Odbor riadenia kybernetickej a informačnej bezpečnosti
Verzia 1.0 | kyberbezpecnost@mirri.gov.sk | marec 2023

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Metodika klasifikácie informačných aktív a kategorizácie sietí a informačných systémov

Obsah

1 Správa dokumentu

Tento dokument je metodickým materiálom slúžiacim pre potreby orgánov verejnej moci, ktorý nie je povinný na použitie a ani nie je záväzný. Dokument je poskytnutý voľne a bezplatne na využitie podľa potrieb konkrétnej organizácie.

Vytvorený dokument je možné použiť i pre potreby vzdelávania pracovníkov organizácií v oblasti kybernetickej a informačnej bezpečnosti.

Vytvorený dokument nie je určený na ďalší predaj alebo akúkoľvek inú komerčnú či obchodnú činnosť.

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej aj „MIRRI“) nezodpovedá za nesprávne použitie predmetného dokumentu zo strany organizácie. Správne použitie a implementácia bezpečnostných opatrení je plne v kompetencii a zodpovednosti konkrétnej organizácie.

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

2 Úvod

2.1 Účel dokumentu

Účelom tohto dokumentu je poskytnúť základné postupy pre klasifikáciu informačných aktív, kategorizáciu sietí a informačných systémov a pre riadenie aktív v organizácii v súlade so:

- zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej aj „zákon o kybernetickej bezpečnosti“),
- vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení,
- zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy,
- súvisiacimi vykonávacími predpismi.

Tento dokument vychádza z nasledujúcich dokumentov prijatých v rámci organizácie:

- Stratégia kybernetickej bezpečnosti,
- Bezpečnostná politika kybernetickej bezpečnosti.

2.2 Rozsah platnosti

Tento dokument je platný pre všetkých zamestnancov organizácie a tiež všetky relevantné tretie strany.

3 Vymedzenie základných pojmov

3.1 Informačné aktívum

Informačné aktívum je v oblasti infomačnej bezpečnosti čokoľvek, čo je nutné z pohľadu organizácie chrániť – môže ísť o dáta, zariadenia a fyzické systémy.

3.2 Klasifikácia

Klasifikácia posúdenie potrieb ochrany informačných aktív z hľadiska dostupnosti, dôvernosti, integrity, autentickosti a i. a ich následné zaradenie do klasifikačnej kategórie (triedy) zodpovedajúcej týmto potrebám. Vyhláška NBÚ č. 362/2018 Z. z. udáva nasledovné klasifikačné stupne:

1. Klasifikačné stupne z hľadiska dôvernosti:
    - Verejné,
    - Interné,
    - Chránené,
    - Prísne chranené.
2. Klasifikačné stupne z hľadiska integrity:
    - Nízka,
    - Stredná,
    - Vysoká.
3. Klasifikačné stupne z hľadiska dostupnosti:
    - Nízka,
    - Stredná,
    - Vysoká.

3.3 Kategorizácia

Rozdelenie informačných systémov a sietí do kategórií podľa klasifikačných kritérií definovaných vo vyhláške NBÚ č. 362/2018 Z. z. Informačné systémy a siete sa kategorizujú do nasledovných kategórií:

- Kategória I.,
- Kategória II.,
- Kategória III.

3.4 Klasifikované informačné aktívum

Klasifikovaným informačným aktívom je také aktívum, ktorého ochrana vyplýva z platnej legislatívy Slovenskej republiky. Pri jeho odovzdávaní inému organizačnému útvaru alebo tretej strane, vlastník informačného aktíva zabezpečuje s odovzdaním aj oznámenie o druhu informačného aktíva a spôsobe narábania s informačným aktívom.

3.5 Vlastník informačného aktíva

Vlastník informačného aktíva je osoba kompetenčne zodpovedná za požadovanú úroveň ochrany informačných aktív, ktoré sú v jej organizačnej pôsobnosti spracúvané, primárne za účelom zabezpečenia chodu procesov.

Typickými vlastníkmi informačných aktív sú v organizácii vedúci pracovníci.

3.6 Opravnená osoba v časti klasifikácia informačných aktív

Oprávnenou osobou je osoba, ktorá je určená vlastníkom informačného aktíva na spracúvanie alebo/a oboznamovanie sa s vymedzeným rozsahom informačného aktíva alebo jej oprávnenie vyplýva zo zákona, resp. z výkonu jej funkcie (pracovnej pozície).

