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



# Obsah

[Obsah 2](#_Toc129013282)

[1 Správa dokumentu 5](#_Toc129013283)

[2 Úvod 6](#_Toc129013284)

[2.1 Rozsah platnosti 7](#_Toc129013285)

[2.2 Skratky a pojmy 8](#_Toc129013286)

[2.2.1 Skratky 8](#_Toc129013287)

[2.2.2 Pojmy 8](#_Toc129013288)

[3 Organizácia bezpečnosti 14](#_Toc129013289)

[3.1 Riadenie bezpečnostnej architektúry 14](#_Toc129013290)

[3.2 Systém riadenia kybernetickej a informačnej bezpečnosti 15](#_Toc129013291)

[3.2.1 Právomoci a povinnosti v systéme riadenia kybernetickej a informačnej bezpečnosti 15](#_Toc129013292)

[3.2.2 Roly kybernetickej a informačnej bezpečnosti 15](#_Toc129013293)

[3.3 Riadenie identít a prístupových práv 16](#_Toc129013294)

[3.3.1 Riadenie identít 17](#_Toc129013295)

[3.3.2 Riadenie prístupových práv 18](#_Toc129013296)

[3.4 Riadenie privilegovaných prístupov 19](#_Toc129013297)

[3.4.1 Prideľovanie privilegovaných prístupových oprávnení 19](#_Toc129013298)

[3.4.2 Vypracovanie pravidiel pre prideľovanie privilegovaných prístupových opatrení 19](#_Toc129013299)

[3.4.3 Žiadosti o pridelenie privilegovaných prístupových oprávnení 19](#_Toc129013300)

[3.4.4 Používanie privilegovaných programov a sieťových služieb 20](#_Toc129013301)

[3.5 Bezpečnostný monitoring a správa bezpečnostných záznamov 21](#_Toc129013302)

[3.5.1 Určenie rozsahu monitorovania 21](#_Toc129013303)

[3.5.2 Monitorovanie a zaznamenávanie činností 21](#_Toc129013304)

[3.5.3 Evidencia a ukladanie záznamov 21](#_Toc129013305)

[4 Riadenie rizík 22](#_Toc129013306)

[4.1 Metodika posudzovania vplyvu na ochranu osobných údajov 22](#_Toc129013307)

[4.2 Metodika posudzovania rizík 22](#_Toc129013308)

[4.3 Riadenie a ošetrovanie rizika 23](#_Toc129013309)

[5 Fyzická bezpečnosť 24](#_Toc129013310)

[5.1 Zabezpečenie oblasti 24](#_Toc129013311)

[5.2 Bezpečnosť zariadení 24](#_Toc129013312)

[5.3 Premiestňovanie technických prostriedkov IKT 25](#_Toc129013313)

[6 Riešenie bezpečnostných incidentov 26](#_Toc129013314)

[7 Riadenie informačných aktív 27](#_Toc129013315)

[7.1 Klasifikácia informácií a kategorizácia sietí a informačných systémov 27](#_Toc129013316)

[7.2 Registratúrny poriadok a registratúrny plán 30](#_Toc129013317)

[8 Pravidlá správania a dobrej praxe 31](#_Toc129013318)

[8.1 Práca na diaľku a používanie mobilných zariadení 31](#_Toc129013319)

[8.1.1 Práca na diaľku 31](#_Toc129013320)

[8.1.2 Fyzická bezpečnosť mobilných zariadení 32](#_Toc129013321)

[8.1.3 Bezpečnosť informácií 32](#_Toc129013322)

[8.2 Riadenie personálnej bezpečnosti 33](#_Toc129013323)

[8.2.1 Opatrenia pred nástupom do zamestnania 33](#_Toc129013324)

[8.2.2 Opatrenia počas zamestnania 33](#_Toc129013325)

[8.2.3 Disciplinárny proces 34](#_Toc129013326)

[8.2.4 Opatrenia pri ukončení a zmene zamestnania 34](#_Toc129013327)

[8.2.5 Program budovania bezpečnostného povedomia 34](#_Toc129013328)

[8.2.6 Povinnosti používateľov 34](#_Toc129013329)

[8.3 Pravidlá komunikácie 35](#_Toc129013330)

[8.3.1 Pravidlá pre prácu s elektronickou poštou 35](#_Toc129013331)

[8.3.2 Pravidlá pre prácu s internetom 37](#_Toc129013332)

[9 Riadenie dodávateľských vzťahov 38](#_Toc129013333)

[9.1 Riadenie dodávateľských služieb 38](#_Toc129013334)

[9.2 Zmluvy s tretími stranami 39](#_Toc129013335)

[10 Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií 41](#_Toc129013336)

[10.1 Vývoj a testovanie informačných systémov 41](#_Toc129013337)

[10.2 Postupy údržby informačných systémov 41](#_Toc129013338)

[10.2.1 Údržba funkčných požiadaviek 42](#_Toc129013339)

[10.2.2 Údržba aplikácií 42](#_Toc129013340)

[10.2.3 Údržba infraštruktúry 42](#_Toc129013341)

[10.3 Riadenie technických zraniteľností a manažment záplat 43](#_Toc129013342)

[10.3.1 Vymedzenie rozsahu a spôsobu zabezpečenia ochrany pred škodlivým softvérom 43](#_Toc129013343)

[10.3.2 Požiadavky na udržanie aktuálnosti systému ochrany pred škodlivým softvérom 43](#_Toc129013344)

[10.3.3 Riadenie technických zraniteľností 43](#_Toc129013345)

[11 Riadenie a prevádzka informačno-komunikačných technológií 45](#_Toc129013346)

[12 Riadenie súladu 46](#_Toc129013347)

[12.1 Audit kybernetickej bezpečnosti 46](#_Toc129013348)

[12.2 Spracúvanie osobných údajov a klasifikovaných informácií 46](#_Toc129013349)

[12.3 Poskytovanie súčinnosti tretím stranám 46](#_Toc129013350)

[13 Riadenie kontinuity procesov činností 48](#_Toc129013351)

[14 Revízia dokumentu 49](#_Toc129013352)

[15 Prílohy 50](#_Toc129013353)

[15.1 Príloha č. 1 – Legislatívny rámec 50](#_Toc129013354)

# Správa dokumentu

Dokument „Politika kybernetickej bezpečnosti a informačnej bezpečnosti“ je vzorovým dokumentom slúžiacim pre potreby orgánov verejnej moci (OVM). 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.

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 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 (ďalej aj „Bezpečnostná politika“ alebo „BP“) definuje pravidlá a zásady pre kybernetickú a informačnú bezpečnosť. Tento dokument spolu so Stratégiou kybernetickej bezpečnosti tvorí základný rámec riadenia kybernetickej a informačnej bezpečnosti a slúži ako základ pre vypracovanie následných interných predpisov (napr. prevádzkové predpisy, pracovné postupy a pod.).

Bezpečnostná politika kybernetickej bezpečnosti bola vypracovaná na základe posúdenia:

* súvisiacej infraštruktúry informačných a komunikačných technológií (ďalej aj „IT“ alebo „IKT“),
* súvisiacej aplikačnej architektúry,
* súvisiacej bezpečnostnej architektúry a implementovaných bezpečnostných opatrení,
* súvisiacich organizačných usporiadaní, pracovných rolí, zodpovednosti a delenia právomocí,
* súvisiacich zaužívaných rámcov riadenia operačných rizík,
* súvisiacej organizačnej kultúry a spoločenskej zodpovednosti.

Bezpečnostná politika kybernetickej 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 BP deklaruje svoju vôľu a postoj k riešeniu kybernetickej a informačnej bezpečnosti. Východiskami pre budovanie systému riadenia kybernetickej a informačnej bezpečnosti sú predovšetkým:

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

Kontrola a aktualizácia BP je vykonávaná minimálne raz ročne. Mimoriadna revízia môže byť vyvolaná:

* zmenami vo vývoji informačných systémov (ďalej aj „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 BP zaisťuje manažér kybernetickej a informačnej bezpečnosti.

Manažér kybernetickej a informačnej bezpečnosti sleduje aktuálnu legislatívu vzťahujúcu sa na prevádzku IS a zodpovedá za zaistenie zhody BP 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 bezpečnostnej politike kybernetickej 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 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 BP, 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 manažér kybernetickej a informačnej bezpečnosti.

Výnimky z dodržiavania tejto politiky môže v mimoriadnych a dostatočne písomne odôvodnených prípadoch povoliť vedenie organizácie alebo manažér kybernetickej 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 a zabezpečiť jej dôsledné plnenie.

## Skratky a pojmy

### Skratky

|  |  |
| --- | --- |
| Skratka | Popis skratky |
| BP | Bezpečnostná politika |
| 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) |
| 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 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,
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** – 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 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** – 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 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, ktoré je potrebné vykonať na obnovu narušenej funkcie kritických procesov v IT prostredí organizácie.

**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.

**Používateľ**– každý zamestnanec organizácie 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 organizácie** – 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 organizácie, 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.

**Rola** – predstavuje priradenie špecifických oprávnení pre výkon konkrétnych 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 kybernetickej 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** – 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 (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.

# Organizácia bezpečnosti

Organizácia kybernetickej a informačnej bezpečnosti vychádza predovšetkým z platných právnych aktov, strategických dokumentov a medzinárodných štandardov uvedených v dokumente „Stratégia kybernetickej bezpečnosti“.

