Odbor riadenia kybernetickej a informačnej bezpečnosti
Verzia 1.1 | kyberbezpecnost@mirri.gov.sk

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Legislatívne požiadavky pre všetky kategórie podľa vyhlášky 179/2020 Z. z.,

ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy

1 Zákonné povinnosti podľa kategórií

Povinnosti jednotlivých kategórií určuje Príloha č.2 k Vyhláške č. 179/2020. Nájdete tam špecifický opis jednotlivých povinností. Tento dokument nenahrádza platnú legislatívu v danej oblasti.

1.1 Povinnosti I. kategórie

1.1.1 Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti

- ☐ **Určenie pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.**
- ☐ **Vypracovanie a implementácia interného riadiaceho aktu, ktorý je pre organizáciu správcu záväzný a obsahuje najmenej:**
  - Určenie povinnosti, zodpovednosti a právomoci pracovníka zodpovedného za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.
  - Základné zásady a opatrenia kybernetickej bezpečnosti a informačnej bezpečnosti, ktoré organizácia správcu má zavedené a riadi sa nimi.

1.1.2 Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti

Kontinuálne riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti:

- ☐ **Vypracovanie analýzy rizík kybernetickej bezpečnosti a informačnej bezpečnosti.**
- ☐ **Návrh a prijatie bezpečnostných opatrení.**
- ☐ **Periodické preskúmavanie rizík.**

1.1.3 Personálna bezpečnosť

- ☐ **Ustanoviť plán rozvoja bezpečnostného povedomia, ktorý obsahuje formu, obsah a rozsah potrebných školení a vykonať bezpečnostné vzdelávanie na zvýšenie bezpečnostného povedomia najmenej každé tri roky.**
- ☐ **Zabezpečenie hodnotenia účinnosti plánu rozvoja bezpečnostného povedomia, vykonávaných školení a ďalších činností spojených s prehlbovaním bezpečnostného povedomia.**
- ☐ **Zamestnávateľ povinnej osoby a tretia strana zabezpečí, že každý zamestnanec a tretia strana sú poučení o povinnosti zachovávať mlčanlivosť o všetkých skutočnostiach, informáciách a osobných údajoch, a to predtým, ako získajú prístup k informačným technológiám verejnej správy. Mlčanlivosť je generálna a trvalá a vzťahuje sa tak na čas výkonu činnosti, ako aj po skončení výkonu činnosti.**
- ☐ **Zabezpečenie oznamovania bezpečnostných incidentov pracovníkovi, ktorý je zodpovedný za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.**
- ☐ **Určenie postupu pri ukončení pracovného pomeru alebo iného obdobného vzťahu zamestnanca a pri ukončení spolupráce s externým pracovníkom alebo treťou stranou, ktorým sa zabezpečí:**
  - vrátenie pridelených zariadení, ktorými sú najmä počítače, pamäťové médiá, čipové karty a navrátenie informačných aktív, ktorými sú najmä programy, dokumenty a údaje,
  - zablokovanie prístupu v zariadeniach pridelených zamestnancovi, ktorými sú najmä počítače, notebooky, pamäťové médiá a ďalšie mobilné elektronické zariadenia,

- zrušenie prístupových práv v informačných systémoch verejnej správy,
- odovzdanie výsledkov práce v súvislosti s informačnými systémami verejnej správy, ktorými sú najmä programy vrátane dokumentácie a vlastné elektronické dokumenty.

☐ **Zabezpečenie zmeny prístupových oprávnení pri zmene postavenia používateľov, administrátorov alebo osôb zastávajúcich bezpečnostné roly.**
☐ **Sankcionovanie porušenia interných riadiacich aktov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti prostredníctvom disciplinárneho procesu organizácie správcu.**

1.1.4 Riadenie prístupov

☐ **Zavedenie pravidiel zakazujúcich zdieľanie používateľských hesiel do informačných technológií verejnej správy.**
☐ **Zavedenie identifikácie používateľa a autentifikácie pri vstupe do informačných technológií verejnej správy.**
☐ **Zavedenie pravidiel na zmenu používateľských hesiel s frekvenciou najmenej jeden rok.**

1.1.5 Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami

☐ **V zmluve s dodávateľmi musí byť určená požiadavka na dodržiavanie všetkých interných riadiacich dokumentov a všeobecne záväzných predpisov týkajúcich sa kybernetickej bezpečnosti a informačnej bezpečnosti. Môže byť uvedený odkaz na zákon, túto vyhlášku alebo na osobitný predpis.**

1.1.6 Bezpečnosť pri prevádzke informačných systémov a sietí

☐ **Na účinnú prevenciu pred stratou dát v organizácii správcu sa zavedie proces na vytváranie záložných kópií dôležitých informácií a softvéru.**
☐ **V organizácii správcu sa vypracuje a dodržiava politika zálohovania, ktorá definuje požiadavky organizácie správcu na zálohovanie vrátane doby uchovávania, testovania záloh, ako aj opatrenia na ochranu záložných médií.**
☐ **Prevádzkové zálohy, kópia archivačnej zálohy a kópie inštalačných médií sú uložené do uzamykateľného priestoru.**

1.1.7 Hodnotenie zraniteľností a bezpečnostné aktualizácie

☐ **Nastavenie automatickej aktualizácie operačného systému a aplikácií.**

1.1.8 Ochrana proti škodlivému kódu

- ☐ **Prijatie adekvátnych opatrení na prevenciu, detekciu škodlivého kódu, ako aj na efektívnu reakciu pri infiltrácie škodlivým kódom.**
- ☐ **V organizácii správcu je zakázané sťahovanie, inštalácia a používanie nelegálneho alebo škodlivého softvéru.**
- ☐ **Prevencia a detekcia škodlivého kódu je pravidelná a zameraná hlavne na:**

- používanie prenosných médií, napríklad USB kľúče, flash disky, CD, DVD,
- škodlivé emailové prílohy a odkazy,
- podozrivé a škodlivé webové stránky a odkazy,
- externú a internú sieťovú komunikáciu v organizácii správcu vrátane webových sídiel,
- prenos súborov z externých sietí.

- ☐ **Vytvorenie procesu alebo postupu na prenos súborov z externých sietí, ktorý zabezpečí kontrolu prenášaných súborov s cieľom detekcie škodlivého kódu.**

1.1.9 Sieťová a komunikačná bezpečnosť

- ☐ **Všetky koncové stanice sú chránené prostredníctvom softvérového personálneho firewallu.**
- ☐ **Na sieťových zariadeniach sa implementujú najmenej tieto bezpečnostné opatrenia:**

- pravidelná aktualizácia firmvéru,
- zmena továrensky nastavených autentifikačných údajov,
- pri bezdrôtových sieťach musí byť nastavené využívanie bezpečného šifrovania a zabezpečenia,
- vypnutie možnosti správy zariadenia na diaľku alebo prijatie iných opatrení zabraňujúcich zneužitiu vzdialeného prístupu.

- ☐ **Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu.**

1.1.10 Akvizícia, vývoj a údržba informačných technológií verejnej správy

- ☐ Obstarávanie alebo vytváranie nových alebo úprava existujúcich informačných technológií verejnej správy sa zadokumentuje a realizuje v súčinnosti s pracovníkom zodpovedným za koordináciu kybernetickej bezpečnosti a informačnej bezpečnosti.

1.1.11 Zaznamenávanie udalostí a monitorovanie

- ☐ Zaznamenávanie úspešných a neúspešných autentifikačných udalostí.

1.1.12 Fyzická bezpečnosť a bezpečnosť prostredia

- ☐ Informačné technológie verejnej správy sa umiestňujú a prevádzkujú takým spôsobom, že sú chránené pred fyzickým prístupom nepovolaných osôb a nepriaznivými prírodnými vplyvmi a vplyvmi prostredia.

1.1.13 Riešenie kybernetických bezpečnostných incidentov

- ☐ **V organizácii správcu sa určí kontaktné miesto a spôsob hlásenia kybernetických bezpečnostných incidentov** podľa:
  - *§ 23 ods. 3 písm. a)*
  - sú zaradení do registra prevádzkovateľov základných služieb podľa osobitného predpisu, nahlasovať spôsobom podľa osobitného predpisu aj kybernetický bezpečnostný incident na ktorý sa nevzťahuje povinnosť nahlasovania podľa osobitného predpisu; ak nie sú do tohto registra zaradení, nahlasujú takýto kybernetický bezpečnostný incident orgánu vedenia ním určeným spôsobom,
  - ods. 4 zákona

Orgán vedenia vo vzťahu k informačným technológiám verejnej správy

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

1.1.14 Kryptografické opatrenia

- ☐ Webové sídlo správcu musí byť prístupné prostredníctvom zabezpečeného protokolu HTTPS s využitím bezpečnej verzie protokolu TLS

https://www.csirt.gov.sk/oznamenia-a-varovania-803.html?id=181

1.1.15 Kontinuita prevádzky informačných technológií verejnej správy

Nevzťahujú sa žiadne bezpečnostné opatrenia.

