**Politika kybernetickej bezpečnosti a informačnej bezpečnosti pre kategóriu I. podľa vyhlášky č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy**



# Obsah

[Obsah 2](#_Toc143615459)

[1 Správa dokumentu 4](#_Toc143615460)

[2 Úvod 4](#_Toc143615461)

[2.1 Rozsah platnosti 6](#_Toc143615462)

[2.2 Skratky a pojmy 7](#_Toc143615463)

[2.2.1 Skratky 7](#_Toc143615464)

[2.2.2 Pojmy 7](#_Toc143615465)

[3 Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti 13](#_Toc143615466)

[3.1 Určenie pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti a určenie jeho povinnosti, zodpovednosti a právomoci 13](#_Toc143615467)

[3.2 Základné zásady a opatrenia kybernetickej bezpečnosti a informačnej bezpečnosti 15](#_Toc143615468)

[4 Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti 16](#_Toc143615469)

[4.1 Vypracovanie analýzy rizík kybernetickej bezpečnosti a informačnej bezpečnosti 16](#_Toc143615470)

[4.2 Návrh a prijatie bezpečnostných opatrení 18](#_Toc143615471)

[4.2.1 Operatívne opatrenia 19](#_Toc143615472)

[4.2.2 Systémové opatrenia 19](#_Toc143615473)

[4.3 Periodické preskúmavanie rizík 19](#_Toc143615474)

[5 Personálna bezpečnosť 20](#_Toc143615475)

[5.1 Plán rozvoja bezpečnostného povedomia 20](#_Toc143615476)

[5.2 Mlčanlivosť 20](#_Toc143615477)

[5.3 Oznamovanie bezpečnostných incidentov 21](#_Toc143615478)

[5.4 Opatrenia pri ukončení pracovného pomeru a zmene postavenia používateľov 21](#_Toc143615479)

[5.5 Disciplinárny proces 21](#_Toc143615480)

[6 Riadenie prístupov 22](#_Toc143615481)

[7 Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu s tretími stranami 23](#_Toc143615482)

[8 Bezpečnosť pri prevádzke informačných systémov a sietí 24](#_Toc143615483)

[9 Hodnotenie zraniteľností a bezpečnostné aktualizácie 26](#_Toc143615484)

[10 Ochrana proti škodlivému kódu 26](#_Toc143615485)

[11 Sieťová a komunikačná bezpečnosť 27](#_Toc143615486)

[12 Akvizícia, vývoj a údržba informačných technológií verejnej správy 28](#_Toc143615487)

[13 Zaznamenávanie udalostí a monitorovanie 28](#_Toc143615488)

[14 Fyzická bezpečnosť a bezpečnosť prostredia 28](#_Toc143615489)

[15 Riešenie kybernetických bezpečnostných incidentov 29](#_Toc143615490)

[15.1 Riešenie kybernetických bezpečnostných incidentov 30](#_Toc143615491)

[15.1.1 Povinnosť informovania dotknutých strán 30](#_Toc143615492)

[15.1.2 Postup pri riešení kybernetického bezpečnostného incidentu 30](#_Toc143615493)

[15.2 Riešenie závažných kybernetických bezpečnostných incidentov 31](#_Toc143615494)

[16 Kryptografické opatrenia 33](#_Toc143615495)

[17 Audit a kontrolné činnosti 33](#_Toc143615496)

[18 Revízia dokumentu 34](#_Toc143615497)

[19 Prílohy 35](#_Toc143615498)

[19.1 Príloha č. 1 – Legislatívny rámec 35](#_Toc143615499)

# Správa dokumentu

Dokument „Politika kybernetickej bezpečnosti a informačnej bezpečnosti“ je vzorovým dokumentom slúžiacim pre potreby orgánov verejnej moci (ďalej aj „OVM“ alebo „organizácia“). Vytvorený vzor dokumentu nie je povinný na použitie a ani nie je záväzný. Dokument je poskytnutý voľne a bezplatne na využitie podľa potrieb konkrétneho OVM.

Metodickým základom pre vypracovanie Politiky kybernetickej bezpečnosti a informačnej bezpečnosti je 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 (ďalej aj „vyhláška č. 179/2020 Z. z.“).

Vytvorený dokument má aj svoj metodický rozmer, nakoľko predovšetkým kapitoly 3, 4 a 5 je možné použiť i pre potreby vzdelávania pracovníkov organizácií v oblasti kybernetickej a informačnej bezpečnosti.

Vytvorený dokument nie je určený na ďalší predaj alebo akúkoľvek inú komerčnú či obchodnú činnosť.

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej aj „MIRRI“) nezodpovedá za nesprávne použitie predmetného dokumentu zo strany OVM. Správne použitie a implementácia bezpečnostných opatrení je plne v kompetencii a zodpovednosti konkrétneho OVM.

MIRRI si vyhradzuje právo na zmenu/úpravu predmetného dokumentu alebo čiastkových textov a tabuliek, a to v potrebnom rozsahu vrátane zmien verzií dokumentov.

Súčasťou každého dokumentu adaptovaného do prostredia OVM je aj nasledovný zmenový list obsahujúci informácie minimálne v nasledovnom rozsahu:

|  |  |
| --- | --- |
| **Verzia** |  |
| **Garant dokumentu** |  |
| **Dátum poslednej revízie** |  |
| **Dátum vydania** |  |
| **Dátum účinnosti** |  |

# Úvod

Politika kybernetickej bezpečnosti a informačnej bezpečnosti definuje základné pravidlá a zásady pre kybernetickú a informačnú bezpečnosť. Tento dokument tvorí základný rámec riadenia kybernetickej a informačnej bezpečnosti a slúži ako základ pre vypracovanie následných interných predpisov (napr. prevádzkové predpisy, pracovné postupy a pod.).

Politika kybernetickej bezpečnosti a informačnej bezpečnosti pokrýva nasledovné oblasti bezpečnosti definované vyhláškou č. 179/2020 Z. z.:

* organizáciu kybernetickej bezpečnosti a informačnej bezpečnosti,
* riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
* personálnu bezpečnosť,
* riadenie prístupov,
* riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
* bezpečnosť pri prevádzke informačných systémov (ďalej aj „IS“) a sietí,
* hodnotenie zraniteľností a bezpečnostné aktualizácie,
* ochranu proti škodlivému kódu,
* sieťovú a komunikačnú bezpečnosť,
* akvizíciu, vývoj a údržba informačných technológií verejnej správy (ďalej aj „ITVS”),
* zaznamenávanie udalostí a monitorovanie,
* fyzickú bezpečnosť a bezpečnosť prostredia,
* riešenie kybernetických bezpečnostných incidentov,
* kryptografické opatrenia,
* audit a kontrolné činnosti.

Politika kybernetickej bezpečnosti a informačnej bezpečnosti čiastočne zahŕňa aj:

* bezpečnostné štandardy, ktoré interpretujú požiadavky platných bezpečnostných politík v konkrétnych situáciách, určujú aktivity, hlavné pravidlá, zodpovednosti a organizáciu riadenia s cieľom podporiť dodržiavanie bezpečnostných politík a
* bezpečnostné návody, ktoré predstavujú súhrn predpísaných krokov na vykonanie bezpečnostných politík a bezpečnostných štandardov prostredníctvom konkrétnych akcií a ktoré opisujú bezpečnostné konfigurácie a poskytujú konkrétne, platformovo závislé usmernenia na podporu bezpečnostných politík a bezpečnostných štandardov.

Vedenie organizácie touto Politikou kybernetickej bezpečnosti a informačnej bezpečnosti deklaruje svoju vôľu a postoj k riešeniu kybernetickej bezpečnosti a informačnej bezpečnosti. Východiskami pre budovanie systému riadenia kybernetickej bezpečnosti a informačnej bezpečnosti sú predovšetkým:

* podmienky dané relevantnými legislatívnymi predpismi,
* všeobecne platné bezpečnostné požiadavky kybernetickej bezpečnosti a informačnej bezpečnosti,
* systémové bezpečnostné požiadavky a podmienky dané vlastnými potrebami organizácie,
* výsledky vykonávaných bezpečnostných auditov a analýz rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
* odporúčania medzinárodných noriem a štandardov.

Aktualizácia Politiky kybernetickej bezpečnosti a informačnej bezpečnosti je vykonávaná minimálne raz ročne. Mimoriadna revízia môže byť vyvolaná:

* zmenami vo vývoji IS a sietí,
* zmenou legislatívy,
* výsledkami analýzy rizík,
* interným alebo externým auditom,
* rozhodnutím vedenia organizácie,
* vyhodnotením kybernetických bezpečnostných incidentov,
* a pod.

Pravidelne ako aj mimoriadne revízie a aktualizácie tejto Politiky kybernetickej bezpečnosti a informačnej bezpečnosti zaisťuje Pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.

Pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti sleduje aktuálnu legislatívu vzťahujúcu sa na prevádzku IS a zodpovedá za zaistenie zhody Politiky kybernetickej bezpečnosti a informačnej bezpečnosti a prípadne aj iných súvisiacich predpisov s platnou legislatívou.

## Rozsah platnosti

Cieľom tohto dokumentu je stanovenie základných bezpečnostných zásad pre prevádzku, používanie a údržbu informačných aktív organizácie.

Zásady a pravidlá uvedené v Politike kybernetickej bezpečnosti a informačnej bezpečnosti sú platné pre všetkých zamestnancov organizácie a pracovníkov tretích strán, ktorí používajú IT prostredie, pripájajú sa z externého prostredia do IT prostredia organizácie alebo sa pripájajú do externého prostredia z IT prostredia organizácie. Dokument obsahuje aj niektoré detaily a špecifiká, ktoré sú určené zamestnancom organizácie a pracovníkom tretích strán priamo zabezpečujúcim aktivity súvisiace s prevádzkou IS a s udržiavaním a zvyšovaním úrovne kybernetickej bezpečnosti a informačnej bezpečnosti.

Uplatňovanie zásad a pravidiel kybernetickej bezpečnosti a informačnej bezpečnosti nie je podmienené spôsobom výkonu správy IT prostredia. Správa IT prostredia organizácie môže byť vykonávaná internými a externými pracovníkmi, pričom zásady a pravidlá sa aplikujú rovnako. Zásady a pravidlá sa primeraným spôsobom uplatňujú i pri používaní mobilných prostriedkov (notebooky, mobilné telefóny a pod.) v externom prostredí.

Zásady a pravidlá sa aplikujú na všetky zariadenia, ktoré sú použité pre pripojenie do IT prostredia organizácie a ktoré sú majetkom organizácie, osobným majetkom zamestnancov organizácie alebo majetkom tretej strany. Zásady a pravidlá sa primerane aplikujú i na externé pripojenia do IT prostredia organizácie a vzťahujú sa na všetky dostupné druhy sieťového pripojenia.

