**Smernica pre riadenie informačnej bezpečnosti**



# Obsah

[Obsah 2](#_Toc143868307)

[1 Správa dokumentu 4](#_Toc143868308)

[2 Účel 5](#_Toc143868309)

[3 Rozsah platnosti 7](#_Toc143868310)

[4 Použité skratky 8](#_Toc143868311)

[5 Základné pojmy informačnej a kybernetickej bezpečnosti 9](#_Toc143868312)

[6 Základný popis princípov ISMS 15](#_Toc143868313)

[6.1 Vedúce postavenie 15](#_Toc143868314)

[6.1.1 Vedúce postavenie a záväzok v oblasti informačnej a kybernetickej bezpečnosti 15](#_Toc143868315)

[6.1.2 Bezpečnostná politika 15](#_Toc143868316)

[6.1.3 Organizačné roly a ich zodpovednosti 15](#_Toc143868317)

[6.2 Plánovanie 16](#_Toc143868318)

[6.2.1 Aktivity na ošetrenie rizík a možností 16](#_Toc143868319)

[6.2.2 Ciele informačnej a kybernetickej bezpečnosti 16](#_Toc143868320)

[6.3 Podpora 17](#_Toc143868321)

[6.3.1 Zdroje 17](#_Toc143868322)

[6.3.2 Kompetencie 17](#_Toc143868323)

[6.3.3 Povedomie 17](#_Toc143868324)

[6.3.4 Komunikácia 17](#_Toc143868325)

[6.3.5 Dokumentované informácie 18](#_Toc143868326)

[6.4 Prevádzka 18](#_Toc143868327)

[6.5 Vyhodnotenie výkonnosti 18](#_Toc143868328)

[6.5.1 Monitorovanie, meranie, analýza a vyhodnotenie 18](#_Toc143868329)

[6.5.2 Interný audit 19](#_Toc143868330)

[6.5.3 Preskúmavanie vedením 19](#_Toc143868331)

[6.6 Zlepšovanie 19](#_Toc143868332)

[6.6.1 Nesúlad a nápravné činnosti 19](#_Toc143868333)

[6.6.2 Kontinuálne zlepšovanie 20](#_Toc143868334)

[7 Štatút bezpečnostného výboru 21](#_Toc143868335)

[7.1 Postavenie bezpečnostného výboru 21](#_Toc143868336)

[7.2 Úlohy bezpečnostného výboru 21](#_Toc143868337)

[7.3 Zloženie bezpečnostného výboru 22](#_Toc143868338)

[7.3.1 Predseda bezpečnostného výboru 23](#_Toc143868339)

[7.3.2 Podpredseda bezpečnostného výboru 23](#_Toc143868340)

[7.3.3 Tajomník bezpečnostného výboru 23](#_Toc143868341)

[7.3.4 Členovia bezpečnostného výboru 24](#_Toc143868342)

[7.4 Zasadnutia bezpečnostného výboru 24](#_Toc143868343)

[7.4.1 Základné ustanovenia 24](#_Toc143868344)

[7.4.2 Uznášaniaschopnosť 25](#_Toc143868345)

[7.4.3 Účasť tretích strán 25](#_Toc143868346)

[7.4.4 Hlasovanie a schvaľovanie uznesení 25](#_Toc143868347)

[7.4.5 Zápisnica zo zasadnutia 26](#_Toc143868348)

[7.5 Schvaľovanie a zmenové konanie štatútu bezpečnostného výboru 26](#_Toc143868349)

[7.6 Záverečné ustanovenia 26](#_Toc143868350)

[8 Proces kontinuálneho vzdelávania v oblasti informačnej a kybernetickej bezpečnosti 27](#_Toc143868351)

[8.1 Všeobecné zásady kontinuálneho 27](#_Toc143868352)

[8.2 Roly zamestnancov z hľadiska potreby školení 28](#_Toc143868353)

[8.3 Obsah školení 29](#_Toc143868354)

[8.3.1 Skupina „Zamestnanec“ 29](#_Toc143868355)

[8.3.2 Skupina “Vedúci zamestnanec” 30](#_Toc143868356)

[8.3.3 Skupina „Administrátor IS“ 30](#_Toc143868357)

[8.3.4 Skupina „Manažér kybernetickej a informačnej bezpečnosti“ 32](#_Toc143868358)

[9 Prílohy 34](#_Toc143868359)

[9.1 Rámcová matica zodpovedností pre aplikáciu bezpečnostných opatrení 34](#_Toc143868360)

[Príloha č. 1 - 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 34](#_Toc143868361)

[Príloha č. 2 - 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 34](#_Toc143868362)

# Správa dokumentu

Dokument „Smernica pre riadenie informačnej bezpečnosti“ je vzorovým dokumentom slúžiacim pre potreby orgánov verejnej moci. Vytvorený vzor dokumentu nie je povinný na použitie a ani nie je záväzný. Dokument je poskytnutý voľne a bezplatne na využitie podľa potrieb konkrétnej organizácie.

Vytvorený dokument má aj svoj metodický rozmer, takže je ho možné použiť i pre potreby vzdelávania pracovníkov organizácií v oblasti kybernetickej a informačnej bezpečnosti.

Vytvorené 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 organizácie. Správne použitie a implementácia bezpečnostných opatrení je plne v kompetencii a zodpovednosti konkrétnej organizácie. Dokument je potrebné upraviť na základe reálnych potrieb a špecifického prostredia organizácie.

MIRRI si vyhradzuje právo na zmenu/úpravu predmetného dokumentu alebo čiastkových textov a tabuliek, a to v potrebnom rozsahu vrátane zmien verzií dokumentov. Dokument je výstupom pilotného projektu na ktorý nadväzuje Reforma Štandardizácia technických a procesných riešení kybernetickej a informačnej bezpečnosti (Plán obnovy a odolnosti).

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

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

# Účel

Účelom tohto dokumentu je popísať základného procesného rámca riadenia informačnej a kybernetickej bezpečnosti.

Súčasťou tohto dokumentu je štatút bezpečnostného výboru, ktorý definuje úlohy výboru a taktiež práva a povinnosti jeho členov.

Dokument sa tiež zameriava na zadefinovanie procesu kontinuálneho vzdelávania v oblasti informačnej a kybernetickej bezpečnosti.

Proces riadenia informačnej a kybernetickej bezpečnosti je založený na zavedení a udržiavaní hlavných princípov systému manažérstva informačnej bezpečnosti (ďalej aj „ISMS“) podľa požiadaviek nasledovných medzinárodných noriem:

* medzinárodná norma ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy),
* medzinárodná norma ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy).

Tento dokument popisuje procesy a prvky ISMS, ich aplikáciu a interakcie s primárnou biznis činnosťou inštitúcie.

Procesný rámec ISMS zahŕňa predovšetkým:

* organizačnú štruktúru,
* procesy,
* zodpovednosti,
* postupy a
* ďalšie informácie,

ktoré spoločne tvoria nástroj na kontinuálne zvyšovanie úrovne informačnej a kybernetickej bezpečnosti v inštitúcii a dosahovanie cieľov ISMS.

Strategické princípy ISMS

Medzi strategické princípy ISMS v podmienkach inštitúcie patria:

* zadefinovanie procesov súvisiacich s informačnou a kybernetickou bezpečnosťou,
* nastavenie a zavedenie princípov ISMS,
* trvalé zlepšovanie účinnosti ISMS jednak vo vzťahu k samotnej inštitúcii, a rovnako tak i k zainteresovaným stranám,
* trvalé zlepšovanie celkovej výkonnosti ISMS.

Hlavné ciele ISMS

Hlavné ciele vychádzajú zo strategických princípov ISMS. Napĺňaním hlavných cieľov sa zavádza a udržiava procesný rámec riadenia informačnej a kybernetickej bezpečnosti.

Hlavné ciele ISMS platné pre inštitúciu:

* Zodpovedný prístup k ochrane informácií vo vlastníctve inštitúcie a informácií získaných od tretích strán v rámci všetkých procesov a činností inštitúcie a uplatňovanie zásad bezpečného nakladania s informáciami.
* Prejav trvalého záujmu inštitúcie chrániť všetky informačné aktíva a aktíva používané na ich spracovanie voči:
* externým a interným hrozbám,
* zneužitiu,
* prezradeniu
* zničeniu,

čo povedie k zvýšeniu dôveryhodnosti organizácie tak u zamestnancov, ako aj v očiach verejnosti a obchodných partnerov.

