SMERNICA
7/2020
MINISTERSTVA SPRAVODLIVOSTI SLOVENSKEJ REPUBLIKY

z 20. apríla 2020

č. 20712/2020/91-17730

o bezpečnostnej politike Ministerstva spravodlivosti Slovenskej republiky

Ministerstvo spravodlivosti Slovenskej republiky (ďalej len „ministerstvo“) na účely zabezpečenia primeranej bezpečnosti svojich informačných aktív ustanovuje:

Čl. 1
Predmet úpravy a rozsah pôsobnosti

(1) Táto smernica upravuje bezpečnostnú politiku v rezorte ministerstva. Cieľom bezpečnostnej politiky je vytvorenie základného rámca pre zaistenie bezpečnosti informačných aktív ministerstva na objektovej, personálnej, organizačnej, počítačovej, administratívnej a komunikačnej úrovni.

(2) Táto smernica sa vzťahuje na
a) ministerstvo,
b) okresné súdy, krajské súdy a Špecializovaný trestný súd (ďalej len „súdy“),
c) Centrum právnej pomoci,
d) Justičnú akadémiu Slovenskej republiky.

(3) Táto smernica sa nevzťahuje na utajované skutočnosti.

Čl. 2
Všeobecné ustanovenie

Ministerstvo vydaním tejto smernice presadzuje stratégiu zabezpečenia informačnej bezpečnosti ako neoddeliteľnej súčasti všetkých riadiacich procesov, uvedomujúc si finančné a personálne náklady s tým spojené.

Čl. 3
Vymedzenie pojmov

Na účely tejto smernice sa rozumie
a) informačným systémom zariadenie alebo skupina navzájom prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré automaticky spracúvajú počítačové údaje,
b) počítačovým údajom zastúpenie skutočností, informácií alebo pojmov vo forme vhodnej na spracovanie v informačnom systéme,

c) informačným aktívom hmotné aktívum alebo nehmotné aktívum, ktoré je súčasťou informačných systémov alebo technológií, najmä údaje vrátane osobných údajov, informácie, databázy údajov, dokumentácia, prostriedky spracúvania údajov, poskytované služby a ďalšie informácie, ktoré považuje ministerstvo za dôležité, dôverné alebo citlivé,
d) bezpečnostným opatrením technický prvok, personálny prvok alebo administratívny prvok ochrany, ktorého účelom je udržiavať bezpečný a spoľahlivý výkon bezpečnostnej politiky,
e) dostupnosťou pomer celkového času z celého časového intervalu, počas ktorého možno funkčnú jednotku (systém, údaj, služba a pod.) používať, k celému zvolenému časovému intervalu; dostupnosť zaručuje, že informačné aktívum bude na požiadavku používateľa prístupné a schopné použitia,
f) dôvernosťou ochrana počítačových údajov proti zneužitiu, odpočúvaniu alebo čítaniu neoprávnenými osobami; zachovanie dôvernosti znamená, že prístup k aktívu je povolený len určenej skupine používateľov,
g) integritou konzistencia komponentov a dát obsiahnutých v informačných systémoch a technológiách a ich zhoda so skutočným stavom; zachovanie integrity znamená, že informačné aktíva neboli zmenené neautorizovaným alebo náhodným spôsobom,
h) kritickým informačným systémom každý informačný systém poskytujúci dostupnosť 24/7 (24 hodín denne, 7 dní v týždni s definovaným časom plánovaného výpadku) alebo informačný systém poskytujúci služby verejnosti alebo informačný systém obsahujúci osobné údaje alebo podporný informačný systém alebo technológie, nevyhnutné na zabezpečenie dostupnosti 24/7 pre iné kritické informačné systémy a technológie,
i) informačnou bezpečnosťou bezpečnosť informačných systémov, informačných technológií, ochrana informácií, ktoré sú v nich uchovávané, spracovávané a prenášané,
j) narušením informačnej bezpečnosti najmä útok na informačné systémy alebo technológie, neoprávnená manipulácia s informáciami, únik osobných údajov, zneužitie informačných systémov alebo technológií na neoprávnené účely, neoprávnený prístup k údajom, neautorizovaná zmena údajov, zníženie dostupnosti alebo výpadok informačného systému alebo technológií,
k) auditným záznamom záznam o prevádzke, prístupoch používateľov alebo o zmenách informačného systému alebo technológie,
l) auditným údajom podmnožina auditného záznamu,
m) prostriedkom spracúvania údajov akýkoľvek systém alebo infraštruktúra spracúvania údajov vrátane fyzických priestorov, v ktorých sa tieto prostriedky nachádzajú,
n) spracúvaním údajov vykonávanie operácií alebo súboru operácií s údajmi, najmä ich prehliadanie, vyhodnocovanie, kopírovanie, modifikácia, uchovávanie, prenos v elektronickej podobe alebo inej podobe a ich likvidácia.