Ak nie je možné dosiahnuť súlad existujúcich organizačných alebo bezpečnostných opatrení s Politikou kybernetickej bezpečnosti a informačnej bezpečnosti, je príslušný vedúci zamestnanec povinný v rámci svojej bezpečnostnej zodpovednosti vyhodnotiť mieru rizika a rozhodnúť o náhradných organizačných, režimových a personálnych opatreniach podstatne znižujúcich toto riziko. Takéto rozhodnutie však musí byť zadokumentované a bez zbytočného odkladu musí byť o tomto rozhodnutí informovaný pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.

Výnimky z dodržiavania tejto Politiky kybernetickej bezpečnosti a informačnej bezpečnosti môže v mimoriadnych a dostatočne písomne odôvodnených prípadoch povoliť vedenie organizácie alebo pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti na nimi presne vymedzený nevyhnutný čas a za podmienok akceptovateľného zvýšenia rizika v príslušnej oblasti.

Vedúci zamestnanci sú povinní preukázateľne oboznámiť všetkých zamestnancov vo svojej riadiacej pôsobnosti s touto Politikou kybernetickej bezpečnosti a informačnej bezpečnosti a zabezpečiť jej dôsledné plnenie.

## Skratky a pojmy

### Skratky

| Skratka | Popis skratky |
| --- | --- |
| BCM | Business Continuity Management – riadenie kontinuity činností |
| CD | Compact Disc (Kompaktny disk) |
| GDPR | Nariadenie EP a rady EÚ č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov |
| HTML | Hypertext Markup Language (Hypertextový značkový jazyk) |
| HW | Hardware (Hardvér) |
| IEC | International Electrotechnical Commission (Medzinárodná elektrotechnická komisia) |
| IS | Informačný systém |
| ISO | International Organization for Standardization (Medzinárodná organizácia pre normalizáciu) |
| IKT | Informačno-komunikačné technológie |
| IT | Informačné technológie |
| LAN | Local Area Network (Lokálna počítačová sieť) |
| NBÚ | Národný bezpečnostný úrad |
| NDA | Non-Disclosure Agreement (Dohoda o mlčanlivosti) |
| P2P | Peer to Peer (Sieť so vzájomným sprístupňovaním) |
| RFC | Request For Change (Požiadavka na zmenu) |
| SLA | Service Level Agreement (Dohoda o úrovni poskytovaných služieb) |
| SW | Software (Softvér) |
| USB | Universal Serial Bus (Univerzálna sériová zbernica) |

### Pojmy

**Aktívum** – čokoľvek, čo má pre organizáciu hodnotu (napr. hardvér, softvér, know-how, dokumentácia, personál).

**Analýza funkčných dopadov (BIA – Bussiness Impact Analysis)** – identifikácia kritických procesov, určenie dopadu nedostupnosti jednotlivých procesov na Organizáciu.

**Analýza rizík** – proces pochopenia podstaty rizika a stanovenia úrovne rizika

**Antimalware produkt**– je to produkt (softvér, hardvér, kombinované riešenie) určený pre ochranu časti IS pred škodlivým softvérom.

**Antimalware systém**– je to súbor antimalware produktov zabezpečujúcich komplexnú ochranu IS pred škodlivým softvérom.

**Archivácia** – je kopírovanie údajov so zachovaním ich pôvodnej štruktúry. Archivácia je vykonávaná za účelom dlhodobého uchovávania informácií, zabezpečenia pred stratou údajov, uvoľnenia pracovných diskov.

**Asymetrická šifra** – šifra, v ktorej sa na šifrovanie používa iný kľúč ako na dešifrovanie alebo aj kryptosystém s verejným kľúčom.

**Auditovateľnosť** – vlastnosť vyjadrujúca sledovateľnosť aktivít entity.

**Autenticita** – vlastnosť vyjadrujúca, že identita entity je tá, ktorá bola deklarovaná.

**Autentizácia** (**Autentifikácia**) – potvrdenie deklarovanej identity určitej entity.

**Autorizácia**– udelenie oprávnení určitej entite na prístup k zdrojom systému/organizácie a/alebo na ich využívanie.

**Autorizovaný hardvér** – hardvér, ktorý:

1. je zo zoznamu schválených IT zariadení alebo komponentov určených do IT prostredia,
2. je inštalovaný a konfigurovaný oprávnenou osobou,
3. má o inštalácii a konfigurácii vedený záznam v elektronickej alebo papierovej podobe.

**Autorizovaný softvér**– je to softvér na technickom prostriedku, ktorý je:

1. licenčne vysporiadaný, legálne nadobudnutý,
2. otestovaný pre používanie v IS organizácie,
3. zaradený do knižnice schválených softvérových produktov,
4. určený pre daný IT technický prostriedok,
5. jeho inštalácia a konfigurácia je vykonaná oprávnenou osobou,
6. inštalácii je vykonaný záznam v elektronickej alebo papierovej podobe.

**Bezpečnostné opatrenie** – technické, organizačné, právne alebo iné riešenie, ktoré úplne alebo čiastočne odstraňuje → zraniteľnosť aktíva, a/alebo znižuje pravdepodobnosť naplnenia hrozby a/alebo

**Certifikát verejného kľúča (certifikát)** – je elektronický dokument, ktorým vydavateľ certifikátu potvrdzuje, že v certifikáte uvedený verejný kľúč patrí entite, ktorej je certifikát vydaný.

**Chybový stav IT infraštruktúry** – udalosť, ktorá spôsobila narušenie funkčnosti, poškodenie, nedostupnosť zariadenia (PC, mobilný prostriedok a pod.), IT prostredia alebo služieb (aplikácie, informačné systémy, sieť a pod.). Za chybový stav treba považovať aj nezvyčajné správanie operačného systému, aplikácii a informačného systému (vynútený reštart, zmeny prostredia alebo funkčnosti aplikácií a pod.). Chybové stavy sú všeobecne považované za incidenty.

**Čiastočné testovanie (Partial simulation)** – overenie DRP v testovacom prostredí IT so simuláciou havarijného stavu.

**Dostupnosť** – požiadavka, aby zdroje systému boli k dispozícii oprávnenej osobe 1. Vždy, keď o to požiada; 2. do času t od okamihu, keď o to požiada; 3. s pravdepodobnosťou meranou podielom doby, keď sú požadované zdroje k dispozícii ku celkovej dobe (napr. 24 x 7 znamená, že systém je dostupný nepretržite 24 hodín denne a 7 dní v týždni).

**Dopad** – výsledok nežiaduceho incidentu.

**Dôvernosť** – 1. pocit istoty (často nepodložený), že (a) systém nezlyhá, (b) že systém robí len to, čo má robiť a nevykonáva žiadne nežiadúce činnosti; 2. vo všeobecnosti, ak entita A dôveruje entite B, znamená, že entita A predpokladá, že sa entita B bude správať presne tak, ako entita A očakáva.

**Elektronická identita používateľa** – jednoznačná identifikácia používateľa rozlíšiteľná mechanizmami informačného systému.

**Elektronický podpis** – je kryptografická metóda zaisťujúca pre digitálne údaje podobné vlastnosti ako vlastnoručný podpis pri bežných papierových dokumentoch.

**Entita** – aktívny prvok so špecifickými vlastnosťami (napr. automatizovaný proces, osoba, skupina osôb, subsystém).

**Externé pripojenie**– všetky pripojenia z externého prostredia do počítačovej siete alebo z prostredia počítačovej siete do externého prostredia.

**Firewall**– softvér/hardvér, kombinácia viacerých zariadení zvyčajne umiestnená na perimetri siete, ktorá chráni vnútornú sieť a údajové zdroje pred neautorizovaným prístupom z vonkajšieho prostredia. Firewall zabezpečuje presadzovanie sieťových bezpečnostných politík a zaznamenávanie pokusov o prieniky.

**Úplne funkčné testovanie (Full simulation)** – overenie DRP v reálnom IT prostredí so simuláciou havarijného stavu.

**Fyzická bezpečnosť** – fyzické prostriedky na ochranu systému pred krádežou, zneužitím, náhodným poškodením, technickými poruchami a prírodnými vplyvmi.

**Hashovacia funkcia** – je spôsob, ako z celého textu vytvoriť krátky reťazec (hash), ktorý s veľmi veľkou pravdepodobnosťou jednoznačne identifikuje pôvodný text.

**Havária** – bezpečnostná udalosť, ktorá spôsobila, že zdroje alebo procesy v organizácii nefungujú tak ako by mali, ich dostupnosť sa nedá obnoviť v požadovanom časovom rámci a vyžaduje si špeciálny zásah. Havária vážne narušuje činnosť organizácie

**Havarijný stav** – narušenie veľkého alebo dlhodobého charakteru, ktorý zasahuje procesy Organizácie a spôsobuje straty veľkého rozsahu alebo poškodenie dobrého mena Organizácie.

**Heslo** – tajný reťazec znakov známy len určitej entite (a overovateľovi dentity), ktorý sa používa na autentifikáciu danej entity.

**Hrozba** – objektívne existujúca potenciálna možnosť priamo alebo nepriamo narušiť systém, informáciách, ktoré sa v ňom spracovávajú alebo iné aktíva organizácie.

**IDS**– (Intrusion Detection System) – systém detekcie prienikov, softvér/hardvér, ktorý deteguje a zaznamenáva nevhodné, nekorektné a nezvyčajné aktivity.

**Incident** *–* udalosť alebo situácia, ktorá spôsobí alebo môže spôsobiť nežiadúce prerušenie činnosti, stratu, núdzový stav alebo krízu v nejakej organizácii, alebo v systéme.

**Informačné aktívum** – aktívum v prostredí IKT (prostriedky spracovania údajov a údaje).

**Informačná bezpečnosť** – 1. ideálny stav systému, kedy systém funguje v súlade s očakávaniami (bezpečnostnou politikou); 2. multiodborová disciplína, ktorá sa zaoberá hrozbami voči systémom/aktívam a metódami, ako aktíva pred hrozbami chrániť; 3. činnosti zamerané na dosiahnutie ideálneho stavu systému.

**Informácia** – základný pojem s rozličnou interpretáciou v rôznych oblastiach. V informatike informácia predstavuje opis nejakej skutočnosti (reálnej alebo fiktívnej) zaznamenaný v podobe údajov. Informácia predstavuje obsah údajov a údaje sú formou zápisu informácie.

**Integrita** – 1. základná bezpečnostná požiadavka na údaje, ktorej naplnenie znamená, že údaje nie je možné zmeniť bez toho, aby to ich vlastník alebo adresát nemohol zistiť; 2. v širšom zmysle je integrita bezpečnostná požiadavka na vylúčenie neoprávnených zmien v systémoch; t. j. zmien hardvéru, programového vybavenia alebo údajov.