* Budovať, udržiavať a neustále zlepšovať efektívny systém riadenia založený na princípoch ISMS a integrovať požiadavky tohto systému do biznis procesov organizácie v súlade s jej strategickým smerovaním.
* Stanovovať, realizovať a monitorovať krátkodobé a dlhodobé ciele ISMS, ktoré sú v súlade s ostatnými cieľmi inštitúcie.
* Zabezpečiť plnenie strategických princípov a hlavných cieľov ISMS ich pravidelným preskúmavaním a hodnotením.
* Dodržiavať záväzky vyplývajúce z aplikovateľných záväzných legislatívnych a iných požiadaviek, ktoré sa inštitúcia zaviazala plniť, pritom ich pravidelne preskúmavať a vyhodnocovať.
* Orientovať a udržiavať štruktúru inštitúcie tak, aby stanovila jednoznačne zodpovednosti a právomoci každého zamestnanca v oblasti informačnej a kybernetickej bezpečnosti.
* Zapojiť všetkých zamestnancov do zlepšovania činností a procesov riadenia informačnej a kybernetickej bezpečnosti.
* Zvyšovať úroveň povedomia v oblasti informačnej a kybernetickej bezpečnosti systematickým odborným vzdelávaním a motiváciou na všetkých organizačných úrovniach inštitúcie.
* Prijímať opatrenia vedúce k neustálemu zlepšovaniu informačnej a kybernetickej bezpečnosti na zabezpečenie dôvernosti, integrity a dostupnosti informácií (vrátane ochrany osobných údajov) v súlade s platnou legislatívou, relevantnými medzinárodnými štandardmi a dobrou praxou.
* Dbať na to, aby náklady na informačnú a kybernetickú bezpečnosť boli vynakladané efektívne, t. j. aby rámcovo zodpovedali cene informácií.
* Vykonávať pravidelnú identifikáciu a posudzovanie informačných rizík.
* Prijímať účinné opatrenia pre zlepšovanie bezpečnosti informačných aktív.
* Vynucovať, aby sa všetci zamestnanci inštitúcie a relevantné tretie strany riadili týmto rámcom riadenia informačnej a kybernetickej bezpečnosti.

Celkové bezpečnostné ciele inštitúcie z hľadiska informačnej a kybernetickej bezpečnosti sú popísané v rámci dokumentu „Stratégie kybernetickej bezpečnosti inštitúcie“.

# Rozsah platnosti

Procesy a pravidlá popísané v tomto dokumente platia pre:

* všetkých zamestnancov inštitúcie,
* tretie strany, ktoré sú s inštitúciou vo zmluvnom vzťahu v rozsahu a podieľajú sa alebo spolupracujú pri činnostiach – priamo či nepriamo – súvisiacich s informačnou a kybernetickou bezpečnosťou.

# Použité skratky

|  |  |
| --- | --- |
| Skratka | Popis skratky |
| EHS | Európske hospodárske spoločenstvo |
| ES | Európske spoločenstvo |
| EÚ | Európska únia |
| GDPR | 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) |
| IKT | Informačné a komunikačné technológie |
| IEC | International Electrotechnical Commission (Medzinárodná elektrotechnická komisia) |
| ISO | International Organization for Standardization (Medzinárodná organizácia pre štandardizáciu) |
| ISMS | Information Security Management System (Systém riadenia informačnej bezpečnosti) |
| IT | Informačné technológie |
| NBÚ | Národný bezpečnostný úrad |
| NIS | 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 |
| SR | Slovenská republika |
| Z. z. | Zbierka zákonov |

# Základné pojmy informačnej a kybernetickej bezpečnosti

V tejto kapitole je uvedený prehľad základných pojmov informačnej a kybernetickej bezpečnosti:

**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 analýzy prostredia a vzťahov medzi jednotlivými atribútmi vo vzťahu k rizikám (aktíva, hrozby, zraniteľnosti, dopady).

**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** – je šifra, ktorá používa verejný kľúč pre šifrovanie a súkromný kľúč pre dešifrovanie.

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

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

**Autentizácia** (**Autentifikácia**) – proces overenia deklarovanej identity entity.

**Autorizácia**– právo alebo povolenie prístupu entity k informačným aktívam a vymedzenie povolených aktivít s informačnými aktívami***.***

**Autorizovaný hardvér** – hardvér, ktorý:

1. je zo zoznamu schválených IT zariadení alebo komponentov určených do IT prostredia inštitúcie,
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 inštitúcie,
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** – činnosť, zariadenie, procedúra alebo mechanizmus, ktorý eliminuje alebo minimalizuje možnosti vzniku, pôsobenia a následky kybernetického bezpečnostného incidentu.

**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 aktívum bolo na požiadavku autorizovanej entity prístupné a schopné použitia.

**Dopad** – výsledok nežiaduceho incidentu.

**Dôvernosť** – požiadavka, aby informačné aktívum nebolo sprístupnené neautorizovaným entitám.

**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 inštitúcie alebo z prostredia počítačovej siete inštitúcie 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** – systém opatrení na zabezpečenie ochrany priestorov pred nepovolanými osobami a pred neoprávnenou manipuláciou s informačnými aktívami.

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

**Havária** – mimoriadna udalosť, ktorá spôsobí odchýlku od ustáleného prevádzkového stavu a má negatívny vplyv na život, zdravie a majetok.

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

**Heslo** – reťazec znakov, ktorý zabezpečuje kontrolu používateľa nad činnosťami, vykonávanými v spojení s identifikačným kontom používateľa.

**Hrozba** – potenciálna príčina nežiaduceho incidentu, ktorý môže mať za následok poškodenie systému alebo iných aktív Organizácie.

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

**Incident** *–* udalosť, ktorá nie je štandardným stavom a ktorá spôsobila, alebo môže spôsobiť prerušenie alebo redukciu kvality dodávanej služby. Incidenty majú zadefinovaný čas, za ktorý musia byť vyriešené.

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

**Informačná bezpečnosť** – súbor aspektov týkajúcich sa dosiahnutia a udržiavania dôvernosti, dostupnosti a integrity informačných aktív.

**Informácie** – interpretácie získané spracovaním údajov a ich vzájomnými vzťahmi.

**Integrita** – požiadavka, aby informačné aktíva neboli stratené, zničené alebo zmenené neautorizovaným alebo náhodným spôsobom.

**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** *–* je náuka o metódach utajovania zmyslu správ prevodom do podoby, ktorá je čitateľná len so špeciálnou znalosťou.

**Kybernetický bezpečnostný incident** – udalosť, ktorá spôsobila narušenie bezpečnosti informačného systému, tzn. že došlo ku strate dôvernosti, k narušeniu integrity alebo dostupnosti dát. Za kybernetický bezpečnostný incident treba považovať aj odhalený pokus o prekonanie bezpečnostných opatrení. Najčastejšie sa vyskytujúce kybernetické bezpečnostné incidenty:

1. odmietnutie služby (Denial of Service) – je kybernetický bezpečnostný incident, ktorý zabraňuje alebo obmedzuje oprávnené používanie sietí, systémov alebo aplikácií tým, že vyčerpáva zdroje,
2. malwarové narušenie (Malicious code) – je kybernetický bezpečnostný incident realizovaný prostredníctvom vírusu, červa, trójskeho koňa alebo inej entity so škodlivým kódom, ktorá infikuje počítač,
3. neautorizovaný prístup (Unauthorized Access) – osoba bez povolenia získa logický alebo fyzický prístup do siete, do systému, do aplikácii, k dátam alebo iným zdrojom,
4. nevhodné použitie (Inappropriate Usage) – osoba porušuje politiku akceptovateľného použitia počítača,
5. chyba (Error) – nesprávna činnosť na úrovni technického prostriedku, sieťovej infraštruktúry, programového vybavenia alebo neúmyselným konaním správcov, resp. používateľov,
6. strata (Loss) – strata údajov, služby, médií, programového vybavenia, technického prostriedku,
7. viaczložkový incident – incident, ktorý tvoria dva alebo viaceré kybernetické bezpečnostné incidenty rôznych kategórií.

**Legálny softvér** – softvér, ktorý môže inštitúcia 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, DVD, 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, ktoré je potrebné vykonať na obnovu narušenej funkcie kritických procesov v IT prostredí inštitúcie.