3.7 Nepovolaná osoba v časti klasifikácia informačných aktív

Nepovolanou osobou je osoba, ktorá nie je určená na spracúvanie alebo/a oboznamovanie sa s informačnými aktívami zaradenými v systéme ochrany alebo rozsah jej určenia nie je postačujúci.

3.8 Vedenie organizácie

Jednotlivec alebo skupina ľudí, ktorí zabezpečujú proces vedenia/riadenia organizácie a zodpovedajú za priebeh tohto procesu. Pod vedením organizácie môžeme rozumieť vedenie organizácie ako celku, ak aj jej jednotlivých organizačných útvarov.

3.9 Iný poverený zamestnanec

Zamestnanec určený vedením organizácie na vykonávanie špecifických úloh organizácie.

3.10 Dôvernosť, integrita a dostupnosť informačných aktív

Dôvernosť je záruka, že údaj nie je prezradený neoprávneným subjektom alebo procesom.

Integrita je záruka, že bezchybnosť, úplnosť alebo správnosť údajov neboli narušené.

Dostupnosť je záruka, že údaj je pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď je údaj potrebný a požadovaný.

3.11 Sieť a informačný systém

Sieťou a informačným systémom sa rozumie elektronická komunikačná sieť, informačný systém, každé zariadenie a komunikačný systém alebo údaje, ktoré sú v nich vytvárané, ukladané, spracúvané, získavané alebo prenášané prostredníctvom elektronickej komunikačnej siete alebo informačného systému, na účely prevádzkovania, používania, ochrany a udržiavania týchto sietí a systémov.

3.12 Vlastník siete / informačného systému

Vlastník siete/informačného systému je osoba kompetenčne zodpovedná za požadovanú úroveň ochrany siete a/alebo informačného systému, ktoré spadajú do jej organizačnej pôsobnosti.

Vlastníci sietí/informačných systémov môžu svoje právomoci delegovať až na úroveň jednotlivcov ako napr.:

- administrátorov sietí,
- administrátorov informačných systémov.

3.13 Oprávnená osoba v časti kategorizácia sietí a informačných systémov

Oprávnenou osobou je osoba, ktorá je určená vlastníkom siete alebo informačného systému na používanie siete alebo informačného systému jej oprávnenie vyplýva zo zákona, resp. z výkonu jej funkcie (pracovnej pozície).

3.14 Nepovolaná osoba v časti kategorizácia sietí a informačných systémov

Nepovolanou osobou je osoba, ktorá nie je určená na používanie siete alebo informačného systému, jej oprávnenie nevyplýva zo zákona, resp. z výkonu jej funkcie (pracovnej pozície).

4 Roly, zodpovednosti a právomoci

4.1 Roly, zodpovednosti a právomoci v rámci klasifikácie informačných aktív

Vlastníci informačného aktíva zodpovedajú za evidenciu a triedenie informačných aktív do klasifikačných stupňov podľa klasifikačnej schémy (viď nasledujúcu kapitolu).

Klasifikácia a evidencia informačných aktív sú vykonávané minimálne raz za rok a vždy v prípade, ak:

- nastane zmena v spravovaní informačných aktív,
- nastane zmena v súvisiacich právnych predpisov,
- vznikne nový typ dokumentu obsahujúci informačné aktíva, ktoré vyžadujú klasifikáciu.

Vedenie organizácie alebo iný poverený zamestnanec:

- zodpovedajú za riadenie a výkon ochrany informačných aktív,
- zabezpečujú aktuálnosť klasifikácie informačných aktív,
- vyhodnocujú správnosť klasifikácie informačných aktív v súlade s definovanou klasifikačnou schémou,
- kontrolujú súlad ochrany informačných aktív podľa definovaných bezpečnostných požiadaviek klasifikačnej schémy.

Za výkon ochrany podľa tohto dokumentu zodpovedajú taktiež osoby prichádzajúce do styku s klasifikovanými a/alebo neklasifikovanými informačnými aktívami.

