059797/2021

Smernica
Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky
č. 12/2021 zo dňa 22. septembra 2021 o politike kybernetickej a informačnej bezpečnosti Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

	Meno	Dátum	Podpis
Vypracoval **Oddelenie bezpečnosti**	Vladimír ŠAFÁRIK	22.09.2021	
Garant **Odbor legislatívy**	Dáša BLAŠKOVÁ	22.09.2021	
Schválil			
riaditeľ *Kancelária ministra*	Ján MAGUŠIN	06.10.2021	
minister	Veronika REMIŠOVÁ	06.10.2021	

Účinnosť od: 07.10.2021

Účinnosť do: **doba neurčitá**

Súvisiace predpisy:
Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 221/2019 Z. z.
Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.
Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy.
Ostatné súvisiace právne predpisy sú uvedené v materiáli.

22. septembra 2021

Na zabezpečenie jednotného postupu pri zabezpečení a ochrane informačných systémov na Ministerstve investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „ministerstvo“) podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy a zákona č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov v znení zákona č. 221/2019 Z. z. a Nariadenia Európskeho parlamentu a Rady (EÚ) č. 2016/679 zo dňa 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) (Ú. v. EÚ L 119, 4. 5. 2016) sa ustanovuje:

PRVÁ ČASŤ
ÚVODNÉ USTANOVENIA

Článok 1
Všeobecné ustanovenia

/1/ Táto smernica upravuje postup organizačných útvarov ministerstva pri zabezpečení a ochrane informačných systémov ministerstva.

/2/ Táto smernica sa nevzťahuje na informácie, procesy a informačné systémy, ktoré sa týkajú utajovaných skutočností.[1])

/3/ Presadzovanie zásad kybernetickej a informačnej bezpečnosti je koordinované, aktívne a sústavné.

/4/ Za presadzovanie zásad kybernetickej a informačnej bezpečnosti je zodpovedný každý zamestnanec ministerstva (ďalej len „zamestnanec“).

/5/ V organizačnej štruktúre ministerstva je nevyhnutné uplatňovať princípy najnižších privilégií a oddelenia právomocí a zodpovedností tak, aby každý zamestnanec mal najnižšie možné prístupové práva, aké potrebuje na vykonávanie svojich pracovných úloh, a aby ten istý zamestnanec nebol zodpovedný za vykonávanie a zároveň aj schvaľovanie bezpečnostne relevantných aktivít a činností.

Článok 2
Vymedzenie základných pojmov

Na účely tejto smernice sa rozumie

a) informačným systémom funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových

[1]) Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

prostriedkov,

b) administrátorskou a prevádzkovou dokumentáciou dokumentácia popisujúca umiestnenie, zapojenie, konfiguráciu a nastavenie všetkých významných informačných systémov, komponentov informačných systémov, informačných a komunikačných technológií, prehľad dôležitých prístupových práv a záznamov o ich prevádzke a údržbe obsahujúca návod na správu a prevádzku informačných systémov,
c) aplikačným programovým vybavením skupina programov, používaná v rámci informačného systému ministerstva, slúžiaca na zabezpečenie realizácie vecných a odborných činností,
d) externým systémom systém, ktorého vlastníkom je iná organizácia ako ministerstvo a za ktorého prevádzku, prideľovanie, modifikáciu a odoberanie prístupových práv zodpovedá táto organizácia,
e) procesom súbor činností vykonávaných vecne príslušným organizačným útvarom ministerstva za účelom zabezpečenia plnenia úloh, za ktoré je organizačný útvar ministerstva zodpovedný podľa interného riadiaceho aktu ministerstva,[2])
f) službou poskytovaná funkcionalita vytvorená jedným alebo viacerými informačnými systémami,
g) periférnym zariadením zariadenie pripojiteľné k systémovej jednotke počítača, ktoré nie je jej integrálnou súčasťou,
h) používateľom informačného systému osoba, ktorá akýmkoľvek spôsobom využíva technické a programové prostriedky informačného systému,
i) privilegovaným prístupovým právom prístupové právo, ktoré umožňuje meniť systémové nastavenia, inštalovať a odinštalovať softvér, vytvárať, rušiť, meniť používateľov alebo prístupové práva na čítanie, modifikáciu alebo mazanie dát, spúšťanie a zastavovanie služieb ako čítanie a úprava záznamov slúžiacich na kontrolu aktivít uskutočňovaných v rámci systémov (napríklad prístupové práva administrátorov, root prístupové práva) alebo vykonávať iné činnosti, pre ktoré nie sú dostatočné oprávnenia bežného používateľa,
j) programovým vybavením súbory softvéru tvoriace systémové a aplikačné programové vybavenie,
k) systémovým programovým vybavením skupina programov slúžiaca na zabezpečenie základnej funkcionality hardvérových zariadení v rámci celého informačného systému, napríklad chodu personálnych počítačov a serverov, zdieľanie zdrojov a periférií, výmenu a prenos dát, bezpečnosti,
l) technickým vybavením pracovné stanice, ich súčasti a periférne zariadenia,
m) treťou stranou dodávatelia a ich subdodávatelia, zamestnanci servisných organizácií, klienti, návštevy a ostatné osoby,
n) zamestnancom fyzická osoba, ktorá je v štátnozamestnaneckom pomere, pracovnom pomere alebo obdobnom pracovnoprávnom vzťahu s ministerstvom,[3])

[2]) Organizačný poriadok Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky zo dňa 1. októbra 2020 v znení Dodatku č. 1 zo dňa 13. novembra 2020, Dodatku č. 2 zo dňa 27. januára 2021, Dodatku č. 3 zo dňa 25.februára 2021, Dodatku č. 4 zo dňa 23. marca 2021, Dodatku č. 5 zo dňa 30. júla 2021 a v znení Dodatku č. 6 zo dňa 31. augusta 2021.

[3]) Napríklad zákon č. 40/1964 Zb. Občiansky zákonník v znení neskorších predpisov, zákon č. 311/2001 Z. z. Zákonník práce v znení neskorších predpisov, zákon č. 552/2003 Z. z. o výkone práce vo verejnom záujme v znení neskorších predpisov, zákon č. 55/2017 Z. z. o štátnej službe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

o) zamestnancom tretej strany fyzická osoba, ktorá nie je zamestnancom ministerstva,
p) vlastníkom informačného systému organizačný útvar ministerstva, pre ktorý je informačný systém prevádzkovaný na zabezpečenie plnenia jeho úloh a činností,
q) aktívom čokoľvek, čo pre ministerstvo predstavuje nejakú hodnotu, najmä programové vybavenie, technické zariadenia, poskytované služby, kvalifikované osoby, dobré meno, informácie, dokumentácia, zmluvy,
r) vlastníkom aktíva je zodpovedný zamestnanec príslušného organizačného útvaru ministerstva, ktorý využíva aktívum na plnenie svojich úloh a činností; vlastníkom aktíva je zamestnanec príslušného organizačného útvaru, ktorý je zodpovedný za adekvátnu ochranu zvereného aktíva počas jeho celého životného cyklu,
s) informačným aktívom všetko, čo má pre ministerstvo cenu a vyžaduje si ochranu (údaje, programové vybavenie, know-how, informačno-komunikačné technológie (ďalej len „IKT“), dokumentácia),
t) bezpečnostným rizikom udalosť, konanie alebo stav, ktorý môže viesť k ohrozeniu aktív, finančným stratám, kompromitácii a poškodeniu dobrého mena ministerstva, poškodeniu, zničeniu informačných aktív, úniku informácií, prerušeniu alebo krátkodobej nedostupnosti informačných systémov a služieb ministerstva,
u) závažným bezpečnostným rizikom udalosť, konanie alebo stav, ktorý môže viesť k ohrozeniu aktív, vysokým finančným stratám, závažnej kompromitácii, závažnému poškodeniu dobrého mena ministerstva, dlhodobému alebo nenávratnému poškodeniu, zničeniu informačných aktív, úniku vysoko citlivých informácií, prerušeniu alebo dlhodobej nedostupnosti informačných systémov a služieb ministerstva,
v) bezpečnostným incidentom akékoľvek narušenie bezpečnosti komunikačnej infraštruktúry ministerstva zneužitím zraniteľností alebo porušenie povinností týkajúcich sa kybernetickej a informačnej bezpečnosti a osobitných predpisov, ktoré má za následok ohrozenie aktív, finančné straty, kompromitáciu, poškodenie dobrého mena ministerstva, poškodenie alebo zničenie informačných aktív, únik informácií, prerušenie alebo nedostupnosť informačných systémov a služieb ministerstva,
w) závažným bezpečnostným incidentom akékoľvek narušenie bezpečnosti komunikačnej infraštruktúry ministerstva zneužitím zraniteľností alebo porušenie povinností týkajúcich sa informačnej bezpečnosti a osobitných predpisov, ktoré má za následok významné ohrozenie aktív, vysoké finančné straty, závažnú kompromitáciu, poškodenie dobrého mena ministerstva, dlhodobé alebo nenávratné poškodenie alebo zničenie informačných aktív, únik vysoko citlivých informácií, prerušenie alebo dlhodobú nedostupnosť informačných systémov a služieb ministerstva,
x) mobilným kódom softvér (kód/skript), ktorý je prenášaný medzi jednotlivými informačnými systémami alebo ich súčasťami prostredníctvom siete alebo internetu spúšťaný na lokálnom počítači bez inštalácie (napríklad JavaScript, VBscript, ActiveX ovládače, Flash animácie),
y) princípom *„Need to Know“* princíp prideľovania prístupových práv k informáciám výlučne v takom rozsahu, ktorý je nevyhnutný pre plnenie služobných alebo pracovných úloh a povinností zamestnanca,
z) autentifikáciou / autentizáciou (authentication) potvrdenie deklarovanej identity určitej entity,
aa) autorizáciou (authorization) udelenie oprávnení určitej entite na prístup k zdrojom systému /

organizácie a / alebo na ich využívanie,

ab) autorizovaným subjektom zariadenie alebo používateľ, ktorý bol náležite overený pred prístupom alebo vykonaním určitej činnosti; tento prístup mu bol riadne pridelený a disponuje všetkými požadovanými vlastnosťami pre vykonanie príslušnej činnosti,

ac) firewallom zariadenie alebo softvér, ktorého funkciou je filtrovanie komunikácie v počítačovej sieti s cieľom zabrániť neautorizovanej komunikácii medzi jednotlivými subjektmi alebo vykonávanie ďalších bezpečnostných opatrení ako je napríklad detekcia prienikov, riadenie kvality komunikácie,

ad) bezpečnostnou udalosťou identifikovaný stav systému, služby alebo siete, poukazujúci na možnosť porušenia kybernetickej a informačnej bezpečnosti alebo zlyhanie bezpečnostných opatrení,

ae) kontinuitou činností strategická a taktická spôsobilosť ministerstva byť pripravený reagovať na bezpečnostné incidenty a narušenie činností ministerstva,

af) krízovou situáciou mimoriadna udalosť, pri ktorej je vyhlásený krízový stav a mimoriadna situácia,

ag) havarijným stavom neplánovaná mimoriadna udalosť, ktorá vznikla alebo jej vznik bezprostredne hrozí v súvislosti s prevádzkou technických zariadení a následne vedie k strate života, poškodeniu alebo ohrozeniu zdravia ľudí, životného prostredia alebo k škode na majetku,

ah) správou informačných systémov alebo služieb je zabezpečenie funkčnosti informačného systému, služby alebo počítačovej siete,

ai) kybernetickým bezpečnostným incidentom akákoľvek udalosť, ktorá má z dôvodu narušenia bezpečnosti siete a informačného systému alebo porušenia bezpečnostnej politiky alebo záväznej metodiky negatívny vplyv na kybernetickú bezpečnosť alebo ktorej následkom je strata dôvernosti údajov, zničenie údajov alebo narušenie integrity systému, obmedzenie alebo odmietnutie dostupnosti základnej služby alebo digitálnej služby, vysoká pravdepodobnosť kompromitácie činností základnej služby alebo digitálnej služby alebo ohrozenie bezpečnosti informácií.