**Plánovanie kontinuity činností** – proces implementácie opatrení a postupov na zachovanie kontinuity kritických činností.

**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 inštitúcie.

**Používateľ**– každý zamestnanec inštitúcie alebo zamestnanec tretej strany využívajúci pri výkone pracovných činností IT prostriedky.

**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 inštitúcie** – rozhoduje o všetkých záležitostiach Organizácie a riadi jej činnosť.

**Princíp potreby poznať (need-to-know)** - pristupovanie k citlivým informáciám a dokumentom aj oprávnených osôb len keď to vyžadujú pracovné úlohy.

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

**Procedúra** – postupnosť definovaných krokov a úloh.

**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)** – riadiaci proces, pri ktorom sú identifikované možné dopady udalostí ohrozujúcich činnosť organizácie a ktorý definuje základný rámec pre prehlbovanie schopností organizácie na takéto udalosti správne a úspešne reagovať.

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

**Riziko** – potenciálna možnosť, že daná hrozba využije zraniteľnosti aktív alebo skupiny aktív a spôsobí tak stratu alebo zničenie aktív.

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

**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 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** – je taká šifra, ktorá pre šifrovanie aj dešifrovanie používa ten istý 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 inštitúcie (poškodenie dát, únik citlivých informácii, znefunkčnenie kritických aplikácii a podobne).

**Spracovanie údajov** – vykonávanie operácií alebo súboru operácií s údajmi, najmä ich prezeranie, kopírovanie, modifikácia, uchovávanie, prenos v elektronickej alebo inej forme a likvidácia.

**Údaj** – reprezentácia informácií vo forme s jednoznačne špecifikovanou štruktúrou.

**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** – ohodnotenie pravdepodobnosti vzniku kybernetického bezpečnostného incidentu, t. j. realizácie hrozby.

**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** – slabé miesto aktíva alebo skupiny aktív, ktoré môže byť zneužité hrozbou.

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

**Zvyškové riziko** – riziko, ktoré zostáva po implementácii opatrení. Množinu zvyškových rizík predstavujú všetky riziká akceptované vedením Organizácie.

# Základný popis princípov ISMS

## Vedúce postavenie

### Vedúce postavenie a záväzok v oblasti informačnej a kybernetickej bezpečnosti

Vedenie inštitúcie sa zaviazalo preukazovať vodcovstvo a záväzok, a to najmä tým že:

* prijalo zodpovednosti za implementáciu princípov ISMS,
* zabezpečuje vytvorenie bezpečnostnej politiky kybernetickej bezpečnosti a jej pravidelné preskúmanie s ohľadom na jej primeranosť a trvalú vhodnosť,
* zabezpečuje vytvorenie, realizáciu a monitorovanie strategických cieľov kybernetickej a informačnej bezpečnosti kompatibilných s kontextom organizácie a v súlade so strategickým smerovaním inštitúcie,
* vykonáva pravidelné preskúmania za účelom zaistenia vhodnosti, primeranosti a efektívnosti ISMS, vrátane hodnotenia príležitostí na zlepšenie a potrebu zmien ISMS a komunikuje o dôležitosti efektívneho ISMS,
* zaisťuje dostupnosť zdrojov na udržiavanie ISMS,
* zabezpečuje dosahovanie plánovaných výsledkov ISMS,
* riadi a podporuje osoby zabezpečujúce efektivitu ISMS,
* podporuje sústavné zlepšovanie.

### Bezpečnostná politika

Prostredníctvom Bezpečnostnej politiky kybernetickej bezpečnosti vedenie inštitúcie deklaruje svoje rozhodnutie zaviesť, udržiavať, rozvíjať a neustále zlepšovať princípy ISMS vo vzťahu k hlavným biznis činnostiam inštitúcie a relevantným tretím stranám.

Politika má:

* byť primeraná účelu, rozsahu činností a služieb inštitúcie
* poskytovať rámec na stanovovanie a preskúmanie cieľov informačnej a kybernetickej bezpečnosti,
* zahŕňať záväzok na sústavné zlepšovanie,
* byť zdokumentovaná, implementovaná, udržiavaná, komunikovaná, zverejnená, preskúmavaná a v rámci inštitúcie pochopená a akceptovaná.

Bezpečnostná politika kybernetickej bezpečnosti sa preskúmava minimálne jedenkrát ročne vedením inštitúcie za účelom zaistenia jej trvalej vhodnosti, primeranosti, efektívnosti a hodnotenia príležitostí na zlepšenie resp. potrebu zmien.

Bezpečnostnú politiku kybernetickej bezpečnosti má inštitúcia vypracovanú vo forme samostatného dokumentu.

### Organizačné roly a ich zodpovednosti

Bezpečnostné roly potrebné na riadenie informačnej a kybernetickej bezpečnosti sa rozdeľujú na tieto zložky:

* riadiacu,
* výkonnú,
* kontrolnú.

Detailný popis rolí kybernetickej bezpečnosti sa nachádza v dokumente „Stratégia kybernetickej bezpečnosti“ inštitúcie.

Súčasťou tohto dokumentu, v rámci kapitoly 7, je štatút bezpečnostného výboru, ktorý je vhodnou formou vrcholového riadiaceho orgánu pre kybernetickú a informačnú bezpečnosť.

## Plánovanie

### Aktivity na ošetrenie rizík a možností

Riziká a príležitosti sa určujú v zmysle interných a externých vplyvov a požiadaviek zainteresovaných strán.

Proces riadenia rizík upravujú najmä nasledovné interné predpisy inštitúcie:

* Stratégia kybernetickej bezpečnosti inštitúcie,
* Bezpečnostná politika kybernetickej bezpečnosti inštitúcie,
* Bezpečnostný projekt informačného systému verejnej správy.

Manažér kybernetickej a informačnej bezpečnosti koordinuje rozvoj postupov pre identifikáciu, kvalifikáciu a riadenie rizík a poskytuje podporu vlastníkom rizík v priebehu implementácie vhodných metód riadenia rizík.

Vlastník rizika predovšetkým:

* identifikuje a špecifikuje možné nástroje ošetrenia rizika a prípadné kontrolné aktivity,
* zodpovedá za realizáciu nápravných a preventívnych opatrení a kontrolných aktivít v zhode so schváleným harmonogramom,
* zodpovedá za reportovanie postupu implementácie opatrení,
* identifikuje v spolupráci s procesným analytikom ukazovatele kľúčových rizík a spolupracuje pri ich monitorovaní a vykazovaní,
* identifikuje a pravidelne prehodnocuje v spolupráci s procesným analytikom identifikované operatívne riziká a ukazovatele kľúčových rizík.

### Ciele informačnej a kybernetickej bezpečnosti

Strategické ciele informačnej a kybernetickej bezpečnosti sú uvedené v dokumente „Stratégia kybernetickej bezpečnosti“ inštitúcie.

## Podpora

### Zdroje

Procesom plánovania sa zabezpečujú zdroje pre udržiavanie a zlepšovanie efektívnosti ISMS.

Manažér kybernetickej a informačnej bezpečnosti najmenej jedenkrát ročne vypracúva správu o potrebe zdrojov pre informačnú a kybernetickú bezpečnosť za účelom zavádzania, udržiavania a zlepšovania efektívnosti ISMS. Túto správu predkladá vedeniu ako vstupný materiál na preskúmanie vedením.

Personálne oddelenie inštitúcie zodpovedá za tvorbu a implementáciu stratégie ľudských zdrojov a politík v oblasti výberu, náboru, vzdelávania, rozvoja, odmeňovania, riadenia výkonnosti, motivácie a stabilizácie zamestnancov. Takisto zabezpečuje vyjednávanie, internú komunikáciu voči zamestnancom v oblasti ľudských zdrojov, návrh a implementáciu nástrojov na podporu rozvoja firemnej kultúry, za prípravu a monitoring plnenia plánu personálnych nákladov inštitúcie.

### Kompetencie

Kontinuálne vzdelávanie všetkých pracovníkov inštitúcie prispeje k plneniu strategických princípov a hlavných cieľov ISMS a dodržaniu záväzkov vyplývajúcich z aplikovateľných záväzných legislatívnych a iných požiadaviek, ktoré sa organizácia zaviazala plniť, pritom ich pravidelne preskúmavať a vyhodnocovať.