1.1.16 Audit a kontrolné činnosti

- ☐ Zabezpečenie výkonu pravidelných auditov kybernetickej bezpečnosti a informačnej bezpečnosti podľa osobitného predpisu.

1.2 Povinnosti II. kategórie

Povinných opatrenia z kategórie I. sú navyše obohatené o nasledujúce povinnosti pre kategóriu II.

1.2.1 Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti

☐ **Vypracovanie a implementácia interného riadiaceho aktu Politika kybernetickej bezpečnosti a informačnej bezpečnosti, ktorý je pre organizáciu správcu záväzný a obsahuje najmenej:**

- určenie povinnosti, zodpovednosti a právomoci manažéra kybernetickej bezpečnosti a informačnej bezpečnosti a všetkých zamestnancov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti,
- základné zásady a opatrenia kybernetickej a informačnej bezpečnosti v štruktúre oblastí definovaných touto vyhláškou.

☐ **Určenie a personálne zabezpečenie roly manažéra kybernetickej bezpečnosti a informačnej bezpečnosti v organizácii správcu zodpovedného za koordináciu a plnenie týchto úloh:**

- vypracovať, udržiavať a aktualizovať Politiku kybernetickej bezpečnosti a informačnej bezpečnosti a ďalšie interné riadiace akty,
- riadiť a zaisťovať kybernetickú a informačnú bezpečnosť podľa všeobecne záväzných právnych predpisov a interných riadiacich aktov,
- metodicky viesť správcov informačných technológií verejnej správy, gestorov informačných technológií verejnej správy, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov,
- v súčinnosti s ostatnými organizačnými útvarmi analyzovať, definovať a monitorovať bezpečnostné hrozby a riziká organizácie,
- navrhovať opatrenia na zamedzenie alebo minimalizáciu rizík a dopadov hrozieb, bezpečnostných udalostí, incidentov, mimoriadnych situácií, monitorovať plnenie a efektivitu týchto opatrení a viesť evidenciu bezpečnostných incidentov,
- koordinovať vypracovanie plánov kontinuity a obnovy činností organizácie správcu,
- predkladať odborné stanoviská, analýzy k procesom, projektom, zmenám a ostatným aktivitám organizácie majúcich vplyv na kybernetickú bezpečnosť a informačnú bezpečnosť organizácie správcu,
- zabezpečiť pravidelné – najmenej raz za dva roky – preskúmanie stavu informačnej bezpečnosti a spolupracovať pri realizácii auditov vykonávaných internými a externými subjektmi,
- zabezpečovať školenia zamestnancov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti,
- spolupracovať s inými orgánmi verejnej moci.

☐ **Vypracovanie a implementácia špecifických interných riadiacich aktov pre vybrané oblasti kybernetickej bezpečnosti a informačnej bezpečnosti v rozsahu a detaile zodpovedajúcom veľkosti a štruktúre organizácie správcu, významu informačných technológií verejnej správy v jeho správe a štruktúre existujúcich interných riadiacich aktov s detailným opisom jednotlivých opatrení a postupov pre tieto oblasti:**

- organizácia kybernetickej bezpečnosti a informačnej bezpečnosti,
- riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
- personálna bezpečnosť,
- riadenie prístupov,
- riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu s tretími stranami,
- bezpečnosť pri prevádzke informačných systémov a sietí,
- hodnotenie zraniteľnosti a bezpečnostné aktualizácie,
- ochrana proti škodlivému kódu,
- sieťová a komunikačná bezpečnosť,

- akvizícia, vývoj a údržba informačných technológií verejnej správy,
- zaznamenávanie udalostí a monitorovanie,
- riadenie kontinuity procesov. fyzická bezpečnosť a bezpečnosť prostredia,
- riešenie kybernetických bezpečnostných incidentov,
- kryptografické opatrenia,
- kontinuita prevádzky informačných technológií verejnej správy,
- audit a kontrolné činnosti.

☐ **Zabezpečenie výkonu pravidelných auditov kybernetickej bezpečnosti a informačnej bezpečnosti podľa osobitného predpisu.**

☐ **Monitorovanie a vyhodnocovanie dodržiavania Politiky kybernetickej bezpečnosti a informačnej bezpečnosti a efektivity jednotlivých opatrení a postupov.**

☐ **Aktualizácia Politiky kybernetickej bezpečnosti a informačnej bezpečnosti najmenej raz za rok.**

1.2.2 Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti

☐ **Identifikácia všetkých významných informačných aktív v organizácii správcu a určenie ich vlastníka, ktorý definuje požiadavky na ich dôvernosť, dostupnosť a integritu.**

☐ **Zaradenie informačných aktív podľa definovaných požiadaviek na ich dôvernosť, dostupnosť a integritu do určených klasifikačných stupňov, pre ktoré sú určené bezpečnostné opatrenia najmenej na ich označovanie, ukladanie, prenos, zverejňovanie a likvidáciu.**

☐ **Klasifikačné stupne pre informačné aktíva ustanovuje osobitný predpis**

☐ **Vypracovanie a implementácia interného riadiaceho aktu na riadenie bezpečnostných rizík, ktorý obsahuje najmenej:**

- zodpovednosť za vykonanie analýzy rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
- proces vykonávania analýzy rizík,
- maticu určenia závažnosti rizika,
- periodicitu vykonávania analýzy rizík,
- spôsob dokumentácie bezpečnostných rizík a prijatých opatrení a postupov na ich zníženie na prijateľnú úroveň v podľa matice určenia závažnosti rizika.

☐ **Vykonávanie analýzy rizík najmenej raz za dva roky.**

1.2.3 Personálna bezpečnosť

☐ **Vypracovanie a pravidelné aktualizovanie dokumentu Bezpečnostné zásady pre koncových používateľov, ktorý obsahuje súhrn povinností a oprávnení v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti pre koncových používateľov, najmä:**

- prideľovanie prístupových práv,
- zásady tvorby a používania hesiel,
- zásady ochrany pred infiltráciou škodlivým kódom,
- zásady bezpečného používania elektronickej pošty,
- zásady bezpečného používania internetu,

- zásady bezpečného používania komunikačných nástrojov a sociálnych sietí,
- zásady používania prenosných zariadení a médií,
- zálohovanie údajov,
- riešenie kybernetických bezpečnostných incidentov,
- ochranu fyzického majetku,
- pohyb v priestoroch organizácie správcu.

☐ **Zavedenie procesu preukázateľného poučenia a oboznámenia nových zamestnancov bezprostredne po nástupe s internými riadiacimi aktmi týkajúcimi sa kybernetickej bezpečnosti a informačnej bezpečnosti.**

☐ **Zavedenie procesu preukázateľného oboznámenia správcov informačných technológií verejnej správy s internými riadiacimi aktmi týkajúcimi sa kybernetickej bezpečnosti a informačnej bezpečnosti.**

☐ **Zavedenie procesu zvyšovania bezpečnostného povedomia zamestnancov s cieľom ich oboznamovania s aktuálnymi bezpečnostnými hrozbami v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti, ako aj opatreniami a postupmi zavedenými v organizácii správcu na ich elimináciu najmenej raz za dva roky.**

☐ **Na prístup k informačným technológiám verejnej správy sa vyžaduje:**
- oboznámenie so spôsobom používania informačných technológií verejnej správy a bezpečnostných mechanizmov informačných technológií verejnej správy v rozsahu svojej pracovnej náplne,
- poučenie na rozoznanie kybernetického bezpečnostného incidentu od bežnej prevádzky a zvládnutie postupu pri kybernetickom bezpečnostnom incidente,
- oboznámenie so zamestnancom, na ktorého je možné sa obracať s otázkami a nejasnosťami pri používaní informačných technológií verejnej správy a bezpečnostných mechanizmov informačných technológií verejnej správy.

1.2.4 Riadenie prístupov

☐ **Vypracovanie a implementácia interného predpisu upravujúceho riadenie prístupu k údajom a funkciám informačných technológií verejnej správy založenom na zásade, že používateľ má prístup len k tým údajom a funkciám, ktoré potrebuje na vykonávanie svojich úloh.**

☐ **Určenie postupu a zodpovednosti v súvislosti s prideľovaním prístupových práv používateľom a ich schvaľovania vlastníkom informačných aktív.**

☐ **Zaznamenávanie zmien v pridelenom prístupe a ich archivácia.**

☐ **Používanie bezpečných postupov identifikácie a autentifikácie jednotlivých používateľov s cieľom minimalizovať možnosť neautorizovaného prístupu.**

☐ **Vytvorenie a presadzovanie politiky a systému správy hesiel, ktorá umožní používateľom najmä:**
- zabezpečiť absolútnu kontrolu nad heslom svojho používateľského účtu,
- presadzovať určenú štruktúru hesla,
- vyžadovať pravidelnú zmenu hesla,
- uchovávať a prenášať používateľské heslá bezpečným spôsobom.