Vedenie organizácie alebo iný poverený zamestnanec, v ktorého pôsobnosti sú vzťahy s verejnosťou, zodpovedajú za výber, postup a rozsah poskytovania verejne prístupných informačných aktív.

Zamestnanci organizácie sú povinní ochraňovať, t. j. nezverejňovať, neposkytovať ani nesprístupňovať nepovolanej osobe všetky klasifikované i neklasifikované informačné aktíva, s ktorými pri plnení svojich pracovných povinností prichádzajú do styku a to aj v prípade, že nie sú oprávnenou osobou.

4.2 Roly, zodpovednosti a právomoci v rámci kategorizácie informačných systémov a sietí

Kategorizácia informačných systémov a sietí je vykonávaná minimálne raz za rok a vždy v prípade, ak:

- nastane zásadná zmena v sieti alebo informačnom systéme,
- nastane zmena v súvisiacich právnych predpisov,
- do produkčnej prevádzky bude uvedená nová sieť alebo informačný systém.

Vedenie organizácie alebo iný poverený zamestnanec:

- zodpovedajú za riadenie a výkon kategorizácie sietí a informačných systémov,
- zabezpečujú aktuálnosť kategorizácie sietí a informačných systémov,
- vyhodnocujú správnosť kategorizácie sietí a informačných systémov v súlade s definovanou kategorizačnou schémou.

Zamestnanci organizácie sú povinní rešpektovať platnú kategorizáciu sietí a informačných systémov

a to aj v prípade, že nie sú oprávnenou osobou.

5 Metodika klasifikácie informačných aktív

Informačné aktíva sa v rámci organizácie vytvárajú, spracúvajú a ukladajú tak, že ich kvalita a spoľahlivosť je primeraná ich klasifikačnému stupňu.

Každé klasifikované informačné aktívum má pridelený jeden klasifikačný stupeň dôvernosti, jeden klasifikačný stupeň integrity a jeden klasifikačný stupeň dostupnosti. Bezpečnostné informačné akti, nastavenia, postupy, smernice a ostatné úkony ohľadom riadenia aktív sa klasifikujú rovnakým alebo vyšším klasifikačným stupňom, akým sú označené informačné aktíva, ktorých riadenie opisujú.

Pri klasifikácii informačných aktív sa uplatňuje odstupňovaný prístup tak, že do nižších úrovní sú zahrnuté také informačné aktíva, pri ktorých sú najnižšie nároky na dôvernosť, integritu, dostupnosť a zodpovednosť vrátane zabezpečovania kvality. Informačné aktíva sa vytvárajú, spracúvajú a ukladajú tak, že ich kvalita a spoľahlivosť je primeraná ich klasifikačnému stupňu.

Organizácia môže na základe racionálneho zváženia skutkového stavu, dostatočného odôvodnenia a schválenia manažérom kybernetickej a informačnej bezpečnosti a relevantným vedúcim pracovníkom jednotlivé informačné aktíva zaradiť do vyššieho alebo nižšieho stupňa ako vyplýva z vykonanej klasifikácie.

Klasifikačné stupne opisujú citlivosť informačných aktív, údajov alebo ďalších s nimi spojených informačných aktív a odrážajú dôležitosť alebo hodnotu týchto aktív pre organizáciu z pohľadu narušenia ich:

- dôvernosti,
- integrity,
- dostupnosti.

Dotazník slúžiaci na určenie klasifikačných stupňov jednotlivých informačných aktív je súčasťou prílohy č. 1.

Konkrétne príklady klasifikovaných informačných aktív sú súčasťou prílohy č. 2.

5.1 Klasifikačné stupne z pohľadu dôvernosti

Z hľadiska dôvernosti sú klasifikačné stupne informačných aktív definované nasledovným spôsobom:

5.1.1 Klasifikačný stupeň – Prísne chránene

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

5.1.2 Klasifikačný stupeň – Chránené

Chránené informačné aktíva sú informačné aktíva, ktoré sú používané a prístupné len určeným skupinám oprávnených osôb a ktorých neautorizované odhalenie, prezradenie alebo zničenie môže mať

pre organizáciu negatívny vplyv. Prístup k údajom klasifikovaným ako „Chránené“ je riadený pomocou zásady „potreby vedieť“ a zásady „najnižších privilégií“ a je vymedzený výhradne vopred definovaným a schváleným útvarom alebo iným jasne vymedzeným skupinám osôb. Tretie strany majú k týmto údajom prístup len v nevyhnutných a jednoznačne definovaných prípadoch schválených vlastníkom.