Čl. 4
Systém riadenia informačnej bezpečnosti

Systém riadenia informačnej bezpečnosti sa uplatňuje
a) pri plnení všetkých úloh, pri ktorých je nevyhnutné zabezpečiť vysokú ochranu informačných aktív,
b) na všetky prevádzkované informačné aktíva až po ich hraničné zariadenia na komunikáciu s externým prostredím.

Čl. 5
Štruktúra systému riadenia informačnej bezpečnosti

(1) Architektúra systému riadenia informačnej bezpečnosti vychádza z organizačnej štruktúry a organizačného poriadku ministerstva, súdov a organizácií v pôsobnosti ministerstva.

(2) Systém riadenia informačnej bezpečnosti je definovaný a presadzovaný touto smernicou a kontrolou jej dodržiavania na všetkých riadiacich úrovniach ministerstva, súdov a organizácií v pôsobnosti ministerstva.

(3) Metodické pokyny[1]) a prevádzková dokumentácia k informačným systémom a technológiám musia byť v súlade s touto smernicou a upravujú ďalšie bezpečnostné požiadavky a opatrenia najmä v oblastiach

a) personálnej bezpečnosti v oblasti informačnej bezpečnosti,
b) riadenia informačných aktív,
c) riadenia prístupov k informačným systémom a technológiám,
d) šifrovania a kryptografie informačných aktív,
e) fyzickej bezpečnosti a bezpečnosti prostredia informačných systémov a technológií,
f) bezpečnosti prevádzky informačných systémov a technológií,
g) akvizície, vývoja a údržby informačných systémov a technológií,
h) riadenia vzťahov s dodávateľmi informačných systémov a technológií,
i) riadenia narušení informačnej bezpečnosti,
j) informačnej bezpečnosti v riadení kontinuity prevádzky informačných systémov a technológií.

Čl. 6
Komisia pre riadenie informačnej bezpečnosti

(1) Na zabezpečenie systému riadenia informačnej bezpečnosti sa zriaďuje komisia pre riadenie informačnej bezpečnosti (ďalej len „komisia“).

(2) Komisia je poradným orgánom ministra.

(3) Komisia najmä

a) vyjadruje sa k návrhom na revíziu tejto smernice, návrhom metodických pokynov v oblasti informačnej bezpečnosti,
b) vyhodnocuje ciele vyplývajúce z tejto smernice a navrhuje opatrenia a postupy na zvýšenie a udržanie primeranej informačnej bezpečnosti, najmä pri zásadných zmenách v informačných systémoch a technológiách,
c) prerokúva výročnú správu o stave informačnej bezpečnosti, ktorú vypracúva sekcia informatiky a riadenia projektov,
d) vyjadruje sa k dokumentom týkajúcim sa informačnej bezpečnosti kritických informačných systémov a technológií ministerstva, súdov a organizácií v pôsobnosti ministerstva,
e) zriaďuje pracovné skupiny na účely zabezpečenia nevyhnutných alebo operatívnych úloh v oblasti informačnej bezpečnosti a kontroluje ich činnosť,

---

[1]) Čl. 4 ods. 6 inštrukcie 1/2006 Ministerstva spravodlivosti Slovenskej republiky z 9. marca 2012 č. 15584/2012/110, ktorou sa mení a dopĺňa inštrukcia 1/2006 Ministerstva spravodlivosti Slovenskej republiky z 2. januára 2006 č. 101/2006-53 o príprave, evidencii a publikovaní interných riadiacich aktov.

f) prijíma riziká v informačných aktívach identifikované pri hodnotení stavu informačnej bezpečnosti.

(4) Komisia pozostáva z

a) predsedu komisie, ktorým je generálny tajomník služobného úradu,
b) podpredsedu komisie, ktorým je generálny riaditeľ sekcie informatiky a riadenia projektov,
c) tajomníka komisie, ktorým je riaditeľ odboru informačnej bezpečnosti,
d) ďalších členov, ktorými sú
   1. riaditeľ odboru prevádzky informačných systémov ministerstva,
   2. zástupcovia krajských súdov a Špecializovaného trestného súdu,
   3. generálny riaditeľ sekcie edičných činností,
   4. zástupca Centra právnej pomoci,
   5. zástupca Justičnej akadémie Slovenskej republiky.