☐ **Zabezpečenie formálneho riadenia a autorizácie prideľovania privilegovaných prístupov do informačných technológií verejnej správy a ich obmedzenie len na nevyhnutné prípady.**

☐ **Preskúmavanie privilegovaných prístupových práv v pravidelných intervaloch najmenej raz za rok.**

☐ **Určenie bezpečnostných zásad na mobilné pripojenie do informačných technológií verejnej správy a na prácu na diaľku.**

☐ **Automatické zaznamenávanie každého prístupu administrátora do informačných technológií verejnej správy a automatické zaznamenávanie prístupu používateľa.**

☐ **Vedenie formalizovanej dokumentácie prístupových práv všetkých používateľov informačných technológií verejnej správy.**

1.2.5 Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami

☐ **Požiadavky v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti sa určujú, odsúhlasujú a formálne zadokumentujú formou zmluvy pre každý dodávateľský vzťah, ktorý si vyžaduje prístup alebo akékoľvek používanie informačných technológií verejnej správy.**

☐ **Zmluvné požiadavky na kybernetickú bezpečnosť a informačnú bezpečnosť obsahujú najmenej záväzok**

- plnenia určených požiadaviek a kritérií pre oblasť kybernetickej bezpečnosti a informačnej bezpečnosti pri dodávke predmetu zmluvy,
- ochrany informácií, ku ktorým je poskytnutý prístup,
- oboznámenia sa a dodržiavania všetkých interných riadiacich aktov týkajúcich sa kybernetickej bezpečnosti a informačnej bezpečnosti a ďalších opatrení a postupov kybernetickej bezpečnosti a informačnej bezpečnosti špecifických na plnenie predmetu zmluvy,
- riadenia a monitorovania prístupov do informačných technológií verejnej správy vrátane spôsobu a mechanizmu,
- možnosti vykonávania kontrolných činností a auditu vrátane rozsahu a spôsobu,
- oznámenia všetkých bezpečnostných rizík, nedostatkov alebo zraniteľností informačných technológií verejnej správy zistených v rámci plnenia predmetu zmluvy, ako aj povinnosť a proces ich ošetrenia,
- spolupráce pri riešení kybernetických bezpečnostných incidentov, najmä zachovania a poskytovania všetkých relevantných informácií, dôkazov a podkladov,
- zachovania úrovne kybernetickej bezpečnosti a informačnej bezpečnosti pri významných zmenách vrátane spôsobu a formy prechodu k inému dodávateľovi.

☐ **Pri využívaní dodávateľských reťazcov sa pred začatím využívania služieb identifikujú možné riziká kybernetickej bezpečnosti a informačnej bezpečnosti a posúdia sa najmä:**

- kritické komponenty a prvky služby,
- možnosti presadzovania a monitorovania bezpečnostných požiadaviek naprieč celým dodávateľským reťazcom,
- možné riziká kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch medzi dodávateľmi a subdodávateľmi,
- ďalšie možné riziká kybernetickej bezpečnosti a informačnej bezpečnosti vyplývajúce zo životného cyklu dodávanej služby a z možnosti ukončenia dodávky služieb alebo prechodu k inému dodávateľovi.

☐ **Pri zmenách služieb poskytovaných treťou stranou sa posudzuje ich vplyv na kybernetickú a informačnú bezpečnosť, a ak je to potrebné, sú navrhnuté a implementované ďalšie opatrenia a postupy kybernetickej bezpečnosti a informačnej bezpečnosti.**

- ☐ **Do zmluvného vzťahu s tretími stranami sa zavedie proces implementácie zmien v oblasti riadenia kybernetickej bezpečnosti a informačnej bezpečnosti v organizácii správcu.**
- ☐ **Pri vývoji aplikácií a systémov realizovaných treťou stranou sa v zmluve určia jasné podmienky týkajúce sa najmä autorských práv, práv duševného vlastníctva, bezpečnostných parametrov, bezpečnostného a funkčného testovania, legislatívnych a regulačných požiadaviek.**

1.2.6 Bezpečnosť pri prevádzke informačných systémov a sietí

- ☐ **Vyhotovenie archivačnej zálohy najmenej v dvoch kópiách.**
- ☐ **Zabezpečenie vykonania testu funkcionality dátového nosiča archivačnej zálohy a prevádzkovej zálohy a pri nefunkčnosti, najmä pri nečitateľnosti alebo chybách pri čítaní, opätovné vytvorenie zálohy na inom dátovom nosiči.**
- ☐ **Zabezpečenie vykonania testu obnovy informačných technológií verejnej správy a údajov z prevádzkovej zálohy najmenej raz za rok.**
- ☐ **Fyzické ukladanie druhej kópie archivačnej zálohy v inom objekte, ako sa nachádzajú technické prostriedky informačných technológií verejnej správy, ktorej údaje sú archivované tak, že je minimalizované riziko poškodenia alebo zničenia dátových nosičov archivačnej zálohy v dôsledku požiaru, záplavy alebo inej živelnej pohromy.**
- ☐ **Prevádzkové postupy informačných technológií verejnej správy sa zadokumentujú, udržiavajú a sú dostupné všetkým používateľom, ktorí ich potrebujú. Za aktuálnosť prevádzkovej dokumentácie zodpovedajú správcovia jednotlivých informačných technológií verejnej správy.**
- ☐ **Všetky zmeny v prevádzkovaných informačných technológiách verejnej správy, ako aj procesoch alebo fyzických objektoch organizácie, ktoré môžu mať vplyv na bezpečnosť informačných aktív, sa zadokumentujú a schvália v procese riadenia zmien.**
- ☐ **Vypracovanie interného riadiaceho aktu riadenia zmien, ktorý obsahuje posúdenie zmien s cieľom identifikácie možných bezpečnostné rizík a návrh adekvátnych opatrení na ich zníženie na akceptovateľnú úroveň.**
- ☐ **Zmeny, pri ktorých ich iniciátor nedokáže jednoznačne určiť alebo vylúčiť možný vplyv na bezpečnosť posudzuje manažér kybernetickej bezpečnosti a informačnej bezpečnosti.**
- ☐ **V rámci formálneho procesu riadenia zmien sa určí aj postup kontrolovanej a autorizovanej implementácie urgentných zmien.**
- ☐ **Na jednotlivých prvkoch informačných technológií verejnej správy sa implementujú implementované bezpečnostné nastavenia podľa odporúčania výrobcov alebo podľa interného riadiaceho aktu. Bezpečnostné nastavenia sa implementujú najmä na týchto prvkoch informačných technológií verejnej správy:**

- operačné systémy,
- virtualizačné prostredia,
- aplikačný softvér,
- pracovné stanice,
- sieťové zariadenia, vrátane bezpečnostných zariadení,

- databázové prostredia.

☐ **Monitorovanie informačných technológií verejnej správy na identifikáciu ich kapacitných požiadaviek a ich trendov tak, že nedôjde ku kritickému výpadku, spomaleniu alebo inej neočakávanej poruche funkčnosti.**

☐ **Vzájomné oddelenie vývojového, testovacieho a prevádzkového prostredia na prevenciu neautorizovaného prístupu alebo zmien v prevádzkovom prostredí, ak je to možné.**

1.2.7 Hodnotenie zraniteľností a bezpečnostné aktualizácie

☐ **V organizácii správcu zaviesť pravidelné zisťovanie a riešenie efektívnych procesov pravidelného zisťovania a riešenia technických zraniteľností systémov a aplikácií pomocou automatizovaných nástrojov.**

☐ **Všetky zistené kritické zraniteľnosti sa odstraňujú v čo najkratšom čase, a to najmä implementáciou opravných softvérových balíkov a aktualizácií riadne vydaných dodávateľom systému alebo aplikácie. Uvedené platí aj na systémy dodávané treťou stranou.**

☐ **Vykonávanie hodnotenie zraniteľností najmenej raz ročne.**

☐ **Vypracovanie a zavedenie procesu riadenia implementácie bezpečnostných aktualizácií a záplat jednotlivých prvkov informačných technológií verejnej správy v organizácii správcu.**

☐ **Vytvorenie a udržiavanie inventárneho zoznamu hardvéru a softvéru jednotlivých prvkov informačných technológií verejnej správy vrátane prvkov v správe tretích strán na identifikáciu relevantných zraniteľností a aktualizácií.**

☐ **Jednotlivé prvky informačných technológií verejnej správy monitorujú zdroje, ktoré poskytujú včasné informácie o nových zraniteľnostiach a bezpečnostných aktualizáciách, ktoré sa vzťahujú na prvky informačných technológií verejnej správy.**

☐ **Primárnymi zdrojmi na identifikáciu nových zraniteľností a bezpečnostných aktualizácií sú:**

- informácie zo systémov a automatizovaných technológií pre aktualizáciu,
- informačný servis výrobcov technológií,
- výstupy z bezpečnostných technológií,
- výsledky penetračných testov,
- oznámenia a varovania orgánov štátnej správy a autorít v oblasti kybernetickej bezpečnosti,
- webové stránky a portály spoločností zameraných na publikovanie zraniteľnosti.