5.1.3 Klasifikačný stupeň – Interné

Interné informačné aktíva sú informačné aktíva, ktoré majú výpovednú hodnotu a význam pre organizáciu, preto sú určené len pre vnútornú potrebu organizácie, sú používané a prístupné pre všetkých používateľov v rámci organizácie bez ohľadu na ich pracovnú rolu. Na sprístupnenie týchto informačných aktív tretím stranám je potrebné schválenie zo strany vlastníka informačného aktíva. Vyžadujú si základnú úroveň ochrany (čistý stôl, primeraná miera potreby prístupu).

5.1.4 Klasifikačný stupeň – Verejné

Verejné informačné aktíva sú informačné aktíva určené pre vonkajšiu komunikáciu a tretie strany, sú získateľné z verejných zdrojov alebo z informačných aktív, ktoré sú pripravené na tento účel alebo sú preklasifikované z inej úrovne prostredníctvom vlastníka a zahŕňajú napríklad informácie z médií, povinne publikované informácie alebo všeobecne dostupné informácie.

5.2 Klasifikačné stupne z pohľadu integrity

Z hľadiska integrity sú klasifikačné stupne informačných aktív definované nasledovným spôsobom:

5.2.1 Klasifikačný stupeň – Vysoká

Tento stupeň zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť organizácie a ktorých chyba alebo nepresnosť bezprostredne ohrozuje činnosť organizácie, s ňou spojené aktivity a reputáciu.

Neautorizovaná modifikácia údajov alebo ich nepresnosť, resp. neúplnosť môže mať veľmi vážny dopad na kritické procesy alebo aktíva organizácie s možným výskytom efektu kumulácie viacerých nepriaznivých dopadov.

5.2.2 Klasifikačný stupeň – Stredná

Tento stupeň zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť organizácie a ktorých chyba alebo nepresnosť môže spôsobiť dopad na kontinuitu činností organizácie alebo strategickú oblasť, v ktorej organizácia vykonáva svoje aktivity.

Neautorizovaná modifikácia údajov alebo ich nepresnosť, resp. neúplnosť môže mať nepriaznivý dopad na procesy alebo aktíva organizácie, s možným výskytom efektu kumulácie viacerých nepriaznivých dopadov.

5.2.3 Klasifikačný stupeň – Nízka

Tento stupeň zahŕňa informačné aktíva, ktorých chyba alebo nepresnosť výrazne neohrozí poskytovanie činností zo strany organizácie.

Neautorizovaná modifikácia údajov alebo ich nepresnosť, resp. neúplnosť nemá významnejší nepriaznivý dopad na procesy alebo aktíva organizácie.

5.3 Klasifikačné stupne z pohľadu dostupnosti

Z hľadiska dostupnosti sú klasifikačné stupne informačných aktív definované nasledovným spôsobom:

5.3.1 Klasifikačný stupeň – Vysoká

Tento klasifikačný stupeň zahŕňa vybrané kľúčové informačné aktíva, ktoré sú kritické pre činnosť organizácie a ktorých zlyhanie bezprostredne ohrozuje poskytovanie služieb zo strany organizácie, s ňou spojené aktivity a dobrú povesť organizácie.

5.3.2 Klasifikačný stupeň - Stredná

Tento klasifikačný stupeň zahŕňa informačné aktíva, ktoré sú dôležité pre činnosť organizácie a ktorých zlyhanie môže mať dopad na kontinuitu poskytovania služieb zo strany organizácie, strategickú oblasť, trhové a operačné riziká.

5.3.3 Klasifikačný stupeň – Nízka

Tento klasifikačný stupeň zahŕňa informačné aktíva organizácie, ktorých výpadok výrazne neohrozí služby poskytované zo strany organizácie alebo pre ktoré existujú alternatívne postupy.