Hlavným cieľom je zapojenie všetkých zamestnancov do zlepšovania činností a procesov riadenia informačnej a kybernetickej bezpečnosti a zvyšovanie úrovne povedomia v oblasti informačnej a kybernetickej bezpečnosti systematickým odborným vzdelávaním a motiváciou na všetkých organizačných úrovniach inštitúcie.

### Povedomie

Každý zamestnanec sa musí oboznámiť s Bezpečnostnou politikou kybernetickej bezpečnosti a ďalšími dokumentmi, ktoré boli alebo budú prijaté a uverejnené zo strany vedenia inštitúcie pre oblasť informačnej a kybernetickej bezpečnosti.

Každý zamestnanec sa zaviaže, že:

* bude dodržiavať Bezpečnostnú politiku kybernetickej bezpečnosti,
* bude postupovať v zmysle ostatných interných predpisov inštitúcie pre oblasť informačnej a kybernetickej bezpečnosti,
* spolupracovať na efektívnom napĺňaní strategických cieľov informačnej a kybernetickej bezpečnosti definovaných vedením inštitúcie.

### Komunikácia

Manažér kybernetickej a informačnej bezpečnosti musí zabezpečiť, aby všetci zamestnanci inštitúcie, ako aj príslušné externé strany, boli oboznámené s Bezpečnostnou politikou kybernetickej bezpečnosti.

Interná komunikácia v oblasti informačnej a kybernetickej bezpečnosti sa realizuje predovšetkým prostredníctvom:

* zasadnutí bezpečnostného výboru,
* pracovných stretnutí a porád,
* interných predpisov,
* intranetu inštitúcie,
* ServiceDesku.

Externá komunikácia prebieha najmä s dodávateľmi, príp. inými zmluvnými stranami a s orgánmi štátnej správy. Na komunikáciu s orgánmi štátnej správy sú písomne splnomocnení jednotliví zamestnanci.

### Dokumentované informácie

Zdokumentované informácie informačnej a kybernetickej bezpečnosti môžu byť vedené v rôznej forme a na rôznych médiách.

Interné riadiace akty inštitúcie pre oblasť informačnej a kybernetickej bezpečnosti sú najmä:

* Stratégia kybernetickej bezpečnosti,
* Bezpečnostná politika kybernetickej bezpečnosti,
* Smernica pre riadenie informačnej bezpečnosti,
* Smernica klasifikácie informácií a kategorizácie sietí a informačných systémov a riadenie aktív,
* Smernica výkonu analýzy rizík a analýzy dopadov,
* Smernica o bezpečnej prevádzke IS a sietí,
* Smernica o monitorovaní a riešení kybernetických bezpečnostných incidentov,
* Politika riadenia kontinuity činností.

Riadenie dokumentovaných informácií vo forme interných predpisov je realizované v zmysle platných interných procedúr inštitúcie.

## Prevádzka

Riadenie a prevádzka IKT inštitúcie je súčasťou dokumentu „Bezpečnostná politika kybernetickej bezpečnosti“ inštitúcie.

## Vyhodnotenie výkonnosti

### Monitorovanie, meranie, analýza a vyhodnotenie

Za účelom preukázania vhodnosti a efektívnosti ISMS a za účelom identifikácie možností pre trvalé zlepšovanie prebieha pravidelné monitorovanie a meranie.

Predmetom monitorovania a merania sú:

* incidenty informačnej a kybernetickej bezpečnosti,
* porušenie mlčanlivosti,
* porušenie ochrany osobných údajov,
* sankcie udelené príslušnými orgánmi verejnej moci za porušenie právnych a iných požiadaviek v oblasti informačnej bezpečnosti.

Hodnotenie sa zaznamenáva vo forme formulárov. Za vedenie dokumentácie monitorovania a merania zodpovedá manažér kybernetickej a informačnej bezpečnosti.

Výsledky monitorovania a merania ISMS sa vedú a uchovávajú formou zdokumentovaných informácií.

Výsledky z monitorovania a merania sa využívajú pri preskúmaní ISMS vedením inštitúcie.

### Interný audit

Inštitúcia v plánovaných intervaloch (minimálne jedenkrát ročne) vykonáva interné audity za účelom zistenia, že princípy riadenia informačnej a kybernetickej bezpečnosti zavedené v rámci inštitúcie zodpovedajú plánovaným opatreniam, požiadavkám normy ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy) a ďalším požiadavkám určených inštitúciou.

Každoročne sa ku koncu roka vypracúva plán interných auditov na nasledovný rok, ktorý schvaľuje vedenie inštitúcie. Program interných auditov sa spracováva s ohľadom na stav a dôležitosť procesov auditovaných oblastí, ako aj výsledkov predchádzajúcich auditov. Výber audítorov a priebeh auditov zaisťuje objektívnosť a nestrannosť procesu auditu. Audítori nesmú preverovať svoju vlastnú prácu. Zloženie audítorského tímu je uvedené v poverení na výkon auditu.

V zdokumentovanom postupe treba definovať zodpovednosť za plánovanie a vykonávanie auditov, za oznamovanie výsledkov a za udržiavanie záznamov, ako aj príslušné požiadavky na tieto činnosti (interný audit, časový plán interných auditov, správa z interného auditu). Manažér kybernetickej a informačnej bezpečnosti zaistí, aby sa činnosti, ktoré majú odstrániť zistené nezhody a ich príčiny, zrealizovali bez zbytočného odkladu.

### Preskúmavanie vedením

Vedenie inštitúcie najmenej jedenkrát ročne preskúmava zavedené princípy ISMS, aby sa zaistili trvalá vhodnosť, primeranosť, efektívnosť a súlad požiadavkami normy ISO 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ku dňu prijatia tohto dokumentu nebol ešte vydaný slovenský preklad danej normy). Vstupy do preskúmania vedením a návrh výstupov pre ISMS predkladá vedeniu manažér kybernetickej a informačnej bezpečnosti. Inštitúcia uchováva výsledky z preskúmania vo forme zdokumentovanej informácie.

## Zlepšovanie

### Nesúlad a nápravné činnosti

Inštitúcia má zavedený a udržiavaný postup na riešenie bezpečnostných incidentov v oblasti informačnej a kybernetickej bezpečnosti s cieľom:

* určiť podstatný nesúlad s požiadavkami a ďalšie faktory, ktoré by mohli zapríčiniť alebo prispievať k výskytu bezpečnostných incidentov,
* určiť potrebu nápravného opatrenia,
* určiť príležitosti na preventívne opatrenie,
* určiť príležitosti na trvalé zlepšovanie.

### Kontinuálne zlepšovanie

Princípy ISMS a úroveň informačnej a kybernetickej bezpečnosti sa môže trvalo zlepšovať prostredníctvom:

* vynucovania Bezpečnostnej politiky kybernetickej bezpečnosti,
* plánovaním, určovaním a hodnotením cieľov informačnej a kybernetickej bezpečnosti definovaných v Stratégii kybernetickej bezpečnosti,
* reagovaním na výsledky interných auditov,
* analýzou údajov z nápravných a preventívnych bezpečnostných opatrení,
* preskúmania informačnej a kybernetickej bezpečnosti vedením,
* systematickým udržiavaním a uchovávaním zdokumentovaných informácií z oblasti riadenia informačnej a kybernetickej bezpečnosti.

# Štatút bezpečnostného výboru

## Postavenie bezpečnostného výboru

Bezpečnostný výbor (ďalej aj „výbor“) je vrcholovým orgánom inštitúcie pre riadenie, spoluprácu a koordináciu činností v oblasti kybernetickej a informačnej bezpečnosti.

Štatút bezpečnostného výboru inštitúcie (ďalej aj „štatút“) upravuje najmä jeho:

* postavenie,
* úlohy,
* zloženie,
* zásady činnosti.

Bezpečnostný výbor je zriadené s cieľom rozhodovať o koncepčných otázkach týkajúcich sa kybernetickej bezpečnosti, legislatívne v rámci Slovenskej republiky upravenej najmä zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a súvisiacimi vykonávacími predpismi. Bezpečnostný výbor inštitúcie sa zriaďuje na dobu neurčitú.

## Úlohy bezpečnostného výboru

Hlavnou úlohou bezpečnostného výboru je pravidelné sledovanie a vyhodnocovanie realizácie Stratégie kybernetickej bezpečnosti a účinnosti vykonávania činností spojených riadením, výkonom, monitorovaním a kontrolou kybernetickej a informačnej bezpečnosti v inštitúcií.