Článok 3
Záväzok vedenia ministerstva v oblasti kybernetickej a informačnej bezpečnosti

/1/ Pre zaistenie neprerušeného a efektívneho plnenia poslania ministerstva je nevyhnutné udržiavať úroveň kybernetickej a informačnej bezpečnosti minimálne na takom stupni, ktorý umožní znížiť identifikované riziká na akceptovateľnú úroveň.

/2/ Vedenie ministerstva prijímaním a implementáciou zásad kybernetickej a informačnej bezpečnosti:

a) zaisťuje primeranú a ekonomicky prijateľnú ochranu aktív ministerstva,

b) minimalizuje riziká ľudského a technického zlyhania, krádeže, podvodu, sprenevery alebo zneužitia prostriedkov a negatívne pôsobenie vonkajších vplyvov na akceptovateľnú úroveň,

c) minimalizuje škody vzniknuté narušením alebo zlyhaním ochrany aktív, tieto udalosti vyhodnocuje a prijíma opatrenia k ich eliminácii,

d) vytvára vo vnútri ministerstva také bezpečnostné povedomie, aby sa kybernetická a

informačná bezpečnosť stala neoddeliteľnou súčasťou každodenného chodu, ako aj celkovej kultúry ministerstva.

/3/ Vedenie ministerstva na dosiahnutie cieľov podľa odseku 2

a) definuje stratégiu kybernetickej bezpečnosti a politiku kybernetickej a informačnej bezpečnosti a aktívne podporuje kybernetickú a informačnú bezpečnosť a jej vplyvy na chod prevádzkovaných základných služieb,
b) pravidelne preskúmava aktuálnosť a účinnosť implementácie politiky kybernetickej a informačnej bezpečnosti,
c) poskytuje spätnú väzbu a viditeľnú podporu bezpečnostným iniciatívam,
d) zaisťuje dostatočné zdroje k realizácii bezpečnostných opatrení.

Článok 4
Bezpečnostná politika kybernetickej bezpečnosti ministerstva

/1/ Účelom bezpečnostnej politiky kybernetickej bezpečnosti ministerstva je formulácia jasnej a záväznej koncepcie riešenia kybernetickej bezpečnosti v organizácii a definícia základných prístupov pri jej budovaní a riadení. Vytvára základ na tvorbu dokumentácie ministerstva, najmä bezpečnostných zásad a postupov, bezpečnostných smerníc a definuje zásady správania sa všetkých užívateľov (vlastných zamestnancov aj zamestnancov tretích strán).

/2/ Poslaním bezpečnostnej politiky kybernetickej bezpečnosti ministerstva je spolu s ďalšími bezpečnostnými dokumentmi a vnútornými predpismi stanoviť stratégiu a konkrétne pravidlá bezpečného správania používateľov pri ich činnostiach v rámci ministerstva.

/3/ Bezpečnostná politika kybernetickej bezpečnosti ministerstva sa vzťahuje na všetky informačné aktíva ministerstva, ktoré priamo súvisia so spracúvaním informácií na zabezpečenie aktivít ministerstva. Je záväzná pre všetkých zamestnancov ministerstva, ďalšie osoby (právnické aj fyzické) a tretie strany, ktoré sa zaviažu ju dodržiavať.

/4/ Bezpečnostná politika kybernetickej bezpečnosti ministerstva sa aktualizuje raz ročne.

/5/ Štruktúra bezpečnostnej politiky kybernetickej bezpečnosti ministerstva je spracovaná integrovanou formou a zahŕňa v sebe všetky požadované čiastkové bezpečnostné politiky:

a) pravidlá správania a dobrej praxe – bezpečnostná politika,
b) organizácia bezpečnosti – bezpečnostná politika,
c) riadenie informačných aktív – bezpečnostná politika,
d) riadenie bezpečnostných rizík – bezpečnostná politika,
e) riadenie a prevádzka IKT – bezpečnostná politika,
f) riadenie dodávateľských vzťahov – bezpečnostná politika,
g) riadenie vývoja a údržby v oblasti IKT – bezpečnostná politika,
h) riadenie kontinuity procesov a činností – bezpečnostná politika,
i) riadenie súladu – bezpečnostná politika.

Článok 5
Bezpečnostná dokumentácia ministerstva

/1/ Bezpečnostná dokumentácia ministerstva obsahuje:
a) schválenú bezpečnostnú stratégiu kybernetickej bezpečnosti ministerstva,
b) schválenú bezpečnostnú politiku kybernetickej bezpečnosti ministerstva (integrovanú, ktorá v sebe zahŕňa všetky požadované čiastkové bezpečnostné politiky),
c) zoznam a klasifikáciu informačných aktív ministerstva,
d) zoznam aktív ministerstva a kategorizáciu sietí a informačných systémov ministerstva,
e) zadokumentované vymedzenie rozsahu a spôsobu plnenia všetkých bezpečnostných opatrení v prostredí ministerstva,
f) vykonanú analýzu rizík kybernetickej bezpečnosti (katalóg rizík a mapu rizík) v prostredí ministerstva vrátane analýzy rizík pre významné informačné systémy ministerstva (v podobe komplexných bezpečnostných projektov významných informačných systémov ministerstva),
g) samohodnotenie, resp. záverečnú správu o výsledkoch auditu kybernetickej bezpečnosti.

/2/ Od základnej (vrcholovej) bezpečnostnej dokumentácie sa odvíja ďalšia štruktúra dokumentácie v oblasti kybernetickej a informačnej bezpečnosti ministerstva, ktorá je uvedená v samostatnom dokumente MIRRI-SEC-A-ZBD (Zoznam bezpečnostnej dokumentácie ministerstva). Táto dokumentácia je záväzná pre všetky organizačné útvary ministerstva, všetkých zamestnancov ministerstva a zamestnancov tretích strán / dodávateľov. V rámci bezpečnostnej dokumentácie ministerstva v kontexte zoznamu MIRRI-SEC-A-ZBD je zavedený nasledovný systém číslovania MIRRI-SEC-X-Y, kde:
a) MIRRI je názov organizácie – ministerstva,
b) SEC je oblasť bezpečnosti (SECURITY),
c) X je veľké písmeno, vyjadrujúce číslo oblasti minimálnych bezpečnostných opatrení v súlade s osobitným predpisom,[4])
d) Y je poradové číslo dokumentu v konkrétnej oblasti minimálnych bezpečnostných opatrení v súlade s osobitným predpisom.[4]) Za týmto poradovým číslom dokumentácie sa v prípade potreby môže uviesť pomlčka a názov informačného systému, resp. konkrétny rok (napr. pri plánoch vzdelávania na konkrétne obdobie a pod.), resp. v prípade potreby ich kombinácia.

/3/ Kompletná bezpečnostná dokumentácia ministerstva pre oblasť kybernetickej a informačnej bezpečnosti je umiestnená na SharePoint ministerstva.[5])

[4]) Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy.
[5]) https://upvi.sharepoint.com/sites/SKBMIRRI.

DRUHÁ ČASŤ
RIADENIE KYBERNETICKEJ A INFORMAČNEJ BEZPEČNOSTI

Článok 6
Koordinácia kybernetickej a informačnej bezpečnosti

/1/ Najvyšším orgánom v procese riadenia kybernetickej a informačnej bezpečnosti je minister investícií, regionálneho rozvoja a informatizácie (ďalej len „minister“).

/2/ Poradným, iniciatívnym a koordinačným orgánom ministra pre oblasť kybernetickej a informačnej bezpečnosti je bezpečnostný výbor ministerstva. Úlohou bezpečnostného výboru ministerstva je riadiť stratégiu kybernetickej a informačnej bezpečnosti ministerstva.

/3/ Sekcia kybernetickej bezpečnosti zodpovedá za oblasť kybernetickej a informačnej bezpečnosti na úrovni ministerstva. Zároveň plní úlohy ústredného orgánu pre sektor verejnej správy, podsektor informačné systémy verejnej správy podľa osobitého predpisu.[6])

/4/ Za koordináciu kybernetickej a informačnej bezpečnosti, určovanie zásad kybernetickej a informačnej bezpečnosti, tvorbu a aktualizáciu politiky kybernetickej a informačnej bezpečnosti zodpovedá manažér kybernetickej a informačnej bezpečnosti.

/5/ Úlohy podľa odseku 4 vykonáva manažér kybernetickej a informačnej bezpečnosti prostredníctvom oddelenia informačných technológií ministerstva.

/6/ Úlohy podľa tejto smernice môže manažér kybernetickej a informačnej bezpečnosti vykonávať aj prostredníctvom iných organizačných útvarov ministerstva.

/7/ Bežná koordinácia kybernetickej a informačnej bezpečnosti môže byť v prípade vzniku mimoriadnych udalostí s významnými dopadmi čiastočne alebo úplne nahradená riadením zo strany bezpečnostného výboru ministerstva.

Zodpovednosť v oblasti kybernetickej a informačnej bezpečnosti

Článok 7
Zamestnanci

/1/ Zamestnanci sú povinní najmä
a) zaisťovať nepretržitú ochranu zverených informačných aktív z pohľadu dôvernosti, integrity a dostupnosti,
b) predchádzať vzniku bezpečnostných incidentov,
c) spolupracovať v prípade vzniku škôd na informačných aktívach pri určení škody a likvidácii následkov,
d) zabezpečiť v oblasti svojej pôsobnosti klasifikáciu informačných aktív, najmä z pohľadu

[6]) Príloha č. 1 k zákonu č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

dostupnosti a dôvernosti,

e) dodržiavať a presadzovať plnenie zásad kybernetickej a informačnej bezpečnosti a súvisiacich interných riadiacich aktov pri každodennej realizácii vlastných činností a v zmluvných vzťahoch s tretími stranami,
f) plniť povinnosti v oblasti kybernetickej a informačnej bezpečnosti a zachovania kontinuity činnosti vyplývajúce zo štátnozamestnaneckého pomeru, pracovného pomeru alebo obdobného pracovnoprávneho vzťahu s ministerstvom,
g) oznamovať ustanoveným spôsobom, včas a úplne každé porušenie zásad kybernetickej a informačnej bezpečnosti, ako aj zistené bezpečnostné riziká.