5.4 Klasifikácia informačných aktív v súvislosti s analýzou rizík a analýzou dopadov

Jednou zo základných úloh vedenia každej organizácie je riadenie zdrojov, do ktorej patrí aj ochrana aktív. Prvým krokom pri ochrane týchto aktív je vytvorenie prehľadného zoznamu aktív a ich vlastníkov, ktorý je jedným z hlavných vstupov do analýzy rizík. Organizácia má zavedené mechanizmy komunikácie rizika, s cieľom podporiť zodpovednosť a vlastníctvo rizika. Tieto mechanizmy zabezpečujú, aby kľúčové komponenty rizika v rámci procesov riadenia rizík boli primerane a včas komunikované zo všetkými zainteresovanými stranami.

V rámci identifikácie aktív je vytvorený katalóg, ktorý popisuje všetky relevantné aktíva. Vytvorenie zoznamu aktív je súčasťou procesu riadenia aktív. Na definícii kritickosti aktív sa významne podieľa aj analýza funkčných dopadov (z angl. „Business Impact Assessment“ – BIA). Podľa potreby môžu byť informačné aktíva logicky usporiadané do hierarchickej štruktúry pre zefektívnenie odkazovania sa na konkrétne aktíva v rámci celej analýzy rizík.

Vykonanie klasifikácie informačných aktív sa odporúča spojiť s výkonom analýzy rizík a analýzy dopadov, nakoľko pri realizácii týchto aktivít častokrát ku samotnej klasifikácii informačných aktív dochádza.

Samotná analýza rizík a analýza dopadov je v organizácii vypracovaná na základe dokumentu „Metodika analýzy rizík a analýzy dopadov“ alebo ako súčasť bezpečnostného projektu príslušného IS.

5.5 Evidencia klasifikovaných informačných aktív

Bližší popis existujúcej evidencie klasifikovaných informačných aktív, vrátane príslušného dokumentu, bude doplnený zo strany príslušnej organizácie.

6 Metodika kategorizácie sietí a informačných systémov

Kategorizácia sietí a informačných systémov je v rámci organizácie založená na klasifikácii informačných aktív.

Kategorizácia sietí a informačných systémov sa vykonáva pre každú sieť a informačný systém vytvorením zoznamu vybraných komponentov sietí a informačných systémov, ktorý identifikuje jednotlivé siete a informačné systémy, ich podporné systémy a podsystémy s uvedením ich bezpečnostnej funkcie a zaradenia do príslušných bezpečnostných kategórií.

Organizácia môže na základe racionálneho zváženia skutkového stavu, dostatočného odôvodnenia a schválenia manažérom kybernetickej a informačnej bezpečnosti a relevantným vedúcim pracovníkom jednotlivé siete a informačné systémy zaradiť do vyššieho alebo nižšieho stupňa ako vyplýva z vykonanej kategorizácie.

Zoznam komponentov sietí a informačných systémov organizácie identifikujúci jednotlivé siete a informačné systémy sa môže skladať z textovej, tabuľkovej a grafickej časti tak, že sú jednoznačne definované:

- hranice vybranej siete a informačného systému,
- rozhrania medzi definovanými hranicami,
- bezpečnostné funkcie komponentov, ktoré majú byť zahrnuté v posudzovaní úrovne bezpečnosti,
- požiadavky príslušných regulačných požiadaviek a technických noriem alebo iných vecne obdobných postupov a metód na ich:
- projektovanie,
- vytváranie,
- implementáciu,
- kontrolu.

Siete a informačné systémy tvoriace hranicu medzi rôznymi bezpečnostnými kategóriami v bezpečnostnom systéme sa zaraďujú do vyššej bezpečnostnej kategórie.

Kategorizácia sietí a informačných systémov zohľadňuje, že zlyhanie siete alebo informačného systému v ľubovoľnej bezpečnostnej úrovni nespôsobí zlyhanie vybranej siete a informačného systému zaradeného do bezpečnostnej úrovne s vyššou kategóriou. Pomocné siete a informačné systémy a podsystémy, ktoré pomáhajú funkciám vybraných informačných systémov, musia byť zaradené do príslušnej bezpečnostnej kategórie s ohľadom na zaradenie nadradeného systému.

V rámci organizácie sa rozoznávajú tri kategórie sietí a informačných systémov:

- kategória I,
- kategória II,
- kategória III.