## Riadenie bezpečnostnej architektúry

Bezpečnostnú architektúru je možné v širšom kontexte chápať ako vymedzenie okolia IS a jeho vzťah k možnému narušeniu bezpečnosti.

Základnými princípmi pre riadenie bezpečnostnej architektúry sú:

* vlastník údajov v spolupráci s manažérom kybernetickej a informačnej bezpečnosti stanovuje minimálne bezpečnostné požiadavky na zabezpečenie ochrany informácií spracovávaných v procesoch z oblasti svojej pôsobnosti, z ktorých vyplývajú požiadavky na bezpečnostnú architektúru,
* návrh zmien v bezpečnostnej architektúre navrhuje manažér kybernetickej a informačnej bezpečnosti takým spôsobom, aby bol v súlade s:
* platnou legislatívou Slovenskej republiky,
* platnými internými predpismi organizácie,
* dobrou praxou v zmysle medzinárodných štandardov,
* návrh zmien v bezpečnostnej architektúre schvaľuje bezpečnostný výbor organizácie,
* všetky prvky bezpečnostnej architektúry musia:
* spĺňať presne zadefinovaný účel v kontexte ochrany IT prostredia organizácie,
* mať priradeného jednoznačného vlastníka,
* byť auditovateľné,
* ochraňovať IT prostredie voči kybernetickým bezpečnostným incidentom,
* umožniť detekciu kybernetických bezpečnostných incidentov.

Bezpečnostnú architektúru tvoria najmä nasledovné typy technických zariadení:

* sieťové prvky podieľajúce sa na vytvorení bezpečnostnej zonácie sietí organizácie,
* firewall,
* IDS sonda,
* IPS sonda,
* sieťová sonda,
* proxy server,
* data loss prevention (DLP),
* záložný zdroj napájania.

## Systém riadenia kybernetickej a informačnej bezpečnosti

Riadenie kybernetickej a informačnej bezpečnosti vychádza primárne zo zákona o kybernetickej bezpečnosti a z týchto medzinárodných štandardov:

* 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)..

### Právomoci a povinnosti v systéme riadenia kybernetickej a informačnej bezpečnosti

Na účely organizácie kybernetickej a informačnej bezpečnosti sa uplatňuje zásada:

* ustanovenia bezpečnostného výboru ako vrcholového orgánu pre riadenie kybernetickej a kybernetickej bezpečnosti,
* určenia manažéra kybernetickej 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 a informačnej bezpečnosti je primerane aplikovaný princíp oddeľovania výkonných a kontrolných funkcií, s cieľom minimalizovať riziko zneužitia privilégií.

Pri obsadzovaní rolí je nevyhnutné dodržiavať aspoň nasledovné pravidlá týkajúce sa nezlučiteľnosti funkcií:

### Roly kybernetickej a informačnej bezpečnosti

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

* riadiacu,
* výkonnú,
* kontrolnú.

Detailný popis rolí kybernetickej a informačnej bezpečnosti sa nachádza v rámci dokumentu “Stratégia kybernetickej bezpečnosti”.

## Riadenie identít a prístupových práv

Riadenie prístupov osôb k sieti a IS 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.

Riadenie prístupov osôb k sieti a informačnému systému zahŕňa:

* vypracovanie zásad riadenia prístupu k informáciám,
* riadenie prístupu používateľov,
* zodpovednosť používateľov,
* riadenie prístupu k sieťam,
* prístup k operačnému systému a jeho službám,
* prístup k aplikáciám,
* monitorovanie prístupu a používania IS a
* riadenie vzdialeného prístupu.

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 načítanie 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 systému v zmysle príslušnej bezpečnostnej politiky.

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.

Vytváranie nových rolí je súčasťou implementácie nových IS v projektovom režime alebo výsledkom požiadavky na zmenu a riadi sa príslušnými internými predpismi.

### Riadenie identít

**Definovanie rolí v informačnom systéme**

Vlastník procesu schvaľuje navrhnuté profily jednotlivých rolí, pričom zohľadňuje stanovisko manažéra kybernetickej a informačnej bezpečnosti. Vlastník procesu zodpovedá za definovanie rolí a vypracovanie funkčného popisu rolí, pričom pri návrhu zohľadňuje:

* požiadavku pokrytia všetkých aktivít procesu, ktoré roly funkčne reprezentujú,
* tzv. princíp need-to-know,
* bezpečnostné úrovne spracovávaných informácií (podľa klasifikácie informácií),
* požiadavky relevantnej legislatívy,
* požiadavky na vytvorenie rolí pre výkon používateľských činností a pre výkon správcovských činností,
* požiadavky na segregáciu povinností.

Administrátor IS implementuje profily schválených rolí v IT prostredí organizácie vzhľadom na:

* možnosti IS,
* tzv. princíp need-to-know,
* bezpečnostné úrovne spracovávaných informácií (podľa klasifikácie informácií),
* požiadavky relevantnej legislatívy,
* požiadavky na segregáciu povinností,
* požiadavku na oddelenie rolí určených pre výkon používateľských a pre výkon správcovských činností,
* požiadavky na konzistentnosť medzi riadením prístupu a pravidlami klasifikácie,
* informačných aktív.

Manažér kybernetickej a informačnej bezpečnosti posudzuje a pripomienkuje návrhy rolí a ich profilov z hľadiska bezpečnostných požiadaviek na:

* tzv. princíp need-to-know,
* bezpečnostné úrovne spracovávaných informácií (podľa klasifikácie informácií),
* segregáciu povinností,
* oddelenie rolí určených pre výkon užívateľských a pre výkon správcovských činností,
* oddelenie rolí pri prideľovaní prístupu do viacerých IS,
* požiadavky na konzistentnosť medzi riadením prístupu a pravidlami klasifikácie informačných aktív.

Manažér kybernetickej a informačnej bezpečnosti vykonáva kontrolu implementácie profilov jednotlivých rolí. O výsledku kontroly podáva správu vlastníkovi procesu.

**Modifikácia rolí v informačnom systéme**

Požiadavku na modifikáciu rolí v IT prostredí organizácie predkladá:

* v prípade funkčnej zmeny – vlastník procesu,
* v prípade zmeny bezpečnostných požiadaviek – manažér kybernetickej a informačnej bezpečnosti,
* v prípade nesplnenia podmienok alebo zmien určených v zmysle platnej legislatívy pre spracovávanie osobných údajov – zodpovedná osoba za ochranu osobných údajov.

Modifikácia rolí sa vykonáva primeranou aplikáciou pravidiel uvedených v bode 3.3.1.

**Dokumentovanie rolí v informačnom systéme**

Dokumentácia rolí musí obsahovať:

* funkčný popis roly – rozsah a štruktúru určuje vlastník procesu,
* technický popis roly – rozsah a štruktúru určuje správca IS v spolupráci s manažérom kybernetickej a informačnej bezpečnosti, pričom sa zohľadnia možnosti konkrétneho IS,
* protokol o funkčnom otestovaní roly – rozsah a štruktúru určuje vlastník procesu.

### Riadenie prístupových práv

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 informačnej bezpečnosti.

Riadenie prístupov je tak logické, ako aj fyzické a tieto prístupy by mali byť ošetrené spoločne.

V rámci riadenia prístupových práv sa zohľadňuje nasledovné:

* bezpečnostné požiadavky jednotlivých podnikových aplikácií,
* pravidlá šírenia informácií a autorizácie, napr. princíp potreby poznať a bezpečnostné úrovne a klasifikáciu informácií,
* konzistentnosť medzi riadením prístupu a pravidlami klasifikácie informácií rôznych systémov a sietí,
* relevantnú legislatívu a všetky zmluvné záväzky o ochrane prístupu k dátam alebo službám,
* riadenie prístupových práv v distribuovanom a sieťovom prostredí, ktoré pozná všetky typy dostupného spojenia,
* segregáciu rolí vzhľadom na riadenie prístupu, napr. požiadavky o udelenie prístupu, jeho autorizáciu a správu prístupu,
* požiadavky na formálnu autorizáciu žiadostí o udelenie prístupu,
* požiadavky na periodickú revíziu prístupových opatrení,
* odňatie prístupových práv,
* archiváciu všetkých záznamov signifikantných udalostí týkajúcich sa používania a riadenia identít používateľov a utajených autentizačných údajov,
* roly s privilegovaným prístupom.

## Riadenie privilegovaných prístupov

### Prideľovanie privilegovaných prístupových oprávnení

Privilegované prístupové oprávnenia sa do produkčného prostredia IS štandardne neprideľujú ani interným ani externým používateľom. Pre vývojové, testovacie a produkčné prostredie každého IS musia byť formálne popísané a zdokumentované pravidlá pre prideľovanie privilegovaných oprávnení, ktoré musia obsahovať minimálne:

* popis postupov pridelenia oprávnení, resp. zriadenia účtov s takýmito oprávneniami,
* popis postupov aktivácie a deaktivácie oprávnení správcami IS,
* popis postupov nastavenia časových obmedzení pre platnosť oprávnení, resp. účtov,
* popis spôsobu monitorovania, zaznamenávania a zdokumentovania vykonaných aktivít privilegovanými používateľmi
* popis postupov finálneho zrušenia/odstránenia oprávnení, resp. účtov.