/2/ Zamestnanci sú oprávnení

a) vyžadovať plnenie zásad kybernetickej a informačnej bezpečnosti a interných riadiacich aktov týkajúcich sa ochrany informačných aktív ministerstva,
b) vyžadovať odbornú a metodickú pomoc od manažéra kybernetickej a informačnej bezpečnosti a oddelenia informačných technológií ministerstva pri riešení problémov v oblasti kybernetickej a informačnej bezpečnosti.

Článok 8
Vedúci zamestnanci

/1/ Vedúci zamestnanci sú povinní

a) aktívne sa podieľať na identifikácii informačných aktív a s nimi spojených bezpečnostných rizík v rozsahu organizačného útvaru ministerstva, ktorý riadia,
b) participovať na návrhu, príprave a implementácii bezpečnostných opatrení určených na elimináciu identifikovaného bezpečnostného rizika pre nimi riadené procesy a činnosti ministerstva,
c) v spolupráci s oddelením informačných technológií ministerstva zabezpečovať implementáciu zodpovedajúcich bezpečnostných opatrení určených pre im zverené informačné aktíva,
d) poznať postupy riešenia krízových situácií a havarijných stavov v oblasti kybernetickej a informačnej bezpečnosti podľa vopred pripravených plánov a riadiacich dokumentov,
e) zabezpečiť riadený prístup k informáciám a systémom vo svojej kompetencii,
f) dodržiavať osobitné predpisy a interné riadiace akty v oblasti kybernetickej a informačnej bezpečnosti, poznať a uplatňovať zásady kybernetickej a informačnej bezpečnosti vo svojej riadiacej činnosti, ako aj dbať na ich dodržiavanie podriadenými zamestnancami,
g) zabezpečovať také podmienky pre zamestnancov ministerstva a zamestnancov tretích strán/dodávateľov, aby mohli bez prekážok plniť určené zásady kybernetickej a informačnej bezpečnosti a včas poskytovať informácie týkajúce sa kybernetickej a informačnej bezpečnosti,
h) vymedziť práva a povinnosti svojich podriadených zamestnancov jednoznačne a adresne tak, aby sa nevyskytovala činnosť, proces ani informačné aktívum, u ktorého by nikto nezodpovedal za stav bezpečnosti alebo by dochádzalo k stretu právomocí,
i) zabezpečovať v spolupráci s manažérom kybernetickej a informačnej bezpečnosti preškolenie podriadených zamestnancov v oblasti kybernetickej a informačnej bezpečnosti a sústavne udržovať a zvyšovať ich povedomie o kybernetickej a informačnej

bezpečnosti,

j) zabezpečovať poučenie podriadených zamestnancov o možných dôsledkoch porušenia kybernetickej a informačnej bezpečnosti a o interných riadiacich aktoch o kybernetickej a informačnej bezpečnosti,
k) vykonávať pravidelnú kontrolu funkčnosti a účinnosti prijatých bezpečnostných opatrení v rámci svojej pôsobnosti a o nefunkčnosti či zníženej účinnosti bezodkladne informovať manažéra kybernetickej a informačnej bezpečnosti,
l) vo svojej kompetencii dojednávať rozsah a spôsob zabezpečovania a plnenia bezpečnostných opatrení v zmluvách so zmluvnými partnermi v súlade so zásadami kybernetickej a informačnej bezpečnosti alebo minimálne v rozsahu ustanovenom v internom riadiacom akte,
m) zabezpečiť okamžité nahlásenie všetkých skutočností, ktoré môžu mať vplyv na zníženie ochrany informačných aktív manažérovi kybernetickej a informačnej bezpečnosti a oddeleniu informačných technológií ministerstva, obzvlášť ak môžu zapríčiniť vznik bezpečnostných incidentov alebo iných mimoriadnych udalostí,
n) podieľať sa na riešení všetkých zistených bezpečnostných incidentov a zaisťovaní bezpečnostne relevantných informácií vo svojej pôsobnosti v spolupráci s manažérom kybernetickej a informačnej bezpečnosti a oddelením bezpečnosti ministerstva a z výsledkov dôsledne vyvodzovať personálne a iné opatrenia u svojich podriadených zamestnancov,
o) zohľadniť opatrenia vyplývajúce z bezpečnostných analýz, auditov a odporučení manažéra kybernetickej a informačnej bezpečnosti a oddelenia informačných technológií ministerstva,
p) implementovať a realizovať určené bezpečnostné opatrenia (administratívne, personálne, organizačné, procesné, technické, technologické a prevádzkové) pri ochrane informačných aktív, systémov, služieb a procesov pre zabezpečenie kontinuity činností ministerstva.

/2/ Vedúci zamestnanci sú oprávnení

a) v spolupráci s manažérom kybernetickej a informačnej bezpečnosti a oddelením bezpečnosti ministerstva prijímať samostatné opatrenia k zaisteniu kybernetickej a informačnej bezpečnosti, ktoré spadajú plne do ich kompetencie,
b) akceptovať riziká týkajúce sa aktív spadajúcich výhradne do ich kompetencie, napríklad riziká týkajúce sa činností organizačného útvaru ministerstva, ktorý riadia a pre túto akceptáciu požadovať podklady, odhad, analýzu rizík a odporúčania od manažéra kybernetickej a informačnej bezpečnosti, oddelenia informačných technológií ministerstva a oddelenia bezpečnosti ministerstva,
c) požadovať spoluprácu pri zaistení bezpečnosti im zverených informačných aktív, procesov a činností od ostatných vedúcich zamestnancov, do ktorých kompetencie spadajú nadväzujúce aktíva, procesy a činnosti,
d) požadovať od manažéra kybernetickej a informačnej bezpečnosti, oddelenia informačných technológií ministerstva a oddelenia bezpečnosti ministerstva odhad, analýzu rizík a návrh opatrení pre zaistenie bezpečnosti v prípadoch, keď kompetencie zatiaľ neboli určené alebo ide o problematiku zahrňujúcu kompetencie viacerých

organizačných útvarov ministerstva.

Článok 9
Vlastníci aktív a procesov

/1/ Vlastníci aktív v rámci svojej pôsobnosti sú povinní
a) riadiť bezpečnostné riziká generované vonkajším alebo vnútorným prostredím ministerstva, ktoré sa týkajú informačných aktív v ich vlastníctve,
b) určiť pravidlá pre nakladanie s informačnými aktívami v ich vlastníctve podľa bezpečnostných štandardov, ak tieto nie sú ustanovené v interných riadiacich aktoch,
c) prijímať a implementovať bezpečnostné opatrenia k zníženiu identifikovaných zraniteľností informačných aktív v ich vlastníctve,
d) dodržiavať bezpečnostné opatrenia prijaté pre elimináciu alebo zníženie bezpečnostných rizík pôsobiacich na informačné aktíva v ich vlastníctve,
e) zabezpečiť obnovenie funkčnosti a nahradenie vlastnených informačných aktív v prípade ich výpadku, poškodenia alebo iného znefunkčnenia v spolupráci s ostatnými organizačnými útvarmi ministerstva,
f) viesť evidenciu informačných aktív v ich vlastníctve podľa interného riadiaceho aktu ministerstva.[7])

/2/ Vlastníci procesov v rámci svojej pôsobnosti sú povinní
a) zaistiť implementáciu zásad procesnej bezpečnosti v nimi spravovaných procesoch a činnostiach,
b) aplikovať postupy analýzy rizík a postupy pre zaistenie kontinuity činností v spravovaných procesoch a činnostiach.

Článok 10
Správcovia informačných systémov a služieb

Správcovia informačných systémov a služieb, ktoré im boli zverené sú povinní najmä
a) zaistiť bezpečnosť a zodpovedajúcu ochranu zverených informačných systémov a služieb v ich pôsobnosti,
b) predchádzať a zamedzovať pôsobeniu škodlivých vplyvov na zverené informačné systémy a služby,
c) navrhovať a realizovať bezpečnostné opatrenia na zverených informačných systémoch a službách v spolupráci s príslušnými organizačnými útvarmi ministerstva,
d) poskytovať informácie o stave informačných systémov a služieb koncovým používateľom,
e) spolupracovať a poskytovať súčinnosť pri odhade a analýze rizík a pri vykonávaní auditov,
f) zhromažďovať informácie o bezpečnostnej situácii, bezpečnostných udalostiach a

[7]) Smernica vedúceho Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 1/2020 zo dňa 13. mája 2020 o inventarizácii a ochrane informačných aktív Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu.

incidentoch a poskytovať ich manažérovi kybernetickej a informačnej bezpečnosti,

g) poskytovať koncovým používateľom základnú konzultáciu pri bežnej prevádzke zverených informačných systémov a služieb a poskytovať konzultáciu ohľadom postupu riešenia v prípade vzniku bezpečnostných udalostí a incidentov.

Článok 11
Manažér kybernetickej a informačnej bezpečnosti

/1/ Manažér kybernetickej a informačnej bezpečnosti je povinný najmä

a) zabezpečovať aplikáciu bezpečnostných opatrení v systéme riadenia kybernetickej bezpečnosti,
b) rozpracovať zásady kybernetickej a informačnej bezpečnosti a povinnosti do ďalších interných riadiacich aktov,
c) zaisťovať vykonávanie kybernetickej a informačnej bezpečnosti podľa osobitných predpisov a interných riadiacich aktov,
d) metodicky viesť správcov informačných systémov, vlastníkov procesov, vlastníkov aktív, vedúcich zamestnancov a ďalších zodpovedných zamestnancov v oblasti kybernetickej a informačnej bezpečnosti,
e) analyzovať, definovať a monitorovať bezpečnostné riziká,
f) prijímať preventívne opatrenia k zamedzeniu alebo minimalizácii bezpečnostných rizík, bezpečnostných incidentov, mimoriadnych situácií a monitorovať plnenie a efektivitu týchto opatrení,
g) koordinovať spracovanie plánov obnovy činností ministerstva,
h) organizovať činnosti týkajúce sa koordinácie kybernetickej a informačnej bezpečnosti, spolupracovať pri riešení mimoriadnych situácií a pri obnove štandardnej situácie pre udržanie kontinuity činností ministerstva,
i) v spolupráci s oddelením bezpečnosti predkladať odborné stanoviská, analýzy k procesom, projektom, zmenám a ostatným aktivitám ministerstva s dopadom na kybernetickú a informačnú bezpečnosť,
j) informovať bezpečnostný výbor ministerstva a ministra o stave kybernetickej a informačnej bezpečnosti na ministerstve, o závažných bezpečnostných rizikách, incidentoch a významných bezpečnostných udalostiach,
k) zabezpečiť nezávislé preskúmanie stavu kybernetickej a informačnej bezpečnosti a spolupracovať pri realizácii auditov vykonávaných internými a externými subjektmi,
l) zabezpečovať školenia zamestnancov v oblasti kybernetickej a informačnej bezpečnosti.

