Odbor riadenia kybernetickej a informačnej bezpečnosti
Verzia 1.1 | kyberbezpecnost@mirri.gov.sk | jún 2023

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

Metodika jednotného výkonu riadenia kontinuity činnosti v sektore verejnej správy

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 riadenie kontinuity činnosti v sektore verejnej správy 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.

2.2 Rozsah platnosti

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

3 Požiadavky na zabezpečenie riadenia kontinuity činnosti

Požiadavky na zabezpečenie riadenia kontinuity činnosti v organizácii pozostávajú najmenej z:

- vypracovania stratégie a krízových plánov na zabezpečenie dostupnosti siete a informačného systému po narušení alebo zlyhaní v dôsledku kybernetického bezpečnostného incidentu na základe vykonania analýzy dopadov kybernetického bezpečnostného incidentu,
- vyčlenenia adekvátnych finančných, materiálno-technických a personálnych zdrojov na zabezpečenie riadenia kontinuity činnosti,
- určenia komunikačného plánu na plnenie havarijných plánov a plánov obnovy spolu s kontaktnými údajmi, určeniami rolí a zodpovednosti na plnenie havarijných plánov a plánov obnovy po kybernetickom bezpečnostnom incidente,
- určenia cieľovej doby obnovy jednotlivých procesov, siete a informačných systémov a aplikácií, a to najmä určením doby obnovy prevádzky, po uplynutí ktorej je obnovená najnižšia úroveň poskytovania základných služieb,
- určenia cieľového bodu obnovy jednotlivých procesov, siete a informačných systémov základnej služby a aplikácií, a to najmä určením najnižšej úrovne poskytovania služieb, ktorá je dostatočná na používanie, prevádzku a správu siete a informačného systému a zachovanie kontinuity činnosti,
- testovania a vyhodnocovania jednotlivých procesov riadenia kontinuity činnosti a realizácie opatrení na zvýšenie odolnosti sietí a informačných systémov,
- určenia plánov havarijnej obnovy a postupov zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní,
- stanovenia práv a povinností administrátorov a osôb zastávajúcich bezpečnostné roly.

4 Spôsob určenia cieľovej doby obnovy a cieľového bodu obnovy informačných aktív

Hodnoty cieľovej doby obnovy (RTO) a cieľového bodu obnovy (RPO) informačných aktív sú získané od vlastníkov a používateľov systémov na základe identifikácie procesov, pre ktoré sú jednotlivé informačné systémy používané ako aj na základe popisu vplyvu nedostupnosti systémov, prípadne vyplývajúcich strát.

4.1 Spôsob určenia cieľovej doby obnovy (RTO)

Prioritný časový rámec na obnovenie činnosti sa nazýva cieľová doba obnovy. Cieľová doba obnovy jednotlivých procesov, siete a informačných systémov a aplikácií je v organizácii určená ako doba obnovy prevádzky, po uplynutí ktorej je po kybernetickom incidente obnovená najnižšia úroveň poskytovania základných služieb. Čas potrebný na to, aby sa dopad kybernetického incidentu stal neprijateľným sa môže líšiť v rozmedzí sekúnd až po niekoľko mesiacov v závislosti od povahy dotknutých aktivít. Aktivity, ktoré sú viac časovo senzitívne sú špecifikované s vyššou presnosťou t. j. na hodiny.

4.2 Spôsob určenia cieľového bodu obnovy (RPO)

Cieľový bod obnovy jednotlivých procesov, siete a informačných systémov a aplikácií je v organizácii určený najnižšou úrovňou poskytovania služieb, ktorá je dostatočná na používanie, prevádzku a správu siete a informačného systému a zachovanie kontinuity základnej služby.

4.3 Určenie hodnôt RTO a RPO

Samotné určenie hodnôt RTO a RPO je v gescii organizácie, ktorá toto určenie vykonáva na základe vykonanej analýzy dopadov. Výkon analýzy dopadov a jej bližší popis je súčasťou dokumentu „Metodika analýzy rizík a analýzy dopadov“.