### Vypracovanie pravidiel pre prideľovanie privilegovaných prístupových opatrení

Pravidlá pre prideľovanie privilegovaných prístupových oprávnení do vývojových, testovacích a produkčných prostredí jednotlivých IS navrhuje manažér kybernetickej a informačnej bezpečnosti alebo ním poverený bezpečnostný pracovník.

Manažér kybernetickej a informačnej bezpečnosti posudzuje návrh pravidiel pre prideľovanie privilegovaných úplných administrátorských oprávnení.

Pravidlá pre prideľovanie privilegovaných prístupových oprávnení schvaľuje príslušný vedúci zamestnanec.

Schválené pravidlá uchováva príslušný administrátor IS.

Pravidlá sú aktualizované podľa potreby na základe podnetov manažéra kybernetickej a informačnej bezpečnosti alebo ním povereného bezpečnostného pracovníka.

### Žiadosti o pridelenie privilegovaných prístupových oprávnení

Požiadavku na pridelenie privilegovaných prístupových oprávnení uplatňuje príslušný administrátor IS na svojho priameho nadriadeného.

Požiadavku na pridelenie privilegovaných prístupových oprávnení pre externých pracovníkov uplatňuje príslušný vlastník údajov alebo vlastník procesu na svojho priameho nadriadeného.

Požiadavka musí obsahovať minimálne:

* dôvody pre pridelenie úplných administrátorských oprávnení resp. dôvody pre zriadenie účtu (účtov) s takýmito oprávneniami,
* stručný popis aktivít, ktoré budú na IKT vykonávané,
* stručný popis kto, kedy a ako bude aktivity realizovať,
* časové obmedzenie pre platnosť oprávnení resp. účtu (účtov),
* identifikáciu IKT, v ktorých majú byť oprávnenia resp. účty zriadené,
* v prípade externých pracovníkov preukázateľné splnenie požiadaviek na zabezpečenie ochrany dôverných informácií (napr. doloženie príslušnej časti zmluvy, podpísaných prehlásení pracovníkov tretej strany, NDA a pod.).

Požiadavku na pridelenie oprávnení schvaľuje / zamieta príslušný vedúci zamestnanec.

### Používanie privilegovaných programov a sieťových služieb

Pri riadení prístupu v IS je potrebné zohľadniť:

* požiadavku na sprístupnenie len tých informácií, na ktoré má používateľ autorizáciu,
* požiadavku na realizáciu len tých operácií, na ktoré má používateľ autorizáciu,
* možnosti riadenia prístupu prostredníctvom dynamického menu IKT.

Používanie privilegovaných programov (utilít), ktoré môžu mať schopnosť obísť systémové a aplikačné opatrenia, musí byť obmedzené a prísne riadené. V súvislosti s ich použitím je potrebné zohľadniť:

* používanie identifikačných, autentifikačných a autorizačných postupov pre systémové utility,
* oddelenie systémových utilít od aplikačného softvéru,
* obmedzenie používania systémových utilít na minimálny počet dôveryhodných a autorizovaných používateľov,
* autorizácia len pre konkrétne použitie systémových utilít,
* obmedzenie dostupnosti systémových utilít (napr. len po dobu trvania autorizovanej zmeny),
* zaznamenávanie každého použitia systémových utilít,
* definovanie a dokumentovanie autorizačných úrovní systémových utilít,
* odstraňovanie všetkých nepotrebných, na softvéri založených utilít zo systémového softvéru,
* nesprístupňovanie systémových utilít osobám, ktoré majú prístup k aplikáciám na systémoch, na ktorých sa vyžaduje uplatnenie segregácie povinností.

Pri riadení prístupu do LAN je potrebné zohľadniť:

* požiadavku na prístup do sietí, na ktoré má používateľ autorizáciu,
* požiadavku na sprístupnenie sieťových služieb, na ktoré má používateľ autorizáciu,
* obmedzenie sieťového prístupu stanovením zvláštnych logických domén,
* používanie špecifických aplikačných systémov a bezpečnostných brán pre externé pripojenia do siete a oddelenie sietí na zabránenie neobmedzenému / nekontrolovanému prechádzaniu po sieti a riadenie povolených komunikácií zdroja s cieľom cez bezpečnostné brány (firewall),
* smerovanie komunikácie v sieti,
* primeranú autentizáciu vzdialených užívateľov,
* stanovenie vyhradených liniek a telefónnych čísel a použitie vyhradených liniek alebo prostriedkov kontroly adresy používateľa siete (napr. procedúr spätného volania),
* využívanie bezpečnostných atribútov komunikačných protokolov.

## Bezpečnostný monitoring a správa bezpečnostných záznamov

Cieľom monitorovania je zabezpečiť dostatočne rozsiahlu databázu údajov o prevádzke IS, aby bolo možné v krátkom čase realizovať opatrenia vedúce k zníženiu rizika výskytu bezpečnostných incidentov.

### Určenie rozsahu monitorovania

Manažér kybernetickej a informačnej bezpečnosti spolu s administrátorom IS, príp. inými relevantnými technickými pracovníkmi sú zodpovední za určenie rozsahu monitorovania informačných aktív.

Monitorovanie informačných aktív poskytujúcich prístup do Internetu a elektronickej pošty sa vykonáva vždy.

Všetky informačné aktíva podliehajúce monitorovaniu, musia mať pridelený jednoznačný identifikátor.

Manažér kybernetickej a informačnej bezpečnosti spolu s administrátorom IS, príp. inými relevantnými technickými pracovníkmi vykonáva revíziu stanoveného rozsahu informačných aktív a monitorovania minimálne raz ročne.

### Monitorovanie a zaznamenávanie činností

Súčasťou (výstupom) monitorovania sú auditné záznamy (logy), pričom ich sledovanie, ukladanie, vyhodnocovanie a zabezpečenie je v kompetencii administrátora IS a príslušného vedúceho zamestnanca.

Monitorovanie prevádzky informačného systému zabezpečuje administrátor IS alebo iná poverená osoba.

Osoby poverené monitorovaním prevádzky zároveň zabezpečujú a spravujú nástroje pre monitorovanie IKT/IS (HW aj SW).

### Evidencia a ukladanie záznamov

Administrátor IS je povinný uchovávať všetky tieto záznamy minimálne po dobu 6 mesiacov.

# Riadenie rizík

## Metodika posudzovania vplyvu na ochranu osobných údajov

Posúdenie vplyvu na ochranu osobných údajov sa vykonáva:

1. pri akýchkoľvek zmenách v spracovaní osobných údajov, napr.:

* pre zavedením nových IT systémov na spracovanie údajov,
* pri zmenách legislatívnych opatrení,
* pred významnými zmenami v spracovaní údajov:
* pri stanovení nového účelu spracovania údajov,
* pri novom spôsobe či prostriedkoch spracovania údajov,

1. ak je pravdepodobné, že spracovanie bude predstavovať vysoké riziko pre práva a slobody jednotlivcov,
2. v prípade monitorovania verejne prístupných miest vo veľkom rozsahu,
3. v prípade systematického a rozsiahleho hodnotenia osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania.

Posúdenie vplyvu na ochranu osobných údajov sa vykonáva priebežne a prehodnocuje sa každé 3 roky.

Za zabezpečenie vykonávania posudzovania vplyvu na ochranu osobných údajov je zodpovedná osoba zodpovedná za ochranu osobných údajov. Manažér kybernetickej a informačnej bezpečnosti poskytuje pomoc a navrhuje vykonanie posudzovania, v závislosti od bezpečnostných alebo prevádzkových potrieb.

## Metodika posudzovania rizík

Za hlavné potenciálne hrozby pre svoje IKT organizácia považuje:

1. prieniky do IS zo strany vonkajších alebo vnútorných subjektov s cieľom modifikovať alebo odcudziť údaje, zvlášť s ohľadom na presun aktivít organizovaného zločinu do oblasti počítačovej kriminality,
2. únik informácií o klientoch a žiadateľoch alebo o vnútornej činnosti organizácie, neoprávnenej manipulácii s týmito informáciami alebo ich zneužitie,
3. stratu alebo nedostupnosť prostriedkov IKT, ktoré sú nevyhnutné na prevádzku IKT alebo zaistenie kontinuity interných procesov,
4. stratu alebo nedostupnosť kritických údajov v rámci IS,
5. závislosť organizácie na externých dodávateľoch technických alebo programových prostriedkov,
6. zneužitie prostriedkov IKT používateľmi (napríklad ukladanie nelegálneho obsahu, hromadné odosielanie nevyžiadanej pošty, poškodenie dobrého mena organizácie prostredníctvom IKT a atď.)

## Riadenie a ošetrovanie rizika

Procesy týkajúce sa riadenia a ošetrovania rizika sú bližšie popísané v rámci dokumentu „Metodika analýzy rizík kybernetickej bezpečnosti“ pripravenej zo strany Národného bezpečnostného úradu. Riadenie a ošetrovanie rizík je súčasťou kapitoly 7 a 8 predmetnej metodiky.

# Fyzická bezpečnosť

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

## Zabezpečenie oblasti

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.

## Bezpečnosť zariadení

Účelom bezpečnosti zariadení je zabrániť stratám, zničeniu, krádeži alebo kompromitovaniu informačných aktív alebo prerušeniu činnosti organizácie.

Umiestnenie zariadení a ich ochrana

Zariadenia sú umiestnené a chránené s cieľom obmedziť riziká vyplývajúce z hrozieb prostredia a riziká a príležitosti neautorizovaného prístupu.