/2/ Manažér kybernetickej a informačnej bezpečnosti je oprávnený

a) zadávať oddeleniu informačných technológií ministerstva úlohy v oblasti riadenia kybernetickej a informačnej bezpečnosti,
b) vyjadrovať sa a schvaľovať použitie bezpečnostných systémov, technológií, služieb a procedúr k podpore bezpečnosti procesov a činností ministerstva,
c) udeľovať výnimky z určených bezpečnostných opatrení,
d) požadovať v rámci vnútorného vyšetrovania bezpečnostných incidentov ústne a písomné vyjadrenia od zúčastnených zamestnancov a požadovať spoluprácu od všetkých

zamestnancov,

e) vstupovať do všetkých objektov a na všetky pracoviská ministerstva pri dodržiavaní interných zásad a pravidiel pre pohyb a prácu na týchto pracoviskách,
f) vykonávať kontroly, audity a bezpečnostné analýzy činností, procesov a zabezpečenia aktív ministerstva,
g) kontrolovať dodržiavanie bezpečnostných štandardov, nahliadať v nevyhnutnom rozsahu pri dodržiavaní osobitných predpisov, interných riadiacich aktov a ustanovených zásad ochrany informácií do všetkých potrebných materiálov, dokladov, záznamov a evidencií a v prípade potreby vytvárať ich kópie,
h) monitorovať činnosť používateľov a bezpečnostne významných udalostí v bezpečnostných a informačných systémoch ministerstva pri zaisťovaní ochrany práv a záujmov ministerstva,
i) vyžadovať plnenie určených bezpečnostných opatrení a ochrany aktív,
j) v prípade hroziaceho nebezpečenstva uplatniť obmedzenia či zákaz výkonu činnosti alebo prevádzkovania informačného systému alebo služby, ktoré vážne a bezprostredne ohrozujú majetok alebo zdravie zamestnancov alebo môžu spôsobiť iné závažné škody.

/3/ Manažéra kybernetickej a informačnej bezpečnosti vymenúva a odvoláva minister.

/4/ Manažér kybernetickej a informačnej bezpečnosti je nezávislý od riadenia prevádzky a vývoja služieb informačných technológií.[8])

Článok 12
Bezpečnostný výbor ministerstva

/1/ Bezpečnostný výbor ministerstva je povinný najmä
a) riadiť stratégiu v oblasti kybernetickej a informačnej bezpečnosti,
b) riadiť bezpečnostné riziká, akceptovať bezpečnostné riziká, ktoré sa týkajú viac ako jedného organizačného útvaru ministerstva,
c) schvaľovať a rozhodovať o návrhoch na implementáciu bezpečnostných opatrení na elimináciu bezpečnostných rizík,
d) odsúhlasiť odporúčania, návrhy strategických a koncepčných materiálov v oblasti kybernetickej a informačnej bezpečnosti pripravených manažérom kybernetickej a informačnej bezpečnosti na schválenie ministrovi,
e) definovať zodpovednosť za implementáciu a uplatňovanie jednotlivých bezpečnostných opatrení.

/2/ Bezpečnostný výbor ministerstva vedie, vytvára, koordinuje, prerokúva, schvaľuje, sprístupňuje, mení, preskupuje a reviduje zoznam bezpečnostnej dokumentácie so samostatným číslovaním jednotlivých bezpečnostných dokumentov ministerstva, a to nasledovne:
a) bezpečnostný výbor ministerstva prostredníctvom manažéra kybernetickej a informačnej

[8]) § 5 písm. a) vyhlášky Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

bezpečnosti ukladá bezpečnostnú dokumentáciu na určené miesto na intranete tak, aby bezpečnostné dokumenty boli prístupné relevantným oprávneným zamestnancom a aj tretím stranám,

b) bezpečnostný výbor ministerstva prostredníctvom manažéra kybernetickej a informačnej bezpečnosti ukladá chránenú a prísne chránenú bezpečnostnú dokumentáciu na určené miesto na intranete tak, aby chránené a prísne chránené bezpečnostné dokumenty boli prístupné len určeným zamestnancom (napr. správcom informačných systémov, členom bezpečnostného výboru ministerstva, resp. iným zamestnancom schváleným manažérom kybernetickej a informačnej bezpečnosti),

c) bezpečnostný výbor ministerstva prideľuje evidenčné čísla bezpečnostným dokumentom podľa nasledujúceho číslovania:
   1. MIRRI-SEC-A: organizácia kybernetickej bezpečnosti,
   2. MIRRI-SEC-B: riadenie rizík kybernetickej bezpečnosti,
   3. MIRRI-SEC-C: personálna bezpečnosť,
   4. MIRRI-SEC-D: riadenie prístupov,
   5. MIRRI-SEC-E: riadenie kybernetickej bezpečnosti vo vzťahoch s tretími stranami,
   6. MIRRI-SEC-F: bezpečnosť pri prevádzke informačných systémov a sietí,
   7. MIRRI-SEC-G: hodnotenie zraniteľností,
   8. MIRRI-SEC-H: ochrana proti škodlivému kódu,
   9. MIRRI-SEC-I: sieťová a komunikačná bezpečnosť,
   10. MIRRI-SEC-J: akvizícia, vývoj a údržba informačných technológií verejnej správy,
   11. MIRRI-SEC-K: zaznamenávanie udalostí a monitorovanie,
   12. MIRRI-SEC-L: fyzická a objektová bezpečnosť prostredia,
   13. MIRRI-SEC-M: riešenie kybernetických a bezpečnostných incidentov,
   14. MIRRI-SEC-N: kryptografické opatrenia,
   15. MIRRI-SEC-O: kontinuita prevádzky informačných technológií verejnej správy,
   16. MIRRI-SEC-P: audit a kontrolné činnosti,
   17. MIRRI-SEC-Q: dokumentácia vládnej jednotky CSIRT.

/3/ Bezpečnostný výbor ministerstva je oprávnený zmeniť rozhodnutie vlastníka aktíva alebo procesu o spôsobe eliminácie alebo akceptácii bezpečnostného rizika.

/4/ Bezpečnostný výbor ministerstva je povinný informovať ministra o všetkých závažných bezpečnostných rizikách v oblasti kybernetickej a informačnej bezpečnosti a o spôsobe ich eliminácie vrátane ich akceptácie.

/5/ Za činnosť bezpečnostného výboru ministerstva zodpovedá jeho predseda, ktorým je generálny tajomník služobného úradu ministerstva. Bezpečnostný výbor ministerstva zasadá pravidelne, najmenej dvakrát ročne. Ak vznikne mimoriadna okolnosť, môže zasadnutie bezpečnostného výboru ministerstva iniciovať ktorýkoľvek z členov bezpečnostného výboru ministerstva.

/6/ Bezpečnostný výbor ministerstva je zložený z

a) generálneho tajomníka služobného úradu ministerstva,

b) generálneho riaditeľa sekcie ekonomiky a projektov EŠIF,

c) generálneho riaditeľa sekcie správy majetku a obstarávania,
d) riaditeľa odboru majetku a služieb,
e) riaditeľa vládnej jednotky CSIRT,
f) manažéra kybernetickej a informačnej bezpečnosti,
g) vedúceho oddelenia bezpečnosti,
h) vedúceho oddelenia informačných technológií,
i)zodpovednej osoby pre ochranu osobných údajov.

/7/ Členov bezpečnostného výboru ministerstva vymenúva a odvoláva minister.

/8/ Na zasadnutia bezpečnostného výboru ministerstva môžu byť prizvané ďalšie osoby, ak si to predmet zasadnutia bezpečnostného výboru ministerstva vyžaduje.

/9/ Členstvo v bezpečnostnom výbore ministerstva je nezastupiteľné.

TRETIA ČASŤ
ZÁKLADNÉ BEZPEČNOSTNÉ ZÁSADY

Článok 13
Riadenie rizík

/1/ Úlohou procesu riadenia bezpečnostných rizík je formálny prístup k bezpečnostným rizikám a ich minimalizácii.

/2/ Za proces riadenia bezpečnostných rizík na ministerstve je zodpovedný manažér kybernetickej a informačnej bezpečnosti. Vrcholným rozhodovacím orgánom pre riadenie rizík je bezpečnostný výbor ministerstva.

/3/ Manažér kybernetickej a informačnej bezpečnosti v úzkej spolupráci s určenými zamestnancami organizačných útvarov ministerstva vykoná analýzu rizík za účelom identifikácie a hodnotenia bezpečnostných rizík a následného návrhu primeraných bezpečnostných opatrení na ich minimalizáciu. Zamestnancov organizačných útvarov ministerstva určí manažér kybernetickej a informačnej bezpečnosti na základe toho, za ktorý informačný systém verejnej správy zodpovedajú. Analýza rizík sa vykoná aspoň jedenkrát za rok alebo pri významných zmenách v informačných a komunikačných technológiách ministerstva a po výskyte závažného kybernetického incidentu.

/4/ Pre každé bezpečnostné riziko identifikované v analýze rizík sú určené primerané bezpečnostné opatrenia tak, aby bolo úplne alebo čiastočne eliminované.

/5/ Podrobnosti procesu riadenia bezpečnostných rizík na ministerstve ustanovuje interný riadiaci akt.[9])

[9]) Smernica vedúceho Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 10/2018 zo dňa 30. novembra 2018 o riešení bezpečnostných incidentov na Úrade podpredsedu vlády Slovenskej republiky pre

Článok 14
Riadenie aktív

/1/ Všetky aktíva ministerstva najmä informácie a informačné systémy sú identifikované, majú určeného konkrétneho vlastníka.

/2/ Vlastníci aktív musia klasifikovať informácie a kategorizovať siete a informačné systémy v správe ministerstva podľa osobitého predpisu.[10]) Klasifikácia informácií a kategorizácia sietí a informačných systémov sa vykonáva na základe významnosti, funkcie a účelu informácií a informačných systémov s ohľadom na dôvernosť, integritu, dostupnosť, kvalitu služby a kontrolnú činnosť.

/3/ Inventarizáciu a ochranu informačných aktív ustanovuje interný riadiaci akt.[7])

Článok 15
Personálna bezpečnosť

V oblasti riadenia ľudských zdrojov sa uplatňujú primerané bezpečnostné opatrenia, a to najmä

a) nový zamestnanec je bezodkladne po nástupe preukázateľne oboznámený so všetkými internými riadiacimi aktmi, ktoré sa týkajú kybernetickej a informačnej bezpečnosti,
b) proces bezpečnostného vzdelávania a zvyšovania bezpečnostného povedomia zamestnancov je nastavený tak, že každý zamestnanec absolvuje školenie o kybernetickej a informačnej bezpečnosti a ochrany osobných údajov minimálne raz ročne,
c) po skončení štátnozamestnaneckého pomeru, pracovného pomeru alebo obdobného pracovnoprávneho vzťahu s ministerstvom je zamestnanec povinný vrátiť všetky aktíva. Oddelenie informačných technológií ministerstva je zodpovedné za zrušenie prístupových práv a za kontrolu technického stavu vráteného prostriedku. Za vrátenie prostriedkov na prácu s informačnými aktívami (napríklad notebooky, tablety, USB disky, USB kľúče) je zodpovedné oddelenie hospodárskej správy ministerstva. Výnimku tvoria fyzické aktíva financované z prostriedkov štrukturálnych fondov a Kohézneho fondu, kde sa fyzické aktíva riadia poriadkom ustanoveným sekciou centrálny koordinačný orgán ministerstva.