5 Riadenie kontinuity činnosti

Riadenie kontinuity činnosti v organizácii je súbor aktivít zabezpečujúcich obnovu činností po ich narušení. V prípade narušenia činností a prieniku hrozby k informačným aktívam organizácie by mohli byť organizácii spôsobené škody značného rozsahu narušením poskytovania služieb, narušením schopnosti plnenia povinností voči národným regulátorom alebo ohrozením dobrého mena organizácie. Hrozby, ktoré ohrozujú organizáciu sa delia do nasledujúcich kategórií:

- úmyselné hrozby,
- náhodné hrozby,
- hrozby spôsobené vplyvom prostredia.

Cieľom riadenia kontinuity činnosti je:

- koordinácia aktivít obnovy a definovanie zodpovednosti počas krízovej situácie,
- minimalizácia strát a návrat do štandardnej prevádzky,
- pravidelné testovanie a aktualizácia plánov.

5.1 Stratégia obnovy

Organizácia vytvára stratégiu obnovy, ktorej úlohou je definovať princípy a postupy, pomocou ktorých bude organizácia schopná zachovať kontinuitu zabezpečovaných činností. Účelom stratégie obnovy je:

- identifikovať kritické aktivity a procesy prostredníctvom analýzy dopadov,
- identifikovať kritické informačné systémy,
- definovať predpoklady a princípy, podľa ktorých budú vykonávané činnosti v havarijnom stave,
- definovať spôsoby riadenia aktivít, ktoré zabezpečujú obnovu aktivít, procesov a informačných systémov po narušení a vyhlásení havarijného stavu.

Súčasťou tvorby stratégie obnovy je aj identifikácia viacerých stratégií a výber optimálnej stratégie. V procese tvorby analýz dopadov a analýzy rizík organizácia identifikuje rôzne možnosti obnovy a vybraný optimálny spôsob vzhľadom na implementované technológie a požiadavky.

5.2 Krízové plány

Organizácia eliminuje riziká nedostupnosti IKT tvorbou krízových plánov. Cieľom krízových plánov je poskytnúť návody a postupy pre rýchle a efektívne obnovenie činností kritických technológií, infraštruktúry, aplikácií a dát po výskyte krízovej udalosti. Výskyt, typ a rozsah krízovej udalosti sa nedá vopred naplánovať a nie je vždy možné predpovedať dopad udalosti.

Filozofiou plánovania obnovy je pochopenie možných hrozieb, ich dopadov na informačné zdroje organizácie a stanovenie stratégie a postupov pre elimináciu týchto dopadov. V oblasti krízových plánov platí, že preventívne opatrenia pre elimináciu rizík sú výrazne efektívnejšie a účinnejšie ako samotné opatrenia, ktoré je nutné vykonať pri výskyte krízovej situácie.

5.2.1 Plány kontinuity činnosti (BCP)

Plány popisujúce obnovu kontinuity činností v organizácii obsahujú najmä:

- ustanovenie tímu zabezpečenia kontinuity a obsadenie jednotlivých pozícií v rámci tímu,
- presne zadefinovaný súbor úloh pre členov tímu,
- kontakty na relevantné tretie strany (napr. dodávatelia),
- alternatívne postupy pri nedostupnosti IKT,
- kroky obnovy činnosti procesu na minimálnej požadovanej úrovni pre prácu v krízovom/havarijnom stave,
- postupy na obnovu plnej prevádzky procesu do štandardného stavu v akom sa nachádzal pred incidentom.

Organizácia aktivuje BCP plán v prípade prerušenia výkonu kritických činností. V prípade BCP plánov organizácia určuje nasledovné zoznamy osôb:

- osoby oprávnené aktivovať BCP plán,
- osoby, ktoré sú súčasťou tímu obnovy.

Nasledujúce opatrenia musia byť vykonané okamžite po objavení incidentu:

- informovať manažéra kybernetickej a informačnej bezpečnosti o incidente,
- požiadať osobu, ktorá identifikovala incident o bližšie informácie,
- potvrdiť potrebu aktivácie krízového riadenia a tímu,
- informovať zamestnancov o situácii a poskytnúť príslušné pokyny,
- informovať tretie strany, ktorých sa incident dotkol,
- upozorniť zamestnancov o spôsoboch komunikácie s médiami a poučiť ich, že informácie týkajúce sa incidentu by nemali byť komunikované prostredníctvom sociálnych médií,
- aktivovať príslušné postupy týkajúce sa nedostupnosti:
  - kritického personálu,
  - sídla organizácie,
  - kritických aplikácií,
  - kritických dát,
  - tretích strán,
  - iného dôležitého materiálu.