Podporné služby

Zariadenia sú chránené pred výpadkami elektrickej energie a inými anomáliami spôsobenými zlyhaním dodávky podporných služieb.

Bezpečnostné kabeláže

Elektrická alebo telekomunikačná kabeláž prenášajúca dáta alebo podporujúce informačné služby je chránená pred odpočúvaním, manipuláciou alebo poškodením.

Údržba zariadení

Zariadenia sú správne udržiavané, aby sa zaistila ich nepretržitá dostupnosť a integrita.

Odnášanie zariadení

Prístroje, informácie alebo softvér sa bez autorizácie nesmú odnášať mimo pracoviska.

Bezpečnosť zariadení mimo organizácie

Bezpečnosť sa aplikuje aj na zariadenia mimo priestorov organizácie. Je potrebné brať do úvahy rozličné riziká vyplývajúce z práce mimo priestorov organizácie.

Bezpečné vyradenie alebo opätovné používanie zariadení

Všetky prvky zariadení obsahujúce úložné médiá sú skontrolované, čím sa zabezpečuje, že všetky citlivé dáta a licencovaný softvér sú bezpečne zmazané alebo prepísané ešte pred vyradením alebo opätovným použitím zariadenia.

Každý používateľ je povinný vrátiť akýkoľvek prostriedok IKT, ktorý už nepoužíva. Táto povinnosť sa vzťahuje aj na nefunkčné, poškodené zariadenia, alebo akékoľvek iné médiá/nosiče. Patria sem najmä:

1. telefóny,
2. pamäťové karty, USB kľúče,
3. CD,
4. notebooky.

Neobsluhované zariadenia

Používatelia zabezpečia, aby aj neobsluhované zariadenia mali vhodnú ochranu.

Politika čistého stola a čistej obrazovky

V rámci organizácie je zavedená politika čistého stola, pokiaľ ide o dokumenty a prenosné médiá, a politika čistej obrazovky, pokiaľ ide o prostriedky spracúvania informácií.

## Premiestňovanie technických prostriedkov IKT

Každý používateľ, ktorému je pridelený akýkoľvek prenosný prostriedok IKT je zodpovedný za jeho stratu alebo poškodenie. Za žiadnych okolností ho nesmie zveriť tretej osobe.

Akýkoľvek prenosný prostriedok IKT nesmie obsahovať dôverné informácie v nezašifrovanej podobe, pričom šifrovací kľúč alebo iné citlivé parametre týkajúce sa šifrovania tiež nesmú byť uložené v nechránenej (nešifrovanej) forme v pamäti alebo v bezprostrednej blízkosti zariadenia.

Používateľ môže prenosný prostriedok IKT pripájať do informačného systému organizácie len prostredníctvom jedného z predinštalovaných a schválených spôsobov. Nie je povolené pripájať prenosný prostriedok IKT súčasne viacerými spôsobmi naraz.

# Riešenie bezpečnostných incidentov

|  |
| --- |
| **Oblasť riešenia bezpečnostných incidentov je bližšie popísaná v dokumente „Smernica o monitoringu a riešení kybernetických bezpečnostných incidentov”.** |

# Riadenie informačných aktív

Každé informačné aktívum môže byť posúdené a ohodnotené z hľadiska významu a citlivosti. Cieľom takéhoto hodnotenia je určiť priority potrebné pre definíciu požiadaviek na ochranu a obnovu tohto aktíva (či procesu, v ktorého rámci je toto aktívum spracovávané) v prípade vzniku mimoriadnej udalosti.

Zodpovednosť za informačné aktíva je rozdelená do niekoľkých oblastí:

1. manažér kybernetickej a informačnej bezpečnosti schvaľuje aktíva IS ich vlastníkom a vedie príslušnú evidenciu aktív,
2. identifikáciu, klasifikáciu a ohodnotenie informačných aktív vo svojej pôsobnosti vykonáva ich vlastník,
3. administrátor IS nastavuje bezpečnostné mechanizmy pre ochranu informačných aktív podľa kategórií stanovených ich hodnotou.

Pri stanovení hodnoty informačného aktíva posudzuje vlastník najmä výšku možnej škody, ktorá môže vzniknúť poškodením alebo stratou informačného aktíva, napríklad:

1. náklady na znovu obstaranie alebo opravu poškodeného informačného aktíva,
2. straty alebo iné škody spôsobené nedostupnosťou informačného aktíva,
3. škody spôsobené ohrozením prostredia – požiar, únik nebezpečných látok a pod.,
4. penále a pokuty za porušenie záväzných predpisov alebo zmlúv.

Vlastníkom informačného aktív je v jednotlivých odboroch určený spravidla vedúci zamestnanec, ktorého zodpovednosť za spravované informačné aktíva vyplýva z popisu činnosti prislúchajúcej jeho funkcii a z popisu činnosti odboru.

Vlastník informačného aktíva vykonáva:

1. posúdenie a stanovenie hodnoty, priority informačných aktív,
2. klasifikáciu informačných aktív vo svojej kompetencii,
3. stanovenie požiadaviek na ochranu informačných aktív vo svojej kompetencii (lehoty pre zachovanie kontinuity prevádzky, požiadavky na zálohovanie a pod.),
4. správu informačných aktív vo svojej kompetencii (pravidlá údržby a kontroly, správnosť a úplnosť označovania, pohyb informačných aktív).

## Klasifikácia informácií a kategorizácia sietí a informačných systémov

**Klasifikácia informačných aktív spracovávaných v prostredí IKT**

Klasifikačné stupne opisujú citlivosť informácií, údajov alebo ďalších nimi spojených informačných aktív z pohľadu narušenia dôvernosti, integrity a dostupnosti a odrážajú dôležitosť alebo hodnotu týchto aktív.

Z hľadiska dôvernosti klasifikuje organizácia informačné aktíva do nasledujúcich klasifikačných stupňov

1. verejné:

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

1. interné:

Informačné aktíva, ktoré sú používané a prístupné pre všetkých používateľov bez ohľadu na ich pracovnú rolu; na sprístupnenie týchto aktív tretím stranám je potrebné schválenie zo strany vlastníka informácie.

1. chránené:

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

1. prísne chránené:

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

Klasifikácia informácií sa vzťahuje na všetky informácie v akejkoľvek podobe a na akomkoľvek nosiči (médiu).

Všetky informácie, ktoré sú bez označenia, alebo ich označenie nie je jednoznačné, sa považujú za interné informácie.

Organizácia z hľadiska integrity klasifikuje informačné aktíva ako:

1. nízka:

Zahŕňa informačné aktíva, ktorých chyba alebo nepresnosť výrazne neohrozí poskytovanú základnú službu.

1. stredná:

Zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť organizácie a ktorých chyba alebo nepresnosť môže spôsobiť dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká.

1. vysoká:

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

Organizácia z hľadiska dostupnosti klasifikuje informačné aktíva ako:

1. nízka:

Zahŕňa informačné aktíva, ktorých výpadok výrazne neohrozí poskytovanú základnú službu alebo pre ktoré existujú alternatívne postupy.

1. stredná:

Zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť organizácie a ktorých zlyhanie môže mať dopad na kontinuitu poskytovanej základnej služby, strategickú oblasť, trhové a operačné riziká.

1. vysoká:

Zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť organizácie a ktorých zlyhanie bezprostredne ohrozuje poskytovanú základnú službu, s ňou spojené aktivity a dobrú povesť.

**Kategorizácia sietí a informačných systémov**

Organizácia kategorizuje siete a informačné systémy do nasledujúcich kategórií:

Kategória I. zahŕňa informačné aktíva v pôsobnosti organizácie,

1. ktorých ohrozenie nemá žiadny negatívny dopad na poskytovanú základnú službu,
2. ktoré sú klasifikované z hľadiska dôvernosti ako verejné alebo v odôvodnených prípadoch interné,
3. ktoré sú klasifikované z hľadiska dostupnosti klasifikačným stupňom nízka alebo v odôvodnených prípadoch stredná,
4. ktoré sú klasifikované z hľadiska integrity klasifikačným stupňom nízka alebo v odôvodnených prípadoch stredná,
5. pri ktorých nie je predpoklad potreby identifikácie zodpovednosti za aktivity používateľov, alebo pri ktorých nie je potrebné vykonávať kontrolnú činnosť.

Kategória II. zahŕňa informačné aktíva v pôsobnosti organizácie,

1. ktorých ohrozenie môže spôsobiť kybernetický bezpečnostný incident I. stupňa,
2. ktoré sú klasifikované z hľadiska dôvernosti ako interné, chránené alebo v odôvodnených prípadoch prísne chránené,
3. ktoré sú klasifikované z hľadiska dostupnosti klasifikačným stupňom stredná alebo v odôvodnených prípadoch vysoká,
4. ktoré sú klasifikované z hľadiska integrity klasifikačným stupňom stredná alebo v odôvodnených prípadoch vysoká,
5. pri ktorých je potrebné identifikovať zodpovednosť za kritické aktivity, najmä však aktivity privilegovaných používateľov,
6. pri ktorých je potrebné vykonávať kontrolnú činnosť,
7. tvoriace základné registre a/alebo referenčné registre,
8. zabezpečujúce vytváranie a vedenie agend, ktoré nepatria do I. bezpečnostnej kategórie,
9. ktoré sú agendové informačné systémy,
10. ktorými sú špecializované portály alebo
11. ktoré sú nevyhnutné na rozhodovanie orgánu štátnej moci.