**IPS (Intrusion Prevention System)** – systém prevencie prienikom, softvér/hardvér, ktorý poskytuje podobné možnosti monitorovania ako IDS, navyše umožňuje na základe množiny definovaných pravidiel automaticky vykonávať protiopatrenia proti podozrivým aktivitám (napr. blokovať podozrivý typ sieťovej prevádzky, zahadzovať podozrivé pakety, blokovať porty, blokovať podozrivé IP adresy a pod.)

**Kľúč (šifrovací kľúč)** – je tajná informácia, použitá na zašifrovanie informácie, bez znalosti ktorej nie je možné zašifrovanú podobu informácie prečítať.

**Konfiguračná databáza**– databáza, ktorá obsahuje všetky relevantné informácie o komponente, podliehajúcej riadeniu konfigurácií. Databáza zvyčajne obsahuje ID komponentu, názov, popis, sériové číslo, umiestnenie, vlastníka a historické informácie o konfigurácii komponentu.

**Kryptografia** *–* vedná disciplína zaoberajúca sa návrhom →kryptosystémov (šifier).

**Kybernetický bezpečnostný incident** – ezpečnostný incident, ktorý má negatívny dopad na kybernetický priestor, jeho časť, alebo prvok.

**Legálny softvér** – softvér, ktorý môže organizácia používať bez porušenia autorských alebo iných práv. Legálnosť je zvyčajne zmluvne ošetrená.

**Manažment hesiel** – systém tvorby, distribúcie, údržby a používania hesiel.

**Médiá** – nosiče informácií listinného charakteru (papierové dokumenty, tlačové zostavy, systémová dokumentácia a pod.) a nelistinného charakteru (CD, USB disk, magnetická páska, disketa, vymeniteľný disk a pod.).

**Mobilné prostriedky** – prenosné počítače (notebook), vreckové počítače (handheldy), mobilné telefóny, elektronické diáre, tablety, smartfóny a pod.

**Nerezidentný skener** - je to modul antimalware systému určený pre kontrolu systému alebo jeho časti, ktorý je spúšťaný len v prípade potreby (samotným používateľom, alebo časovačom vo vopred nadefinovaných intervaloch).

**Oprávnená osoba**– správca IKT alebo používateľ.

**Ohodnotenie rizík** – výstupy analýzy rizík – identifikácia a určenie úrovne rizika vzhľadom na pravdepodobnosť jeho realizácie a možné dopady.

**Osobný počítač**– IBM PC kompatibilný počítač vo forme pracovnej stanice v sieti, samostatnej pracovnej stanice alebo notebooku vrátane k nemu pripojených periférnych zariadení

**Plán obnovy (DRP – Disaster Recovery Plan)** – postupnosť krokov na čo najrýchlejšie odstránenie následkov havárie/katastrofy a obnovu kritickej →informačnej infraštruktúry organizácie.

**Plánovanie kontinuity činností** – vytváranie, implementácia, testovanie a revízie plánov kontinuity činnosti.

**Počiatočné testovanie** (Walkthrough) – teoretické overenie DRP, vykonávané na papieri.

**Počítačová sieť**– WAN/LAN sieť poskytujúca služby aj pre ostatné komunikačné siete tvoriace internú komunikačnú infraštruktúru.

**Používateľ**– osoba s minimálnymi privilégiami, ktoré má prístup k systému, vybraným zdrojom s ktorými môže vykonávať obmedzenú množinu operácií.

**Povolený softvér** – je softvér, ktorého inštalácia bola povolená.

**Požiadavka na zmenu (RFC)** – (Request For Change) formálna požiadavka na zmenu, obsahujúca popis požadovanej zmeny, dotknuté komponenty infraštruktúry, finančné náklady, požiadavku na zdroje a pod.

**Vedenie organizácie** – rozhoduje o všetkých záležitostiach organizácie a riadi jej činnosť.

**Princíp potreby poznať (need-to-know)** - iná verzia princípu najmenšieho privilégia: človek má prístup len k tým informáciám, ktoré potrebuje poznať na plnenie svojich pracovných povinností.

**Problém** – je neznáma koreňová príčina vzniku jedného alebo viacerých incidentov.

**Procedúra** – pecifický spôsob, ako vykonať nejakú činnosť alebo proces.

**Rezidentný skener** - je to modul antimalware systému spúšťaný automaticky pri každom štarte systému. Zodpovedá za nepretržité monitorovanie a ochranu systému pred škodlivým softvérom.

**Riadenie kontinuity činností** **(BCM – Bussiness Continuity Management)** – systematická činnosť zameraná na zabezpečenie dostupnosti kľúčových zdrojov organizácie a služieb/činností, pomocou alebo prostredníctvom ktorých organizácia napĺňa svoje poslanie. Organizácia identifikuje svoje kritické aktíva, scenáre naplnenia hrozieb, prijme opatrenia na minimalizáciu rizík, vytvorí kapacity na riešenie bezpečnostných incidentov, vypracuje a nacvičí postup v prípade krízovej situácie, zabezpečí náhradné zdroje na fungovanie v provizórnych podmienkach, plány obnovy, zdroje a postupy na ich realizáciu.

**Riadenie a správa rizík** – proces analýzy a manažmentu rizík, ktoré môžu mať vplyv na IT prostredie organizácie, s vynaložením akceptovateľných nákladov.

**Riziko** – veličina závisiaca od závažnosti (možného dopadu) hrozby a pravdepodobnosti, že sa hrozba naplní.

**Rola** – predstavuje priradenie špecifických povinností, zodpovedností a právomocí osobe na zabezpečenie výkonu požadovaných pracovných činností.

**Rola** – trieda používateľov s ekvivalentnými oprávneniami na prístup k systémom, resp. úlohami v informačnej bezpečnosti. Príkladmi rolí sú používateľ, správca systému, operátor, audítor, bezpečnostný manažér a i.

**Segregácia povinností** – opatrenia, ktorých zámerom je vylúčiť možnosť, aby jednotlivec mohol byť zodpovedný za výkon kritických činností v procese takým spôsobom, že nevedomé chyby a úmyselné podvody by nebolo možné zistiť štandardnými postupmi v priebehu procesu. Cieľom opatrení je prevencia pred podvodmi a zlomyseľnými aktivitami.

**Segregácia rolí** – implementácia rolí v IKT, so zohľadnením požiadaviek na segregáciu povinností.

**Service Desk** – Kontaktné centrum IT - je centrálny bod nahlasovania prevádzkových incidentov pre interných zákazníkov. Úloha útvaru je zameraná všeobecne na zbieranie prevádzkových incidentov v oblasti služieb poskytovaných IT.

**SIEM** – (Security Information and Event Management) – systém pre manažment kybernetickej bezpečnosti a informačnej bezpečnosti, ktorý umožňuje monitorovanie a vyhodnocovanie bezpečnosti IT prostredia analýzou hlásení pochádzajúcich zo zdrojov informácií (firewall, sieťové aktívne prvky, IDS/IPS, antivírový systém, operačný systém a pod.).

**Symetrická šifra** – šifra, v ktorej sa na šifrovanie a dešifrovanie používa ten istý tajný kľúč.

**Stratégia obnovy** – vopred definovaný, otestovaný a manažmentom schválený priebeh činností, ktoré majú byť vykonané počas reakcie na haváriu.

**Šifra (šifrovanie)** – je kryptografický algoritmus, ktorý prevádza čitateľnú správu alebo prostý text na jej nečitateľnú podobu alebo šifrovaný text.

**Škodlivý softvér** – je to softvér alebo časť programového kódu (ako napr. vírusy, červy, trójske kone, adware, spyware, a podobne), ktorý svojím pôsobením môže spôsobiť priame alebo nepriame škody v IT prostredí (poškodenie dát, únik citlivých informácii, znefunkčnenie kritických aplikácii a podobne).

**Spracovanie údajov** – zber, prenos, uchovávanie (vlastné spracovávanie: triedenie, spájanie výber), používanie, archivácia a ničenie informácie.

**Údaj** – orma záznamu informácie v informačných a komunikačných systémoch.

**Update AMS** – pravidelná (zvyčajne denná) aktualizácia jednotlivých databáz AMS (antivírusové, antispyware-ové, antispamové a pod.). Vzhľadom na frekvencie vydávania týchto aktualizácii a potrebu ich čo najrýchlejšieho rozdistribuovania v rámci IKT, nepodliehajú procesu testovania a ich sťahovanie z Internetu a distribúcia v rámci IKT je plne automatická.

**Upgrade AMS** – nepravidelné aktualizácie komponentov AMS vydávané z dôvodu opravy známych problémov, prípadne zdokonalenia a rozšírenia vlastností daného komponentu AMS. Do tejto kategórie patria patch-e, hotfix-y, service pack-y, feature pack-y a nové verzie jednotlivých komponentov AMS.

**Úroveň rizika** – hodnota rizika; v kvantitatívnom vyjadrení stredná hodnota dopadu príslušnej hrozby na dané aktívum; pri kvalitatívnom vyjadrení hodnota zohľadňujúca dopad hrozby na aktívum a pravdepodobnosť jej naplnenia.

**Worst case scenario** – najhorší možný variant narušenia procesu resp. lokality, pričom nie je podstatné z akého dôvodu narušenie nastane.

**Zamestnanec** – osoba, ktorá je v zamestnaneckom pomere k organizácii.

**Záloha** *–* je kópia údajov uložená na inom nosiči alebo mieste (úložisku) pre prípad straty na pôvodnom úložisku.

**Zálohovanie** – je prevencia pred stratou údajov, pričom sa údaje pravidelne alebo nepravidelne ukladajú z pracovného miesta (napr. servera) na záložné médiá.

**Zdieľané zdroje** – pre účely tohoto interného predpisu sú to: zdieľané zložky na súborových serveroch, verejné zložky elektronickej pošty, distribučné zoznamy, zdieľané tlačiarne.

**Zraniteľnosť** – vlastnosť, spôsob použitia alebo okolnosť umožňujúce naplnenie nejakej špecifickej hrozby. Napr. pripojenie nechráneného počítača k Internetu umožňuje hackerský útok, neaktuálna databáza vírusov je zraniteľnosťou umožňujúcou napadnutie počítača zlomyseľným softvér

**Zodpovednosť (Accountability)** – priradenie jednoznačnej zodpovednosti za vykonávané aktivity entity.

**Zvyškové riziko** – riziko, ktoré ostalo po prijatí opatrení.

# Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti

## Určenie pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti a určenie jeho povinnosti, zodpovednosti a právomoci

Organizácia je povinná určiť pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.

Pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti je zodpovedný za predchádzanie kybernetickým bezpečnostným incidentom a minimalizovanie vplyvu kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania služieb organizácie.

Pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti musí spĺňať znalostné štandardy na túto funkciu a musí byť nezávislý od riadenia prevádzky a vývoja IT služieb.

Pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti najmä:

* spolupracuje pri príprave východiskového strategického dokumentu, ktorý určuje prístup k zabezpečovaniu kybernetickej bezpečnosti a informačnej bezpečnosti, t. j. dokumentu „Stratégia kybernetickej bezpečnosti“ a zodpovedá za jej pravidelnú revíziu a aktualizáciu,
* spolupracuje na vyhodnocovaní bezpečnostných cieľov v súlade a v periodicite definovanej dokumentom „Stratégia kybernetickej bezpečnosti“,
* tvorí návrhy politík, smerníc a pravidiel pre oblasť kybernetickej bezpečnosti a informačnej bezpečnosti,
* spolupracuje na príprave rozpočtu pre kybernetickú bezpečnosť a informačnú bezpečnosť,
* spolupracuje pri analýze rizík a pri jej aktualizácii (riziká týkajúce sa kybernetickej bezpečnosti a informačnej bezpečnosti),
* v rámci procesu klasifikácie a evidencie informácii posudzuje odôvodnenia spracovateľov informácií a odsúhlasuje zverejnenie informácií v súlade so zákonom č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov,
* predkladá návrhy a oznamuje informácie v oblasti kybernetickej bezpečnosti a informačnej bezpenčosti priamo vedeniu organizácie,
* spolupracuje pri implementácii nových technických riešení (IT architektúra, riadenie zmien, riadenie projektov a pod.) z pohľadu vplyvu na oblasť kybernetickej bezpečnosti a informačnej bezpečnosti,
* dohliada na prijímanie, dodržiavanie a preverovanie účinnosti prijatých opatrení v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti,
* spolupracuje pri uzatváraní zmluvy o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností s externým dodávateľom, ktorý poskytuje služby týkajúce sa vývoja, implementácie a prevádzky IS v správe organizácie,
* zaisťuje, že ak dôjde ku kybernetickým bezpečnostným incidentom alebo narušeniu dôvernosti, integrity alebo dostupnosti informačných aktív, tieto incidenty sa vyriešia pohotovo a účinne v budú ohlásené v súlade s platnou legislatívou,
* zaisťuje, že budú prijaté opatrenia minimalizujúce možnosť opakovania kybernetických bezpečnostných incidentov.

Pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti taktiež spolupracuje s inými útvarmi v nasledovných oblastiach:

* vyšetrovanie a forenzné analýzy,
* sociálne a personálne aspekty (napr. tzv. „background checks“),
* IT architektúra (najmä z pohľadu kybernetickej bezpečnosti a informačnej bezpečnosti),
* bezpečnostné nástroje,
* kontroly plnenia bezpečnostných opatrení,
* riadenie prístupových práv,
* riadenie zmien a projektov,
* konfiguračný manažment,
* riadenie rizík v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti, identifikácia možných dopadov relevantných hrozieb a pravdepodobnosti ich uplatnenia,
* analýzy funkčného dopadu,
* riadenie vzťahov s dodávateľmi v kontexte dodržiavania pravidiel kybernetickej bezpečnosti a informačnej bezpečnosti,
* stanovovanie a kontrola dodržiavania pravidiel kybernetickej bezpečnosti a informačnej bezpečnosti zo strany zamestnancov a dodávateľov,
* zvyšovanie povedomia o kybernetickej bezpečnosti a informačnej bezpečnosti a zaškoľovanie/preškoľovanie všetkých zamestnancov a dodávateľov,
* inovácie v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti,
* atď.

Pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti je ďalej povinný:

* pravidelne reportovať stav a výkonnosť kybernetickej bezpečnosti a informačnej bezpečnosti vedeniu organizácie,
* riadiť riešenie kybernetických bezpečnostných incidentov,
* bezodkladne hlásiť závažný kybernetický bezpečnostný incident prostredníctvom Jednotného informačného systému kybernetickej bezpečnosti,
* spolupracovať s Národným bezpečnostným úradom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj vlastné informácie dôležité pre riešenie kybernetického bezpečnostného incidentu,
* v čase kybernetického bezpečnostného incidentu zabezpečiť dôkaz alebo dôkazný prostriedok tak, aby mohol byť použitý v trestnom konaní,
* oznámiť orgánu činnému v trestnom konaní alebo Policajnému zboru skutočnosti, že bol spáchaný trestný čin, ktorého sa kybernetický bezpečnostný incident týka,
* oznámiť a preukázať Národnému bezpečnostnému úradu vykonanie reaktívneho opatrenia a jeho výsledok, v prípade ak bolo prijaté reaktívne opatrenie,
* informovať v nevyhnutnom rozsahu tretiu stranu o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie zmluvy s treťou stranou stalo nemožným.

Pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti má právo od iných organizačných útvarov organizácie žiadať:

* doplňujúce informácie,
* logy,
* akúkoľvek súvisiacu podpornú dokumentáciu,
* umožnenie kontroly dodržiavania prijatých bezpečnostných opatrení kybernetickej bezpečnosti a informačnej bezpečnosti.

## Základné zásady a opatrenia kybernetickej bezpečnosti a informačnej bezpečnosti

Na účely organizácie kybernetickej bezpečnosti a informačnej bezpečnosti sa uplatňuje zásada:

* určenia pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti (bod 3.1 tejto Politiky kybernetickej bezpečnosti a informačnej bezpečnosti),
* najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené privilégiá v maximálnom rozsahu potrebnom na splnenie pridelených úloh,
* oddeľovania zodpovedností, podľa ktorej žiaden používateľ nemá oprávnenie pristupovať, upravovať alebo používať informačné aktíva prevádzkovateľa základnej služby bez autorizácie alebo overenia identity,
* dodržiavania a vykonávania nezávislého hodnotenia, merania a preskúmavania efektivity a účinnosti prijatých opatrení na ošetrenie rizík,
* jasného vymedzenia právomoci, povinnosti a zodpovednosti, ktoré sú súčasťou pracovnej náplne alebo obdobného opisu pracovných činností.

V oblasti organizačných zásad kybernetickej bezpečnosti a informačnej bezpečnosti je primerane aplikovaný princíp oddeľovania výkonných a kontrolných funkcií, s cieľom minimalizovať riziko zneužitia privilégií.

Základnými opatreniami kybernetickej bezpečnosti a informačnej bezpečnosti sú:

* dodržiavanie všetkých pravidiel informačnej bezpečnosti definovaných Politikou kybernetickej bezpečnosti a informačnej bezpečnosti a prípadne aj inými súvisiacimi predpismi,
* nakladať s osobnými údajmi v zmysle platných právnych predpisov,
* zachovávať mlčanlivosť o všetkých chránených skutočnostiach,
* bezpečne nakladať s IKT a ochraňovať informácie vo svojej pôsobnosti,
* zodpovedne používať pridelené prístupy v súlade s touto Politikou kybernetickej bezpečnosti a informačnej bezpečnosti a inými súvisiacimi predpismi,
* povinnosť zachovávať všetky heslá a prihlasovacie kódy v tajnosti,
* zákaz zdieľania pridelených používateľských hesiel,
* neinštalovať akýkoľvek software na hociktorý prostriedok IKT bez schválenia príslušného vedúceho zamestnanca alebo pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti; platí to aj pre legálne zakúpený software alebo software zadarmo (napr. freeware),
* nekopírovať a neposielať dokumenty obsahujúce interné a dôverné informácie (vrátane osobných údajov) na súkromné a iné adresy (pokiaľ to nesúvisí s oznamovacími povinnosťami vyplývajúcimi z výkonu práce).

# Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti

## Vypracovanie analýzy rizík kybernetickej bezpečnosti a informačnej bezpečnosti

Analýza rizík kybernetickej bezpečnosti a informačnej bezpečnosti (ďalej aj „analýza rizík“) je zameraná na získanie aktuálnych a vierohodných poznatkov o pravdepodobných rizikách týkajúcich sa aktív informačného systému verejnej správy a jeho okolia. Analýza rizík sa vykonáva pre informačný systém verejnej správy priebežne počas celého projektu v súlade so zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskoršách predpisov a priamo nadväzuje na dokument „Bezpečnostný zámer“ (resp. je jeho súčasťou).

Pre správnu analýzu rizík nestačí iba poznať hrozby, zraniteľnosti a dopady na aktíva. Chýbajúci faktor pri posudzovaní závažnosti nebezpečenstva, pred ktorým je aktíva organizácie potrebné chrániť, je pravdepodobnosť naplnenia hrozby.

Riziko je veličina spájajúca pravdepodobnosť naplnenia hrozby a dopad hrozby. Následne, po vyjadrení hodnoty rizík, je potrebné zamerať sa na ošetrenie rizík s najväčšou hodnotou a optimalizovať využívanie zdrojov.

Metodika analýzy rizík pre uplatnenie v procesoch riadenia rizika v zmysle požiadaviek zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov je podrobne spracovaná v dokumente „Metodika analýzy rizík a analýzy dopadov“.

V dokumente je podrobne popísaná oblasť:

1. procesu a metodiky riadenia rizík,
2. stanovenia kontextu rizika (identifikácia aktív, hrozieb, zraniteľností, dopadov, existujúcich opatrení a závažnosti rizík),
3. kvalitatívnej analýzy rizík,
4. ošetrovania rizík vrátane návrhu bezpečnostných opatrení,
5. akceptácie zvyškového rizika,
6. komunikácie rizika.

Metodika kvalitatívnej analýzy rizík pozostáva z nasledujúcich fáz:

* identifikácia scenárov rizík
* vyhodnotenie výsledného rizika pre identifikované hrozby, škodlivé udalosti alebo scenáre
* odhad pravdepodobnosti naplnenia hrozieb, škodlivých udalostí alebo ich kombinácie (tzv. scenárov rizík),
* odhad dopadov,
* určenie úrovne výsledných rizík.

Scenáre rizík predstavujú špecifické situácie realizácie rizík v kontexte vybraných aktív, pričom môžu byť kombináciou viacerých hrozieb a zraniteľností ústiacimi do rôznych dopadov.

Pred samotným výkonom analýzy rizík je potrebné identifikovať všetky podkladové materiály pre popis scenárov rizík, ako sú zoznam aktív a ich vlastníkov, katalóg hrozieb, katalóg zraniteľností. Súčasťou tejto fázy je aj identifikácia existujúcich opatrení pre všetky analyzované oblasti bezpečnosti a súvisiace scenáre rizík.