☐ **Výnimky z implementácie bezpečnostných aktualizácií sa schvaľujú a evidujú manažérom kybernetickej bezpečnosti a informačnej bezpečnosti, ktorý určuje bezpečnostné opatrenia na ochranu pred zneužitím zraniteľnosti, na elimináciu ktorej je bezpečnostná aktualizácia vydaná.**

☐ **Súbory s bezpečnostnými aktualizáciami sa získavajú výhradne z dôveryhodného zdroja, primárne priamo od výrobcu. Pri nejasnostiach alebo inom zdroji je potrebné porovnanie kontrolných súčtov jednotlivých súborov bezpečnostných aktualizácií s kontrolnými súčtami súborov výrobcu tak, že nedôjde k poskytnutiu škodlivých aktualizácií.**

☐ **Pred implementáciou aktualizácií sú vykonané opatrenia na možnosť obnovenia pôvodného stavu prvku informačných technológií verejnej správy pred aktualizáciou pri neočakávaných stavoch, chybách alebo odchýlkach od požadovanej funkcionality spôsobených aktualizáciou.**

☐ **Po implementácii aktualizácie sa aktualizuje prvok informačných technológií verejnej správy verifikovaný, najmä jeho správna funkcionalita.**

1.2.8 Ochrana proti škodlivému kódu

☐ **Zavedenie ochrany informačných technológií verejnej správy pred škodlivým kódom najmenej v rozsahu**

- kontroly prichádzajúcej elektronickej pošty na prítomnosť škodlivého kódu a nepovolených typov príloh,
- detekcie prítomnosti škodlivého kódu na všetkých používaných informačných technológiách verejnej správy,
- kontroly súborov prijímaných zo siete internet a odosielaných do siete internet na prítomnosť škodlivého softvéru,
- detekcie prítomnosti škodlivého kódu na všetkých webových sídlach organizácie správcu.

☐ **Zavedenie ochrany pred nevyžiadanou elektronickou poštou.**

1.2.9 Sieťová a komunikačná bezpečnosť

☐ **Prenos informácií akýmkoľvek spôsobom je riadený. Na jednotlivé druhy komunikácie sa určia bezpečnostné opatrenia adekvátne identifikovaným bezpečnostným rizikám.**

☐ **Zabezpečenie ochrany prenášaných informácií najmä pred odpočúvaním, kopírovaním, zmenou, presmerovaním alebo zničením.**

☐ **Správa počítačových sietí je riadená a kontrolovaná.**

☐ **Pri prenose údajov prostredníctvom verejnej siete alebo bezdrôtovej siete sa implementujú opatrenia na zaistenie dôvernosti a integrity informácií, ako aj všeobecné opatrenia na zaistenie požadovanej dostupnosti sieťových služieb.**

☐ **Na všetky sieťové služby sa identifikujú a zadokumentujú bezpečnostné mechanizmy, úroveň služieb a požiadavky na manažment.**

☐ **Sieťové služby, používatelia a jednotlivé prvky informačných technológií verejnej správy musia byť v počítačových sieťach oddelené do skupín (segmenty) podľa požiadaviek na dôvernosť, dostupnosť a integritu a taktiež podľa charakteru poskytovaných služieb. Jednotlivé skupiny (segmenty) musia byť v počítačovej sieti adekvátne oddelené na logickej, kde je to potrebné, tak aj na fyzickej úrovni.**

☐ **Ochrana vonkajšieho a interného prostredia sa realizuje prostredníctvom firewallu s filtrovaním prichádzajúcej a odchádzajúcej sieťovej prevádzky na princípe najnižšieho privilégia.**

☐ **Bezdrôtové siete sa chránia a umiestňujú tak, že je zamedzený priamy prístup k citlivým údajom správcu.**

☐ **Vytvorenie a pravidelné aktualizovanie dokumentácie počítačovej siete obsahujúcej najmä evidenciu všetkých miest prepojenia sietí vrátane prepojení s externými sieťami, topológiu siete a využitie IP rozsahov.**

☐ **Na prenos informácií k tretím stranám sa uzatvára zmluva o prenose informácií s definovaným rozsahom, technickými štandardmi prenosu, bezpečnostnými opatreniami, ako aj právomocami a zodpovednosťami.**

☐ **Všetky formy výmeny elektronických správ sú riadené a pri ich používaní implementované adekvátne bezpečnostné opatrenia zamerané na zaistenie ochrany prenášaných správ, a to najmä proti neautorizovaného prístupu, porušeniu dôvernosti, modifikácii alebo zneužitiu.**

- ☐ **Pri prenose citlivých informácií v zmysle požiadaviek na dôvernosť sa s treťou stranou uzavrie zmluva o mlčanlivosti alebo o utajení ešte pred ich poskytnutím. Toto sa nevzťahuje na všeobecne známe alebo verejne dostupné informácie o organizácii.**
- ☐ **Vzdialený prístup do vnútornej siete organizácie správcu musí podliehať autentifikácii a autorizácii.**

1.2.10 Akvizícia, vývoj a údržba informačných technológií verejnej správy

Pri vytváraní nových alebo úprave existujúcich informačných technológií verejnej správy sa identifikujú a špecifikujú požiadavky na kybernetickú a informačnú bezpečnosť.

- ☐ **Pri identifikácii požiadaviek sa prihliada najmä na požiadavky na dôvernosť, dostupnosť a integritu informačných aktív, všetky známe bezpečnostné hrozby, kybernetické bezpečnostné incidenty, zraniteľnosti, aktuálne politiky a štandardy organizácie správcu, ako aj požiadavky všeobecne záväzných právnych predpisov.**
- ☐ **Informácie prenášané prostredníctvom verejných sietí sa šifrujú alebo iným adekvátnym opatrením chránia najmä pred neoprávneným prístupom, modifikáciou alebo nedostupnosťou.**
- ☐ **Informácie v transakciách informačných technológií verejnej správy alebo medzi informačnými technológiami verejnej správy sú chránené tak, že sa zabráni nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prístupu prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpovediam, a to najmä použitím elektronického podpisu, elektronickej pečate na kvalifikovanej úrovni bezpečnosti, certifikátov, šifrovaním komunikačných kanálov a zabezpečením komunikačných protokolov.**
- ☐ **Všetky zmeny v informačných technológiách verejnej správy a aplikáciách počas ich vývoja sa riadia prostredníctvom formálnych postupov riadenia zmien.**
- ☐ **Vykonávanie bezpečnostného testovania v pravidelných intervaloch podľa možnosti pri všetkých vydaniach alebo verziách počas vývojového cyklu kritických informačných technológií verejnej správy tak, že je možné už v počiatočných fázach identifikovať a odstrániť bezpečnostné nedostatky alebo prípadné chyby v dizajne.**
- ☐ **Súčasťou akceptačného testovania informačných technológií verejnej správy je aj testovanie implementovaných bezpečnostných opatrení najmä bezpečnostne dôležitých prvkov aplikácií, alebo systémov, ako sú autentizačné, autorizačné mechanizmy, prístupové roly a ďalšie opatrenia zaisťujúce požadovanú dôvernosť, dostupnosť a integritu.**
- ☐ **Dáta slúžiace na testovanie sa vyberajú s ohľadom na ich citlivosť pre organizáciu správcu, ako aj na požiadavky regulácie. Ak je to možné, sú citlivé údaje organizácie správcu pred testovaním adekvátne pozmenené tak, že zostanú zachované logické súvislosti, ale ich spätné obnovenie nie je možné. Osobné údaje je možné použiť pri testovaní len vo výnimočných prípadoch po schválení osobou zodpovednou za ochranu osobných údajov.**

1.2.11 Zaznamenávanie udalostí a monitorovanie

- ☐ **Zaznamenávanie, uchovávanie a pravidelné kontrolovanie všetkých významných udalostí informačných technológií verejnej správy.**

☐ **Pre každý prvok informačných technológií verejnej správy sa vyšpecifikujú a zadokumentujú udalosti, ktoré musia byť zaznamenávané, a jednotlivé prvky informačných technológií verejnej správy musia byť podľa tejto špecifikácie nakonfigurované.**

☐ **Podľa typu systému alebo zariadenia sa zaznamenávajú do log súborov najmenej tieto udalosti:**

- úspešné a neúspešné autorizačné udalosti,
- úspešné a neúspešné privilegované operácie (vykonávané pod privilegovanými účtami),
- úspešné a neúspešné prístupy k log súborom,
- úspešné a neúspešné prístupy k systémovým zdrojom,
- vytváranie, úprava a mazanie používateľských účtov, skupinových účtov a objektov vrátane súborov, adresárov a používateľských účtov,
- zmeny v prístupových oprávneniach,
- aktivácia a deaktivácia bezpečnostných mechanizmov,
- spustenie a zastavenie procesov,
- konfiguračné zmeny systému špecificky zmeny bezpečnostných nastavení a politík,
- spustenie, vypnutie, reštartovanie systému alebo aplikácie, chyby a výnimky,
- významné aktivity v sieťovej komunikácii,
- požiadavka na autentizačné služby vrátane označenia požadujúcej entity,
- IP adresy pridelené prostredníctvom služby DHCP.