(5) Predsedu komisie v čase jeho neprítomnosti zastupuje podpredseda komisie.

(6) Komisia zasadá aspoň dvakrát do roka a vždy, keď mimoriadne zasadnutie komisie zvolá predseda komisie. Komisia je uznášaniaschopná, ak je prítomná nadpolovičná väčšina všetkých jej členov; na prijatie uznesenia je potrebný súhlas nadpolovičnej väčšiny prítomných členov komisie.

Čl. 7
Bezpečnostné role ministerstva, súdov a organizácií v pôsobnosti ministerstva

(1) Na zabezpečenie úloh súvisiacich s riadením informačnej bezpečnosti sa zriaďujú bezpečnostné role, pridelené vybraným zamestnancom na základe organizačnej štruktúry ministerstva, súdov a organizácií v pôsobnosti ministerstva. Zriadením týchto bezpečnostných rolí sa nerozširujú pracovné úlohy a oprávnenia dotknutých zamestnancov. Bezpečnostné role sú:

a) osoba zodpovedná za oblasť informačnej bezpečnosti ministerstva je riaditeľ odboru informačnej bezpečnosti,
b) špecialista na posudzovanie stavu informačnej bezpečnosti v informačných systémoch a technológiách (ďalej len „interný špecialista“) je zamestnanec odboru informačnej bezpečnosti,
c) osoba zodpovedná za oblasť informačných systémov a technológií je poverený zamestnanec odboru prevádzky informačných systémov a vedúci oddelenia informatiky súdov a organizácií v pôsobnosti ministerstva,
d) správca informačných systémov je poverený zamestnanec odboru prevádzky informačných systémov alebo poverený zamestnanec oddelenia informatiky súdu,
e) bezpečnostný správca je poverený zamestnanec odboru informačnej bezpečnosti,
f) osoba zodpovedná za informačné aktíva je generálny riaditeľ sekcie ministerstva alebo riaditeľ samostatného organizačného útvaru ministerstva, riaditeľ správy súdu alebo riaditeľ organizácie v pôsobnosti ministerstva,
g) vlastník informačného aktíva je správca informačných systémov alebo bezpečnostný správca alebo vedúci zamestnanec na úrovni odboru poverený prevádzkou špecifickej aplikácie v zodpovednosti odboru,
h) používateľmi informačného aktíva sú všetci zamestnanci ministerstva, súdov a organizácií v pôsobnosti ministerstva a používatelia služieb e-Governmentu.

(2) Osoba zodpovedná za oblasť informačnej bezpečnosti ministerstva

a) navrhuje, pripravuje a presadzuje bezpečnostnú politiku organizácie,
b) vykonáva činnosti podľa organizačného poriadku ministerstva,
c) vypracúva výročnú správu o stave informačnej bezpečnosti,
d) zabezpečuje vypracúvanie a aktualizáciu interných riadiacich aktov v oblasti informačnej bezpečnosti,
e) kontroluje dodržiavanie informačnej bezpečnosti, koordinuje systém riadenia informačnej bezpečnosti a overuje a hodnotí súlad praktického stavu informačnej bezpečnosti ministerstva s pravidlami uvedenými v tejto smernici.

(3) Interný špecialista je zodpovedný za výkon kontroly v oblasti informačnej bezpečnosti.

(4) Osoba zodpovedná za oblasť informačných systémov a technológií

a) plní ciele tejto smernice, zabezpečuje súlad praktického stavu informačnej bezpečnosti s cieľmi a zásadami definovanými v tejto smernici, poskytuje súčinnosť osobe zodpovednej za oblasť informačnej bezpečnosti ministerstva a internému špecialistovi,
b) predkladá osobe zodpovednej za oblasť informačnej bezpečnosti ministerstva návrhy na posilnenie informačnej bezpečnosti v oblasti svojej pôsobnosti,
c) vykonáva administráciu, prevádzku a kontrolu informačných systémov a technológií,
d) monitoruje, eviduje a vyhodnocuje udalosti a narušenia informačnej bezpečnosti, vykonáva reviziu rizík, vyhodnocuje ich závažnosť a informuje o nich osobu zodpovednú za oblasť informačnej bezpečnosti ministerstva,
e) dokumentuje stav bezpečnosti informačných systémov a technológií a o probléme alebo narušení informačnej bezpečnosti vedie záznam vo forme správy, ktorú predkladá osobe zodpovednej za oblasť informačnej bezpečnosti ministerstva,
f) podieľa sa na príprave podkladov do správ o stave informačnej bezpečnosti.