Praktický výkon a mieru detailu dokumentácie tejto fázy je v praxi vhodné prispôsobiť veľkosti organizácie, zložitosti jej procesov a informačných systémov a celkovému významu kybernetickej bezpečnosti a informačnej bezpečnosti pre správny chod organizácie. Detail je tiež závislý od pohľadu, ktorý sa použil pre usporiadanie hierarchie informačných aktív.

Výsledné riziko v identifikovanom scenári sa určuje ako prienik príslušnej hodnoty pravdepodobnosti naplnenia scenára rizika a hodnoty úrovne dopadov, ktoré bude mať na informačné aktíva organizácie.

Pri určovaní týchto hodnôt a pri samotnom vyčíslovaní výsledného rizika sa vychádza aj z úrovne existujúcich opatrení, ktoré môžu mať vplyv na hodnoty pravdepodobnosti či dopadu. Existujúce opatrenia musia byť zahrnuté v popise každého analyzovaného rizika.

Určenie pravdepodobnosti naplnenia scenára rizika je požiadavkou na vyhodnotenie daného scenára rizika. Riziko s veľkým dopadom, ktoré sa však vyskytne iba raz za dlhý časový horizont môže mať menší negatívny vplyv na bezpečnosť ako riziko s nízkym dopadom, avšak s častejším výskytom. Poznať, resp. správne odhadnúť pravdepodobnosť výskytu je preto dôležitou súčasťou hodnotenia výsledného rizika. Do výslednej hodnoty pravdepodobnosti sú zohľadňované aj existujúce bezpečnostné opatrenia súvisiace s daným scenárom rizika.

Pri určovaní pravdepodobnosti naplnenia scenára rizika sa vychádza z jeho predpokladaného naplnenia v časovom horizonte dvoch rokov. V analýze rizík je táto pravdepodobnosť vyjadrená nasledujúcim rozsahom:

|  |  |
| --- | --- |
| Pravdepodobnosť | Pravdepodobnosť opisne |
| Vysoká | je takmer isté, že v dohľadnom čase nastane naplnenie scenára rizika |
| Stredná | je pravdepodobné, že v dohľadnom čase nastane naplnenie scenára rizika |
| Nízka | je možné, že v dohľadnom čase nastane naplnenie scenára rizika |
| Veľmi nízka | je nepravdepodobné, že by v dohľadnom čase malo nastať naplnenie scenára rizika |

Pri stanovovaní pravdepodobnosti je potrebné prihliadať aj na frekvenciu výskytu incidentov v minulosti, ktorých podstatou bolo zneužitie príslušnej zraniteľnosti. Ak takýto údaj existuje, mal by byť v súlade so odhadovanou úrovňou pravdepodobnosti.

Pri ohodnocovaní závažnosti dopadov v rámci jednotlivých scenárov rizík sú dopady klasifikované podľa úrovne ich závažnosti. Úroveň závažnosti dopadov je vyjadrená podľa nasledovných významov:

| Dopad | Dopad popisne |
| --- | --- |
| Zanedbateľný | dopad akceptovateľného charakteru, ktorý môže byť zvládnutý v rámci plnenia bežných pracovných povinností bez potreby dodatočných zdrojov na odstránenie dôsledkov |
| Minimálny | dopad neakceptovateľného charakteru, ktorý však môže byť zvládnutý v rámci plnenia bežných pracovných povinností s minimálnymi personálnymi a finančnými nárokmi |
| Stredný | dopad neakceptovateľného charakteru, ktorý nie je zvládnuteľný v rámci plnenia bežných pracovných povinností a generuje mimoriadne personálne a finančné nároky (napr. zapojenie externých špecialistov a zdroje nad rámec bežného rozpočtu) |
| Závažný | prerušenie výkonu určitej konkrétnej služby alebo spôsobenie preukázateľného narušenia bezpečnosti, výdavky na riešenie bezpečnostného incidentu, zvýšené nároky na použitie mimoriadnych personálnych a finančných zdrojov na odstránenie dôsledkov, resp. prerušenie stredne významných činností, |
| Katastrofický | zásadné ohrozenie výkonu a funkčnosti primárnych procesov, kľúčových aktív; v extrémnom prípade ohrozenie bezpečnosti až existencie kritických aktív vo veľkom rozsahu, resp. celej organizácie |

## Návrh a prijatie bezpečnostných opatrení

Návrhy bezpečnostných opatrení, ktoré organizácia prijíma na základe výsledkov analýzy rizík kybernetickej bezpečnosti a informačnej bezpečnosti, vychádzajú z nasledovných princípov:

* pri návrhu opatrení sa vychádza z hodnoty a charakteru výsledného rizika určeného podľa stanovenej metodiky,
* pre každé výsledné riziko, ktoré nie je akceptovateľné, je popísaný spôsob jeho ošetrenia pomocou navrhovaných bezpečnostných opatrení,
* opatrenia sú navrhované v kontexte identifikovaných hrozieb,
* cieľom je navrhnúť systém bezpečnostných opatrení takým spôsobom, aby po ich implementácii boli všetky riziká znížené na úroveň zodpovedajúcu akceptovateľným rizikám.

Typy opatrení v kontexte životného cyklu informačného aktíva:

* existujúce opatrenia (z angl. Existing controls) – opatrenia inherentne zabudované už v čase návrhu, resp. implementácie systému,
* rozšírené (tiež „vylepšené“) opatrenia (z angl. Enhanced controls) – aplikované na implementovaný systém s cieľom ošetrenia rizika identifikovaného už v rámci bežnej prevádzky systému; typicky ich navrhuje pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti,
* dodatočné opatrenia (z angl. Additional, Complementary controls) – odporúča ich typicky audítor v správe auditu s cieľom ošetrenia rizika identifikovaného v rámci výkonu auditu kybernetickej bezpečnosti.

Z hľadiska realizácie opatrení na zníženie rizika je potrebné opatrenia rozdeliť na:

* operatívne – t. j. opatrenia, ktorých implementácia je z časového a finančného hľadiska nenáročná, ale ktorých účinok prináša bezprostredný efekt na zníženie rizika,
* systémové – t. j. organizačné a rozsiahlejšie technické opatrenia s dlhodobým účinkom na znižovanie rizika.

Postupnosť, akou budú navrhované opatrenia realizované, tzv. implementačný plán, je rozpracovaná v rámci bezpečnostnej stratégie, resp. bezpečnostného projektu. Tento program závisí od viacerých faktorov, ktoré je potrebné pri jeho návrhu zohľadniť. K takýmto faktorom prináležia:

* priority vyplývajúce z ohodnotenia rizík,
* výška nákladov potrebných na realizáciu opatrení,
* pripravenosť a spôsobilosť organizácie na realizáciu opatrení (technická, organizačná, finančná),
* podpora manažmentu organizácie na realizáciu opatrení.

### Operatívne opatrenia

Cieľom operatívnych opatrení je uplatnenie takých zmien procesov a technológií, ktoré budú viesť k urýchlenému zníženiu identifikovaného rizika s čo najnižšími nákladmi a najvyšším účinkom.

Za rozhodnutie o prijatí operatívnych opatrení je zodpovedný pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti, s následnou povinnosťou potvrdenia prijatých opatrení zo strany vedenia.

### Systémové opatrenia

Cieľom systémových opatrení je zvoliť optimálnu hranicu medzi účinnosťou bezpečnostných mechanizmov a požiadavkami, ktoré sú kladené na prevádzku aktív. Výsledkom systémových opatrení musí byť proaktívny prístup k riadeniu rizika, ktoré umožní:

* identifikovať riziko v počiatočnom štádiu pôsobenia príslušnej hrozby a existencie príslušnej zraniteľnosti,
* monitorovať riziko počas pôsobenia príslušnej hrozby a existencie príslušnej zraniteľnosti,
* eliminovať dopad hrozby na funkčnosť IS,
* zdokumentovať priebeh rizika.

Navrhované systémové opatrenia musia byť predložené na najbližšom rokovaní vedenia na schválenie a následnú realizáciu.

## Periodické preskúmavanie rizík

Riziká kybernetickej bezpečnosti a informačnej bezpečnosti je nevyhnutné pravidelne preskúmavať. Toto preskúmavanie spočíva v realizácii analýzy rizík najmenej raz za dva roky a v prípade každej významnej zmeny s dopadom na kybernetickú bezpečnosť a informačnú bezpečnosť.

# Personálna bezpečnosť

## Plán rozvoja bezpečnostného povedomia

Všetci zamestnanci organizácie, ako aj všetci ostatní používatelia, musia byť pri nástupe, resp. pred zahájením používania IS (pred prevzatím údajov k používateľskému účtu) preukázateľne oboznámení s Politikou kybernetickej bezpečnosti a informačnej bezpečnosti a tiež preškolení v ostatných bezpečnostných pravidlách a súvisiacich smerniciach platných pre používateľov IKT.

Všetci zamestnanci a zmluvní partneri musia:

* byť dostatočne oboznámení o ich rolách a o zodpovednosti spojených s informačnou bezpečnosťou ešte predtým ako im bude udelený prístup k citlivým informáciám a informačným systémom,
* obdržať smernice zaoberajúce sa tým, čo sa od nich očakáva z hľadiska výkonu ich roly v organizácii,
* byť motivovaní k napĺňaniu bezpečnostných politík organizácie,
* dosiahnuť určitú úroveň bezpečnostného povedomia potrebnú na výkon ich roly,
* podriadiť sa pracovnej náplni a podmienkam zamestnania,
* udržiavať dostatočné zručnosti a kvalifikáciu vo vzťahu k IS.

Pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti je povinný zaužívanou formou oznámiť všetkým používateľom zmeny v Politike kybernetickej bezpečnosti a informačnej bezpečnosti, pričom každý používateľ je povinný následne bez zbytočného odkladu oboznámiť sa s aktualizovaným znením Politiky kybernetickej bezpečnosti a informačnej bezpečnosti a súvisiacimi predpismi.

Organizácia je povinná zabezpečiť hodnotenie:

* účinnosti plánu rozvoja bezpečnostného povedomia,
* vykonávaných školení a
* ďalších činností spojených s prehlbovaním bezpečnostného povedomia.

## Mlčanlivosť

Organizácia zabezpečuje, že každý zamestnanec a tretia strana sú poučení o povinnosti zachovávať mlčanlivosť o všetkých skutočnostiach, informáciách a osobných údajoch, a to predtým, ako získajú prístup k IS. Mlčanlivosť je generálna a trvalá a vzťahuje sa tak na čas výkonu činnosti, ako aj po skončení výkonu činnosti.

Dohoda o mlčanlivosti a dodržiavaní pravidiel Politiky kybernetickej bezpečnosti a informačnej bezpečnosti organizácie je uvedená vo všetkých pracovných zmluvách, ako aj v zmluvách s externými dodávateľmi, ktorí môžu pri poskytovaní služieb prísť do styku s IS organizácie.