Bezpečnostný výbor taktiež predkladá vedeniu inštitúcie na schválenie odporúčania v oblasti kybernetickej a informačnej bezpečnosti.

Bezpečnostný výbor monitoruje, skúma a vyjadruje sa najmä k:

* strategickým otázkam týkajúcich oblasti kybernetickej a informačnej bezpečnosti,
* výkonnosti v plnení strategických bezpečnostných cieľov vzhľadom na výkonnostný rámec stanovený v Stratégii kybernetickej bezpečnosti,
* pokroku dosiahnutému pri plnení bezpečnostných cieľov v oblasti kybernetickej a informačnej bezpečnosti,
* realizácii komunikačnej stratégie týkajúcej sa kybernetickej a informačnej bezpečnosti dovnútra inštitúcie,
* realizácii projektov v oblasti kybernetickej a informačnej bezpečnosti,
* dosiahnutému pokroku v rámci realizácie projektov a opatreniam na presadzovanie udržateľného rozvoja kybernetickej a informačnej bezpečnosti v rámci inštitúcie,
* pokroku v implementácii bezpečnostných opatrení kybernetickej a informačnej bezpečnosti v organizačnej, personálnej a technickej oblasti,
* k ročnému indikatívnemu plánu projektov kybernetickej a informačnej bezpečnosti a bezpečnostných opatrení kybernetickej a informačnej bezpečnosti v organizačnej, personálnej a technickej oblasti,
* následným úlohám a opatreniam prijatým vzhľadom na zistenia hodnotení,
* všetkým závažným kybernetickým bezpečnostným incidentom v inštitúcií,
* rozširovaniu bezpečnostných opatrení pre potreby zabezpečenia kybernetickej a informačnej bezpečnosti,
* plánu vzdelávania zamestnancov zameraného na kybernetickú a informačnú bezpečnosť,
* účinnosti prijatých bezpečnostných opatrení,
* vykonávaniu auditov kybernetickej bezpečnosti,
* obsahu zmlúv s externými subjektmi a odsúhlasuje ich obsah z hľadiska požiadaviek kybernetickej a informačnej bezpečnosti.

Bezpečnostný výbor ďalej:

* rozhoduje o záležitostiach týkajúcich sa kybernetickej bezpečnosti presahujúcich rámec:
* stratégie kybernetickej bezpečnosti,
* bezpečnostnej politiky kybernetickej bezpečnosti,
* interných smerníc kybernetickej bezpečnosti,
* ďalších dokumentov súvisiacich s kybernetickou bezpečnosťou,
* právomocí manažéra kybernetickej a informačnej bezpečnosti,
* v oblasti výberu a obstarávania bezpečnostných riešení a systémov:
* posudzuje ich vhodnosť a potrebu pre inštitúciu,
* navrhuje obstaranie tovarov a služieb a ich implementáciu,
* sa vyjadruje k predmetu obstarávania,
* sa po odbornej stránke vyjadruje k podkladom pre obstarávanie,
* schvaľuje technickú časť podkladov k obstarávaniu.

Bezpečnostný výbor taktiež schvaľuje:

* zámery projektov súvisiace s kybernetickou a informačnou bezpečnosťou,
* projekty súvisiace s kybernetickou a informačnou bezpečnosťou,
* zápisy zo zasadnutí bezpečnostného výboru.

Bezpečnostný výbor okrem pravidelných zasadnutí zasadá i mimoriadne, a to v prípade vzniku mimoriadnych udalostí alebo nutnosti prerokovania dôležitých otázok týkajúcich sa kybernetickej a informačnej bezpečnosti.

## Zloženie bezpečnostného výboru

Bezpečnostný výbor je zložený z nasledovných rolí:

* predseda bezpečnostného výboru,
* podpredseda bezpečnostného výboru,
* tajomník bezpečnostného výboru,
* členovia bezpečnostného výboru.

Členov bezpečnostného výboru vymenúva a odvoláva predseda výboru. Menovanie a odvolanie je realizované prostredníctvom menovacieho / odvolacieho dekrétu.

Každý člen bezpečnostného výboru s výnimkou tajomníka má hlasovacie právo.

Predseda a podpredseda výboru sú zároveň členmi výboru.

Menný zoznam členov bezpečnostného výboru je vedený tajomníkom bezpečnostného výboru. Pri zmene v zložení bezpečnostného výboru tajomník upraví tento zoznam a v elektronickej forme ho zašle všetkým členom výboru.

### Predseda bezpečnostného výboru

Predsedom bezpečnostného výboru (ďalej aj „predseda“) je zástupca vedenia inštitúcie.

Predseda bezpečnostného výboru vykonáva najmä nasledujúce činnosti:

* riadi celkovú činnosť bezpečnostného výboru,
* zastupuje bezpečnostný výbor navonok,
* zodpovedá za dodržiavanie tohto štatútu,
* vymenúva a odvoláva podpredsedu bezpečnostného výboru,
* vymenúva členov bezpečnostného výboru,
* odvoláva členov bezpečnostného výboru na základe návrhu na odvolanie alebo v iných prípadoch stanovených týmto štatútom,
* zvoláva zasadnutia bezpečnostného výboru,
* navrhuje program zasadnutí bezpečnostného výboru,
* riadi zasadnutia bezpečnostného výboru,
* vyhodnocuje činnosť bezpečnostného výboru.

### Podpredseda bezpečnostného výboru

Podpredsedom bezpečnostného výboru (ďalej aj „podpredseda“) je manažér kybernetickej a informačnej bezpečnosti.

Podpredseda bezpečnostného výboru zastupuje predsedu bezpečnostného výboru v prípade jeho neprítomnosti a v plnom rozsahu plní úlohy predsedu bezpečnostného výboru.

Na predsedu a podpredsedu bezpečnostného výboru sa primerane vzťahujú ustanovenia vzťahujúce sa na členov bezpečnostného výboru.

### Tajomník bezpečnostného výboru

Tajomník zabezpečuje logistiku a fungovanie bezpečnostného výboru najmä plnením nasledovných administratívnych a technicko-organizačných úloh:

* administratívne a technicko-organizačné zabezpečenie zasadnutí bezpečnostného výboru,
* poskytovanie informácií o zasadnutiach a programe zasadnutí výboru,
* poskytovanie podkladov na zasadnutia výboru,
* vypracúvanie zápisnice zo zasadnutí výboru,
* vedenie, aktualizácia a distribuovanie zoznamu členov bezpečnostného výboru,
* zabezpečenie ostatných činností nevyhnutných pre fungovanie bezpečnostného výboru podľa pokynov predsedu.

Tajomník bezpečnostného výboru nemá hlasovacie právo.

### Členovia bezpečnostného výboru

Členov bezpečnostného výboru vymenúva a odvoláva predseda bezpečnostného výboru.

Člen bezpečnostného výboru je do svojej funkcie menovaný na základe menovacieho dekrétu parafovaným predsedom bezpečnostného výboru. Členstvo vo výbore vzniká dňom uvedeným v menovacom dekréte.

Členstvo v bezpečnostnom výbore nie je spojené s nárokom na odmenu.

Členstvo v bezpečnostnom výbore zaniká:

* dňom zrušenia pracovného pomeru člena bezpečnostného výboru s inštitúciou,
* na základe odvolania člena bezpečnostného výboru predsedom bezpečnostného výboru (odvolanie člena je účinné dňom vydania rozhodnutia predsedu o jeho odvolaní):
* na základe návrhu vedúceho príslušnej organizačnej zložky inštitúcie zastúpenej v bezpečnostnom výbore,
* v prípade, ak sa člen bez riadneho ospravedlnenia neúčasti nezúčastní na dvoch po sebe nasledujúcich zasadnutiach bezpečnostného výboru,
* v prípade ak člen neplní úlohy definované v tomto štatúte,
* vzdaním sa členstva zo strany člena bezpečnostného výboru (člen sa môže vzdať svojho členstva písomným oznámením o vzdaní sa členstva, ktoré doručí predsedovi alebo tajomníkovi bezpečnostného výboru),
* z iných závažných dôvodov (napr. dňom smrti člena bezpečnostného výboru alebo jeho vyhlásením za mŕtveho).