(5) Správca informačných systémov

a) plní ciele tejto smernice, zabezpečuje súlad praktického stavu informačnej bezpečnosti s cieľmi a zásadami definovanými v tejto smernici,
b) predkladá osobe zodpovednej za oblasť informačnej bezpečnosti ministerstva návrhy na posilnenie informačnej bezpečnosti v oblasti svojej pôsobnosti,
c) definuje, nastavuje a overuje prístupové práva pre skupiny používateľov a jednotlivých používateľov informačných aktív,
d) monitoruje a kontroluje dodržiavanie povinností a pravidiel informačnej bezpečnosti v oblasti svojej pôsobnosti.

(6) Bezpečnostný správca

a) plní ciele tejto smernice, zabezpečuje súlad praktického stavu informačnej bezpečnosti organizácie s cieľmi a zásadami definovanými v tejto smernici,
b) predkladá osobe zodpovednej za oblasť informačnej bezpečnosti ministerstva návrhy na posilnenie informačnej bezpečnosti v oblasti svojej pôsobnosti,
c) zodpovedá za informačnú bezpečnosť informačných aktív a správu informačných systémov a technológií v oblasti svojej pôsobnosti,
d) monitoruje a kontroluje bezpečnostný stav (napr. pokusy o neoprávnený prienik alebo zneužitie) informačných systémov a technológií v oblasti svojej pôsobnosti,
e) dokumentuje bezpečnostné problémy a incidenty a bezodkladne informuje o bezpečnostných problémoch a incidentoch osobu zodpovednú za ochranu osobných údajov,

f) podieľa sa na príprave podkladov do správy o stave informačnej bezpečnosti ministerstva.

(7) Osoba zodpovedná za informačné aktíva v rozsahu svojich oprávnení a pôsobnosti
a) presadzuje a zabezpečuje dodržiavanie tejto smernice,
b) poskytuje súčinnosť pri stanovení hodnoty skupiny informačných aktív, formuluje požiadavky na dostupnosť, dôvernosť a integritu informačných aktív v oblasti svojej pôsobnosti,
c) presadzuje bezpečné využívanie informačných aktív a nasadenie primeraných opatrení na zaistenie ich bezpečnosti,
d) vykonáva kontrolu dodržiavania bezpečnostných opatrení,
e) formuluje základné bezpečnostné požiadavky pri príprave zmluvných vzťahov s tretími stranami,
f) spolupracuje s vedúcim oddelenia informatiky súdu, s riaditeľom odboru informačnej bezpečnosti a interným špecialistom v rámci procesu riadenia informačnej bezpečnosti,
g) zodpovedá za poskytovanie súčinnosti pri zaistení primeranej úrovne ochrany skupiny informačných aktív, ktorá je využívaná primárne za účelom zabezpečenia procesov z oblasti svojej pôsobnosti, definovanie pravidiel na narábanie stouto skupinou informačných aktív a výkon kontrolných činností v oblasti svojej pôsobnosti.

(8) Vlastník informačného aktíva
a) zodpovedá v rozsahu svojich oprávnení za spracúvanie, využívanie a ochranu konkrétneho informačného aktíva,
b) predkladá osobe zodpovednej za oblasť informačnej bezpečnosti ministerstva návrhy na posilnenie informačnej bezpečnosti v oblasti svojej pôsobnosti,
c) riadi prístupy ku zvereným informačným aktívam podľa skutočných potrieb používateľov a zásady dôvernosti informačného aktíva,
d) v spolupráci so správcami informačných systémov a technológií dohliada na nasadenie bezpečnostných opatrení súvisiacich s použitím informačného aktíva,
e) zodpovedá v rozsahu svojich oprávnení za zabezpečenie spracúvania a zaistenie primeranej úrovne ochrany skupiny informačných aktív v konkrétnom informačnom systéme, ako aj za definovanie pravidiel pre narábanie s informačnými aktívami a výkon prevádzkových činností v oblasti svojej pôsobnosti.

(9) Používateľ informačného aktíva je
a) povinný dodržiavať pravidlá a požiadavky ustanovené touto smernicou a ďalšími internými aktmi v oblasti informačnej bezpečnosti,
b) povinný nahlásiť každé narušenie informačnej bezpečnosti bezpečnostnému správcovi.