Článok 16
Prevádzkové postupy a zodpovednosti

/1/ Prevádzku prostriedkov určených na spracovanie informácií a prevádzkové postupy a štandardy pre vybrané oblasti bezpečnosti ustanovené v politike kybernetickej a informačnej bezpečnosti zdokumentuje vlastník daného informačného systému verejnej správy v spolupráci s dodávateľom informačného systému a so zamestnancami sekcie

investície a informatizáciu v znení Dodatku č. 1 zo dňa 13. mája 2020.
[10]) Vyhláška č. 362/2018 Z. z.

kybernetickej bezpečnosti ministerstva.

/2/ Všetky zmeny informačných systémov na ministerstve zdokumentuje príslušný organizačný útvar ministerstva, ktorý má konkrétny informačný systém vo svojej správe. Za zdokumentovanie zmien je zodpovedné vždy konkrétne oddelenie ministerstva alebo odbor ministerstva. Správu systému META IS vykonáva oddelenie plánovania, organizácie a hodnotenia IT ministerstva. Správu IS CSRU a IS IOMO vykonáva oddelenie IT zdrojov verejnej správy ministerstva. Každá zmena s výnimkou informačných systémov , META IS, IS CSRU a IS IOMO, ktorá má alebo môže mať vplyv na bezpečnosť informačného systému na ministerstve, musí byť preskúmaná a schválená manažérom kybernetickej a informačnej bezpečnosti.

/3/ Manažér kybernetickej a informačnej bezpečnosti je oprávnený v procese hodnotenia zmien informačného systému požadovať od oddelenia informačných technológií ministerstva alebo tretej strany štúdiu uskutočniteľnosti, analýzu dopadov a odhad bezpečnostných rizík alebo analýzu bezpečnostných rizík tak, aby mohol konkrétnu zmenu posúdiť z pohľadu kybernetickej a informačnej bezpečnosti a rozhodnúť o jej implementácii.

/4/ O možnosti vplyvu zmeny na bezpečnosť informačného systému rozhodne manažér kybernetickej a informačnej bezpečnosti, ktorý môže určiť okruh zmien informačného systému, ktoré nebudú podliehať preskúmaniu z pohľadu kybernetickej a informačnej bezpečnosti ani jeho schváleniu.

/5/ Ak sa identifikuje bezpečnostné riziko v procese schvaľovania zmeny informačného systému, musia byť určené a implementované primerané bezpečnostné opatrenia na jeho minimalizáciu alebo musí byť požadovaná zmena vzhľadom na závažnosť rizika zamietnutá.

/6/ Bezpečnostné opatrenia na minimalizáciu identifikovaných rizík navrhuje oddelenie informačných technológií ministerstva po vykonaní odhadu rizík alebo analýzy rizík v spolupráci s organizačným útvarom ministerstva, ktorý zmenu informačného systému požaduje. Manažér kybernetickej a informačnej bezpečnosti posúdi identifikované bezpečnostné riziká a bezpečnostné opatrenia na ich elimináciu a rozhodne o implementácii zmeny.

/7/ Ak sú rozpory týkajúce sa bezpečnostných rizík pri zmenovom konaní, rozhoduje o implementácii zmeny bezpečnostný výbor ministerstva.

/8/ Pri prevádzke informačných systémov musia byť jednotlivé zodpovednosti oddelené tak, aby bola v čo najprijateľnejšej miere znížená možnosť ich zneužitia, neautorizovaného zásahu, zmeny alebo prístupu.

/9/ Zamestnanci zodpovední za výkon činností v informačných systémoch a službách nesmú zároveň byť aj schvaľovateľmi týchto činností alebo zamestnancami, ktorí zodpovedajú za kontrolu ich vykonania. Výnimky po analýze a následnom preskúmaní a pokrytí možných

bezpečnostných rizík navrhovanými bezpečnostnými opatreniami schvaľuje bezpečnostný výbor ministerstva.

/10/ Pri vývoji a testovaní informačných systémov musí byť prevádzkové prostredie vhodne oddelené od vývojového a testovacieho prostredia za účelom zamedzenia neoprávneného prístupu a zásahov do prevádzkovaných informačných systémov.

/11/ Podrobnosti procesu bezpečnosti pri správe a prevádzke informačných systémov na ministerstve ustanovuje interný riadiaci akt.[11])

Článok 17
Riadenie dodávky služieb poskytovaných tretími stranami

/1/ Zástupcovia zodpovedného organizačného útvaru ministerstva sú pri uzatváraní zmluvy s treťou stranou na dodávku informačného systému alebo služby povinní do zmluvy zahrnúť záväzky vyplývajúce z práv ochrany duševného vlastníctva a povinnosti z tejto smernice a z ďalších interných riadiacich aktov týkajúcich sa kybernetickej a informačnej bezpečnosti tak, aby platili pre všetkých zamestnancov tretej strany, ktorí budú pracovať s informačnými aktívami ministerstva.

/2/ Pred poskytnutím akýchkoľvek informácií týkajúcich sa informačného systému ministerstva vrátane žiadosti o návrh riešenia, musí byť s treťou stranou uzavretá dohoda o mlčanlivosti, ak nejde o výkon auditu podľa osobitných predpisov.

/3/ Bez dohody o mlčanlivosti nesmú byť poskytnuté tretej strane žiadne informácie týkajúce sa informačného systému ministerstva, požadovaných riešení alebo služieb. Výnimku tvoria všeobecne známe skutočnosti a informácie, ktoré nie sú predmetom mlčanlivosti.

/4/ Pri nákupe informačného systému alebo dodávke informačného systému a služieb od tretích strán musia byť bezpečnostné požiadavky a opatrenia určené v príslušnej dokumentácii už pri špecifikovaní technických požiadaviek. Bezpečnostné požiadavky a opatrenia sú uvedené na webovom sídle https://www.csirt.gov.sk/doc/Metodika_OPII_vRC1.0.pdf.

/5/ Informačné systémy a služby dodávané tretími stranami musia spĺňať všetky zásady a opatrenia ustanovené internými riadiacimi aktmi pre oblasť informačnej bezpečnosti.

/6/ Zamestnanci tretej strany, ktorí pracujú s informačnými aktívami ministerstva musia byť rovnako preukázateľne oboznámení s platnými bezpečnostnými zásadami a opatreniami. Záznam o tomto oboznámení zamestnancov musí byť súčasťou dokumentácie dodávaného informačného systému alebo služby.

[11]) Smernica vedúceho Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 9/2018 zo dňa 30. novembra 2018 o správe a prevádzke informačných systémov na Úrade podpredsedu vlády Slovenskej republiky pre investície a informatizáciu v znení Dodatku č. 1 zo dňa 13. mája 2020.

/7/ Za oboznamovanie tretích strán a ich zamestnancov s internými riadiacimi aktmi týkajúcimi sa informačnej bezpečnosti je zodpovedný vlastník informačného aktíva. Spôsob a formu oboznámenia určí manažér kybernetickej a informačnej bezpečnosti.

/8/ Dodávateľ alebo tretia strana musí prehlásiť znalosť a schopnosť implementovať bezpečnostné zásady a opatrenia ustanovené v interných riadiacich aktoch a v dokumentácii navrhovaného diela.

/9/ Výnimku z bezpečnostných požiadaviek a opatrení môže v odôvodnených prípadoch na žiadosť zadávateľa udeliť manažér kybernetickej a informačnej bezpečnosti. V prípade rozporu o udelenie výnimky rozhoduje bezpečnostný výbor ministerstva.

/10/ Výnimka z bezpečnostných požiadaviek a opatrení podľa odseku 9 je udelená výhradne na dobu pokiaľ trvajú dôvody, pre ktoré je požadovaná. Po uplynutí dôvodu je výnimka bezodkladne zrušená.

/11/ Udelenie výnimky podľa odseku 10 má písomnú formu a je súčasťou dokumentácie dodávaného diela alebo služby. Udelená výnimka musí obsahovať najmä

a) popis výnimky s odkazom na príslušné ustanovenie tejto smernice,
b) dôvod, prečo je výnimka udelená,
c) časové ohraničenie trvania výnimky najviac však po dobu 6 mesiacov,
d) osobu zodpovednú za zrušenie výnimky po uplynutí dôvodu, pre ktorý bola udelená.

/12/ Zachovávanie bezpečnostných opatrení v informačných systémoch a službách dodaných tretími stranami musí byť priebežne monitorované a kontrolované tretími stranami, ako aj ministerstvom. Prípadné nedostatky musí tretia strana odstrániť v čo najkratšej dobe.

/13/ Ak sa identifikujú nové bezpečnostné riziká pri dodávke informačného systému tretími stranami, musia byť určené bezpečnostné opatrenia na ich elimináciu.

/14/ Bezpečnostné opatrenia informačných systémov a služieb dodaných tretími stranami musia byť prehodnotené aj v prípade ich významnej zmeny. V prípade vzniku bezpečnostného rizika pri zmene informačného systému alebo služby musia byť treťou stranou dodatočne implementované bezpečnostné opatrenia eliminujúce zistené riziká.

/15/ Povinnosť určiť, implementovať, prevádzkovať a monitorovať bezpečnostné opatrenia je uvedená v zmluve s treťou stranou. Povinnosť určiť, implementovať, prevádzkovať a monitorovať bezpečnostné opatrenia na ochranu osobných údajov ministerstva spravovaných treťou stranou (tzv. sprostredkovateľ) je uvedená v zmluve s treťou stranou v samostatnej kapitole.

Článok 18
Plánovanie a akceptácia informačných systémov

/1/ Za účelom redukcie rizika neakceptovateľného výkonu alebo zlyhania informačných systémov je potrebné monitorovať kapacitu jednotlivých informačných systémov, zisťovať súlad s požiadavkami na ich výkon, ich kapacitné limity a na tomto základe plánovať a optimalizovať kapacity v dostatočnom predstihu. Za plánovanie, monitorovanie a optimalizáciu kapacít je zodpovedný organizačný útvar ministerstva, ktorý spravuje konkrétny informačný systém. V prípade IS CSRU a IS IOMO je za plánovanie, monitorovanie a optimalizáciu kapacít zodpovedné oddelenie riadenia IT zdrojov verejnej správy, v prípade META IS je to oddelenie plánovania, organizácie a hodnotenia IT ministerstva.

/2/ Pre každý nový informačný systém alebo službu sú v návrhu a dokumentácii uvedené a dohodnuté kritériá pre jeho akceptáciu. Nový informačný systém musí byť testovaný podľa dohodnutých akceptačných kritérií skôr, ako bude prijatý do prevádzky.

/3/ Súčasťou akceptačných kritérií musí byť aj preverenie implementácie dohodnutých bezpečnostných zásad a opatrení.

Článok 19
Ochrana proti škodlivému softvéru a kódu

/1/ Za účelom ochrany proti škodlivému kódu musí byť inštalovaný a pravidelne aktualizovaný antivírusový softvér na všetkých pracovných staniciach vrátane prenosných zariadení (notebooky) a všetkých systémoch s internetovými rozhraniami (najmä elektronická pošta, prístup na internet, webové sídlo).