## Zasadnutia bezpečnostného výboru

### Základné ustanovenia

Zasadnutie bezpečnostného výboru zvoláva predseda, ktorý zároveň určí miesto, dátum a čas zasadnutia a takisto navrhne program zasadnutia.

Zasadnutia bezpečnostného výboru môžu byť:

* riadne,
* mimoriadne.

Riadne zasadnutie výboru zvoláva predseda podľa uváženia, najmenej však dvakrát za kalendárny rok. Riadne zasadnutia sa v prípade potreby môžu konať i v kratších časových intervaloch.

Mimoriadne zasadnutie bezpečnostného výboru zvoláva predseda:

* z vlastného podnetu,
* z dôvodu ohrozenia kybernetickej a informačnej bezpečnosti,
* z podnetu nadpolovičnej väčšiny všetkých členov bezpečnostného výboru, a to na základe písomnej žiadosti adresovanej predsedovi alebo tajomníkovi.

Oznámenie o mieste a termíne zasadnutia, návrh program a ďalšie podklady na riadne zasadnutie bezpečnostného výboru zasiela tajomník všetkým členom výboru výlučne elektronicky, a to minimálne päť pracovných dní pred termínom riadneho zasadnutia výboru. V prípade mimoriadneho zasadnutia výboru tajomník zasiela oznámenie minimálne jeden pracovný deň pred konaním mimoriadneho zasadnutia výboru.

Všetci členovia môžu pri schvaľovaní programu zasadnutia podať návrh na rozšírenie programu zasadnutia.

Zasadnutia bezpečnostného výboru vedie vždy predseda alebo podpredseda.

Všetci členovia bezpečnostného výboru sú povinní zúčastňovať sa zasadnutí výboru osobne.

Ak sa člen bezpečnostného výboru zo závažných dôvodov nemôže zúčastniť zasadnutia výboru, túto skutočnosť oznámi písomne alebo elektronicky tajomníkovi bezpečnostného výboru.

### Uznášaniaschopnosť

Na začiatku zasadnutia bezpečnostného výboru tajomník overí uznášaniaschopnosť výboru a túto skutočnosť oznámi predsedovi. Bezpečnostný výbor je uznášaniaschopný, ak je na zasadnutí prítomná nadpolovičná väčšina členov výboru s právom hlasovať.

### Účasť tretích strán

Predseda bezpečnostného výboru môže – na základe vlastného uváženia alebo na základe návrhu niektorého z členov výboru – na zasadnutie prizvať aj ďalších relevantných zamestnancov alebo tretích strán, ktorí sú odborníkmi v oblasti, ktorá je predmetom zasadnutia výboru. Prizvané osoby sa spravidla zúčastňujú zasadnutia bezpečnostného výboru len vo veci, ktorá je dôvodom ich prizvania. Po ukončení rokovania k bodu, na prerokovanie ktorého boli prizvaní, môžu byť predsedom požiadaní, aby opustili zasadnutie bezpečnostného výboru.

Prizvané osoby nemajú hlasovacie právo.

### Hlasovanie a schvaľovanie uznesení

Rozhodnutia bezpečnostného výboru sú prijímané vo forme uznesení schvaľovaných na zasadnutiach bezpečnostného výboru.

Proces hlasovania o prijatí uznesenia na zasadnutiach bezpečnostného výboru vedie predseda. Každý člen výboru disponuje jedným hlasom, s výnimkou tajomníka. Hlasovanie nie je tajné.

Člen bezpečnostného výboru s právom hlasovať môže hlasovať:

* za uznesenie alebo
* proti uzneseniu alebo
* sa zdržať hlasovania o uznesení.

Pre prijatie uznesenia sa vyžaduje súhlas nadpolovičnej väčšiny prítomných členov bezpečnostného výboru. V prípade rovnosti hlasov rozhoduje hlas predsedu.

Prijaté uznesenia sú pre členov bezpečnostného výboru záväzné.

Uznesenia bezpečnostného výboru zaznamenáva tajomník do zápisnice zo zasadnutia.

### Zápisnica zo zasadnutia

Vypracovanie zápisnice zo zasadnutia bezpečnostného výboru (ďalej aj „zápisnica“) zabezpečuje tajomník.

Zápisnica obsahuje:

* prezenčnú listinu,
* zhrnutie prerokovaných bodov,
* prijaté uznesenia,
* ďalšie informácie a prílohy súvisiace s programom zasadnutia.

Schválenie zápisnice zo zasadnutia svojím podpisom potvrdzuje predseda.

Tajomník zasiela zápisnicu a všetky jej prílohy všetkým členom bezpečnostného výboru. V prípade súhlasu predsedu môže byť zápisnica alebo jej časť zaslaná i prizvaným osobám. Zápisnica sa adresátom zasiela najneskôr do 10 pracovných dní od ukončenia zasadnutia bezpečnostného výboru.

## Schvaľovanie a zmenové konanie štatútu bezpečnostného výboru

Štatút bezpečnostného výboru schvaľujú členovia bezpečnostného výboru na prvom zasadnutí výboru nadpolovičnou väčšinou hlasov.

Zmeny štatútu musia byť vykonané formou písomného a očíslovaného dodatku. Každú zmenu štatútu schvaľujú členovia bezpečnostného výboru nadpolovičnou väčšinou hlasov.

## Záverečné ustanovenia

Štatút bezpečnostného výboru je záväzný pre všetkých členov výboru a prizvané osoby.

Štatút nadobúda platnosť a účinnosť dňom jeho schválenia bezpečnostným výborom.

# Proces kontinuálneho vzdelávania v oblasti informačnej a kybernetickej bezpečnosti

Kontinuálne vzdelávanie všetkých pracovníkov prispieva k plneniu strategických princípov a hlavných cieľov ISMS a dodržaniu záväzkov vyplývajúcich z aplikovateľných záväzných legislatívnych a iných požiadaviek, ktoré sa inštitúcia zaviazala plniť, pritom ich pravidelne preskúmavať a vyhodnocovať.

Hlavným cieľom je zapojenie všetkých zamestnancov do zlepšovania činností a procesov riadenia informačnej a kybernetickej bezpečnosti a zvyšovanie úrovne povedomia v oblasti informačnej a kybernetickej bezpečnosti systematickým odborným vzdelávaním a motiváciou na všetkých organizačných úrovniach.

## Všeobecné zásady kontinuálneho

Všeobecné pravidlá platné pre všetky skupiny sú nasledovné:

1. Všetci zamestnanci inštitúcie musia absolvovať príslušné školenie v oblasti bezpečnostného povedomia a musia dostať pravidelne aktualizované verzie politík a postupov organizácie, tak ako si to vyžaduje ich pracovné zaradenie.

2. Program kontinuálneho vzdelávania v oblasti informačnej a kybernetickej bezpečnosti má hlavný cieľ, aby sa zamestnanci oboznamovali so svojou zodpovednosťou v oblasti informačnej a kybernetickej bezpečnosti a významom, ak túto zodpovednosť nedodržia.

3. Program kontinuálneho vzdelávania v oblasti informačnej a kybernetickej bezpečnosti je vyhotovený v súlade s Bezpečnostnou politikou kybernetickej bezpečnosti a musí zohľadňovať ochranu informácií v rámci inštitúcie a opatrenia, ktoré sa prijali na ich ochranu.

4. Program kontinuálneho vzdelávania v oblasti informačnej a kybernetickej bezpečnosti musí byť plánovaný so zameraním na roly zamestnancov v inštitúcii. Program sa musí pravidelne aktualizovať, aby stále sledoval platné interné politiky a postupy, a mal by byť tvorený aj ako poučenie z incidentov informačnej a kybernetickej bezpečnosti.

5. Školenie na zvyšovanie povedomia sa musí vykonávať na základe požiadaviek stanovených v Programe kontinuálneho vzdelávania na zvyšovanie bezpečnostného povedomia. Školenie na zvyšovanie povedomia môže využívať rôzne spôsoby uskutočňovania školení, ako napr. prezenčne v skupinách , na diaľku, pomocou webu, formou externých školení pre špecialistov a doplnkovo samovzdelávaním.