Čl. 8
Zálohovanie údajov

(1) Zálohovanie údajov z informačných systémov a technológií sa vykonáva manuálne alebo automatizovane pomocou skriptov alebo zálohovacích softvérov na zálohovacie zariadenie.

(2) Rozsah a frekvencia zálohovania údajov zohľadňuje oprávnené požiadavky používateľov informačných aktív a hodnotu informačných aktív z hľadiska zabezpečenia kontinuity prevádzky informačných systémov a technológií.

(3) Zálohovanie údajov sa vykonáva tak, aby v prípade poškodenia alebo zničenia, straty alebo krádeže originálnych údajov bola možná ich obnova zo zálohy v primeranom čase od výpadku.

(4) Záloha údajov je uložená fyzicky oddelene od úložiska originálnych údajov.

(5) Zálohovanie údajov vykonáva správca informačného systému na základe prevádzkovej dokumentácie, ktorá určuje rozsah, periodicitu a spôsoby ich zálohovania.

Čl. 9
Monitorovanie bezpečnosti a aktualizácia softvéru

(1) Na hlásenie narušení informačnej bezpečnosti, problémov alebo zraniteľností informačných systémov a technológií osoba zodpovedná za oblasť informačnej bezpečnosti ministerstva zriadi kontaktné miesto, aplikáciu alebo kontaktnú e-mailovú adresu.

(2) Monitorovanie stavu informačných systémov a technológií sa vykonáva na všetkých úrovniach ich štruktúry.

(3) V rámci monitorovania stavu informačnej bezpečnosti vykonáva bezpečnostný správca vyhodnocovanie štatistík používania elektronickej pošty a štatistík prístupu používateľov k internetovým stránkam. V prípade nálezu bezpečnostného incidentu preskúma obsah správ elektronickej pošty, v prípade potvrdenia existencie bezpečnostného incidentu incident oznámi osobe zodpovednej za ochranu osobných údajov a osobe zodpovednej za oblasť informačnej bezpečnosti ministerstva.

(4) Neobvyklé aktivity v informačných systémoch a technológiách a narušenia informačnej bezpečnosti zaznamenáva, identifikuje a vyhodnocuje v centrálnom systéme pre správu narušení informačnej bezpečnosti bezpečnostný správca na odbore informačnej bezpečnosti.

(5) Správca informačných systémov pri aktualizácii softvéru odstraňuje identifikované závažné zraniteľnosti a problémy v oblasti svojej pôsobnosti.

(6) Správca informačných systémov vykonáva evidenciu nainštalovaného programového vybavenia a hlásení problémov antivírového systému na účely evidencie stavu informačnej bezpečnosti.

Čl. 10
Hodnotenie rizík

(1) Hodnotenie rizík vykonáva osoba zodpovedná za oblasť informačnej bezpečnosti ministerstva pri príprave správy o stave informačnej bezpečnosti v súčinnosti s osobou zodpovednou za informačné aktíva alebo s vlastníkom informačného aktíva.

(2) Hodnotenie rizík je založené na priebežných činnostiach, ktorými sú
a) identifikácia skupín informačných aktív,
b) identifikácia skupín hrozieb a rizík pôsobiacich na tieto skupiny informačných aktív,
c) analýza a ohodnotenie rizík,
d) formulácia bezpečnostných opatrení na zníženie alebo odstránenie rizík,
e) nasadenie primeraných bezpečnostných opatrení,
f) kontrola stavu skupín informačných aktív,
g) kontrola a hodnotenie stavu informačnej bezpečnosti.

(3) Výdavky na bezpečnostné opatrenia na zníženie nájdeného rizika musia byť finančne alebo iným spôsobom kvantifikovateľné a primerané potenciálnym stratám. Hodnotenie rizík musí byť súčasťou každého kritického alebo nového informačného systému alebo technológie.

(4) Kritickými informačnými aktívami sú
a) osobné údaje,
b) autentifikačné údaje,
c) kritické informačné systémy alebo technológie.

(5) Hrozbou pôsobiacou na kritické informačné aktíva je narušenie ich
a) dôvernosti,
b) integrity,
c) dostupnosti.

(6) Hodnotenie rizík hodnotí kritické informačné aktíva osobitne z hľadiska pravdepodobnosti narušenia ich dôvernosti, dostupnosti a integrity, zohľadňujúc pri tom rôzne zdroje uvedených hrozieb a rozsah možného narušenia v oblastiach podľa čl. 5 ods. 3 tejto smernice.