/2/ Internetové rozhranie služby elektronickej pošty musí byť ochránené antispamovým softvérom.

/3/ Ak je identifikované riziko infiltrácie škodlivým kódom pri iných súčastiach informačného systému, ktoré nie sú uvedené v odseku 1, je nevyhnutné implementovať primerané bezpečnostné opatrenia na elimináciu tohto rizika.

/4/ Ak je akékoľvek podozrenie z infiltrácie škodlivým kódom, používatelia sú povinní skontrolovať všetky doručené, zaslané alebo inak sprístupnené súbory na prítomnosť škodlivého kódu prostredníctvom antivírusového softvéru. Ide najmä o súbory neznámeho pôvodu prijaté od neznámeho odosielateľa, o súbory skopírované alebo súbory prenášané na neznámom médiu.

/5/ Na ministerstve je povolené používať a inštalovať výhradne legálne zakúpený a ministerstvom schválený softvér.

/6/ Ustanovenie odseku 5 sa nevzťahuje na pomocný softvér (utilities) používaný pri správe

informačného systému. Pomocný softvér môže byť použitý výhradne v súlade s licenčnými podmienkami a takým spôsobom, aby neznižoval úroveň bezpečnosti informačného systému, služieb alebo ostatných prvkov informačných a komunikačných technológií. Za používanie, legálnosť a bezpečnosť pomocného softvéru je zodpovedný príslušný správca informačného systému, služby alebo prvku informačných a komunikačných technológií.

/7/ Voľne používateľný softvér (open-source) je možné inštalovať a používať iba po schválení manažérom kybernetickej a informačnej bezpečnosti v súlade s jeho licenčnými podmienkami.

/8/ Pre používanie mobilného kódu (napríklad ActiveX, Javascript) musia byť prijaté primerané reštriktívne opatrenia za účelom ochrany pred infiltráciou škodlivým kódom.

/9/ Pre používanie mobilného kódu sa vyžaduje, aby bol digitálne podpísaný, publikovaný a autentifikovaný dôveryhodným zdrojom.

/10/ Informačné systémy a pracovné stanice musia byť konfigurované tak, aby odolali všetkým všeobecne známym spôsobom zneužitia škodlivým kódom.

/11/Ochrana proti škodlivému kódu tvorí súčasť programu pre zvyšovanie bezpečnostného povedomia.

/12/Všetky infiltrácie škodlivým kódom alebo podozrenia z infiltrácie musia byť nahlásené manažérovi kybernetickej a informačnej bezpečnosti a zdokumentované ako bezpečnostný incident.

Článok 20
Zálohovanie

/1/ Na ministerstve je vykonávaná pravidelná záloha dát. Za týmto účelom je vypracovaná stratégia zálohovania dát, ktorá je v súlade

a) s osobitnými predpismi,
b) s požiadavkami na kontinuitu činností ministerstva,
c) s požiadavkami vlastníkov informačných aktív na ich dostupnosť.

/2/ Vlastníkom výsledku zálohovania vrátane dokumentácie je konkrétny vlastník informačného systému, dodávateľ informačného systému a manažér kybernetickej a informačnej bezpečnosti. V prípade META IS, IS CSRU a IS IOMO je vlastníkom procesu zálohovania Datacentrum.

/3/ Stratégia zálohovania obsahuje proces zálohovania v zložení

a) typ informácie, ktorý je zálohovaný,
b) plán vykonávania záloh pre konkrétne informácie alebo informačný systém,

c) manažment zálohovacích médií (retenčná perióda, zálohovacie cykly),
d) metóda zálohovania (vytváranie, validácia a označovanie záloh),
e) metóda pre validáciu obnovy informácií alebo informačného systému,
f) evidencia záložných médií.

/4/ Zálohovacie prostriedky a médiá musia byť zabezpečené bezpečnostnými opatreniami, ktorými sú najmä
a) šifrovanie médií,
b) používanie digitálneho podpisu,
c) fyzická bezpečnosť médií,
d) riadenie prístupu k médiám, skladovanie médií podľa podmienok určených výrobcom,
e) opatrenia na ochranu médií pri ich prenose.

/5/ Obnova vybraných dát zo zálohy musí byť testovaná podľa potreby, najmenej raz ročne.

Článok 21
Riadenie sietí

/1/ Za účelom ochrany sieťovej infraštruktúry, prenášaných informácií a prepojených informačných systémov a služieb musia byť na ministerstve realizované bezpečnostné opatrenia.

/2/ Za realizáciu bezpečnostných opatrení sieťovej infraštruktúry ministerstva je zodpovedné oddelenie informačných technológií ministerstva.

/3/ Bezpečnostné opatrenia sú určené na základe posúdenia bezpečnostných rizík, a to najmä ochrany
a) prenášaných informácií,
b) uchovávaných informácií (napríklad dočasných súborov, obsahu uloženého do medzipamätí - cache),
c) dizajnu sieťovej infraštruktúry,
d) informácií o konfigurácii sietí, sieťových zariadení, definícií kontroly prístupu, oprávnení, správcovských hesiel a kryptografických kľúčov,
e) sieťových ciest a trás,
f) sieťových zdrojov (napríklad šírky pásma),
g) hranice a obvodu siete,
h) rozhrania informačného systému do sietí.

/4/ Konfigurácia sieťových zariadení musí byť zdokumentovaná. Zmeny konfigurácie sieťových zariadení, definícií kontroly prístupu, smerovania a prihlasovacích údajov musia byť zdokumentované a kontrolované.

/5/ Na sieťových zariadeniach musia byť použité aspoň tieto bezpečnostné opatrenia
a) všetky prístupy a konfiguračné zmeny sieťových zariadení musia byť logované,
b) pre prístup musí byť použitý zabezpečený (šifrovaný) kanál, prípadne viacfaktorová

autentifikácia,
c) konfigurácie zariadení musia byť zálohované bezpečným spôsobom.

/6/ Ak sú na základe klasifikácie informačných aktív prenášané interné alebo chránené informácie alebo na základe posúdenia rizík iné citlivé údaje je nutné použiť šifrovanie dát, správ alebo trasy prenosu (SSH, SSL, TSL, VPN tunel a iné).

/7/ Pri používaní lokálnych bezdrôtových sietí (Wi-Fi sieť) musia byť použité aspoň tieto bezpečnostné opatrenia
a) silné šifrovanie WPA2,
b) silné heslo pre pripojenie (minimálne desať znakov),
c) autentifikácia používateľov.

/8/ Ak sa poskytuje bezdrôtová sieť (Wi-Fi) externým subjektom (napríklad konferencie, návštevy), musí byť bezdrôtová sieť oddelená od lokálnej počítačovej siete.

/9/ Na sieťových zariadeniach je nastavené logovanie a monitorovanie všetkých dôležitých udalostí, a to najmä nastavenie
a) sieťovej komunikácie odchádzajúcej mimo infraštruktúru ministerstva,
b) internej sieťovej komunikácie týkajúcej sa citlivých informácií a informačných systémov,
c) bezpečnostných incidentov na sieťových zariadeniach, ako napríklad prihlásenie a zmena konfigurácie,
d) bezpečnostných udalostí na systémoch poskytujúcich autentifikačné a autorizačné služby v sieťovej infraštruktúre.

/10/ Aktivity v informačných systémoch a počítačových sieťach ministerstva sú za účelom odhalenia možného bezpečnostného incidentu monitorované, analyzované a vyhodnocované prostredníctvom ďalších bezpečnostných zariadení (NIDS - Network Intrusion Detection System, SIEM - Security Information and Event Management).

/11/ Za monitorovanie sieťovej infraštruktúry je zodpovedné oddelenie informačných technológií ministerstva.

/12/ Ucelené bezpečnostné požiadavky a opatrenia sú uvedené na webovom sídle: https://www.csirt.gov.sk/doc/Metodika_OPII_vRC1.0.pdf.

Článok 22
Manipulácia s médiami, prenos, výmena informácií a používanie softvéru

/1/ Používanie prenosných médií (napríklad USB diskov, USB kľúčov) je na ministerstve povolené.

/2/ Pri používaní prenosných médií sú používatelia povinní zachovávať primerané bezpečnostné opatrenia, ktoré eliminujú riziko prezradenia, zneužitia alebo neautorizovaného prístupu k citlivým informáciám.

/3/ Bezpečnostnými opatreniami podľa odseku 2 sú najmä

a) ochrana média pred stratou alebo krádežou jeho bezpečným skladovaním a prenášaním,
b) externé prenosné médiá a informácie na nich uložené musia byť chránené šifrovaním s nastavením silného hesla minimálne desať alfanumerických znakov na otvorenie dokumentov,
c) používanie prenosných médií iba na dôveryhodných počítačoch.

/4/ Za dodržiavanie bezpečnostných opatrení podľa odseku 3, ako aj za prípadné škody spôsobené zneužitím, prezradením, neautorizovaným prístupom k informáciám uloženým na prenosných médiách zodpovedá ich používateľ.

/5/ Všetky nepotrebné prenosné médiá vo vlastníctve ministerstva musia byť zlikvidované bezpečným spôsobom tak, aby nebolo možné z týchto médií extrahovať žiadne citlivé informácie.

/6/ Za likvidáciu nepotrebných médií podľa odseku 5 je zodpovedné oddelenie informačných technológií ministerstva.

/7/ Pri manipulácii a prenose informácií sú dodržané bezpečnostné opatrenia. Bezpečnostné opatrenia sú uplatňované najmä pri

a) fyzickom prenose informácií (napríklad dokumentov),
b) emailovej komunikácii vrátane zasielania príloh,
c) elektronickom prenose,
d) prenose, zobrazovaní informácií v informačnom systéme,
e) používaní mobilných prostriedkov,
f) telefonickej komunikácii, vrátane zasielania správ,
g) faxovej komunikácii,
h) zasielaní rýchlych správ (napríklad Instant Messaging, chat).

/8/ Pri výmene alebo prenose informácií medzi ministerstvom a tretími stranami je vykonaný odhad možných bezpečnostných rizík a určené bezpečnostné opatrenia na ochranu prenášaných informácií.

/9/ Vlastník informačného aktíva uzavrie s treťou stranou zmluvu o prenose informácií, ktorá obsahuje ustanovenia o bezpečnostných opatreniach (technologických, procesných, personálnych), ktoré boli určené pre tento prenos, ako aj zodpovednosť za ich dodržiavanie.

/10/Ucelené bezpečnostné požiadavky a opatrenia sú uvedené na webovom sídle: https://www.csirt.gov.sk/doc/Metodika_OPII_vRC1.0.pdf.

Článok 23
Bezpečnostný monitoring

/1/ Pre umožnenie kontroly prístupov, monitoringu činností, vyšetrovania bezpečnostných incidentov sú na všetkých systémoch informačných a komunikačných technológií

ministerstva, vrátane pracovných staníc, vytvárané auditné log záznamy, v ktorých sa zaznamenáva dátum a presný čas s informáciami o

a) aktivitách správcov systémov, administrátorov,
b) prihlasovaní a odhlasovaní používateľov,
c) činnosti systému vrátane chýb a zlyhaní,
d) neúspešných pokusoch o prihlásenie do systémov,
e) iných bezpečnostne relevantných udalostiach.