6. Vzdelávanie a školenie o informačnej a kybernetickej bezpečnosti musí obsahovať všeobecné aspekty, ako sú:

* vyjadrenie podpory manažmentu na presadzovanie informačnej a kybernetickej bezpečnosti v organizácii,
* potreba dôverne sa oboznámiť a mať súlad s aplikovanými pravidlami a povinnosťami informačnej a kybernetickej bezpečnosti, ako ich definujú politiky, normy, zákony, nariadenia, zmluvy a dohody,
* osobná zodpovednosť za jednotlivé činnosti, za nečinnosť, všeobecná zodpovednosť smerom k zabezpečeniu alebo ochrane informácií patriacich organizácii alebo zmluvným partnerom,
* základné postupy informačnej a kybernetickej bezpečnosti (ako informovanie o incidentoch informačnej a kybernetickej bezpečnosti) a základné opatrenia (ako ochrana heslom, opatrenia proti malvéru, politika čistého stola),
* kontaktné miesta a zdroje pre dodatočné informácie a rady týkajúce sa záležitostí informačnej a kybernetickej bezpečnosti vrátane ďalšieho materiálu na vzdelávanie a školenie.

7. Školenia o informačnej a kybernetickej bezpečnosti sa musia konať pravidelne a opakovane. Úvod do vzdelávania a úvodné školenie by mali absolvovať nielen noví zamestnanci, ale aj všetci, ktorí sa presunuli na nové pozície alebo roly s čiastočne iným rozsahom požiadaviek na informačnú a kybernetickú bezpečnosť, pričom by sa vzdelávanie alebo školenie malo vykonať predtým, ako začnú byť na novej pozícii aktívni, prípadne hneď po presune.

8. Pri vytváraní programu kontinuálneho vzdelávania je dôležité, aby zamestnanci rozumeli dôvodom, cieľom informačnej a kybernetickej bezpečnosti, možným dôsledkom, pozitívnym alebo negatívnym, na organizáciu podľa ich správania.

9. Povedomie, vzdelávanie a školenie sa môžu čiastočne alebo úplne vykonávať spolu s inými školiacimi aktivitami, ako sú napr. všeobecné školenie o IT, všeobecné bezpečnostné školenie, školenie pri nástupe do zamestnania. Aktivity na zvyšovanie povedomia, vzdelávanie a školenie musia mať náplň primeranú pre každú danú pozíciu, zodpovednosť a byť v súlade so schopnosťami vzdelávaných.

10. Posúdenie porozumenia zamestnancami sa môže vykonať na konci kurzu na zvyšovanie povedomia, vzdelávania a školenia formou testu.

## Roly zamestnancov z hľadiska potreby školení

Z hľadiska organizácie informačnej a kybernetickej bezpečnosti boli v Stratégii kybernetickej bezpečnosti zadefinované nasledovné skupiny bezpečnostných rolí:

* riadiace,
* výkonné,
* kontrolné.

Z hľadiska potreby školení v oblasti informačnej a kybernetickej bezpečnosti je nutné zamestnancov rozdeliť do skupín podľa potreby školení, ich rozsahu, obsahu a frekvencie.

Pri definovaní kategórií je nutné vychádzať z predpokladu, že každý účastník má mať minimálne také znalosti z informačnej a kybernetickej bezpečnosti, aby pokryl plnohodnotne plnenie svojich úloh, keďže nedostatočné vedomosti môžu viesť chybám z neznalosti. Na druhej strane snahy o plošné nadbytočné vzdelávanie môžu zapríčiniť neporozumenie všetkých dotknutých používateľov a neefektívnosť vynaloženého úsilia.

Navrhujeme preto nasledovné skupiny zamestnancov z hľadiska potreby školení:

| **Skupina** | **Zodpovednosť** |
| --- | --- |
| Zamestnanec | Každý vlastník aktíva je zodpovedný za ochranu integrity, dostupnosti a dôvernosť jednotlivých informačných aktív. Všetky bezpečnostné incidenty a nedostatky musia byť nahlásené manažérovi kybernetickej a informačnej bezpečnosti. Incidenty spojené s ochranou osobných údajov sú hlásené DPO. |
| Vedúci zamestnanec | Zodpovedný za implementáciu a dodržiavanie ISMS v rámci odboru. |
| Administrátor IS | Implementácia, dodržiavanie pridelených zodpovedností v rámci ISMS a podpora užívateľov |
| Manažér kybernetickej a informačnej bezpečnosti | Operačnú koordináciu ISMS, rovnako ako jeho udržiavanie. Vzdelávanie a osvetové programy informačnej a kybernetickej bezpečnosti pre zamestnancov. |

## Obsah školení

### Skupina „Zamestnanec“

Cieľom školenia pre skupinu zamestnanec je porozumenie základnej koncepcii riadenia informačnej a kybernetickej bezpečnosti, zodpovednosti za informačné aktíva, ochranu integrity, dostupnosť, dôvernosť jednotlivých informačných aktív a identifikáciu a hlásenie bezpečnostných incidentov.

Po absolvovaní školenia každý zamestnanec svojim podpisom potvrdzuje, že bol oboznámený s Bezpečnostnou politikou kybernetickej bezpečnosti a ďalšími dokumentmi informačnej a kybernetickej bezpečnosti. Súčasťou tohto vyhlásenia je aj záväzok zamestnanca, že bude dodržiavať túto politiku a všetky ostatné uvedené dokumenty ISMS a spolupracovať na efektívnom ISMS a že si je vedomý následkov nesplnenie súladu s požiadavkami ISMS.

Vzdelávanie v skupine Zamestnancov je možné rozdeliť na dve skupiny, a to na budovanie:

a) bezpečnostného povedomia, t. j. poznanie základných pojmov, hrozieb, rizík, bezpečnostných mechanizmov a princípov súvisiacich s používaním informačných a komunikačných technológií (ďalej aj „IKT“) a ich významu, teda ide o „základnú predstavu o tom, čo a prečo treba robiť, resp. čo a prečo sa robiť nemá“. Ide o oblasti ako: komunikácia elektronickou poštou, internet, autentizácia a zálohovanie. Je tiež potrebné poznanie bezpečnostných požiadaviek formulovaných v bezpečnostných politikách/predpisoch a schopnosť tieto požiadavky naplniť,

b) praktických zručností pri používaní IKT a ich bezpečnostných mechanizmov tak, aby boli laici schopní vykonať konkrétne úkony a porozumieť im. Ide o aktivity ako prihlásenie/odhlásenie sa zo systému, narábanie s heslom a jeho zmena, vhodná reakcia na bezpečnostné a iné upozornenia systému (operačného, antivírusového, webovej aplikácie a pod.), spôsob zálohovania a obnovy vlastných súborov atď. V tomto smere zohrávajú nezastupiteľnú úlohu školenia konkrétnych IKT a dobre a intuitívne navrhnuté aplikácie.

Školenie pre skupinu „Zamestnanec“ by malo obsahovať najmä nasledovné okruhy tém:

* pravidlá pre bezpečnosť pri práci na diaľku a pri použití mobilných zariadení,
* platné smernice a predpisy pre oblasť informačnej a kybernetickej bezpečnosti,
* základy fyzickej bezpečnosti,
* základy ochrany IT prostriedkov,
* pravidlá pre používanie hesiel,
* bezdrôtové siete,
* prenosné médiá (USB, CD, DVD),
* internetové služby, bezpečné správanie v sieti a surfovanie na internete,
* pravidlá pre používanie cloud služieb,
* škodlivý kód a jeho šírenie,
* identifikácia možných bezpečnostných incidentov a reakcia zamestnancov pri bezpečnostnom incidente,
* phishing,
* sociálne inžinierstvo,
* základy ochrany osobných údajov.