Kategória III. zahŕňa informačné aktíva v pôsobnosti organizácie,

1. ktorých ohrozenie môže spôsobiť kybernetický bezpečnostný incident II. a III. stupňa,
2. ktoré sú klasifikované z hľadiska dôvernosti ako prísne chránené,
3. ktoré sú klasifikované z hľadiska dostupnosti klasifikačným stupňom vysoká,
4. ktoré sú klasifikované z hľadiska integrity klasifikačným stupňom vysoká,
5. pri ktorých je potrebné auditovať aktivity všetkých používateľov,
6. prostredníctvom ktorých sa poskytuje základná služba a ktorých výpadok alebo poškodenie spôsobí poškodenie alebo znemožnenie poskytovania základnej služby,
7. ktoré sú označené ako utajované skutočnosti alebo ako tajomstvo podľa osobitných predpisov,
8. ktoré sú nevyhnutné a potrebné z hľadiska plnenia úloh týkajúcich sa obrany a bezpečnosti štátu alebo
9. ktorým je ústredný portál verejnej správy.

## Registratúrny poriadok a registratúrny plán

Správu a archiváciu dokumentov je upravená príslušným interným predpisom organizácie.

# Pravidlá správania a dobrej praxe

## Práca na diaľku a používanie mobilných zariadení

Používateľ preberá úplnú zodpovednosť za bezpečnosť prideleného mobilného prostriedku a informácií v ňom uchovávaných.

Používateľ je povinný využívať pridelené mobilné prostriedky výhradne na plnenie pracovných povinností.

Používateľ je povinný pripojiť mobilný prostriedok do siete organizácie za účelom aktualizácie antivírusového softvéru a inštalácie bezpečnostných aktualizácií. Povinnosť sa týka všetkých používateľov prenosných počítačov (notebook) a ostatných mobilných prostriedkov, ktorých softvér sa pravidelne aktualizuje pri pripojení do siete organizácie.

Používateľ je povinný, zúčastňovať sa predpísaných školení a poučení o používaní mobilných prostriedkov.

### Práca na diaľku

Prácou na diaľku sa označuje každá forma práce z prostredia mimo kancelárie vrátane netradičných pracovných prostredí, ktoré sa zvyčajne nazývajú aj ako „komunikácia cez siete“, „flexibilné pracovné miesto“, „vzdialené pracovisko“ a „virtuálne pracovisko“.

Pri zabezpečovaní výkonu práce na diaľku organizácia berie do úvahy nasledujúce skutočnosti:

* existujúcu fyzickú bezpečnosť pracoviska pre prácu na diaľku, berúc do úvahy fyzickú bezpečnosť budovy a miestne prostredie,
* navrhované prostredie pre prácu na diaľku,
* požiadavky na bezpečnosť komunikácie, majúc na zreteli potrebu diaľkového prístupu k interným systémom organizácie, citlivosť informácií, ku ktorým bude možný prístup, prenos komunikačnou linkou a citlivosť interného systému,
* poskytnutie prístupu na virtuálnu pracovnú plochu, čo zabráni spracúvaniu a ukladaniu informácií na zariadeniach v súkromnom vlastníctve,
* hrozbu neautorizovaného prístupu k informáciám alebo prostriedkom inými ľuďmi (používajúc dané ubytovanie), napr. rodinou a priateľmi,
* použitie domácich sietí a požiadavky alebo obmedzenia týkajúce sa konfigurácie bezdrôtových sieťových služieb,
* politiky a postupy na predchádzanie nezrovnalostiam týkajúcim sa práv duševného vlastníctva vyvinutého na vybavení v súkromnom vlastníctve,
* prístup k zariadeniu v súkromnom vlastníctve (kontrolu bezpečnosti stroja,
* dohody o licenciách na softvér, ktoré hovoria o tom, že organizácia je zodpovedná za zabezpečenie licencií na softvér na pracovných staniciach v súkromnom vlastníctve zamestnancov, zmluvných partnerov alebo používateľov v pozícií tretích strán;
* ochranu pred malvérom a požiadavky na firewall.

Organizácia pri výkone práce na diaľku zabezpečuje nasledovné opatrenia týkajúce sa:

* poskytnutie vhodného vybavenia na pracovné aktivity vykonávané na diaľku, ak nie je povolené používanie zariadení v súkromnom vlastníctve,
* definovanie povolenej práce, pracovného času, klasifikáciu informácií, ktoré môžu byť držané, a interných systémov a služieb, ku ktorým má pracovník na diaľku povolený prístup,
* zabezpečenie vhodného komunikačného vybavenia vrátane metód bezpečného vzdialeného prístupu,
* fyzickú bezpečnosť,
* pravidlá a návody na prístup rodiny a návštevníkov k zariadeniu a informáciám,
* poskytnutie hardvérovej a softvérovej podpory a údržby,
* zabezpečenie poistenia,
* postupy zálohovania a kontinuity činnosti,
* audit a monitorovanie bezpečnosti,
* odvolanie oprávnení a prístupových práv a návrat zariadenia po ukončení práce na diaľku.

### Fyzická bezpečnosť mobilných zariadení

Používateľ je povinný prenášať mobilné prostriedky v ochrannom obale (taška, puzdro a pod.) tak, aby zabránil prípadnému fyzickému poškodeniu prostriedku.

Ak pri odchode zamestnanca z pracoviska počas pracovnej doby alebo po skončení pracovnej doby zostáva mobilný prostriedok v priestoroch organizácie, je používateľ povinný použiť bezpečnostné mechanizmy alebo odložiť mobilný prostriedok do chránených priestorov (uzamykateľná skriňa, trezor a pod.), aby tak zabránil prípadnému neautorizovanému použitiu alebo odcudzeniu.

Mobilné prostriedky prenášané mimo organizácie musia byť pod neustálym dohľadom používateľa.

Používateľ nesmie ponechávať mobilné prostriedky v dopravnom prostriedku (automobil, prostriedky hromadnej prepravy a pod.) bez dohľadu.

Pri používaní mobilného prostriedku mimo organizácie (práca v teréne a pod.), v priestoroch tretích strán (pracovné stretnutia a pod.) nesmie používateľ ponechať mobilný prostriedok bez dohľadu (prestávka na občerstvenie, obed a pod.).

Pri používaní mobilného prostriedku mimo organizácie, je používateľ povinný chrániť ho vhodným spôsobom pred odcudzením (napr. zabezpečenie dohľadu, bezpečné uloženie na hoteli v trezore a pod.).

Pri používaní mobilného prostriedku na pracovné účely doma, musí používateľ zabezpečiť príslušné opatrenia, aby zamedzil poškodeniu, odcudzeniu, alebo neautorizovanému použitiu.

### Bezpečnosť informácií

Súbory, s ktorými musí používateľ nevyhnutne pracovať mimo organizácie, môžu byť uložené lokálne v mobilnom prostriedku.

Súbory obsahujúce klasifikované informácie, uložené lokálne v mobilnom prostriedku, musia byť uložené v zašifrovanej podobe, s využitím autorizovaných šifrovacích prostriedkov (napr. softvér pre šifrovanie diskov).

Používateľ je zodpovedný za pravidelné zálohovanie informácií uložených lokálne v mobilnom prostriedku.

Pri práci s mobilným prostriedkom vo verejných priestoroch je používateľ povinný zabezpečiť diskrétnosť informácií výberom vhodného prostredia alebo spôsobu použitia mobilného prostriedku. Medzi vhodné bezpečnostné opatrenia patria najmä:

* používanie dôveryhodných prístupových bodov do internetu,
* nastavenie automatického zablokovania mobilného prostriedku pri nepoužívaní,
* používanie pravidelne aktualizovaného antimalvér softvéru,
* ochrana mobilných prostriedkov pred neoprávneným používaním a tiež pred stratou a krádežou,
* ochrana informácií uložených na mobilných prostriedkov šifrovaním.

## Riadenie personálnej bezpečnosti

Všetky prostriedky IKT organizácie slúžia výhradne pre výkon pracovných činností a procesov spojených s aktivitami organizácie. Ich využívanie je teda obmedzené len na pracovnú činnosť a je zakázané používať akýkoľvek prostriedok IKT na iné ako pracovné účely.

Používatelia môžu používať výhradne programové vybavenie (SW) schválené pre použitie v organizácii s platnou licenciou.

Nie je povolené používať/inštalovať akýkoľvek iný SW na HW organizácie a to ani v prípade, že má používateľ súkromne zakúpenú licenciu.

### Opatrenia pred nástupom do zamestnania

Organizácia vykonáva verifikačnú previerku personálneho pozadia všetkých uchádzačov o zamestnanie v súlade s príslušnými právnymi predpismi a etikou, ako aj s prihliadnutím na budúcu pracovnú pozíciu, ktorú bude uchádzač zastávať.

Verifikačná previerka sa zameriava najmä na nasledovné oblasti:

* dostupnosť uspokojivých referencií o povahových vlastnostiach,
* overenie životopisu uchádzača,
* potvrdenie uvedenej akademickej a profesijnej kvalifikácie,
* nezávislé overenie identity,
* detailnejšie previerky ako napr. výpis z registra trestov.