6.1 Kategórie sietí a informačných systémov

6.1.1 Kategória I.

Kategória I. zahŕňa informačné aktíva v pôsobnosti organizácie:

- ktorých ohrozenie nemá žiadny negatívny dopad na poskytovanú základnú službu (v zmysle zákona č, 69/2018 Z. z. o kybernetickej bezpečnosti),
- ktoré sú klasifikované z hľadiska dôvernosti ako verejné alebo v odôvodnených prípadoch interné,
- ktoré sú klasifikované z hľadiska dostupnosti klasifikačným stupňom nízka alebo v odôvodnených prípadoch stredná,
- ktoré sú klasifikované z hľadiska integrity klasifikačným stupňom nízka alebo v odôvodnených prípadoch stredná,
- pri ktorých nie je predpoklad potreby identifikácie zodpovednosti za aktivity používateľov,
- pri ktorých nie je potrebné vykonávať kontrolnú činnosť.

6.1.2 Kategória II.

Kategória II. zahŕňa informačné aktíva v pôsobnosti organizácie:

- ktorých ohrozenie môže spôsobiť kybernetický bezpečnostný incident I. stupňa (v zmysle vyhlášky Národného bezpečnostného úradu č. 165/2018 Z. z.),
- ktoré sú klasifikované z hľadiska dôvernosti ako interné, chránené alebo v odôvodnených prípadoch prísne chránené,
- ktoré sú klasifikované z hľadiska dostupnosti klasifikačným stupňom stredná alebo v odôvodnených prípadoch vysoká,
- ktoré sú klasifikované z hľadiska integrity klasifikačným stupňom stredná alebo v odôvodnených prípadoch vysoká,
- pri ktorých je potrebné identifikovať zodpovednosť za kritické aktivity, najmä však aktivity privilegovaných používateľov,
- pri ktorých je potrebné vykonávať kontrolnú činnosť,
- zabezpečujúce vytváranie a vedenie agend, ktoré nepatria do I. bezpečnostnej kategórie,
- ktoré sú agendové informačné systémy,
- ktorými sú špecializované portály,
- ktoré sú nevyhnutné na rozhodovanie orgánu štátnej moci.

6.1.3 Kategória III.

Kategória III. zahŕňa informačné aktíva v pôsobnosti organizácie:

- ktorých ohrozenie môže spôsobiť kybernetický bezpečnostný incident II. a III. stupňa (v zmysle vyhlášky Národného bezpečnostného úradu č. 165/2018 Z. z.),

- ktoré sú klasifikované z hľadiska dôvernosti ako prísne chránené,
- ktoré sú klasifikované z hľadiska dostupnosti klasifikačným stupňom vysoká,
- ktoré sú klasifikované z hľadiska integrity klasifikačným stupňom vysoká,
- pri ktorých je potrebné auditovať aktivity všetkých používateľov,
- prostredníctvom ktorých sa poskytuje základná služba a ktorých výpadok alebo poškodenie spôsobí poškodenie alebo znemožnenie poskytovania základnej služby,
- ktoré sú označené ako utajované skutočnosti alebo ako tajomstvo podľa osobitých predpisov (napr. zákona č. 215/2004 Z. z. o utajovaných skutočnostiach),
- ktoré sú nevyhnutné a potrebné z hľadiska plnenia úloh týkajúcich sa obrany a bezpečnosti štátu alebo,
- ktorým je ústredný portál verejnej správy.

7 Revízia dokumentu

Tento dokument sa reviduje a aktualizuje najmenej raz ročne.

Dokument sa aktualizuje aj častejšie, ak:

- vzíde požiadavka na jeho aktualizáciu,
- pri zásadných zmenách v organizácii a štruktúre organizácie,
- pri zásadných zmenách v legislatíve Slovenskej republiky, s vplyvom na niektorú časť tohto dokumentu (príslušná relevantná legislatíva je súčasťou prílohy č. 1 Bezpečnostnej politiky kybernetickej bezpečnosti).

Za pravidelnú revíziu a aktualizáciu dokumentu zodpovedá manažér kybernetickej a informačnej bezpečnosti.

Tento dokument a všetky následné aktualizácie schvaľuje vedenie organizácie.

8 Prílohy

Príloha 1 – Dotazník slúžiaci na určenie klasifikačných stupňov jednotlivých informačných aktív

Príloha 2 – Príklady vykonanej klasifikácie informačných aktív