### Skupina “Vedúci zamestnanec”

Vedúci zamestnanci sú na jednej strane používateľmi IKT, ale na druhej strane zodpovedajú za ochranu aktív inštitúcie, ktoré sú v ich pôsobnosti, resp. rozhodujú o bezpečnostnej politike, o prostriedkoch na jej realizáciu, informačno-bezpečnostnom manažmente a pod. Títo pracovníci sú často zodpovední za napĺňanie legislatívnych informačno-bezpečnostných požiadaviek v inštitúcii (napr. požiadavky súvisiace s ochranou osobných údajov, utajovaných skutočností a pod.). Na plnenie týchto úloh potrebujú mať manažéri a vedúci pracovníci, na rozdiel od radových zamestnancov, hlbšie poznatky najmä v nasledujúcich oblastiach informačnej a kybernetickej bezpečnosti:

* znalosť a porozumenie základnému rámca riadenia informačnej a kybernetickej bezpečnosti,
* oboznámenie sa z platnými smernicami a platnými dokumentami v inštitúcii pre oblasť informačnej a kybernetickej bezpečnosti (bezpečnostná stratégia, bezpečnostná politika, bezpečnostný projekt),
* znalosť procesu riadenia bezpečnostných incidentov,
* znalosť procesu riadenia kontinuity činností,
* roly a o zodpovednosti spojených s informačnou a kybernetickou bezpečnosťou v rámci inštitúcie,
* platné legislatívne požiadavky súvisiace s informačnou a kybernetickou bezpečnosťou,
* princípy personálnej bezpečnosti,
* základné princípy zabezpečenia kontinuity činností,
* autorské práva a IT,
* ekosystém technických prostriedkov,
* životný cyklus prístupu k bezpečnosti informácií
* základy problematiky kybernetických hrozieb,
* narábanie s citlivými informáciami,
* mazanie a skartovanie informácií,
* klasifikácia informácií,
* ochrana osobných údajov – legislatíva a pravidlá.

### Skupina „Administrátor IS“

V tejto kategórii sú zaradení informatici/zamestnanci, ktorí sa nešpecializujú len na informačnú a kybernetickú bezpečnosť. Pôsobia ako návrhári softvérových a hardvérových systémov, ako programátori, správcovia systémov, sietí a užívateľskej podpory. Obyčajne majú čiastkové (v niektorých oblastiach aj detailné) poznatky z tých aspektov informačnej a kybernetickej bezpečnosti, ktoré sa dotýkajú ich každodenných činností. V má táto skupina často najväčší vplyv na stav informačnej a kybernetickej bezpečnosti v organizácii. Širší základný prehľad a pochopenie bezpečnostných požiadaviek a opatrení (či už z pohľadu návrhu, vývoja alebo prevádzky) preto vedie k zvyšovaniu bezpečnostnej úrovne IKT. Vzdelávacie potreby v tejto skupine sú do veľkej miery závislé od konkrétnej profesijnej orientácie. Základný obsah, spoločný pre všetkých v tejto skupine zahŕňa:

* pochopenie hrozieb, zraniteľností a výsledných rizík spojených s IKT, mechanizmov a opatrení na ich elimináciu alebo redukciu, ako aj predpokladov a dôsledkov ich realizácie,
* pochopenie podstaty bezpečnostných požiadaviek na IKT a možností ich naplnenia,
* schopnosť navrhnúť, realizovať, udržiavať a prevádzkovať (v súlade s príslušnou profesijnou orientáciou) mechanizmy na naplnenie bezpečnostných požiadaviek na IKT,
* schopnosť byť kvalifikovaným partnerom pre spoluprácu so špecialistami v informačnej a kybernetickej bezpečnosti (tam, kde sa profesijné orientácie prekrývajú).

Špecifické vzdelávacie potreby pre oblasť návrhu a vývoja zahŕňajú najmä bezpečnostné otázky súvisiace so životným cyklom vývoja softvéru, s autentizáciou, riadením prístupu, logovaním, testovaním softvéru, implementáciou kryptografických mechanizmov a pod. Špecifické vzdelávacie potreby pre oblasť prevádzky zahŕňajú najmä bezpečnostné otázky súvisiace s prostredím, v ktorom sa IKT prevádzkujú (siete, operačné systémy, databázy a pod.) a procesmi (zálohovanie a obnova, riešenie incidentov, plánovanie kontinuity činností a pod.).

Školenie pre túto skupinu by malo obsahovať oblasti uvedené pre skupinu „Vedúci zamestnanec“ a súčasne aj nasledovné oblasti:

* princípy riadení projektov a procesoch prevádzky IKT,
* bezpečnostné požiadavky a očakávanie softvérového vývoja,
* faktory ovplyvňujúce bezpečnosť softvéru,
* hľadanie zraniteľností v softvéri,
* nakladanie so zraniteľnosťami v cudzom kóde,
* nakladanie so zraniteľnosťami spôsobenými ľudským faktorom,
* bezpečnosť vo fáze návrhu,
* prevencia zraniteľností platformy,
* implementácia ochranných mechanizmov,
* autentizácia a autorizácia,
* šifrovanie,
* certifikáty, kľúče a práca s nimi,
* uskutočňovanie bezpečnostných testov aplikácií,
* aktuálne využívané technológie v rámci inštitúcie (MS SWL, Windows Server, MS .NET framework 4.0, HP DataProtector, sieťové prvky HP, CISCO).

### Skupina „Manažér kybernetickej a informačnej bezpečnosti“

Do tejto kategórie patrí samotný manažér kybernetickej a informačnej bezpečnosti a interný audítor so zameraním na informačnú a kybernetickú bezpečnosť. U týchto špecialistov sa predpokladajú a vyžadujú dostatočné vedomosti o IKT, o hrozbách, zraniteľnostiach, rizikách, právnych požiadavkách na ochranu IKT, protiopatreniach, správe rizík, zaisťovaní kontinuity činnosti, štandardoch, normách, certifikácii a akreditácii a iných oblastiach informačnej a kybernetickej bezpečnosti. Špecialisti v informačnej a kybernetickej bezpečnosti majú mať základné vedomosti vo všetkých oblastiach informačnej a kybernetickej bezpečnosti vrátane pochopenia príslušných princípov, modelov, procesov, bezpečnostných techník a ich vzájomných vzťahov.

Školenia majú obsahovať rovnaké základy ako pre skupinu „Administrátor IS“ a naviac ďalšie školenia zamerané na úzku oblasť IKT. Tieto externé školenia sú obyčajne vysoko špecializované a nie je ich možné absolvovať v rámci jedného roka. Každý rok je potrebné vybrať podľa možností a potrieb inštitúcie niekoľko oblastí z nižšie uvedených a absolvovať príslušné školenia, obyčajne zakončené skúškou a certifikátom:

* aktuálne legislatívne požiadavky súvisiace s informačnou a kybernetickou bezpečnosťou na Slovensku,
* tvorba smerníc a dokumentov organizácie pre oblasť informačnej a kybernetickej bezpečnosti,
* bezpečnostné analýzy a hodnotenia, audit informačnej a kybernetickej bezpečnosti v organizácii,
* hrozby, útoky a zraniteľnosti,
* riadenie identity a prístupu,
* riadenie rizík,
* kryptografia a PKI,
* riadenie IT s dôrazom na riadenie rizík,
* nástroje pre spoluprácu a ich využitie v organizačnej bezpečnosti,
* integrácie pokročilých autorizačných a autentizačných techník,
* kryptografické nástroje,
* bezpečnostné nástroje pre koncové body,
* bezpečnostné nástroje pre mobilné zariadenia,
* zabezpečenie sietí,
* bezpečný vývojový cyklus softvéru a zabezpečenie v návrhu systémov,
* integrácia rôznych technológií v rámci bezpečných architektúr,
* reakcie na bezpečnostné incidenty a zotavenie sa z nich,
* riešenie rizík v informačnej bezpečnosti,
* analýza hrozieb zbierajúcich dáta o prostredí,
* analýza útokov na počítače a sieťové prostredie,
* analýza techník používaných po útoku,
* riadenie zraniteľností v organizácii,
* plánovanie a cielenie penetračných testov pre zhodnotenie bezpečnosti,
* zber bezpečnostných informácií a dát,
* analýza logov,
* uskutočňovanie aktívnej analýzy koncových zariadení a sietí,
* reakcie na bezpečnostné incidenty,
* vyšetrovanie bezpečnostných incidentov,
* riešenie problémov v bezpečnostnej architektúre,
* aktívny a pasívny zber dát,
* analýza zraniteľností,
* využívanie zraniteľností koncových bodov,
* testovanie aplikácií,
* aktivity nadväzujúce na využitie zraniteľností,
* analýza a reportovanie výsledkov penetračných testov,
* aktuálne využívané technológie v rámci inštitúcie (MS SWL, Windows Server, MS .NET framework 4.0, HP DataProtector, sieťové prvky HP, CISCO),
* školenia CISA, SEH, CISSP, CCISO
* a pod.

# Prílohy

## Rámcová matica zodpovedností pre aplikáciu bezpečnostných opatrení

### Príloha č. 1 - 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

### Príloha č. 2 - 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