Ak je osoba prijímaná na určitú bezpečnostnú rolu, organizácia by sa mala presvedčiť, že kandidát:

* má potrebné kompetencie na výkon bezpečnostnej roly,
* môže byť poverený pracovať na takejto role.

### Opatrenia počas zamestnania

Všetci zamestnanci a zmluvní partneri by mali:

* 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 role,
* podriadiť sa pracovnej náplni a podmienkam zamestnania,
* udržiavať si dostatočné zručnosti a kvalifikáciu,
* byť vybavení anonymným informačným kanálom na informovanie o porušení bezpečnostnej politiky a postupov.

### 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 by mal zabezpečiť korektné a férové zaobchádzanie so zamestnancami, ktorí sú podozriví zo spôsobenia narušenia bezpečnosti. Formálny disciplinárny proces by mal zabezpečiť 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.

### Opatrenia pri ukončení a zmene zamestnania

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 by malo zahŕňať aj pokračujúce bezpečnostné požiadavky, príp. zodpovednosť obsiahnutú v rámci dohody o zachovaní dôvernosti.

Zodpovednosť a povinnosti platné po ukončení pracovného pomeru by mali byť jasne definované v pracovnej zmluve.

### Program budovania 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 Bezpečnostnou politikou kybernetickej bezpečnosti a tiež preškolení v ostatných bezpečnostných pravidlách a súvisiacich smerniciach platných pre používateľov IKT.

Manažér kybernetickej a informačnej bezpečnosti je povinný zaužívanou formou oznámiť všetkým používateľom zmeny v Bezpečnostnej politike kybernetickej bezpečnosti, pričom každý používateľ je povinný následne bez zbytočného odkladu oboznámiť sa s aktualizovaným znením Bezpečnostnej politiky kybernetickej bezpečnosti a súvisiacimi predpismi.

### Povinnosti používateľov

Medzi povinnosti všetkých používateľov patrí najmä:

1. dodržiavanie všetkých pravidiel informačnej bezpečnosti definovaných Bezpečnostnou politikou kybernetickej bezpečnosti a prípadne aj inými súvisiacimi predpismi,
2. nakladať s osobnými údajmi v zmysle GDPR,
3. zachovávať mlčanlivosť o všetkých chránených skutočnostiach,
4. bezpečne nakladať s IKT a ochraňovať informácie vo svojej pôsobnosti,
5. zodpovedne používať pridelené prístupy v súlade s touto bezpečnostnou politikou a inými súvisiacimi predpismi,
6. neinštalovať akýkoľvek software na hociktorý prostriedok IKT bez schválenia príslušného vedúceho zamestnanca alebo manažéra kybernetickej a informačnej bezpečnosti. Platí to aj pre legálne zakúpený software alebo software zadarmo (napr. freeware),
7. povinnosť zachovávať všetky heslá a prihlasovacie kódy v tajnosti,
8. 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).

Porušenie vymenovaných povinností zamestnancom je závažným porušením pracovnej disciplíny so všetkými dôsledkami v zmysle Zákonníka práce.

Dohoda o mlčanlivosti a dodržiavaní pravidiel Bezpečnostnej politiky kybernetickej 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“.

Každé porušenie Bezpečnostnej politiky kybernetickej 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 BP. Ak bude v dôsledku porušenie povinnosti uvedených v tejto Bezpečnostnej politike 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 BP. 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 Bezpečnostnej politiky kybernetickej bezpečnosti môže príslušný vedúci zamestnanec alebo manažér kybernetickej a informačnej bezpečnosti nariadiť obmedzenie alebo zablokovanie prístupových oprávnení do doby vyriešenia bezpečnostného incidentu a zjednania nápravy.

## Pravidlá komunikácie

### Pravidlá pre prácu s elektronickou poštou

Pre prácu s elektronickou poštou môže používateľ používať len aplikácie schválené pre použitie v prostredí IKT. Tieto aplikácie je používateľ povinný využívať výhradne na plnenie pracovných povinností.

Používateľ je povinný počas prítomnosti na pracovisku priebežne kontrolovať svoju došlú poštu a udržiavať objem schránky elektronickej pošty v pridelených limitoch. Tie určuje prevádzka IKT na základe technických a prevádzkových možností infraštruktúry IKT. Veľkosť správ elektronickej pošty vrátane príloh je obmedzená prostriedkami IKT.

Pokiaľ je to možné, používateľovi je odporúčané používať digitálny podpis na zabezpečenie integrity správ.

E-mailová komunikácia je monitorovaná (kontrola odosielateľa, adresáta, typ príloh a pod.).

Obsah e-mailových správ a príloh je kontrolovaný na výskyt škodlivého kódu (napr. vírusy) resp. škodlivého obsahu (napr. spam, phishing a pod.). V prípade zistenia výskytu škodlivého kódu resp. škodlivého obsahu sú e-mailové správy podľa typu zistenia automaticky odstraňované resp. modifikované (napr. odstránenie vírusu) a doplnené o príslušnú informáciu. Obsah e-mailových správ a príloh nie je monitorovaný ani kontrolovaný iným ako vyššie uvedeným spôsobom.

Používateľ nesmie otvárať ani preposielať podozrivé e-maily (neznámy alebo podozrivý odosielateľ, podozrivý predmet, obsah alebo príloha e-mailu a podobne).

Používateľ nesmie spúšťať spustiteľné prílohy (programy, scripty a pod.) nevyžiadanou elektronickou poštou z podozrivých zdrojov alebo s podozrivým obsahom. Používateľ je povinný takúto nevyžiadanú elektronickú poštu poskytnúť na kontrolu manažérovi kybernetickej a informačnej bezpečnosti.

Všetky podozrivé e-maily je používateľ povinný zmazať, prípadne nahlásiť manažérovi kybernetickej a informačnej bezpečnosti.

Používateľ nesmie odpovedať na nevyžiadané podozrivé alebo reklamné e-maily (spamy) a využívať služby ponúkané takouto formou.

Používateľ nesmie používať elektronickú poštu na posielanie alebo uchovávanie informácií s obsahom protizákonným, diskriminačným, ohrozujúcim alebo poškodzujúcim dobré meno organizácie, ani na šírenie poplašných správ.

Používateľ nesmie používať elektronickú poštu na hromadné šírenie správ (napr. posielanie správ všetkým používateľom a pod.). V odôvodnených prípadoch, pri hromadnom rozposielaní mailov, je na zadanie adresy prijímateľa, odosielateľ povinný použiť namiesto kolónky „Komu“ (To), kolónku „Skrytá“ (Bcc).

Pokiaľ to nie je nevyhnutné, používateľ nesmie klikať na odkazy http://… vložené do e-mailov.

Pokiaľ to nie je nevyhnutné, používateľ nesmie používať HTML formát pre e-maily.

Používateľovi je odporúčané nepoužívať Tablo na čítanie (Preview Panel) v aplikácii pre prácu s elektronickou poštou.

Pokiaľ to nie je nevyhnutné, používateľ nesmie zviditeľňovať svoju e-mailovú adresu na web stránkach, newsgroup zoznamoch, diskusných fórach a podobne.

V rámci práce s elektronickou poštou sa v organizácii využíva aj elektronická schránka. Podľa zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov ide o elektronické úložisko, v ktorom sa uchovávajú elektronické správy a notifikácie. Elektronická schránka umožňuje komunikovať občanom a podnikateľským subjektom s verejnou správou elektronicky. Pre prácu s elektronickou schránkou platia rovnaké pravidlá ako pre prácu s elektronickou poštou.

### Pravidlá pre prácu s internetom

Pre prácu s internetom smie používateľ používať len aplikácie schválené pre použitie v prostredí IKT.

Používateľ sa nesmie do internetu pripájať cez iné ako schválené pripojenia.

Používanie internetu je zabezpečené prostriedkami IKT, ktoré presadzujú bezpečnostné, prevádzkové a legislatívne požiadavky (obmedzenie veľkosti a typu prenášaných údajov, obmedzenie prístupu na stránky propagujúce pornografiu, rasizmus, ponúkajúce nelegálny softvér a pod.).

Používanie internetu je monitorované a zaznamenávané (napr. kategórie navštevovaných stránok, použité protokoly, dátum a čas prístupu na internet, použitá šírka pásma a pod.).

Používateľ nesmie vedome navštevovať web stránky, ktoré:

* porušujú autorské práva (sprístupňujú nelegálny softvér, hudbu, video a podobne),
* sú v rozpore s dobrými mravmi (pornografia, rasizmus, sektárstvo a pod.),
* poskytujú nelegálne aplikácie a nástroje (generátory vírusov, hackerské utility, password crackers, a pod.),
* obsahujú nebezpečný obsah (adware, spyware, nebezpečné skripty, vírusy a pod.).

Používateľ nesmie v prostredí IKT používať P2P aplikácie (napr. Torrent a pod.).

Používateľ nesmie vykonávať alebo pokúšať sa o prieniky do iných systémov v internete.

Používateľ nesmie prostredníctvom internetu vystupovať v mene organizácie do právne relevantných vzťahov s tretími stranami bez predchádzajúceho súhlasu priameho nadriadeného.

Používateľ nesmie ukladať dôverné informácie o organizácii do formulárov vystavených v internete vrátane prípadov, pre ktoré je zadanie informácií podmienkou pre získanie prístupu k informáciám, alebo službám dostupným cez internet.