☐ **Jednotlivé záznamy v log súboroch obsahujú najmenej tieto informácie o každej zaznamenanej udalosti, ak sú k dispozícii:**

- čas a dátum udalosti,
- identifikácia používateľa,
- identifikácia zariadenia,
- informácia týkajúca sa udalosti,
- indikácia úspešnosti, alebo zlyhania operácie,
- pri sieťových službách zdrojová IP adresa, cieľová IP adresa, protokol, zdrojový port, cieľový port.

☐ **Záznamy udalostí sa uchovávajú najmenej šesť mesiacov a adekvátne sa chránia pred zničením alebo modifikáciou.**

☐ **Kontrolu zaznamenaných udalostí, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sú povinní vykonávať správcovia jednotlivých prvkov informačných technológií verejnej správy, ak to nie je možné, použitím automatizovaných nástrojov najmenej na dennej báze.**

☐ **Bezpečnostne relevantné udalosti sa analyzujú bezodkladne s cieľom určiť, či ide o kybernetický bezpečnostný incident.**

☐ **Na zachovanie správnosti, presnosti a možnosti spätného dohľadania je čas na všetkých relevantných prvkoch informačných technológií verejnej správy synchronizovaný prostredníctvom presného časového zdroja.**

1.2.12 Fyzická bezpečnosť a bezpečnosť prostredia

☐ **Umiestnenie informačných technológií verejnej správy v zabezpečenom priestore tak, že ich najdôležitejšie komponenty sú chránené pred nepriaznivými prírodnými vplyvmi a vplyvmi prostredia, možnými dôsledkami havárií technickej infraštruktúry a fyzickým prístupom nepovolaných osôb. Zabezpečeným priestorom je najmä serverovňa.**

☐ **Oddelenie zabezpečených priestorov od ostatných priestorov fyzickými prostriedkami stenami a zábranami.**

☐ **Prístup do zabezpečeného priestoru môže byť povolený len osobám, ktoré tento prístup nevyhnutne potrebujú na výkon svojich pracovných činností. Prístup k serverovým a sieťovým komponentom je umožnený len oprávneným osobám.**

☐ **Vypracovanie a implementovanie interného riadiaceho aktu, ktorý upravuje prácu v zabezpečených priestoroch, ako aj pravidlá**

- údržby, uchovávania a evidencie technických komponentov informačných technológií verejnej správy a zariadení informačných technológií verejnej správy,
- používania zariadení informačných technológií verejnej správy na iné účely, než na aké sú pôvodne určené,
- používania zariadení informačných technológií verejnej správy mimo určených priestorov,
- vymazávania, vyraďovania a likvidovania zariadení informačných technológií verejnej správy a všetkých typov relevantných záloh,
- prenosu technických komponentov informačných technológií verejnej správy alebo zariadení informačných technológií verejnej správy mimo priestorov orgánu riadenia,
- narábania s elektronickými dokumentmi, dokumentáciou systému, pamäťovými médiami, vstupnými a výstupnými údajmi informačných technológií verejnej správy tak, že sa zabráni ich neoprávnenému zverejneniu, odstráneniu, poškodeniu alebo modifikácii.

☐ **Prvky informačných technológií verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečujú opatreniami na ochranu pred výpadkom zdroja elektrickej energie.**

1.2.13 Riešenie kybernetických bezpečnostných incidentov

☐ **Interný riadiaci akt určí spôsob hlásenia kybernetických bezpečnostných incidentov podľa § 23 ods. 3 písm. a) a ods. 4 zákona, bezpečnostne relevantné udalosti, zistené zraniteľnosti, alebo bezpečnostné slabé miesta informačných technológií verejnej správy, ktoré sú zistené pri ich používaní alebo správe.**

☐ **V organizácii správcu je na včasné prijatie preventívnych a nápravných opatrení vypracovaný a presadzovaný interný riadiaci akt na riešenie kybernetických bezpečnostných incidentov, ktorý obsahuje povinnosť, postup pri hlásení, spôsob riešenia a evidencie kybernetických bezpečnostných incidentov.**

☐ **Interný riadiaci akt podľa písmena b) obsahuje aktuálne kontaktné údaje správcov jednotlivých komponentov informačných technológií verejnej správy, zamestnancov tretích strán zodpovedných za správu alebo podporu informačných technológií verejnej správy potrebných pri riešení kybernetických bezpečnostných incidentov, ako aj kontaktné údaje na príslušnú jednotku CSIRT/CERT.**

☐ **S interným riadiacim aktom podľa písmena b), najmä povinnosťou ohlasovať kybernetické bezpečnostné incidenty, sa primeraným a preukázateľným spôsobom oboznámia všetci používatelia informačných technológií verejnej správy vrátane správcov jednotlivých komponentov, ako aj zamestnanci tretích strán, ktorí vykonávajú správu alebo podporu informačných technológií verejnej správy.**

☐ **Na ohlasovanie kybernetických bezpečnostných incidentov a odhalených zraniteľností v prevádzkovaných informačných technológiách verejnej správy sa vytvára kontaktné miesto.**

☐ **Každá nahlásená bezpečnostne relevantná udalosť, zistená zraniteľnosť alebo bezpečnostná slabina informačných technológií verejnej správy sa odborne posudzuje na určenie, či ide o kybernetický bezpečnostný incident, bez zbytočného odkladu.**

- ☐ **Proces odborného posúdenia a analýzy oznámení podľa písmena f) realizuje Manažér kybernetickej bezpečnosti a informačnej bezpečnosti v spolupráci so správcami jednotlivých komponentov a s vlastníkom/gestorom informačných technológií verejnej správy alebo príslušnou jednotkou CSIRT/CERT.**
- ☐ **Jednotlivé aktivity pri riešení bezpečnostných incidentov sa dokumentujú v evidencii kybernetických bezpečnostných incidentov.**
- ☐ **Na identifikáciu, zber, získavanie a uchovávanie dôkazov pri riešení bezpečnostných incidentov sú určené postupy a princípy, ktoré zaručia možnosť použitia dôkazu v sporových konaniach podľa platnej legislatívy.**
- ☐ **Poznatky získané z procesu riešenia bezpečnostného incidentu, najmä z analýzy a spôsobu vyriešenia, sa premietajú do zlepšenia prevencie najmä na zníženie pravdepodobnosti a následkov budúcich incidentov, ako aj na zlepšenie detekcie alebo spôsobu riešenia obdobných bezpečnostných incidentov.**

1.2.14 Kryptografické opatrenia

- ☐ **Pri informačných technológiách verejnej správy s vysokou požiadavkou na integritu sa zabezpečuje autenticita a integrita súborov s použitím kryptografických prostriedkov, ktorým je najmä elektronický podpis.**
- ☐ **Pri informačných technológiách verejnej správy s vysokou požiadavkou na dôvernosť musí byť na zabezpečenie dôvernosti použité šifrovanie, a to najmä:**

- elektronických dokumentov,
- dát na prenosných zariadeniach, ktoré sú vynášané mimo priestory organizácie správcu,
- emailovej komunikácie prostredníctvom PGP alebo S/MIME,
- komunikačných kanálov na výmenu nešifrovaných dát,
- centrálnych úložísk,
- záloh.

- ☐ **Na zabezpečenie správneho a efektívneho používania kryptografických prostriedkov a šifrovania sa vytvára a implementuje interný riadiaci akt, ktorý obsahuje najmä:**

- princípy ochrany informačných aktív s využitím kryptografických prostriedkov,
- definovanie požadovanej úrovne ochrany a štandardy šifrovania,
- roly a zodpovednosti jednotlivých subjektov pri používaní šifrovania,
- riadenie šifrovacích kľúčov.

