísne** **chránené** informačné aktíva, ktoré sú používané a prístupné len jednotlivým vybraným používateľom prevádzkovateľa základnej služby a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať s vysokou pravdepodobnosťou negatívny vplyv na poskytovanie základnej služby; prístup k údajom klasifikovaným ako „Prísne chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a výhradne konkrétnym, vopred definovaným a schváleným osobám; tretie strany majú k týmto údajom prístup len vo výnimočných a jednoznačne definovaných prípadoch schválených vlastníkom alebo na základe ustanovení osobitných predpisov.

**Ak nie je informačné aktívum explicitne klasifikované je považované za interné.**

**Integrita**

Z hľadiska integrity sú klasifikačné stupne informačných aktív definované ako

**nízka** zahŕňa informačné aktíva, ktorých chyba alebo nepresnosť výrazne neohrozí poskytovanú základnú službu,

**stredná** zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých chyba alebo nepresnosť môže spôsobiť dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká,

**vysoká** zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých chyba, nepresnosť bezprostredne ohrozuje poskytovanú základnú službu, s ňou spojené aktivity a reputáciu prevádzkovateľa základnej služby.

**Dostupnosť**

Z hľadiska dostupnosti sú klasifikačné stupne informačných aktív definované ako

**nízka** zahŕňa informačné aktíva prevádzkovateľa základnej služby, ktorých výpadok výrazne neohrozí poskytovanú službu alebo pre ktoré existujú alternatívne postupy,

**stredná** zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie môže mať dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká,

**vysoká** zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť prevádzkovateľa základnej služby a ktorých zlyhanie bezprostredne ohrozuje poskytovanú základnú službu, s ňou spojené aktivity a dobrú povesť prevádzkovateľa základnej služby.