Každý zamestnanec, ktorý je zodpovedný za uzavretie zmluvy s externým dodávateľom je povinný dbať na to, aby bola v zmluve dostatočne riešená dohoda o mlčanlivosti.

## Oznamovanie bezpečnostných incidentov

Organizácia musí umožniť zamestnancom a zmluvným tretím stranám oznamovanie bezpečnostných incidentov pracovníkovi zodpovednému za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.

Na tento účel sa odporúča zriadiť anonymný informačný kanál, prostredníctvom ktorého je možné pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti informovať o zistenom porušení Politiky kybernetickej bezpečnosti a informačnej bezpečnosti a súvisiacich bezpečnostných postupov.

## Opatrenia pri ukončení pracovného pomeru a zmene postavenia používateľov

Organizácia má definované zodpovednosti a povinnosti v oblasti informačnej bezpečnosti, ktoré budú platiť po ukončení alebo zmene zamestnania.

Oznámenie o ukončení zodpovednosti v súvislosti s ukončením pracovného vzťahu zahŕňa aj pokračujúce bezpečnostné požiadavky, príp. zodpovednosť obsiahnutú v rámci dohody o zachovaní mlčanlivosti.

Zodpovednosť a povinnosti platné po ukončení pracovného pomeru sú jasne definované v pracovnej zmluve.

Organizácia má zavedený postup pri ukončení pracovného pomeru alebo iného obdobného vzťahu zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou zahŕňajúci:

* vrátenie pridelených zariadení, ktorými sú najmä počítače, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,
* zablokovanie prístupu v zariadeniach pridelených zamestnancovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,
* zrušenie prístupových práv v IS,
* odovzdanie výsledkov práce v súvislosti s IS, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty.

Pri zmene postavenia používateľov, administrátorov alebo osôb zastávajúcich bezpečnostné roly musí organizácia zabezpečiť zmenu prístupových oprávnení.

## Disciplinárny proces

Organizácia má zavedený a komunikovaný disciplinárny proces pre zamestnancov.

Disciplinárny proces by sa nemal začať bez predchádzajúceho overenia, či naozaj došlo k narušeniu bezpečnosti. Formálny disciplinárny proces musí zabezpečiť korektné a férové zaobchádzanie so zamestnancami, ktorí sú podozriví zo spôsobenia narušenia bezpečnosti. Formálny disciplinárny proces tiež zabezpečí postupnú reakciu, ktorá berie do úvahy povahu faktorov, ako je závažnosť narušenia bezpečnosti a vplyv na organizáciu, tiež či ide o prvý alebo opakovaný priestupok alebo prípadne iné relevantné faktory.

Porušenie povinností vzťahujúcich sa na oblasť kybernetickej bezpečnosti a informačnej bezpečnosti zamestnancom je závažným porušením pracovnej disciplíny so všetkými dôsledkami v zmysle Zákonníka práce.

Každé porušenie Politiky kybernetickej bezpečnosti a informačnej bezpečnosti, bezpečnostných predpisov a pravidiel bezpečnosti je považované za porušenie pracovnej disciplíny a bude riešené v zmysle Zákonníka práce. Každý používateľ zodpovedá za škodu, ktorá vznikne organizácii v dôsledku porušenia ustanovení tejto Politiky kybernetickej bezpečnosti a informačnej bezpečnosti. Ak bude v dôsledku porušenia povinností uvedených v tejto Politike kybernetickej bezpečnosti a informačnej bezpečnosti používateľom právoplatne uložená sankcia zo strany štátnych orgánov vykonávajúcich dohľad v príslušnej oblasti, bude sa táto sankcia považovať za škodu, ktorá vznikla organizácii v dôsledku porušenia povinností používateľa podľa tejto politiky. Konkrétny postih bude stanovený na základe posúdenia závažnosti, miery zavinenia a konkrétneho rizika, prípadne miery dopadu a následkov bezpečnostného incidentu.

Pri obzvlášť závažných alebo opakovaných porušeniach Politiky kybernetickej bezpečnosti a informačnej bezpečnosti môže príslušný vedúci zamestnanec alebo pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti nariadiť obmedzenie alebo zablokovanie prístupových oprávnení do doby vyriešenia bezpečnostného incidentu a zjednania nápravy.

# Riadenie prístupov

Riadenie prístupov osôb k sieti a informačným systémom je založené na zásade, že používateľ má prístup len k tým aktívam a funkcionalitám v rámci siete a informačného systému, ktoré sú nevyhnutné na plnenie zverených úloh používateľa. Na to sa vypracúvajú zásady riadenia prístupu osôb k sieti a informačnému systému, ktoré definujú spôsob prideľovania a odoberania prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systému.

Riadenie prístupov k sieťam a IS sa uskutočňuje v závislosti od prevádzkových a bezpečnostných potrieb organizácie, pričom sú prijaté bezpečnostné opatrenia, ktoré slúžia na zabezpečenie ochrany údajov, ktoré sú používané pri prihlásení do sietí a IS a ktoré zabraňujú zneužitiu týchto údajov neoprávnenou osobou.

V rámci riadenia prístupov k sieťam sa:

* každému používateľovi siete a IS prideľuje jednoznačný identifikátor na autentizáciu na vstup do siete a IS,
* zabezpečuje riadenie jednoznačných identifikátorov používateľov vrátane prístupových práv a oprávnení používateľských účtov,
* využíva nástroj na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a IS a nástroj na riadenie prístupových oprávnení, prostredníctvom ktorého je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie a zápis údajov a na zmeny oprávnení a prostredníctvom ktorého sa zaznamenávajú použitia prístupových oprávnení (prevádzkové záznamy),
* v pravidelných intervaloch vykonáva kontrola prístupových účtov a prístupových oprávnení na overenie súladu schválených oprávnení so skutočným stavom oprávnení a detekciu a následné zmazanie nepoužívaných prístupových účtov,
* určí osoba zodpovedná za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich formálnu evidenciu a vedenie úplných prevádzkových záznamov o každom prístupe do siete a informačného systémuy.

Pre riadenie prístupu k sieťam a IS sa používa metóda prístupu založeného na roliach. Používateľ dostáva oprávnenia pre prístup k IS prostredníctvom rolí, ktoré sú mu pridelené. Riadenie prístupu s využitím rolí zabezpečuje, že každý používateľ s rovnako pridelenými rolami má v rámci IT prostredia rovnaké oprávnenia.

Je prísne zakázané zdieľanie pridelených používateľských hesiel.

Vlastníci procesov by mali určiť vhodné pravidlá a obmedzenia na riadenie prístupov pre určité roly vzhľadom na informačné aktíva a s dostatočnou presnosťou na súvisiace riziká kybernetickej bezpečnosti a informačnej bezpečnosti.

Organizácia v rámci IS zabezpečí vynútenie zmeny používateľských hesiel s frekvenciou najmenj jeden rok.

# Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu s tretími stranami

Princípy riadenia dodávateľských vzťahov a služieb musia byť uplatňované minimálne vo vzťahu s dodávateľmi, ktorých činnosti priamo súvisia alebo môžu mať vplyv na dostupnosť, dôvernosť a integritu prevádzky sietí a informačných systémov organizácie.

S dodávateľmi organizácia uzatvára zmluva, do ktorej organizácia zahrnie požiadavku na dodržiavanie všetkých interných riadiacich dokumentov a všeobecne záväzných predpisov týkajúcich sa kybernetickej bezpečnosti a informačnej bezpečnosti.

Do zmluvy organizácia uvedie odkaz na nasledovné platné právne predpisy:

* zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
* 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,
* zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
* 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,
* nariadenie 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) – GDPR,
* zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Zmluva s dodávateľom by mala ideálne obsahovať:

* obdobie trvania zmluvy,
* ustanovenie záväzku tretej strany dodržiavať bezpečnostné politiky prijaté organizáciou a vyjadrenie súhlasu s nimi,
* ustanovenie o povinnosti chrániť všetky informácie poskytnuté zo strany organizácie dodávateľovi,
* ustanovenie o povinnosti dodržiavať a prijímať bezpečnostné opatrenia dodávateľom, konkrétnu špecifikáciu a rozsah bezpečnostných opatrení, ktoré prijíma dodávateľ a vyjadrenie súhlasu s nimi,
* konkrétny rozsah činnosti dodávateľa,
* zoznam pracovných rolí dodávateľa, ktoré majú mať prístup k informáciám a údajom organizácie, s povinnosťou oznámiť prevádzkovateľovi základnej služby každú zmenu v personálnom obsadení; osoba zúčastnená na predmete plnenia podpisuje vyjadrenie o zachovávaní mlčanlivosti,
* ustanovenie o rozsahu, spôsobe a možnosti vykonávania kontrolných činností a auditu zo strany organizácie v tretej strane,
* vymedzenie podmienok a možnosti zapojenia ďalšieho dodávateľa úplne alebo čiastočne zabezpečujúceho plnenie pre prevádzkovateľa základnej služby namiesto dodávateľa,
* ustanovenia o povinnosti informovať organizáciu o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti a informačnej bezpečnosti,
* ustanovenia o spôsobe a forme hlásenia ďalších informácií požadovaných organizáciou na plnenie jeho povinností vyplývajúcich z platných právnych predpisov a ich vymedzenie,
* ustanovenie o spôsobe a forme hlásenia všetkých informácií majúcich vplyv na zmluvu,
* ustanovenie o sankčných mechanizmoch pri porušení zmluvy,
* ustanovenia o podmienkach a spôsobe ukončenia zmluvy,
* záväzok dodávateľa po ukončení zmluvného vzťahu vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým má dodávateľ počas trvania zmluvného vzťahu prístup,
* záväzok dodávateľa po ukončení zmluvného vzťahu udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy; tento záväzok dodávateľa zostáva v platnosti aj po ukončení zmluvného vzťahu po dobu dohodnutú zmluvnými stranami, ktorá nesmie byť kratšia ako päť rokov po ukončení zmluvného vzťahu.

# Bezpečnosť pri prevádzke informačných systémov a sietí

Na účinnú prevenciu pred stratou dát, má organizácia zavedený proces na vytváranie záložných kópií dôležitých informácií a softvéru.

V rámci organizácie je vypracovaná a dodržiavaná politika zálohovania, ktorá definuje:

* opatrenia na ochranu záložných médií, medzi ktoré patria najmä:
* spôsob fyzickej ochrany a ochrany pred negatívnymi vplyvmi prostredia (požiar, záplava alebo iná živelná pohroma),
* vyhotovenie archivačnej zálohy najmenej v dvoch kópiách,
* uloženie prevádzkových záloh, kópií archivačnej zálohy a kópií inštalačných médií do uzamykateľného priestoru,
* fyzické ukladanie druhej kópie archivačnej zálohy v inom objekte, ako sa nachádzajú technické prostriedky IS, ktorého údaje sú archivované,
* frekvenciu a spôsob pravidelného testovania záloh,
* spôsob šifrovania záložných médií (ak to technologická vyspelosť organizácie umožňuje).
* doby uchovávania záloh v závislosti od typu a dôležitosti zálohovaných dát,
* postup testovania záloh formou obnovy, ktorá odhalí:
* nečitateľnosť zálohy,
* chyby pri čítaní médií.