Organizácia ma spracovaný BC plán v samostatnom dokumente. Vypracovaný BC plán by mal obsahovať nasledovné náležitosti a údaje:

- **účel a rozsah,**
- **ciele,**
- **roly zodpovednosti a právomoci,**
- **komunikačné požiadavky a procesy toku informácií,**

- **interné a externé previazanosti a interakcie,**
- **požiadavky na zdroje,**
- **procesy dokumentovania.**

5.2.2 Plány obnovy (DRP)

Organizácia dokumentuje postupy obnovy a navrátenie prevádzky z dočasných opatrení prijatých na podporu obnovenia bežného chodu prevádzky. Ciele plánov obnovy sú dosiahnuté najmä nasledujúcimi spôsobmi:

- opravou vzniknutých škôd,
- premiestnením prevádzky z dočasných priestorov späť do sídla organizácie,
- presunom na novú lokalitu.

Zdokumentované postupy ustanovujú podrobné posúdenie situácie a jej vplyvu na určenie úloh a krokov potrebných na obnovu. Počas vykonávania plánov obnovy organizácia najmä:

- zriaďuje zdroje a infraštruktúru slúžiacu na obnovu,
- obnovuje poškodené zariadenia a systémy,
- zabezpečuje núdzové obstarávanie a financovanie,
- obnovuje stratené zadokumentované dáta,
- primerane komunikuje so zainteresovanými stranami,
- vykonáva kontrolu po uskutočnení plánov obnovy.

Plány obnovy obsahujú informácie v prehľadnom členení tak, aby ich bolo možné rýchlo vyhľadať. Plány obnovy pozostávajú z nasledujúcich častí:

- identifikácia plánu,
- organizácia,
- inicializácia,
- procedúry obnovy,
- harmonogram postupu,
- návrat do normálneho stavu.

Organizácia ma spracovaný DR plán v samostatnom dokumente. Vypracovaný DR plán by mal obsahovať nasledovné náležitosti a údaje:

- **účel a rozsah,**
- **roly a zodpovednosti,**
- **kritéria na aktivovanie plánu,**
- **vlastník a správca dokumentácie,**

- **kontaktné údaje.**

5.3 Vyčlenenie zdrojov na zabezpečenie riadenia kontinuity procesov

Organizácia určuje nástroje a vyčleňuje zdroje na zabezpečenie riadenie kontinuity procesov najmä týmito spôsobmi:

- určením tímov alebo jednotlivcov s primeraným oprávnením dohliadať na pripravenosť, reakciu a obnovu po incidentoch,
- logistickými možnosťami a postupmi na lokalizáciu, získanie, uloženie, distribúciu, údržbu, testovanie a zodpovednosť za služby, personál, zdroje, materiály a zariadenia vyrobené alebo poskytnuté na podporu riadenia kontinuity procesov,
- finančnými, logistickými a administratívnymi postupmi na podporu opatrení na zabezpečenie riadenia kontinuity procesov pred, počas a po incidente. Tieto postupy by mali zabezpečiť:
  - urýchlenie finančných rozhodnutí,
  - súlad so zavedenými úrovňami právomocí, zásadami riadenia a účtovníctva.
- cieľmi riadenia zdrojov pre časy odozvy, personál, vybavenie, školenie, financovanie, poistenie, kontrolu zodpovednosti, odborné znalosti, materiály a časovým rámcom, v rámci ktorého bude každý z cieľov vyžadovaný zo zdrojov organizácie a tiež od všetkých dodávateľov,
- postupmi, ktoré sa týkajú vzájomnej pomoci a komunikácie medzi zainteresovanými stranami.

5.3.1 Finančné zdroje

Organizácia určuje možnosti na zabezpečenie potrebných finančných prostriedkov. Tieto možnosti zahŕňajú:

- poskytovanie finančných prostriedkov na núdzové nákupy,
- uhrádzanie personálnych nákladov,
- vysoké výdavky napr. za účelom nákupu.