/2/ Súbory s log záznamami informačných systémov a služieb sú uložené mimo informačných systémov a služieb, ktoré ich vytvárajú pre ich zachovanie v prípade kompromitácie informačného systému alebo služby, ich znefunkčnenia alebo neoprávnenej modifikácie lokálnych log záznamov.

/3/ Prístup k úložisku log záznamov majú iba zamestnanci za uplatnenia princípu rozdelenia právomocí a zodpovedností podľa čl. 16 ods. 8 a 9.

/4/ Používanie informačných systémov a služieb je monitorované oddelením informačných technológií ministerstva za účelom zistenia nežiaducich, neautorizovaných činností alebo iných bezpečnostne relevantných udalostí.

/5/ Oddelenie informačných technológií ministerstva pravidelne vyhodnocuje výstupy z bezpečnostného monitoringu a zároveň odstraňuje zistené nedostatky alebo vyhodnotené výstupy označí a spracuje ako bezpečnostný incident.

/6/ Pre zabezpečenie jednotnosti, jednoznačnosti, správnosti bezpečnostného monitoringu, vyšetrovania bezpečnostných incidentov a získavania relevantných dôkazov je na všetkých informačných systémoch a službách synchronizovaný čas prostredníctvom jednotného zdroja presného času.

/7/ Podrobnosti vytvárania auditných log záznamov a monitorovania pre systémy META IS, IS CSRU a IS IOMO ustanoví dodávateľ konkrétneho informačného systému v rámci aktuálne platnej rámcovej dohody na poskytovanie služieb systémovej a aplikačnej podpory informačných systémov.

/8/ Ucelené bezpečnostné požiadavky a opatrenia sú uvedené na webovom sídle: https://www.csirt.gov.sk/doc/Metodika_OPII_vRC1.0.pdf.

Článok 24
Riadenie prístupu

/1/ Prístup ku všetkým informačným systémom a službám ministerstva je udeľovaný výhradne na základe štátnozamestnaneckého pomeru, pracovného pomeru alebo obdobného pracovnoprávneho vzťahu s ministerstvom.

/2/ Pri prideľovaní prístupových práv sa postupuje v súlade so zásadou najmenších možných privilégií (need to know).

/3/ Pre prideľovanie, zmenu a zrušenie prístupových práv musí byť určený formálny proces, v rámci ktorého prístupové práva podliehajú schváleniu vlastníkom informačného systému alebo služby a nadriadeným zamestnancom, v prípade tretích strán zodpovedným zamestnancom ministerstva podľa čl. 17 ods. 6 a 7 a manažérom kybernetickej a informačnej bezpečnosti súčasne.

/4/ Každý používateľ musí mať zriadený vlastný používateľský účet. Používanie cudzieho používateľského účtu alebo používanie jedného používateľského účtu viacerými používateľmi je zakázané.

/5/ Vytváranie privilegovaných prístupov musí byť kontrolované. Privilegované prístupy na pracovných staniciach a privilegované prístupy tretích strán musia byť preskúmané a schválené manažérom kybernetickej a informačnej bezpečnosti.

/6/ Používateľské heslá používané v informačných systémoch a službách ministerstva sú dostatočne silné a spĺňajú tieto požiadavky:

a) dĺžka hesla je minimálne desať znakov,
b) heslo je jedinečné, je zakázané jeho opätovné použitie v iných informačných systémoch,
c) pri vytváraní hesla sú použité veľké písmená, malé písmená a minimálne dve číslice, pričom číslice nesmú nasledovať po sebe vzostupne alebo zostupne,
d) heslo nie je zhodné s užívateľským menom alebo vytvorené napríklad z vlastného mena, priezviska, mena blízkeho príbuzného, emailovej adresy, mena obľúbeného zvieraťa, dátumu narodenia a podobne jednoducho odhaliteľných slov,
e) heslo je zmenené najmenej každých 90 dní,
f) pri zmene hesla nie je použitých desať predchádzajúcich hesiel.

/7/ Pre systémy META IS, IS CSRU a IS IOMO na základe samostatne stanovených pravidiel môžu byť používateľské heslá modifikované v rámci bezpečnostných dokumentov prislúchajúcich systémov META IS, IS CSRU a IS IOMO.

/8/ Používateľské heslá sú uložené v informačných systémoch takým spôsobom, aby ich nebolo možné prečítať, skopírovať alebo zneužiť.

/9/ Používateľské heslo vrátane jeho zmeny alebo jeho znovunastavenie (reset hesla) sa poskytuje používateľovi bezpečným spôsobom. Ak sa použije inicializačné heslo, používateľ je povinný ho po jeho prvom použití okamžite zmeniť, tak aby samotné heslo poznal výlučne iba on sám.

/10/ Používateľské prístupy a heslá štandardne nastavené na zariadeniach výrobcami sú po uvedení zariadení do prevádzky v informačných a komunikačných technológiách ministerstva okamžite zmenené alebo zablokované.

/11/ Prístupové práva používateľov musia byť preskúmané minimálne jedenkrát za rok alebo pri každej väčšej zmene informačných a komunikačných technológií ministerstva. Za preskúmanie prístupových práv je zodpovedný vlastník informačného systému.

/12/ Proces prideľovania, zmeny a odoberania používateľských prístupov a hesiel ustanoví oddelenie informačných technológií ministerstva.

/13/ Používatelia informačných systémov a služieb musia zaobchádzať s informačnými prostriedkami bezpečne tak, aby minimalizovali riziko zneužitia, krádeže alebo neoprávneného prístupu.

Článok 25
Riadenie prístupu do počítačovej siete

/1/ Na ministerstve môžu byť povolené iba služby počítačovej siete, ktoré sú nevyhnutné pre jednotlivé činnosti a plnenie úloh ministerstva.

/2/ Prístup do počítačovej siete ministerstva je povolený iba autorizovaným a schváleným subjektom teda používateľom, informačným systémom a službám. Prístup autorizovaných subjektov musí byť riadený a kontrolovaný prostredníctvom zariadení počítačovej siete ministerstva.

/3/ Za účelom blokovania nežiaducej prichádzajúcej, odchádzajúcej komunikácie, neautorizova nému prístupu (hacking) a blokovania škodlivého kódu musia byť všetky prípojné body, rozhrania počítačovej siete ministerstva do siete internet ochránené sieťovými zariadeniami na filtrovanie a kontrolu sieťovej prevádzky (firewall).

/4/ Povolenie prístupu do počítačovej siete alebo zmeny prístupu a zmeny dizajnu počítačovej siete ministerstva autorizuje a schvaľuje manažér kybernetickej a informačnej bezpečnosti.

/5/ Riadenie prístupu a dizajn počítačovej siete ministerstva musí byť riadne zdokumentovaný a dokumentácia priebežne aktualizovaná.

/6/ Vzdialený prístup do siete ministerstva je povolený výhradne prostredníctvom šifrovaného spojenia (VPN tunel). Pre povolenie vzdialeného prístupu musí existovať formálny proces.

/7/ Na všetkých zariadeniach počítačovej siete ministerstva, najmä na zariadeniach pre riadenie smerovania v sieťach, autorizáciu prístupu, ochranu a filtrovanie sieťovej prevádzky (firewall) musia byť aplikované primerané bezpečnostné opatrenia za účelom eliminácie rizika neautorizovaného prístupu a ich zneužitia. Za implementáciu bezpečnostných opatrení na týchto zariadeniach zodpovedajú ich správcovia.

/8/ Jednotlivé skupiny používateľov, informačných systémov, služieb a zariadení (napríklad používatelia pracovných staníc, zastupiteľské úrady, servery informačných systémov) musia byť v sieti ministerstva oddelené na logickej alebo fyzickej úrovni do vyhradených a

vzájomne oddelených segmentov siete. Prevádzka medzi jednotlivými segmentmi počítačovej siete musí byť riadená a filtrovaná.

Článok 26
Riadenie prístupu do operačného systému

Pre operačné systémy používané na ministerstve musia byť určené primerané bezpečnostné opatrenia

a) operačné systémy musia byť nakonfigurované podľa bezpečnostných praktík (hardening),
b) prihlasovacie procedúry do operačných systémov musia byť bezpečné,
c) každý používateľ musí mať unikátne používateľské meno a používateľské heslo,
d) operačný systém musí presadzovať určenú politiku hesiel (napríklad ich dĺžka, komplexnosť, zložitosť, zmena),
e) používatelia musia mať nastavené čo najnižšie možné používateľské privilégiá, musí byť nastavené automatické zablokovanie alebo zamknutie operačného systému po uplynutí ustanoveného času, ktorý je štandardne 15 minút.

Článok 27
Riadenie prístupu k aplikáciám a informáciám

/1/ Používateľské informácie v informačných systémoch a službách ministerstva musia byť ukladané do takej štruktúry, aby nebolo možné získať prístup k dátam iného používateľa.

/2/ Pre systémy, ktoré sú obzvlášť kritické pre plnenie úloh a nepodliehajú inému režimu prevádzkovania podľa osobitného predpisu,[1]) musia byť prijaté dodatočné bezpečnostné opatrenia.

Článok 28
Mobilné počítačové spracúvanie a práca na diaľku

/1/ Pre použitie mobilných prostriedkov pre počítačové spracovanie (napríklad mobilné telefóny, notebooky, tablety) musia byť určené primerané bezpečnostné opatrenia, ktorými sú najmä

a) ochrana mobilných prostriedkov pred stratou, krádežou a neoprávneným používaním,
b) ochrana uložených informácií šifrovaním,
c) blokovanie alebo zamknutie systému mobilného prostriedku pri jeho prenose,
d) nastavenie automatického zablokovania zariadenia pri nečinnosti,
e) používanie dôveryhodných prístupových bodov do internetu,
f) používanie pravidelne aktualizovaného antivírusového softvéru,
g) bezpečné používanie a kontrola prenosných médií.

/2/ Pre prácu na diaľku používatelia dodržiavajú bezpečnostné opatrenia uvedené v odseku 1 a pre vzdialené pripojenie používajú iba schválený mobilný prostriedok a spôsob pripojenia.

Článok 29
Bezpečnostné požiadavky na informačné systémy

/1/ Pri akvizícii, vývoji alebo údržbe informačných systémov a služieb musí byť pri ich plánovaní, ako aj v procese realizácie vykonaný odhad alebo analýza bezpečnostných rizík, ktorých účelom je identifikovať bezpečnostné riziká a určiť bezpečnostné opatrenia na ich elimináciu.

/2/ Odhad alebo analýzu rizík vykoná oddelenie informačných technológií ministerstva alebo tretia strana v spolupráci s manažérom kybernetickej a informačnej bezpečnosti a vlastníkom informačného systému alebo služby. Oddelenie informačných technológií ministerstva navrhne bezpečnostné opatrenia na elimináciu zistených rizík. Pre systémy, META IS, IS CSRU a IS IOMO analýzu rizík vykoná príslušný organizačný útvar ministerstva určený manažérom kybernetickej a informačnej bezpečnosti v spolupráci s treťou stranou alebo s manažérom kybernetickej a informačnej bezpečnosti.