# Hodnotenie zraniteľností a bezpečnostné aktualizácie

Organizácia vhodným nakonfigurovaním zabezpečí nastavenie automatickej aktualizácie operačného systému a aplikácií.

Táto automatická aktualizácia pozostáva z:

* upgradu operačného systému / aplikácie,
* updatu operačného systému / aplikácie.

Pred plošnou distribúciou aktualizácií organizácia zabezpečí ich otestovanie.

# Ochrana proti škodlivému kódu

Organizácia zabezpečuje ochranu všetkých informačných aktív, ktoré sú bežne postihnuteľné škodlivým kódom. Implementované kontrolné mechanizmy v organizácii poskytujú ochranu pred všetkými známymi typmi malvéru. Ide najmä o nasledovné:

* vírus,
* trojský kôň,
* červ,
* spyware,
* adware,
* ransomware,
* rootkit.

Organizácia má jasne definované postupy a zodpovednosti v procese ochrany proti škodlivému softvéru. Tieto postupy a roly sú pravidelne aktualizované za účelom zabezpečenia účinného riadenia ochrany. Medzi takéto postupy patrí najmä:

* zabránenie šírenia malvéru,
* izolácia prostredia, kde môžu nastať katastrofické následky,
* implementácia plánov kontinuity na zabezpečenie obnovy činností po útoku malvéru (vrátane všetkých potrebných opatrení na zálohovanie a obnovu dát).

Ochrana proti škodlivému kódu je v organizácii založená predovšetkým na:

* detegovaní škodlivého softvéru,
* opravnom softvéri,
* primeranom systéme prístupu,
* opatreniach na riadenie zmien,
* dostatočnom bezpečnostnom povedomí zamestnancov organizácie.

Organizácia prijme sériu adekvátnych opatrení na prevenciu, detekciu škodlivého kódu, ako aj na efektívnu reakciu pri infiltrácii škodlivým kódom, ktorá sa zameriava na:

* sťahovanie, inštaláciu a používanie nelegálneho alebo škodlivého softvéru,
* používanie prenosných médií (napríklad USB kľúče, flash disky, CD, DVD),
* škodlivé emailové prílohy a odkazy,
* podozrivé a škodlivé webové stránky a odkazy,
* externú a internú sieťovú komunikáciu v organizácii správcu vrátane webových sídiel,
* prenos súborov z externých sietí.

Organizácia zabezpečí kontrolu súborov prenášaných z externých sietí s cieľom detekcie škodlivého kódu.

Softvérové programy určené na ochranu pred škodlivým kódom sú v organizácii pravidelne aktualizované.

# Sieťová a komunikačná bezpečnosť

Organizácia zabezpečuje ochranu informácií v sieťach a v podporných zariadeniach, ktoré ich v sieťach spracúvajú.

Siete sú v organizácií primerane riadené a spravované, čím sa zabezpečuje ochrana informácií v systémoch a aplikáciách.

Opatrenia sú v organizácií implementované na zaistenie bezpečnosti dát v sieťach a na ochranu pripojených služieb pred neautorizovaným prístupom. Organizácia má implementované nasledovné bezpečnostné opatrenia:

* ochrana vonkajšieho a interného prostredia je realizovaná prostredníctvom firewallu,
* všetky koncové stanice sú chránené prostredníctvom softvérového personálneho firewallu,
* na sieťových zariadeniach organizácia implmentuje najmenej tieto bezpečnostné opatrenia:
* pravidelná aktualizácia firmvéru,
* zmena továrensky nastavených autentifikačných údajov,
* pri bezdrôtových sieťach musí byť nastavené využívanie bezpečného šifrovania a zabezpečenia,
* vypnutie možnosti správy zariadenia na diaľku alebo prijatie iných opatrení zabraňujúcich zneužitiu vzdialeného prístupu,
* zavedenie osobitných opatrení na zabezpečenie dôvernosti a integrity dát prenášaných verejnými sieťami alebo bezdrôtovými sieťami a na ochranu pripojených systémov a aplikácií osobitné opatrenia môžu byť potrebné aj na udržiavanie dostupnosti sieťových služieb a pripojených počítačov,
* vykonávanie tvorby vhodných záznamov a monitorovanie, čím je zabezpečené zaznamenávanie činností, ktoré môžu ovplyvniť alebo byť relevantné pre informačnú bezpečnosť,
* systémy v sieti sú overené,
* všetky koncové stanice organizácie sú chránené prostredníctvom softvérového personálneho firewallu.

# Akvizícia, vývoj a údržba informačných technológií verejnej správy

Organizácia zabezpečí, že obstarávanie alebo vytváranie nových alebo úprava existujúcich ITVS sa zadokumentuje a realizuje v súčinnosti s pracovníkom zodpovedným za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.

# Zaznamenávanie udalostí a monitorovanie

Organizácia zaznamenáva úspešné a neúspešné autentifikačné udalosti najmenej pre operačné systémy, databázy a aplikácie inštalované v rámci IS vo vlastnej správe (servery, stolové počítače, notebooky a pod.).

Rovnako tak zaznamenáva úspešné a neúspešné autentifikačné udalosti aj pre centrálne sieťové prvky, ktoré sú v jej správe.

Organizácia zabezpečuje prevádzkové záznamy najmenej tak, že:

* sú čitateľné výlučne osobám povereným ich analýzou,
* zamedzuje možnosti prepísania alebo vymazania záznamu,
* záznamy prenášané alebo presmerované od pôvodného zdrojového zariadenia do bezpečnostného monitorovacieho systému sú presmerované prostredníctvom zabezpečených kanálov alebo prostredníctvom dedikovanej správcovskej siete.

Za monitorovanie prevádzkových záznamov je zodpovedný pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti, resp. organizácia má určenú zodpovednú osobu za monitorovanie prevádzkových záznamov, ich vyhodnocovanie a vykonávanie nahlásenia podozrivej aktivity.

# Fyzická bezpečnosť a bezpečnosť prostredia

Cieľom fyzickej bezpečnosti je zabrániť neautorizovanému fyzickému prístupu, zničeniu alebo zasahovaniu do informácií alebo zariadení spracúvajúcich informácie.

Organizácia zabezpečuje, že ITVS sa umiestňujú a prevádzkujú takým spôsobom, že sú chránené pred fyzickým prístupom nepovolaných osôb, nepriaznivými prírodnými vplyvmi a vplyvmi prostredia.

Perimeter fyzickej bezpečnosti

Bezpečnostné perimetre sú použité na ochranu citlivých alebo kritických informácií a zariadení spracúvajúcich tieto informácie.

Riadenie fyzických prístupov

Zabezpečené oblasti sú chránené primeranými opatreniami na vstupe, aby sa zabezpečilo, že vstúpiť môžu len autorizované osoby.

Zabezpečenie kancelárií, miestností a prostriedkov

Organizácia má navrhnutú a aplikovanú fyzickú bezpečnosť pre miestnosti, kancelárie a zariadenia.

Ochrana pred externými hrozbami prostredia

Organizácia počíta s vytvorením a aplikovaním fyzickej ochrany pred prírodnými katastrofami, útokmi alebo nehodami.

Práca v bezpečnostných priestoroch

Organizácia má navrhnuté a aplikované príslušné postupy pre prácu v zabezpečených oblastiach.

Priestory na nakladanie a vykladanie

Prístupové body, akými sú priestory na nakladanie a vykladanie, ako aj iné body, kde môže neautorizovaná osoba získať prístup do priestorov organizácie, sú chránené, aby sa zabránilo neautorizovanému prístupu.

# Riešenie kybernetických bezpečnostných incidentov

V organizácii sa určí kontaktné miesto a spôsob hlásenia kybernetických bezpečnostných incidentov.

Organizácia vo vzťahu k ITVS:

* vykonáva činnosti na účely riešenia kybernetického bezpečnostného incidentu, jeho predchádzania alebo odstraňovania a hodnotenia zraniteľnosti,
* zbiera, spracúva a vyhodnocuje systémové informácie na účely predchádzania kybernetickým bezpečnostným incidentom, ich riešenia a obnovenia kybernetickej bezpečnosti a informačnej bezpečnosti,
* vykonáva pravidelné neinvazívne hodnotenie zraniteľnosti služby verejnej správy, služby vo verejnom záujme, verejnej služby a ďalších služieb informačných technológií poskytovaných prostredníctvom siete internet alebo prostredníctvom Govnetu,
* môže na žiadosť orgánu riadenia za tento orgán riadenia vykonať bezpečnostný audit alebo preň vykonať hodnotenie zraniteľnosti.

V procese riešenia kybernetického bezpečnostného incidentu a závažného kybernetického bezpečnostného incidentu prebiehajú nasledovné aktivity:

* určenie charakteru ohláseného kybernetického bezpečnostného incidentu (klasifikácia bezpečnostného incidentu),
* určenie rozsahu kybernetického bezpečnostného incidentu (dotknuté subjekty a systémy organizácie),
* ustanovenie priority vyriešenia kybernetického bezpečnostného incidentu a kľúčových cieľov ako napr.:
  + úplná alebo čiastočná náprava,
  + obnovenie pôvodného stavu,
  + identifikácia pôvodu kybernetického bezpečnostného incidentu,
  + obmedzenia šírenia kybernetického bezpečnostného incidentu,
  + odstránenie príčiny vzniku kybernetického bezpečnostného incidentu a pod.
* predbežný odhad náročnosti riešenia kybernetického bezpečnostného incidentu,
* rozhodnutie o informovaní zamestnancov organizácie, prípadne iných dotknutých organizácií/osôb, inštitúcií štátnej správy alebo verejnosti,
* stanovenie spôsobu riešenia a potrebných kapacít,
* identifikácia dôležitých kvalifikačných zručností potrebných na vyriešenie kybernetického bezpečnostného incidentu,
* rozhodnutie o možnom zapojení externých subjektov do riešenia kybernetického bezpečnostného incidentu,
* rozhodnutie o možnom právnom pokračovaní riešenia incidentu,
* riadenie riešenia kybernetického bezpečnostného incidentu podľa stanoveného postupu,
* počas riešenia kybernetického bezpečnostného incidentu vykonanie korekcie v odhadoch, rozhodnutiach a stanovenom postupe podľa potreby,
* rozhodnutie o spôsobe uzavretia incidentu,
* rozhodnutie o nápravných opatreniach.