5.3.2 Materiálno-technické zdroje

V organizácii sú materiálno-technické zdroje určené na zabezpečenie riadenia kontinuity činnosti zabezpečené týmito spôsobmi:

- uskladnením dodatočných materiálno-technických zdrojov na inom mieste,
- dohodami o dodávke materiálno-technických zdrojov v skrátenom čase,
- presmerovaním dodávok materiálno-technických zdrojov na iné miesta,
- identifikáciou alternatívnych dodávok materiálno-technických zdrojov.

5.3.3 Personálne zdroje

Organizácia určuje vhodné opatrenia na udržanie a rozšírenie zručností a znalostí v prípade, že výsledkom incidentu je zníženie personálu. Tieto opatrenia zahŕňajú zamestnancov, dodávateľov

a iné zainteresované strany. Medzi tieto opatrenia patria:

- zoznam kvalifikovaných odborníkov,
- mnohostranné školenie zamestnancov a dodávateľov,
- oddelenie zamestnancov so základnými schopnosťami na viac ako jednom mieste,
- využitie tretích strán,
- dokumentovanie procesov a iných foriem uchovávania a riadenia znalostí.

5.4 Komunikačný plán

Organizácia ustanovuje a implementuje komunikačný plán, ktorý popisuje:

- odhalenie incidentu a varovanie zodpovedného personálu,
- pokračovanie v monitorovaní incidentu,
- internú komunikáciu medzi rôznymi úrovňami a pozíciami v rámci organizácie,
- externú komunikáciu so zainteresovanými stranami,
- prijímanie, dokumentovanie a reakciu na komunikáciu od ostatných zainteresovaných strán,
- prijímanie, dokumentovanie a reakcia na akýkoľvek vnútroštátny alebo regionálny poradenský systém rizika alebo jeho ekvivalent,
- upozornenie zainteresovaných strán, ktoré by mohli byť postihnuté aktuálnym alebo potenciálnym incidentom,
- zabezpečenie dostupnosti komunikačných prostriedkov počas mimoriadnej udalosti,
- zaznamenávanie dôležitých informácií o incidente, prijatých opatreniach a prijatých rozhodnutiach,

5.5 Určenie rolí a zodpovedností

Za kontinuitu prevádzky organizácie zodpovedá vedením organizácie určený zodpovedný vedúci pracovník, ktorý je zodpovedný za pravidelné preskúmanie a rozvoj politiky v súlade s potrebami organizácie.

Pre proces riadenia kontinuity procesov sú ďalej ustanovené nasledovné roly:

- sponzor
- správca,
- koordinátor,
- plánovač,
- vykonávateľ.

Sponzor:

- sponzorom je zástupca vedenia organizácie,
- schvaľuje programy testovania.

Správca:

- zamestnanec zodpovedný za bezpečnosť – vyhradený pre oblasť krízového plánovania,
- koordinuje prípravu plánu obnovy, navrhuje stratégiu a metodiku tvorby plánov obnovy v súlade so stratégiou riadenia kontinuity činností,
- zodpovedá za vypracovanie komplexných plánov obnovy,
- zabezpečuje dostupnosť plánov obnovy,
- zodpovedá za zabezpečenie materiálnych a finančných predpokladov obnovy,
- zabezpečuje pravidelné testovanie plánov obnovy, stanovuje rozsah a spôsob testovania,
- je informovaný o zmenách procedúr/služieb/infraštruktúry/informačných zdrojov, overuje súlad plánu s aktuálnym prostredím.

Koordinátor:

- zodpovedný zamestnanec spravujúci relevantné informačné systémy,
- v prípade vyhlásenia krízového stavu aktivuje komplexný plán obnovy,
- zodpovedá za vypracovanie plánov obnovy ku konkrétnemu informačnému systému,
- vypracúva základné postupy pre plánovanie obnovy – zodpovednosti, poradie obnovy, riadenie (kompetencie), alokuje ľudské zdroje,
- ustanovuje plánovačov a pridelí im na spracovanie jednotlivé havarijné procedúry,
- posudzuje a schvaľuje plány obnovy v spolupráci so správcom,
- je informovaný o zmenách procedúr,
- ak doba obnovy prevýši požadovanú dobu obnovy, konzultuje túto skutočnosť so správcom,
- zabezpečuje testovanie plánov obnovy,
- pri zmene technológií organizačne zabezpečuje zmenu plánov obnovy a ich otestovanie.