/3/ Za koordináciu identifikácie rizík, určenie a schválenie bezpečnostných opatrení pri akvizícii, vývoji a údržbe informačného systému je zodpovedný manažér kybernetickej a informačnej bezpečnosti.

/4/ Bezpečnostné opatrenia vo forme bezpečnostných požiadaviek musia byť zapracované do projektovej dokumentácie alebo zadania tretej strane a musia byť súčasťou akceptačného testovania informačného systému alebo služby. Za zapracovanie bezpečnostných požiadaviek je zodpovedný vlastník informačného aktíva.

/5/ Interná štruktúra spracovania, vstupné a výstupné funkcie aplikácií, informačných systémov a služieb ministerstva musia byť navrhnuté a vytvorené tak, aby bol proces spracovania informácií v týchto systémoch bezpečný, a aby sa vylúčilo riziko

a) chybného spracovania,
b) prerušenia prevádzky,
c) neoprávneného prístupu,
d) zneužitia a úniku informácií alebo
e) inej kompromitácie systému.

/6/ Zmeny vykonávané na informačných systémoch a službách ministerstva musia byť vykonávané na základe formálneho postupu, ktorý okrem dokumentácie zmeny musí vyžadovať odhad alebo analýzu bezpečnostných rizík a schválenie zmeny manažérom kybernetickej a informačnej bezpečnosti.

/7/ Za účelom odstránenia zraniteľností musia byť na všetkých informačných systémoch vrátane pracovných staníc ministerstva aplikované bezpečnostné záplaty publikované výrobcom. Za aplikáciu bezpečnostných záplat zodpovedajú správcovia jednotlivých informačných systémov.

Článok 30
Riadenie incidentov kybernetickej a informačnej bezpečnosti

/1/ Zamestnanci, ako aj zamestnanci tretích strán, ktorí pri svojej činnosti vytvárajú, spravujú alebo inak využívajú informačné systémy a služby ministerstva, sú povinní hlásiť manažérovi kybernetickej a informačnej bezpečnosti všetky bezpečnostné incidenty, podozrenia alebo bezpečnostne relevantné udalosti, ktoré môžu byť príčinou bezpečnostného incidentu, o ktorých sa dozvedeli pri svojej pracovnej alebo inej činnosti.

/2/ Na ministerstve musí byť vypracovaný proces zvládania bezpečnostných incidentov, ktorý musí obsahovať najmä

a) spôsob nahlasovania a evidencie bezpečnostných incidentov,
b) evidenciu bezpečnostných incidentov a všetkých relevantných dôkazov,
c) zoznam zodpovedných osôb a vedúcich zamestnancov,
d) zoznam osôb zodpovedných za riešenie bezpečnostných incidentov podľa jednotlivých oblastí s uvedením kontaktných informácií.

/3/ Manažér kybernetickej a informačnej bezpečnosti pravidelne vyhodnocuje bezpečnostné incidenty, minimálne raz za šesť mesiacov, za účelom prehodnotenia a zmeny bezpečnostných opatrení tak, aby opakovane nedochádzalo k obdobným bezpečnostným incidentom.

/4/ V prípade závažného bezpečnostného incidentu musí manažér kybernetickej a informačnej bezpečnosti vykonať prehodnotenie a zmenu bezpečnostných opatrení bez zbytočného odkladu.

/5/ Za proces riešenia bezpečnostných incidentov je zodpovedný manažér kybernetickej a informačnej bezpečnosti.

Článok 31
Riadenie kontinuity činnosti

/1/ Za účelom predchádzania nežiaducim výpadkom a prerušeniam činností ministerstva musí byť zavedený proces riadenia kontinuity činnosti. Pre zavedenie procesu riadenia kontinuity činnosti musí byť vykonaná a priebežne aktualizovaná analýza dopadov za účelom identifikácie kritických informačných systémov a služieb ministerstva.

/2/ Za určenie a hodnotenie dopadov výpadkov alebo prerušení činnosti informačných systémov alebo služieb je zodpovedný vlastník informačného aktíva.

/3/ Pre informačné systémy a služby ministerstva identifikované v analýze dopadov ako kritické musia byť vypracované detailné plány obnovy, ktoré znížia dopady výpadkov na minimálnu úroveň.

/4/ Proces a stratégiu riadenia kontinuity činnosti metodicky riadi manažér kybernetickej a

informačnej bezpečnosti.

/5/ Za vypracovanie plánov obnovy je zodpovedný správca informačného aktíva.

Článok 32
Súlad s legislatívnymi požiadavkami

/1/ Pri prevádzke informačných systémov a služieb ministerstva musia byť identifikované všetky povinnosti vyplývajúce z osobitných predpisov a zmluvných vzťahov týkajúcich sa informačných systémov a služieb.

/2/ Pre informačné systémy a služby musia byť v zmluvných vzťahoch s tretími stranami jasne definované práva a povinnosti najmä v oblastiach kybernetickej bezpečnosti, ochrany osobných údajov a práv duševného vlastníctva.

Článok 33
Súlad s politikou kybernetickej a informačnej bezpečnosti a bezpečnostnými štandardami a audit

/1/ Súlad stavu kybernetickej a informačnej bezpečnosti s politikou kybernetickej a informačnej bezpečnosti a bezpečnostnými štandardami musí byť pravidelne preverovaný vedúcimi zamestnancami a najmenej jedenkrát ročne manažérom kybernetickej a informačnej bezpečnosti.

/2/ Pre zaistenie efektivity bezpečnostných opatrení a primeraného zabezpečenia informačných a komunikačných technológií musí byť vykonané nezávislé hodnotenie kybernetickej a informačnej bezpečnosti formou bezpečnostného auditu najmenej každé tri roky alebo vždy pri významných zmenách informačných a komunikačných technológií ministerstva.

/3/ Za účelom identifikácie zraniteľností informačných systémov a služieb ministerstva musí byť vykonané interné a externé zisťovanie zraniteľností prostredníctvom automatických nástrojov najmenej raz ročne.

/4/ Automatická identifikácia zraniteľností môže byť vykonaná interne alebo treťou stranou. Za koordináciu identifikácie zraniteľností je zodpovedný manažér kybernetickej a informačnej bezpečnosti.

Článok 34
Porušenie služobnej a pracovnej disciplíny

/1/ Za závažné porušenie služobnej disciplíny alebo pracovnej disciplíny v oblasti kybernetickej a informačnej bezpečnosti je považované najmä

a) umožnenie prístupu neautorizovanej osobe alebo zverejnenie citlivých informácií, s ktorými sa zamestnanec oboznámil pri plnení služobných alebo pracovných úloh (napríklad poskytnutie strategických dokumentov, zámerov alebo iných neverejných

informácií osobe, ktorá nie je v štátnozamestnaneckom, pracovnom alebo obdobnom pracovnoprávnom vzťahu s ministerstvom) alebo ich zverejnenie, ak neboli zverejnené odborom komunikácie ministerstva alebo sprístupnené podľa osobitného predpisu,[12])

b) vykonanie neautorizovaných zmien údajov v informačných systémoch so závažným následkom (napríklad úmyselné pozmenenie účtovných údajov),

c) sprístupnenie prihlasovacích údajov alebo prostriedkov (napríklad certifikátov) inej osobe alebo použitie prihlasovacích údajov inej osoby a spôsobenie závažného následku (napríklad poskytnutie vlastného používateľského mena a hesla osobe, ktorej nebol prístup do informačného systému schválený alebo prihlasovanie sa pod iným používateľským menom a heslom do informačného systému, do ktorého prístup nebol schválený),

d) zneužitie vlastných privilegovaných prístupových oprávnení na vykonanie neautorizovaných zmien, neoprávneného prístupu, neschválených bezpečnostných alebo iných nastavení v informačných systémoch, serveroch a ostatných prvkoch informačno-komunikačnej infraštruktúry ministerstva (napríklad zneužitie vyšších oprávnení pre vykonanie svojvoľných zmien v informačnom systéme, alebo databáze bez schválenia oprávnenou osobou, vypnutie antivírusového programu a spôsobenie zavírenia a nedostupnosti celej počítačovej siete ministerstva),

e) umožnenie prístupu neautorizovanej tretej osobe do komunikačnej infraštruktúry ministerstva (napríklad umožnenie pripojenia do vnútornej siete osobe, ktorá nemá oprávnenie pripojiť sa vlastným notebookom a spôsobenie zavírenia a odstávky počítačovej siete, neoprávnený zber informácií a údajov ministerstva),

f) neoprávnené, alebo vopred neschválené zhromažďovanie, spracovávanie, alebo prenos informácií z komunikačnej infraštruktúry ministerstva (napríklad neschválené monitorovanie prevádzky počítačovej siete, zachytávanie cudzej emailovej, alebo inej komunikácie, obídenie ochrany a vytvorenie nekontrolovaného kanálu na prenášanie informácií smerom von z počítačovej siete ministerstva),

g) úmyselné dlhodobé znefunkčnenie alebo poškodenie informačného systému, služby alebo nenávratné poškodenie významných dát potrebných pre plnenie úloh a činností ministerstva (napríklad úmyselné zmazanie dôležitých dokumentov a materiálov alebo fyzické zničenie pracovnej stanice).

/2/ Za menej závažné porušenie služobnej disciplíny alebo pracovnej disciplíny sa považuje také porušenie služobnej disciplíny alebo pracovnej disciplíny, ktoré nie je porušením služobnej disciplíny alebo pracovnej disciplíny podľa odseku 1.

Článok 35
Revízia politiky kybernetickej a informačnej bezpečnosti ministerstva

/1/ Táto smernica sa upraví vždy, keď sa zmení akákoľvek časť podporujúca niektorý zo základných procesov ministerstva, najmä strategický zámer, bezpečnostné ciele, štruktúra ministerstva, aktíva ministerstva a ich štruktúra. Na vykonanie revízie vydá pokyn generálny

[12]) Zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov.

tajomník služobného úradu manažérovi kybernetickej a informačnej bezpečnosti, ktorý zabezpečí revíziu politiky kybernetickej a informačnej bezpečnosti ministerstva.

/2/ Revízia tejto smernice sa vykonáva minimálne raz ročne alebo v prípadoch, ak sa zmení akákoľvek časť podporujúca niektorý zo základných procesov ministerstva.

/3/ Dôvodom na vykonanie mimoriadnej revízie môžu byť aj navrhované opatrenia pri zistených nedostatkoch z interného alebo externého auditu alebo šetrenia bezpečnostného incidentu na kritické aktíva ministerstva.

ŠTVRTÁ ČASŤ
ZÁVEREČNÉ USTANOVENIA

Článok 36
Zrušovacie ustanovenie

Zrušuje sa Smernica vedúceho Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 7/2018 zo dňa 30. novembra 2018 o politike informačnej bezpečnosti v znení Dodatku č. 1 zo dňa 14. mája 2020.

Článok 37
Účinnosť

Táto smernica nadobúda účinnosť 07. októbra 2021.

Veronika Remišová
ministerka investícií, regionálneho rozvoja
a informatizácie