(7) Riziká prijíma komisia nasledovne:
a) prijatie nízkeho rizika je možné len vtedy, ak neohrozuje dôvernosť osobných údajov alebo kritický informačný systém alebo technológie zabezpečujúce prístup k osobným údajom,
b) stredné a vysoké riziká ohrozujúce dôvernosť a integritu osobných údajov alebo kritických informačných systémov a technológií nesmú byť prijaté.

Čl. 11
Kontrola a hodnotenie stavu informačnej bezpečnosti

(1) Cieľmi kontroly stavu informačnej bezpečnosti sú najmä
a) hodnotenie plnenia zavedených bezpečnostných opatrení,
b) posudzovanie dostatočnosti a účinnosti bezpečnostných opatrení,
c) príprava návrhov nových bezpečnostných opatrení a reakcií na prípadné incidenty,
d) havarijné situácie alebo bezpečnostné incidenty,
e) zlepšovanie procesov riadenia a nasadenia informačnej bezpečnosti,
f) posúdenie odstránenia nálezov kontrol a auditu informačnej bezpečnosti.

(2) Kontrolu stavu informačnej bezpečnosti vykonáva osoba zodpovedná za oblasť informačnej bezpečnosti ministerstva alebo interný špecialista na posudzovanie stavu informačnej bezpečnosti spravidla raz ročne.

(3) Audit informačnej bezpečnosti vykonáva fyzická osoba alebo právnická osoba, ktorá má odbornú spôsobilosť na túto činnosť, spravidla raz za štyri roky.

(4) Bezpečnostný mechanizmus informačného systému alebo technológie musí zabezpečiť, aby boli zaznamenávané a ukladané bezpečnostne relevantné informácie o udalostiach a realizovaných operáciách tak, aby bolo možné dodatočne kontrole alebo auditu informačnej bezpečnosti preukázať, že dané udalosti v danom čase a rozsahu v informačnom systéme prebehli.

(5) Auditné údaje musia byť zabezpečené proti náhodnému prepisu a prístupu neautorizovaných osôb. Auditné záznamy sa nesmú stať úložiskom osobných údajov.

(6) V prípade vývoja a nasadzovania nových informačných systémov alebo technológií je kontrola stavu informačnej bezpečnosti vykonávaná i formou testov pri ich vývoji a nasadení do prevádzky. Testovacie scenáre musia byť vytvorené v súlade s touto smernicou.

Čl. 12
Revízia stavu bezpečnostnej politiky

(1) Reviziu stavu bezpečnostnej politiky zabezpečuje osoba zodpovedná za oblasť informačnej bezpečnosti ministerstva najmenej raz ročne.

(2) Reviziu stavu bezpečnostnej politiky zabezpečuje osoba zodpovedná za oblasť informačnej bezpečnosti ministerstva aj po každom periodickom hodnotení rizík informačných systémov alebo technológií, po ohrození kritických informačných aktív, na základe výsledkov auditu informačnej bezpečnosti alebo ako dôsledok bezpečnostných potrieb vyvolaných zmenou právnej úpravy, spoločenských podmienok alebo technologických podmienok.

Čl. 13
Spoločné ustanovenia

(1) Každé informačné aktívum alebo skupina informačných aktív ministerstva musí mať určenú osobu zodpovednú za informačné aktíva a vlastníka. Určuje ich generálny riaditeľ sekcie, predseda súdu alebo riaditeľ organizácie v pôsobnosti ministerstva.

(2) Každé informačné aktívum možno použiť v rozsahu a spôsobom, ktorý ustanovuje osobitný predpis, uznesenie vlády Slovenskej republiky alebo interný riadiaci akt ministerstva alebo ktorý je nevyhnutný na výkon práv alebo splnenie povinností Slovenskej republiky, ministerstva alebo jeho zamestnancov, ktoré vyplývajú z osobitného predpisu, uznesenia vlády Slovenskej republiky alebo interného riadiaceho aktu ministerstva. Ak špecifické použitie informačného aktíva nie je upravené alebo nie je dostatočne upravené a zároveň nie

je nevyhnutné na výkon práv a plnenie povinností podľa prvej vety, informačné aktívum sa použije v súlade s pokynmi a so súhlasom osoby zodpovednej za oblasť informačnej bezpečnosti ministerstva.

Čl. 14
Účinnosť

Táto smernica nadobúda účinnosť dňom vyhlásenia v Zbierke inštrukcií a oznámení Ministerstva spravodlivosti Slovenskej republiky.

Mária Kolíková v. r.
ministerka spravodlivosti Slovenskej republiky