- ☐ **Každé použitie kryptografického prostriedku v informačných technológiách verejnej správy sa zadokumentuje v dokumentácii k informačným technológiám verejnej správy, najmenej na úrovni využívaného algoritmu a verzie.**
- ☐ **Správca pravidelne prehodnocuje využívané kryptografické prostriedky a overuje, či nedošlo k zverejneniu zraniteľností s nimi súvisiacich.**

1.2.15 Kontinuita prevádzky informačných technológií verejnej správy

- ☐ **Na zachovanie kontinuity prevádzky vykonáva analýza rizík a posúdenie vplyvov na dostupnosť jednotlivých informačných technológií verejnej správy a služieb, ktoré zabezpečujú.**
- ☐ **Na informačné technológie verejnej správy s vysokou požiadavkou na dostupnosť sa vypracuje plán**

kontinuity prevádzky, ktorý zabezpečí včasnú a adekvátnu reakciu pri mimoriadnej udalosti alebo núdzovej situácie s cieľom minimalizácie rizika prerušenia prevádzky informačných technológií verejnej správy a čo najrýchlejšej obnovy, ak dôjde k prerušeniu prevádzky informačných technológií verejnej správy.

☐ **Plán kontinuity prevádzky obsahuje najmä:**

- roly a zodpovednosti v procese zabezpečenia kontinuity prevádzky,
- možné vplyvy na prevádzku informačných technológií verejnej správy,
- časový rámec obnovy,
- identifikáciu zdrojov potrebných na obnovu prevádzky,
- identifikáciu zamestnancov potrebných na obnovu prevádzky,
- identifikáciu dát a systémov potrebných na obnovu prevádzky (potrebné procesy zálohovania a obnovy, potrebný personál a vybavenie),
- identifikáciu priestorov potrebných na obnovu prevádzky,
- stanovenie spôsobu komunikácie a náhradnej komunikácie (spôsob kontaktovania personálu, dodávateľov, používateľov),
- identifikáciu vybavenia potrebného na obnovu prevádzky (procesy obnovy alebo výmeny kľúčových zariadení, alternatívne zdroje, vzájomná pomoc),
- spotrebný materiál potrebný na obnovu prevádzky (procesy výmeny zásob a kľúčových dodávok, zabezpečenie núdzových súčastí),
- konkrétne havarijné procedúry slúžiace na obnovu prevádzky.

☐ **Funkčnosť a aktuálnosť plánu kontinuity sa overuje raz ročne.**

1.2.16 Audit a kontrolné činnosti

☐ **Vypracovanie programu posúdenia bezpečnosti na definované informačné technológie verejnej správy, hodnotenie zraniteľností a penetračné testy.**

☐ **Na výkon posúdenia sa vypracuje plán, ktorý obsahuje ciele posúdenia, referenčné dokumenty, dátumy a miesta vykonania posúdenia, organizačné útvary, ktoré sú predmetom posúdenia, roly a zodpovednosti.**

☐ **Dodržiavanie politík, štandardov, postupov a ostatných opatrení určených v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti sa preveruje a identifikuje sa ich možný nesúlad.**

☐ **Ak je identifikovaný nesúlad s opatreniami kybernetickej bezpečnosti a informačnej bezpečnosti, prijmú sa opatrenia na jeho odstránenie. Ak je zistená nízka efektivita alebo neúčinnosť opatrení, prehodnotia a upravia sa tieto opatrenia tak, že je bezpečnostné riziko znížené na prijateľnú úroveň.**

1.3 Povinnosti III. kategórie

Keďže III. kategória je najvyššia, povinnosti pre ňu sú prirodzene najkomplexnejšie. Okrem povinností z nižších kategórií obsahujú navyše nasledujúce bezpečnostné opatrenia.

1.3.1 Organizácia kybernetickej bezpečnosti a informačnej bezpečnosti

☐ **Vytvorenie bezpečnostného výboru s rozsahom povinností a právomocí určených štatútom.**
☐ **Bezpečnostný výbor pri výkone svojej činnosti najmä:**

- riadi stratégie v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti,
- riadi bezpečnostné riziká v rozsahu celej organizácie, akceptuje bezpečnostné riziká, ktoré sa týkajú viac ako jednej organizačnej jednotky organizácie správcu,
- schvaľuje a rozhoduje o implementácii významných bezpečnostných opatrení a postupov,
- schvaľuje odporúčania, návrhy strategických a koncepčných materiálov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti, predkladaných manažérom kybernetickej bezpečnosti a informačnej bezpečnosti,
- predkladá štatutárnemu orgánu na schválenie návrh zodpovednosti za implementáciu a uplatňovanie jednotlivých opatrení a postupov kybernetickej bezpečnosti a informačnej bezpečnosti v organizácii.

☐ **Bezpečnostný výbor sa skladá najmenej z:**

- štatutára správcu, jeho zástupcu alebo ním poverenej osoby,
- manažéra kybernetickej bezpečnosti a informačnej bezpečnosti,
- vedúceho zamestnanca organizačného útvaru zodpovedného za správu informačno-komunikačnej infraštruktúry,
- vedúceho zamestnanca organizačného útvaru zodpovedného za právne a legislatívne služby,
- zodpovednej osoby za ochranu osobných údajov.

Minimálne zloženie bezpečnostného výboru možno doplniť o ďalšie osoby.

☐ **Vytvorenie pozície manažéra kybernetickej bezpečnosti a informačnej bezpečnosti v organizácii správcu mimo organizačného útvaru zodpovedného za správu a prevádzku informačných technológií verejnej správy.**

☐ **Manažér kybernetickej bezpečnosti a informačnej bezpečnosti pri výkone svojej činnosti najmä:**

- navrhuje stratégie v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti,
- informuje bezpečnostný výbor alebo štatutárny orgán správcu o stave informačnej bezpečnosti v organizácii správcu najmenej raz za rok,
- bezodkladne informuje bezpečnostný výbor alebo štatutárny orgánu správcu o závažných bezpečnostných rizikách, kybernetických bezpečnostných incidentoch a významných bezpečnostných udalostiach,
- zabezpečuje nezávislé preskúmanie stavu informačnej bezpečnosti a spoluprácu pri realizácii auditov vykonávaných internými a externými subjektmi.

☐ **Zabezpečenie kontinuálneho vzdelávania manažéra kybernetickej bezpečnosti a informačnej bezpečnosti.**

☐ **Uplatňovanie princípu oddelenia právomocí a zodpovedností v celej organizačnej štruktúre organizácie správcu tak, že rovnaká osoba nie je zodpovedná za vykonávanie a zároveň aj schvaľovanie alebo kontrolu bezpečnostne relevantných aktivít a činností.**

☐ **Zabezpečenie preskúmania a identifikácie bezpečnostných rizík v počiatočných fázach procesu riadenia projektov v organizácii správcu a určenie adekvátnych opatrení na zníženie každého identifikovaného rizika na prijateľnú úroveň. Definovanie osoby zodpovednej za kybernetickú a informačnú bezpečnosť v projektovom tíme.**

- ☐ **Zabezpečenie vypracovania bezpečnostného projektu informačného systému verejnej správy.**

1.3.2 Riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti

- ☐ **Vytvorenie a udržiavanie zoznamu informačných aktív každého organizačného útvaru organizácie správcu, ktorý je zároveň ich vlastníkom a ktorý určí požiadavky na dôvernosť, dostupnosť a integritu každého informačného aktíva v jeho vlastníctve.**
- ☐ **Vykonávanie analýzy rizík a vyhodnocovanie súladu implementovaných opatrení s touto vyhláškou najmenej raz ročne.**

1.3.3 Personálna bezpečnosť

- ☐ **Vytvorenie evidencie informačných technológií verejnej správy s priradením konkrétnych správcov, ktorí sú zodpovední za implementáciu a prevádzku bezpečnostných opatrení a postupov.**
- ☐ **Systematické zvyšovanie bezpečnostného povedomia tak, že pokrýva všetky oblasti ustanovené touto vyhláškou, zákonom a osobitnými predpismi7) a najnovšími poznatkami v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti v rozsahu pracovného zaradenia najmenej raz ročne.**

1.3.4 Riadenie prístupov

- ☐ **Implementácia centrálnej správy identít (IDM).**
- ☐ **Preskúmanie prístupových opatrení v spolupráci s vlastníkom najmenej raz za rok.**
- ☐ **Vypracovanie a pravidelná aktualizácia zoznamu privilegovaných prístupových oprávnení a ich preskúmavanie každých šesť mesiacov.**
- ☐ **Implementácia, vynucovanie prístupových rolí v informačných technológiách verejnej správy.**
- ☐ **Zamedzenie možnosti zmeny log záznamov prístupu každého používateľa vrátane administrátora do informačných technológií verejnej správy, zamedzenie možnosti vymazania týchto záznamov a uchovávanie týchto záznamov šesť mesiacov.**
- ☐ **Používanie silných autentizačných metód na overenie identity používateľov, ako je viacfaktorová autentizácia pri informačných technológiách verejnej správy, ktoré obsahujú prísne chránené informačné aktíva v zmysle klasifikácie informačných aktív.**