# Riadenie dodávateľských vzťahov

## Riadenie dodávateľských služieb

Nasledujúce princípy riadenia dodávateľských vzťahov a služieb musia byť uplatňované minimálne vo vzťahu s dodávateľmi a tretími stranami, ktorých činnosti priamo súvisia alebo môžu mať vplyv na dostupnosť, dôvernosť a integritu prevádzky sietí a informačných systémov organizácie ako prevádzkovateľa základnej služby. Za identifikáciu dodávateľov priamo podporujúcich prevádzku základnej služby zodpovedá manažér kybernetickej a informačnej bezpečnosti.

S dodávateľmi je uzatvorená zmluva podľa zákona o kybernetickej bezpečnosti. Povinnosť uzatvoriť zmluvu v zmysle tohto bodu neplatí, ak je dodávateľ prevádzkovateľom základnej služby, poskytovateľom digitálnej služby alebo ak je riziko vo vzťahu k činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov organizácie prostredníctvom tohto dodávateľa nízke.

V rámci riadenia dodávateľských služieb a akvizície informačných systémov sa pred uzatvorením zmluvy s treťou stranou analyzujú riziká dodávateľských služieb, akvizície, vývoja alebo údržby informačných systémov spôsobom popísaným v dokumente „Metodika analýzy rizík a analýzy dopadov“ . Táto analýza sa vykonáva ešte pred uzatvorením zmluvy s dodávateľom.

Za riadenie procesu posudzovania rizík spojených s dodávateľom a vyhotovenie analýzy bezpečnostných rizík zodpovedá manažér kybernetickej a informačnej bezpečnosti. Dodávateľ alebo tretia strana musí prehlásiť znalosť a schopnosť implementovať požadované bezpečnostné opatrenia, ktoré musia byť uvedené aj v zadaní a dokumentácii navrhovaného riešenia a zároveň musia byť súčasťou akceptačného testovania dodávaného riešenia, prípadne priamo vychádzajú z platnej legislatívy.Pre riadenie vzťahov s tretími stranami:

* požiadavky na nový informačný systém alebo na rozšírenie / zmenu existujúceho systému musia obsahovať aj požiadavky na bezpečnostné opatrenia,
* musí byť zaistené, že bezpečnostné opatrenia definované v zmluve s dodávateľmi sú implementované a dodržiavané.

Monitorovanie poskytovaných služieb musí zabezpečiť preukázateľné dodržiavanie dohodnutých bezpečnostných opatrení. Rozsah monitorovania a proces monitorovania musí preukázať:

* výkonnostné a kvalitatívne parametre poskytovaných služieb,
* poskytovanie informácií o bezpečnostných incidentoch a spôsob správy bezpečnostných incidentov,
* spôsob zaznamenávania záznamov pre audit, procesy vyhodnocovania a kontroly záznamov pre audit, bezpečnostných udalostí a prevádzkových problémov,
* spôsob riešenia iných problémov.

Zmeny v poskytovaní služieb, vrátane udržovania a zlepšovania existujúcich bezpečnostných politík, postupov a bezpečnostných opatrení sa riadia s ohľadom na kritickosť systémov a procesov Organizácie, ktoré sú súčasťou opakovaného hodnotenia rizík. Proces riadenia zmien služieb poskytovaných dodávateľmi by mal zohľadniť nutné zmeny vykonané zamestnancami Organizácie i nutné zmeny služieb poskytovaných dodávateľmi. Pri všetkých zmenách a aktualizáciách bude uplatňované štandardné zmenové konanie.

## Zmluvy s tretími stranami

Zmluva s treťou stranou obsahuje najmenej:

* obdobie trvania zmluvy,
* ustanovenie záväzku tretej strany dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby a vyjadrenie súhlasu s nimi,
* ustanovenie o povinnosti chrániť všetky informácie poskytnuté prevádzkovateľom základnej služby tretej strane,
* ustanovenie o povinnosti dodržiavať a prijímať bezpečnostné opatrenia treťou stranou, konkrétnu špecifikáciu a rozsah bezpečnostných opatrení, ktoré prijíma tretia strana a vyjadrenie súhlasu s nimi,
* konkrétny rozsah činnosti tretej strany,
* zoznam pracovných rolí tretej strany, ktoré majú mať prístup k informáciám a údajom prevádzkovateľa základnej služby, 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 prevádzkovateľom základnej služby 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 prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti,
* ustanovenia o spôsobe a forme hlásenia ďalších informácií požadovaných prevádzkovateľom základnej služby na plnenie jeho povinností vyplývajúcich zo zákona 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 tretej strany po ukončení zmluvného vzťahu vrátiť, previesť alebo aj zničiť všetky informácie, ku ktorým má tretia strana počas trvania zmluvného vzťahu prístup, prevádzkovateľovi základnej služby,
* záväzok tretej strany po ukončení zmluvného vzťahu udeliť, poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovanej základnej služby na prevádzkovateľa základnej služby; tento záväzok tretej strany stáva v platnosti aj po ukončení zmluvného vzťahu po dobu dohodnutú zmluvnými stranami, ktorá nesmie byť kratšia ako päť rokov po ukončení zmluvného vzťahu.

Zmluva uzatvorená s treťou stranou obsahuje minimálne bezpečnostné opatrenia pre oblasť:

* technických zraniteľností systémov a zariadení,
* riadenia bezpečnosti sietí a informačných systémov,
* riadenia prístupov,
* riešenia kybernetických bezpečnostných incidentov,
* monitorovania, testovania bezpečnosti a bezpečnostných auditov.

Organizácia vedie evidenciu všetkých uzatvorených zmlúv s tretími stranami a táto evidencia je súčasťou bezpečnostnej dokumentácie.

# Riadenie vývoja a údržby v oblasti informačno-komunikačných technológií

## Vývoj a testovanie informačných systémov

Organizácia má vytvorené, zdokumentované, udržiavané a zavedené princípy bezpečného vývoja systémov pre všetky činnosti spojené so zavedením informačných systémov. Bezpečný vývoj je požiadavka na vytvorenie bezpečnej služby, architektúry, softvéru a systému.

Princípy bezpečného vývoja a vytvorené postupy vývoja sa v organizácii pravidelne preskúmavajú, aby sa zabezpečilo efektívne zohľadnenie vyžadovaných noriem bezpečnosti vnútri procesu vývoja. Organizácia pravidelne preskúmava ich aktuálnosť, aby ostali použiteľné na technológie a riešenia, ktoré už boli implementované.

Vytvorené princípy bezpečného vývoja systémov sa v rámci organizácie používajú všade, kde je to možné, na systémy vyvíjané externými zdrojmi prostredníctvom zmlúv a inými väzbami medzi organizáciou a dodávateľom, u ktorého si organizácia objednáva dodávku.

Vývoj softvéru prostredníctvom outsourcingu (externých zdrojov) je plne pod dohľadom organizácie, aby boli aktivity vývoja systému, ktorý sa vykonáva formou outsourcingu monitorované.

Testovanie bezpečnostných funkcií sa v organizácii vykonáva počas vývoja.

Pre nový informačný systém, aktualizáciu a novú verziu systému sú v organizácii vytvorené programy akceptačného testovania s príslušnými kritériami.

## Postupy údržby informačných systémov

Údržba informačných systémov sa v organizácii rozdeľuje podľa dôvodu na:

* preventívnu údržbu,
* korektívnu údržbu,
* adaptívnu údržbu,
* zdokonaľovaciu údržbu,
* funkčnú údržbu.

Preventívna údržba

Jedná sa o periodickú údržbu zameranú na zvyšovanie spoľahlivosti a bezpečnosti informačného systému. Cieľom je predchádzať vzniku problémov.

Korektívna údržba

Korektívna údržba slúži na odstraňovanie chýb v informačnom systéme. Vykonáva sa keď chovanie systému nezodpovedá špecifikácii (zlé výstupy, pád systému a pod.).

Adaptívna údržba

Adaptívna údržba slúži na modifikácie nutné na prispôsobenie systému okolitému prostrediu. Vykonáva sa keď informačný systém vyžaduje úpravu v dôsledku zmien vyvolaných okolím (zmena pripojeného systému, formátu vstupov a pod.).

Zdokonaľovacia údržba

Cieľom zdokonaľovacej údržby je zaisťovanie a zvyšovanie kvality služieb poskytovaných systémom. Uplatňuje sa pri prispôsobovaní informačného systému novým užívateľským požiadavkám na kvalitu (t. j. rýchlosť, spoľahlivosť, užívateľské pohodlie, efektívnosť a pod.) a vykonáva sa napr. v prípade zvyšovania záťaže systému, z dôvodu nárastu počtu užívateľov a pod.

Funkčná údržba

Vykonáva sa, keď je potrebné systém doplniť o nové funkcie, alebo je potrebné niektoré existujúce funkcie zmeniť.

### Údržba funkčných požiadaviek

Má za cieľ udržiavať funkčné požiadavky na systém stále aktuálne.

* Korektívna údržba – odstraňuje chyby obsiahnuté vo funkčných požiadavkách.
* Adaptívna údržba – úpravy požiadaviek, vynútené z dôvodu zmeny v okolí informačného systému.
* Zdokonaľovacia údržba – úpravy požiadaviek na kvalitu.
* Funkčná údržba – úpravy alebo rozvoj funkčných požiadaviek na základe zmenových požiadaviek.