## Riešenie kybernetických bezpečnostných incidentov

### Povinnosť informovania dotknutých strán

V prípade, že kybernetický bezpečnostný incident má dopad na dotknuté strany (typicky používatelia, zákazníci, dodávatelia, ďalšie dotknuté osoby, verejnosť), organizácia je povinná tieto strany o incidente informovať.

Úlohou môže vedenie organizácie poveriť oddelenie komunikácie, resp. iné oddelenie alebo konkrétnu zodpovednú osobu.

### Postup pri riešení kybernetického bezpečnostného incidentu

Pre prístup k informáciám pri riešení kybernetického bezpečnostného incidentu, musí byť zachovaný tzv. princíp „*need to know*“.

Za vykonanie vyšetrovania kybernetického bezpečnostného incidentu je zodpovedný pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti, ktorý môže poveriť vykonaním čiastkových činností iných zamestnancov organizácie. Zamestnanec, ktorý bol zainteresovaný do riešenia kybernetického bezpečnostného incidentu, je zodpovedný za pravdivosť a komplexnosť poskytovaných informácií o vzniknutom kybernetickom bezpečnostnom incidente.

Vyšetrovanie kybernetického bezpečnostného incidentu zahŕňa najmä:

* výpovede svedkov,
* analýzu incidentu,
* analýzu písomných záznamov, predpisov, návodov a inej relevantnej dokumentácie,
* analýzu elektronických záznamov (napr. záznamy logov alebo iné výstupy z informačných systémov).

Počas riešenia kybernetického bezpečnostného incidentu je pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti oprávnený vyžadovať informácie a súčinnosť od všetkých zamestnancov organizácie a zamestnancov tretích strán, ktorí pri svojej činnosti vytvárajú, používajú, spravujú alebo inak využívajú IS organizácie.

V prípade vzniku kybernetického bezpečnostného incidentu, ktorý má dopad na ochranu osobných údajov musí byť o takomto incidente upovedomená zodpovedná osoba určená organizačným dohľadom nad ochranou osobných údajov. Následné riešenie kybernetického bezpečnostného incidentu musí byť vykonané v plnej súčinnosti s touto osobou.

V prípade, že analýza incidentu potvrdí, že ide o taký kybernetický bezpečnostný incident, ktorý už má z minulosti definovaný osvedčený spôsob riešenia uložený v znalostnej databáze, použije sa rovnaký postup (resp. jeho modifikácia).

V rámci riešenia kybernetického bezpečnostného incidentu sa uchovávajú záznamy o zdroji informácií, dátume a mieste ich získania, o osobe, ktorá informácie získala a prípadne aj o svedkoch.

Ak kybernetický bezpečnostný incident má alebo môže mať vážny dopad na činnosť organizácie, musia byť podniknuté kroky vedúce k aktivácii príslušných plánov kontinuity. V prípade, že to vyžaduje závažnosť kybernetického bezpečnostného incidentu, môže pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti vymenovať operačný tím podieľajúci sa na vyšetrovaní, návrhu bezpečnostných opatrení ako aj na ich implementácii. Operačný tím schvaľuje vedenie organizácie.

Pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti pri riešení závažného kybernetického bezpečnostného incidentu ďalej:

* určuje predbežný rámec vyšetrovania a taktiež zodpovedných zamestnancov, ktorí budú spolupracovať pri riešení závažného kybernetického bezpečnostného incidentu,
* spolu s vedením organizácie rozhoduje o realizácii zásahov (realizácia vybraných, plánovaných bezpečnostných a preventívnych opatrení),
* určuje a koordinuje vyšetrovanie závažného kybernetického bezpečnostného incidentu, a o jeho priebehu informuje vedenie organizácie.

Ak sa na vyšetrovaní podieľajú aj iné orgány, súčinnosť a koordináciu vyšetrovania za organizáciu zabezpečuje pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti alebo osoba určená vedením organizácie.

Pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti, na základe záveru z vyšetrovania kybernetického bezpečnostného incidentu, navrhne a odsúhlasí opatrenia na:

* riešenie kybernetického bezpečnostného incidentu,
* odstránenie jeho následkov,
* zamedzenie opakovaného vzniku obdobných kybernetických bezpečnostných incidentov.

V prípade vzniku akýchkoľvek rozporov ohľadom opatrení navrhnutých pracovníkom zodpovedným za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti rozhodne vedenie organizácie.

Pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti skontroluje implementáciu určených opatrení a v prípade ak sú stanovené opatrenia splnené, kybernetický bezpečnostný incident uzavrie. Uzavretím kybernetického bezpečnostného incidentu sa rozumie ukončenie všetkých schválených zásahov a bezpečnostných opatrení, informovanie príslušných vedúcich zamestnancov o výsledku a kompletizácia relevantnej dokumentácie.

## Riešenie závažných kybernetických bezpečnostných incidentov

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 (ďalej aj „vyhláška č. 165/2018 Z. z.“) určuje, že kybernetický bezpečnostný incident sa považuje za závažný, ak spĺňa aspoň jedno identifikačné kritérium pre kategóriu závažného kybernetického bezpečnostného incidentu.

Organizácia je povinná hlásiť každý závažný kybernetický bezpečnostný incident, ktorý identifikuje na základe presiahnutia kritérií pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov podľa prílohy č. 1 k vyhláške č. 165/2018 Z. z.

V prípade, ak vznikne závažný kybernetický bezpečnostný incident, tak pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti bezodkladne informuje vedenie organizácie. V prípade závažného porušenia ochrany osobných údajov sa na riešení incidentu podieľa aj zodpovedná osoba zodpovedná za dohľad nad ochranou osobných údajov.

Vedenie organizácie rozhodne o správnosti vyhodnotenia, že niektoré základné kritériá hodnotenia závažného kybernetického bezpečnostného incidentu dosiahli hraničnú úroveň definovanú vyhláškou č. 165/2018 Z. z. Ak vedenie organizácie potvrdí, že sa skutočne jedná o závažný kybernetický bezpečnostný incident, následne dá pokyn na jeho nahlásenie Národnému bezpečnostnému úradu (ďalej aj „NBÚ“).

Zamestnanec, ktorý je zodpovedný za ohlasovanie závažných kybernetických bezpečnostných incidentov NBÚ, vykoná nahlásenie do Jednotného informačného systému kybernetickej bezpečnosti NBÚ.

Hlásenie závažných kybernetických bezpečnostných incidentov obsahuje, v rozsahu potrebnom na riadnu identifikáciu, najmä informácie o:

* ohlasovateľovi závažného kybernetického bezpečnostného incidentu:
  + identifikačné údaje,
  + kontaktné údaje,
* závažnom kybernetickom bezpečnostnom incidente:
  + časové údaje priebehu kybernetického bezpečnostného incidentu,
  + detailný opis priebehu kybernetického bezpečnostného incidentu,
  + rozsah vzniknutých škôd z dôvodu kybernetického bezpečnostného incidentu,
* základnej službe zasiahnutej závažným kybernetickým bezpečnostným incidentom:
  + konkrétny popis všetkých zasiahnutých aktív,
  + vplyv závažného kybernetického bezpečnostného incidentu na poskytovanú základnú službu,
* riešení závažného kybernetického bezpečnostného incidentu:
  + stav riešenia závažného kybernetického bezpečnostného incidentu,
  + vykonané nápravné opatrenia,
  + popis následkov závažného kybernetického bezpečnostného incidentu.

Ak do okamihu hlásenia závažného kybernetického bezpečnostného incidentu nepominuli jeho účinky, organizácia zašle neúplné hlásenie závažného kybernetického bezpečnostného incidentu, v ktorom vyznačí identifikátor neukončeného hlásenia, a bezodkladne po obnove riadnej prevádzky siete a informačného systému toto hlásenie doplní.

# Kryptografické opatrenia

Jedinou požiadavkou vyhlášky č. 179/2020 Z. z. je, aby organizácia zabezpečila, že jej webové sídlo je prístupné prostredníctvom zabezpečeného protokolu HTTPS s využitím bezpečnej verzie protokolu TLS.

# Audit a kontrolné činnosti

Schválením tejto Politiky kybernetickej bezpečnosti a informačnej bezpečnosti organizácia deklaruje, že sa podrobí auditu kybernetickej bezpečnosti v zmysle § 29 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej aj „zákon o kybernetickej bezpečnosti“), ktorého cieľom je preverenie účinnosti prijatých bezpečnostných opatrení a plnenia požiadaviek stanovených zákonom o kybernetickej bezpečnosti.

Organizácia je povinná preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených zákonom o kybernetickej bezpečnosti vykonaním auditu kybernetickej bezpečnosti v rozsahu stanovenom vyhláškou Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti, a to v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov po každej zmene majúcej významný vplyv na realizované bezpečnostné opatrenia a v určenom časovom intervale.

Audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti, ktorým je fyzická osoba, spoločník, štatutárny orgán alebo zamestnanec právnickej osoby.

Organizácia môže v období od 1. augusta 2021 do 31. decembra 2023 pre I. a II. kategóriu sietí a informačných systémov zabezpečiť plnenie povinnosti podľa § 29 zákona o kybernetickej bezpečnosti v znení účinnom od 1. augusta 2021 vykonaním samohodnotenia, ktorým sa preverí účinnosť prijatých bezpečnostných opatrení a plnenia požiadaviek ustanovených zákonom o kybernetickej bezpečnosti.

Organizácia si je vedomá povinnosti predložiť záverečnú správu o výsledkoch auditu Národnému bezpečnostnému úradu spolu s opatreniami na nápravu a s lehotami na ich odstránenie do 30 dní od ukončenia auditu.

# Revízia dokumentu

Tento dokument sa reviduje a aktualizuje najmenej raz ročne.

Dokument sa aktualizuje aj častejšie, ak:

* vzíde požiadavka na jeho aktualizáciu,
* pri zásadných zmenách v organizácii a štruktúre organizácie,
* pri zásadných zmenách v legislatíve Slovenskej republiky, s vplyvom na niektorú časť tohto dokumentu.

Za pravidelnú revíziu a aktualizáciu dokumentu zodpovedá pracovník zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.

Tento dokument a všetky následné aktualizácie schvaľuje vedenie organizácie.

# Prílohy

## Príloha č. 1 – Legislatívny rámec

Nasledujúci legislatívny rámec pozostáva z vybraných platných právnych predpisov Slovenskej republiky pokrývajúcich oblasť kybernetickej bezpečnosti a informačnej bezpečnosti:

* zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
* 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. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
* vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti,
* zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
* vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
* nariadenie 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) – GDPR,
* zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
* autorský zákon č. 185/2015 Z. z. v znení neskorších predpisov.