1.3.5 Riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami

- ☐ **Pre informačné technológie verejnej správy, ktoré spracúvajú kritické informačné aktíva v zmysle požiadaviek na ich dôvernosť, dostupnosť a integritu, sa implementuje technológia pre riadenie privilegovaných prístupov a zaznamenávanie aktivít správcov.**
- ☐ **Interný predpis ustanovujúci zásady kybernetickej bezpečnosti a informačnej bezpečnosti pre dodávateľov a**

tretie strany obsahuje najmenej bezpečnostné požiadavky:

- pri riadení vzťahov s dodávateľmi,
- pri ošetrení kybernetickej bezpečnosti a informačnej bezpečnosti v zmluvách s dodávateľmi,
- dodávateľských reťazcov informačných technológií verejnej správy,
- monitorovania a preskúmavania dodávateľských služieb,
- riadenia zmien v službách dodávateľa,
- na prístupové práva a účty,
- na fyzickú bezpečnosť,
- na ochranu a zálohovanie dát,
- na mobilné prostriedky a vzdialený prístup.

☐ **Vytvorenie a využívanie procesu pravidelného monitorovania a preskúmavania kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahu s dodávateľmi.**

1.3.6 Bezpečnosť pri prevádzke informačných systémov a sietí - Zhodná s kategóriou II

☐ **Vyhotovenie archivačnej zálohy najmenej v dvoch kópiách.**

☐ **Zabezpečenie vykonania testu funkcionality dátového nosiča archivačnej zálohy a prevádzkovej zálohy a pri nefunkčnosti, najmä pri nečitateľnosti alebo chybách pri čítaní, opätovné vytvorenie zálohy na inom dátovom nosiči.**

☐ **Zabezpečenie vykonania testu obnovy informačných technológií verejnej správy a údajov z prevádzkovej zálohy najmenej raz za rok.**

☐ **Fyzické ukladanie druhej kópie archivačnej zálohy v inom objekte, ako sa nachádzajú technické prostriedky informačných technológií verejnej správy, ktorej údaje sú archivované tak, že je minimalizované riziko poškodenia alebo zničenia dátových nosičov archivačnej zálohy v dôsledku požiaru, záplavy alebo inej živelnej pohromy.**

☐ **Prevádzkové postupy informačných technológií verejnej správy sa zadokumentujú, udržiavajú a sú dostupné všetkým používateľom, ktorí ich potrebujú. Za aktuálnosť prevádzkovej dokumentácie zodpovedajú správcovia jednotlivých informačných technológií verejnej správy.**

☐ **Všetky zmeny v prevádzkovaných informačných technológiách verejnej správy, ako aj procesoch alebo fyzických objektoch organizácie, ktoré môžu mať vplyv na bezpečnosť informačných aktív, sa zadokumentujú a schvália v procese riadenia zmien.**

☐ **Vypracovanie interného riadiaceho aktu riadenia zmien, ktorý obsahuje posúdenie zmien s cieľom identifikácie možných bezpečnostné rizík a návrh adekvátnych opatrení na ich zníženie na akceptovateľnú úroveň.**

☐ **Zmeny, pri ktorých ich iniciátor nedokáže jednoznačne určiť alebo vylúčiť možný vplyv na bezpečnosť posudzuje manažér kybernetickej bezpečnosti a informačnej bezpečnosti.**

☐ **V rámci formálneho procesu riadenia zmien sa určí aj postup kontrolovanej a autorizovanej implementácie urgentných zmien.**

☐ **Na jednotlivých prvkoch informačných technológií verejnej správy sa implementujú implementované bezpečnostné nastavenia podľa odporúčania výrobcov alebo podľa interného riadiaceho aktu. Bezpečnostné nastavenia sa implementujú najmä na týchto prvkoch informačných technológií verejnej správy:**

- operačné systémy,
- virtualizačné prostredia,
- aplikačný softvér,
- pracovné stanice,
- sieťové zariadenia, vrátane bezpečnostných zariadení,
- databázové prostredia.

☐ **Monitorovanie informačných technológií verejnej správy na identifikáciu ich kapacitných požiadaviek a ich trendov tak, že nedôjde ku kritickému výpadku, spomaleniu alebo inej neočakávanej poruche funkčnosti.**

☐ **Vzájomné oddelenie vývojového, testovacieho a prevádzkového prostredia na prevenciu neautorizovaného prístupu alebo zmien v prevádzkovom prostredí, ak je to možné.**

1.3.7 Hodnotenie zraniteľností a bezpečnostné aktualizácie

☐ **Preskúmavanie a odstraňovanie zraniteľností sa vykoná najmenej každých šesť mesiacov.**

☐ **Bezpečnostné a ostatné aktualizácie sa implementuje najmä prostredníctvom automatizovaného nástroja.**

1.3.8 Ochrana proti škodlivému kódu

☐ **Implementácia centralizovaného systému riešenia ochrany pred škodlivým kódom s pravidelným monitorovaním jeho hlásení v organizácii správcu.**

☐ **Detekcia inštalácie nelegálneho, alebo škodlivého softvéru sa vykonáva prostredníctvom automatizovaných nástrojov.**

☐ **Vypracovanie postupov obnovy a odstránenia infiltrácie škodlivým kódom na efektívne zvládanie infiltrácie škodlivým kódom.**

1.3.9 Sieťová a komunikačná bezpečnosť

☐ **V organizácii správcu sa implementuje technológia detekcie a prevencie prieniku IPS najmenej na perimetri siete umiestnenej pred chránenú časť siete.**

☐ **Na všetkých serveroch podporujúcich základné služby informačných technológií verejnej správy správcu sa implementujú sondy detekcie a prevencie prieniku technológia HIPS.**

☐ **Všetky verejne dostupné a kritické webové aplikácie sa chránia webovým aplikačným firewallom.**

1.3.10 Akvizícia, vývoj a údržba informačných technológií verejnej správy – Zhodná s kategóriou II

Pri vytváraní nových alebo úprave existujúcich informačných technológií verejnej správy sa identifikujú a špecifikujú požiadavky na kybernetickú a informačnú bezpečnosť.

☐ **Pri identifikácii požiadaviek sa prihliada najmä na požiadavky na dôvernosť, dostupnosť a integritu**

informačných aktív, všetky známe bezpečnostné hrozby, kybernetické bezpečnostné incidenty, zraniteľnosti, aktuálne politiky a štandardy organizácie správcu, ako aj požiadavky všeobecne záväzných právnych predpisov.

- ☐ **Informácie prenášané prostredníctvom verejných sietí sa šifrujú alebo iným adekvátnym opatrením chránia najmä pred neoprávneným prístupom, modifikáciou alebo nedostupnosťou.**
- ☐ **Informácie v transakciách informačných technológií verejnej správy alebo medzi informačnými technológiami verejnej správy sú chránené tak, že sa zabráni nekompletným prenosom, nesprávnemu smerovaniu, neautorizovaným úpravám správ, neautorizovanému prístupu prezradeniu, neautorizovanému duplikovaniu správ alebo neautorizovaným odpovediam, a to najmä použitím elektronického podpisu, elektronickej pečate na kvalifikovanej úrovni bezpečnosti, certifikátov, šifrovaním komunikačných kanálov a zabezpečením komunikačných protokolov.**
- ☐ **Všetky zmeny v informačných technológiách verejnej správy a aplikáciách počas ich vývoja sa riadia prostredníctvom formálnych postupov riadenia zmien.**
- ☐ **Vykonávanie bezpečnostného testovania v pravidelných intervaloch podľa možnosti pri všetkých vydaniach alebo verziách počas vývojového cyklu kritických informačných technológií verejnej správy tak, že je možné už v počiatočných fázach identifikovať a odstrániť bezpečnostné nedostatky alebo prípadné chyby v dizajne.**
- ☐ **Súčasťou akceptačného testovania informačných technológií verejnej správy je aj testovanie implementovaných bezpečnostných opatrení najmä bezpečnostne dôležitých prvkov aplikácií, alebo systémov, ako sú autentizačné, autorizačné mechanizmy, prístupové roly a ďalšie opatrenia zaisťujúce požadovanú dôvernosť, dostupnosť a integritu.**
- ☐ **Dáta slúžiace na testovanie sa vyberajú s ohľadom na ich citlivosť pre organizáciu správcu, ako aj na požiadavky regulácie. Ak je to možné, sú citlivé údaje organizácie správcu pred testovaním adekvátne pozmenené tak, že zostanú zachované logické súvislosti, ale ich spätné obnovenie nie je možné. Osobné údaje je možné použiť pri testovaní len vo výnimočných prípadoch po schválení osobou zodpovednou za ochranu osobných údajov.**