### Údržba aplikácií

Pokrýva údržbu aplikácií, databázových štruktúr a sprievodnej dokumentácie. Obvykle je vyvolaná údržbou funkčných požiadaviek na informačný systém.

* Korektívna údržba - vyžadujú ju aplikácie, ktoré nezodpovedajú požiadavkám.
* Adaptívna údržba - vykonáva sa pri zmenám v dátovej alebo technickej infraštruktúre, ktorú dané aplikácie používajú.
* Zdokonaľovacia údržba - úpravy na splnenie vyšších požiadaviek na kvalitu.
* Funkčná údržba - úprava aplikácie na prispôsobenie novým, alebo zmeneným funkčným požiadavkám.

### Údržba infraštruktúry

Táto údržba sa týka akejkoľvek údržby nutnej k zaisteniu súladu funkcie technickej infraštruktúry s požiadavkami na ňu kladenými.

* Preventívna údržba - periodické nastavovanie a testovanie všetkých prvkov zariadení. Jej cieľom je prevencia chýb a porúch, alebo ich včasné odhalenie.
* Korektívna údržba - samotné opravovanie chýb a porúch v infraštruktúre.
* Adaptívna údržba - potreba upraviť niektoré časti infraštruktúry s ohľadom na zmeny v iných častiach tejto infraštruktúry.
* Zdokonaľovacia údržba - úpravy na splnenie vyšších požiadaviek na kvalitu infraštruktúry.
* Funkčná údržba - rozširovaniu funkcií technickej infraštruktúry.

## Riadenie technických zraniteľností a manažment záplat

Administrátor IS zabezpečuje automatickú inštaláciu bezpečnostných záplat na koncových zariadeniach (desktopoch).

### Vymedzenie rozsahu a spôsobu zabezpečenia ochrany pred škodlivým softvérom

Informačný systém je chránený pred škodlivým kódom a počítačovými vírusmi zodpovedajúcou ochranou (antivírusová a antispamová ochrana) aplikovanou na všetky relevantné komponenty IKT vrátane koncových pracovných staníc.

Všetky koncové pracovné stanice sú pravidelne kontrolované prostriedkami antivírusovej a antispamovej ochrany. Používateľ nesmie túto ochranu akýmkoľvek spôsobom blokovať alebo vypínať.

### Požiadavky na udržanie aktuálnosti systému ochrany pred škodlivým softvérom

Administrátor IS zodpovedá za pravidelnú aktualizáciu a inštaláciu bezpečnostných záplat všetkých IS podľa servisnej zmluvy.

### Riadenie technických zraniteľností

Organizácia vykonáva primerané a včasné kroky s cieľom reagovať na identifikáciu potenciálnej technickej zraniteľnosti. Vysoko rizikové systémy ošetruje organizácia prednostne.

Organizácia má definované a zavedené roly a zodpovednosti spojené s riadením technickej zraniteľnosti vrátane monitorovania zraniteľnosti, ohodnotenia rizík výskytu zraniteľnosti, aplikácie záplat, sledovania aktív a akejkoľvek požadovanej koordinačnej zodpovednosti.

Informačné zdroje, ktoré sa použijú na identifikáciu príslušnej technickej zraniteľnosti a na udržiavanie povedomia o ich prítomnosti by mali byt identifikované pre softvér a iné technológie. Tieto informačné zdroje by mali byť aktualizované na základe zmien v inventárnom zozname alebo v prípade, že sa nájdu nové alebo užitočné zdroje.

Organizácia má určený časový harmonogram s cieľom vhodne reagovať na oznámenia potenciálnej technickej zraniteľnosti.

Po identifikácii potenciálnej technickej zraniteľnosti organizácia identifikuje príslušné riziká, ako aj kroky, ktoré je potrebné vykonať (napr. aplikácia záplat na zraniteľné systémy). V prípade, že je záplata dostupná, riziká spojené s jej inštaláciou by mali byť ohodnotené. Ohodnotením záplat pred inštaláciou sa zaručí ich efektivita, ako aj to, že s ich použitím nie sú spojené nijaké vedľajšie efekty, ktoré nie je možné tolerovať. Zároveň by sa mali zvážiť opatrenia, akými napr. sú:

* vypnutie služieb a funkcií spojených so zraniteľnosťou,
* osvojenie si a pridanie opatrení na riadenie prístupu (napr. firewall na hraniciach siete),
* zvýšené monitorovanie s cieľom detegovať útoky a predchádzať im,
* zvýšenie povedomia o zraniteľnosti.

Organizácia uchováva auditný záznam o všetkých vykonaných procedúrach. Organizácia tiež pravidelne monitoruje zhodnocuje proces riadenia technickej zraniteľnosti s cieľom zabezpečiť hospodárnosť a efektivitu.

Efektívny proces riadenia technickej zraniteľnosti je v súlade s aktivitami riadenia incidentov, aby bolo možné oznamovať údaje o zraniteľnosti funkciám odpovedajúcim na incidenty a vykonávať technické postupy, ak sa objaví incident.

Organizácia definuje postup na označenie situácie, kde bola zraniteľnosť identifikovaná, ale nie je k dispozícii vhodné protiopatrenie. V tejto situácii by organizácia mala vyhodnocovať riziká v súvislosti so zraniteľnosťou a definovať vhodné detektívne a nápravné aktivity.

# Riadenie a prevádzka informačno-komunikačných technológií

|  |
| --- |
| **Oblasť riadenia a prevádzky informačno-komunikačných technológií je bližšie popísaná v dokumente „Smernica o bezpečnej prevádzke IS a sietí”.** |

# Riadenie súladu

## Audit kybernetickej bezpečnosti

Schválením tejto bezpečnostnej politiky organizácia deklaruje, že sa podrobí auditu kybernetickej bezpečnosti v zmysle § 29 zákona o kybernetickej bezpečnosti (ďalej aj „audit“), 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 podľa všeobecne záväzného právneho predpisu, ktorý vydá úrad, 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.

## Spracúvanie osobných údajov a klasifikovaných informácií

Organizácia má zostavenú a implementovanú politika ochrany súkromia a osobných údajov. Zodpovednosť za ochranu osobných údajov, ako aj za zabezpečenie primeraného povedomia o princípoch ochrany údajov by sa riadi platnou legislatívou a právnymi nariadeniami. Na ochranu osobných údajov sú implementované príslušné technické a organizačné opatrenia.

Organizácia má určenú zodpovednú osobu nad vykonávaním dohľadu nad ochranou osobných údajov.

|  |
| --- |
| **Bližší popis spracúvania osobných údajov a klasifikovaných informácií a tiež relevantná interná dokumentácia bude doplnená zo strany organizácie.** |

## Poskytovanie súčinnosti tretím stranám

Organizácia má zavedené postupy, ktoré určujú, kedy a kým majú byť úradné autority (napr. orgány činné v trestnom konaní, regulačné orgány, orgány dohľadu) kontaktované a ako sa majú včas oznamovať zistené incidenty informačnej bezpečnosti (napr. v prípade podozrenia, že sa porušil zákon).

Organizácia udržiava kontakty s orgánmi štátnej a verejnej správy. Tieto kontakty sú užitočné, pretože umožnia predvídať a včas sa pripraviť na budúce zmeny v zákonoch a právnych nariadeniach, ktorých sa musí držať. Kontakty s ďalšími typmi úradných autorít zahŕňajú verejnoprospešné služby, pohotovostné služby a služby pôsobiace v oblasti zdravia a bezpečnosti všeobecne, napr. požiarne zbory (v spojitosti s kontinuitou činnosti), telekomunikační operátori (v spojitosti s prenosovými trasami a dostupnosťou), dodávatelia vody (v spojitosti s chladiacimi zariadeniami).

Organizácia udržiava príslušné kontakty so špecifickými záujmovými skupinami alebo inými fórami bezpečnostných špecialistov a s profesijnými komorami.

Členstvo v špeciálnych záujmových skupinách alebo iných fórach bezpečnostných špecialistov možno považovať za prostriedok, ktorý slúži na:

* zlepšovanie poznatkov a najlepšej praxe a udržiavanie aktuálnych poznatkov z oblasti bezpečnosti,
* zabezpečenie toho, že vedomosti o prostredí informačnej bezpečnosti sú aktuálnej a úplné,
* získavanie včasných varovaní, rád a záplat ošetrujúcich pokusy o útok a výskyt zraniteľnosti,
* získanie prístupu k poradenstvu o informačnej bezpečnosti od špecialistov na túto oblasť,
* získavanie a výmenu informácií o nových technológiách, produktoch, hrozbách alebo o zraniteľnosti,
* získanie potrebných styčných bodov pri riešení incidentov informačnej bezpečnosti.

Organizácia poskytuje plnú súčinnosť najmä nasledujúcim subjektom:

* Národný bezpečnostný úrad,
* Úrad na ochranu osobných údajov,
* orgány činné v trestnom konaní.

# Riadenie kontinuity procesov činností

|  |
| --- |
| **Oblasť riadenia kontinuity procesov činností je bližšie popísaná v dokumente „Politika riadenia kontinuity činností ”.** |

# 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 manažér kybernetickej 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 a informačnej bezpečnosti:

* zákon 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“),
* 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 (ďalej aj „vyhláška NBÚ č. 362/2018 Z. z.“),
* vyhláška Národného bezpečnostného úradu č. 436/2019 Z. z. o audite kybernetickej bezpečnosti a znalostnom štandarde audítora,
* 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.