1.3.11 Zaznamenávanie udalostí a monitorovanie

- ☐ **Správca vypracuje a zavedie do praxe interný riadiaci akt na zaznamenávanie udalostí a monitorovanie bezpečnosti informačných technológií verejnej správy.**
- ☐ **Záznamy udalostí sa uchovávajú aj mimo konkrétneho prvku informačných technológií verejnej správy, ktoré ich vytvára tak, že sa vylúči ich odstránenie alebo modifikácia.**
- ☐ **Kontrola a vyhodnocovanie zaznamenaných udalostí sa vykonáva automatizovaným spôsobom prostredníctvom nástrojov, ktoré umožňujú generovať okamžité výstrahy a oznámenia pri bezpečnostne významných udalostiach.**
- ☐ **Výstrahy z monitorovacích nástrojov, ako aj výstrahy generované ostatnými bezpečnostnými technológiami sa preverujú bezodkladne, kritické výstrahy okamžite po ich doručení.**
- ☐ **Bezpečnostný dohľad podľa písmen c) a d) sa vykonáva v režime 24 hodín denne sedem dní v týždni.**
- ☐ **Systémy určené na vytváranie záznamov o udalostiach, ako aj samotné tieto súbory sa zabezpečujú pred neoprávnenými zásahmi a neautorizovaným prístupom, najmä pred zmenami a zničením.**
- ☐ **Kapacita systémov uchovávajúcich záznamy musí byť adekvátna tak, že nedochádza k nežiaducemu**

prepisovaniu týchto záznamov alebo znefunkčneniu systému logovania.

1.3.12 Fyzická bezpečnosť a bezpečnosť prostredia

- ☐ **Podporná infraštruktúra informačných technológií verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečuje ochranou pred výpadkom zdroja elektrickej energie pomocou záložného generátora.**
- ☐ **Pre informačné technológie verejnej správy s požiadavkou na vysokú dostupnosť sa zabezpečujú záložné kapacity zabezpečujúce funkčnosť alebo náhradu týchto informačných technológií verejnej správy, ktoré sú umiestnené v sekundárnom zabezpečenom priestore, dostatočne vzdialenom od zabezpečeného priestoru.**
- ☐ **Ďalšie opatrenia fyzickej bezpečnosti a bezpečnosti prostredia sa prijímajú podľa osobitného predpisu.**

1.3.13 Riešenie kybernetických bezpečnostných incidentov

- ☐ **Interný riadiaci akt na riešenie kybernetických bezpečnostných incidentov okrem uvedených náležitostí podľa Kategórie II obsahuje povinnosti a zodpovednosti najmä v oblastiach:**
  - plánovania a prípravy na riadené zvládnutie kybernetických bezpečnostných incidentov,
  - monitorovania, detekcie, posúdenia a ohlasovania bezpečnostne relevantných udalostí a kybernetických bezpečnostných incidentov,
  - hodnotenia a rozhodovania o bezpečnostných udalostiach, zraniteľnostiach a kybernetických bezpečnostných incidentoch,
  - klasifikačnej schémy kybernetických bezpečnostných incidentov,
  - evidencie kybernetických bezpečnostných incidentov,
  - nakladania s forenznými dôkazmi,
  - externej a internej komunikácie,
  - eskalácie a kontrolovanej obnovy,
  - plánovania a implementácie opatrení na zlepšenie prevencie, detekcie, alebo reakcie na kybernetický bezpečnostný incident.
- ☐ **Zamestnanci poverení riešením kybernetických bezpečnostných incidentov10) sú odborne spôsobilí, pravidelne školení a zastupiteľní.**
- ☐ **V organizácii správcu sú vytvorené plány na riešenie kybernetických bezpečnostných incidentov.**

1.3.14 Kryptografické opatrenia – Zhodné s kategóriou II

- ☐ **Pri informačných technológiách verejnej správy s vysokou požiadavkou na integritu sa zabezpečuje autenticita a integrita súborov s použitím kryptografických prostriedkov, ktorým je najmä elektronický podpis.**
- ☐ **Pri informačných technológiách verejnej správy s vysokou požiadavkou na dôvernosť musí byť na zabezpečenie dôvernosti použité šifrovanie, a to najmä:**
  - elektronických dokumentov,
  - dát na prenosných zariadeniach, ktoré sú vynášané mimo priestory organizácie správcu,
  - emailovej komunikácie prostredníctvom PGP alebo S/MIME,
  - komunikačných kanálov na výmenu nešifrovaných dát,

- centrálnych úložísk,
- záloh.

☐ **Na zabezpečenie správneho a efektívneho používania kryptografických prostriedkov a šifrovania sa vytvára a implementuje interný riadiaci akt, ktorý obsahuje najmä:**

- princípy ochrany informačných aktív s využitím kryptografických prostriedkov,
- definovanie požadovanej úrovne ochrany a štandardy šifrovania,
- roly a zodpovednosti jednotlivých subjektov pri používaní šifrovania,
- riadenie šifrovacích kľúčov.

☐ **Každé použitie kryptografického prostriedku v informačných technológiách verejnej správy sa zadokumentuje v dokumentácii k informačným technológiám verejnej správy, najmenej na úrovni využívaného algoritmu a verzie.**

☐ **Správca pravidelne prehodnocuje využívané kryptografické prostriedky a overuje, či nedošlo k zverejneniu zraniteľností s nimi súvisiacich.**

1.3.15 Kontinuita prevádzky informačných technológií verejnej správy – Zhodná s kategóriou II

☐ **Na zachovanie kontinuity prevádzky vykonáva analýza rizík a posúdenie vplyvov na dostupnosť jednotlivých informačných technológií verejnej správy a služieb, ktoré zabezpečujú.**

☐ **Na informačné technológie verejnej správy s vysokou požiadavkou na dostupnosť sa vypracuje plán kontinuity prevádzky, ktorý zabezpečí včasnú a adekvátnu reakciu pri mimoriadnej udalosti alebo núdzovej situácie s cieľom minimalizácie rizika prerušenia prevádzky informačných technológií verejnej správy a čo najrýchlejšej obnovy, ak dôjde k prerušeniu prevádzky informačných technológií verejnej správy.**

☐ **Plán kontinuity prevádzky obsahuje najmä:**

- roly a zodpovednosti v procese zabezpečenia kontinuity prevádzky,
- možné vplyvy na prevádzku informačných technológií verejnej správy,
- časový rámec obnovy,
- identifikáciu zdrojov potrebných na obnovu prevádzky,
- identifikáciu zamestnancov potrebných na obnovu prevádzky,
- identifikáciu dát a systémov potrebných na obnovu prevádzky (potrebné procesy zálohovania a obnovy, potrebný personál a vybavenie),
- identifikáciu priestorov potrebných na obnovu prevádzky,
- stanovenie spôsobu komunikácie a náhradnej komunikácie (spôsob kontaktovania personálu, dodávateľov, používateľov),
- identifikáciu vybavenia potrebného na obnovu prevádzky (procesy obnovy alebo výmeny kľúčových zariadení, alternatívne zdroje, vzájomná pomoc),
- spotrebný materiál potrebný na obnovu prevádzky (procesy výmeny zásob a kľúčových dodávok, zabezpečenie núdzových súčastí),
- konkrétne havarijné procedúry slúžiace na obnovu prevádzky.

☐ **Funkčnosť a aktuálnosť plánu kontinuity sa overuje raz ročne.**

1.3.16 Audit a kontrolné činnosti – Zhodné s kategóriou II

- ☐ **Vypracovanie programu posúdenia bezpečnosti na definované informačné technológie verejnej správy, hodnotenie zraniteľností a penetračné testy.**
- ☐ **Na výkon posúdenia sa vypracuje plán, ktorý obsahuje ciele posúdenia, referenčné dokumenty, dátumy a miesta vykonania posúdenia, organizačné útvary, ktoré sú predmetom posúdenia, roly a zodpovednosti.**
- ☐ **Dodržiavanie politík, štandardov, postupov a ostatných opatrení určených v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti sa preveruje a identifikuje sa ich možný nesúlad.**
- ☐ **Ak je identifikovaný nesúlad s opatreniami kybernetickej bezpečnosti a informačnej bezpečnosti, prijmú sa opatrenia na jeho odstránenie. Ak je zistená nízka efektivita alebo neúčinnosť opatrení, prehodnotia a upravia sa tieto opatrenia tak, že je bezpečnostné riziko znížené na prijateľnú úroveň.**