Plánovač:

- určený zodpovedný zamestnanec,
- spracúva havarijnú procedúru za svoju oblasť,
- informuje o procedúre tím obnovy,
- predkladá procedúru na schválenie koordinátorovi,
- testuje procedúru spolu s členmi tímu obnovy,
- pri zmene technológií prípadne pri iných významných zmenách zabezpečí informovanie koordinátora, správcu,
- spolupracuje pri vytvorení/zmene plánu obnovy a jeho otestovaní,

Vykonávateľ DRP:

- člen tímu obnovy,

- zodpovedá za výkon jemu prislúchajúcich úloh v havarijnej procedúre,

Pre každú rolu v tíme obnovy musí byť stanovený zástupca. Pre rolu Koordinátora musí byť stanovený aj zástupca druhej úrovne.

5.6 Spôsob testovania a vyhodnocovania procesov riadenia kontinuity

Plány obnovy organizácie sú preverované viacerými testami počas celej doby ich tvorby.

V rámci organizácie má testovanie obnovy tieto formy:

- Skúška – preverenie funkčnosti niektorých detailných postupov a súčastí testu. Skúšky sú vykonávané v priebehu testovania členmi tímu.
- Kontrola obsahu – verbálny prechod krokmi plánu obnovy s cieľom preveriť efektívnosť plánu a identifikovať jeho nedostatky.
- Simulácia – simulácia krízy na základe definovaného scenáru. Touto formou je možné preveriť funkčnosť inicializačných procedúr, procedúr obnovy a komunikácie medzi členmi tímu ako aj dodávateľmi.
- Funkčný test – reálny výkon procedúr obnovy. Presun a obnova systémov v určených lokalitách.
- Úplné prerušenie – simulácia úplného výpadku. Test umožňuje preveriť funkčnosť plánu obnovy, avšak je pri ňom najväčšie riziko prerušenia prevádzky. Test je možné vykonať až po úspešnom ukončení všetkých predchádzajúcich druhov testov.

Plány obnovy sú preverené viacerými testami počas celej doby ich tvorby. Testy všetkých plánov obnovy, ich rozsah a ciele sú zahrnuté v programe testov. Program testov vypracúva Správca DRP po základnom preverení stratégií obnovy a definovaní osnov postupov.

Správca DRP vychádza z podkladov od jednotlivých plánovačov a vytvára program testovania podľa potrieb organizácie tak, aby pokrýval všetky plány obnovy a v nich preveril najmä:

- inicializáciu – preverenie adekvátnosti procedúr inicializácie, aktuálnosť kontaktov a dostupnosť zamestnancov organizácie,
- výkon – preverenie adekvátnosti procedúr obnovy,
- kľúčové dokumenty – preverenie dostupnosti kľúčových dokumentov a informačných zdrojov,
- odozvu dodávateľov – preverenie schopnosti dodávateľov plniť zmluvné záväzky.

V programe testovania sú definované testy pre vyvíjané plány obnovy ako aj testy pre už platné plány obnovy. Vzhľadom k neustálym zmenám v technológiách je potrebné aby boli vykonávané testy obnovy aj pre platné plány obnovy minimálne 1x ročne. V závislosti od vývoja tvorby a testovania plánov Správca DRP upravuje program testovania a predkladá ho na schválenie Sponzorovi DRP.

Forma, rozsah a ciele jednotlivých testov sú stanovené s ohľadom na schopnosti a možnosti tímov obnovy, podmienky prostredia a riziko spojené s výkonom testu. Test funkčnosti plánu obnovy nesmie zapríčiniť výpadok služieb informačného systému. Každý test musí by starostlivo pripravený. Prípravu a celkový výkon testu vedie koordinátor, ktorý dopredu stanoví účastníkov a harmonogram testu tak, aby boli splnené ciele definované v programe testov. Príprava na test musí obsahovať:

- stanovenie cieľov testu,
- scenár udalosti,

- definovanie času a miesta testu,
- obmedzenia pre výkon testu,
- predpoklady pre výkon testu,
- harmonogram výkonu testu,
- body návratu a rollback procedúry.

Testu sa zúčastňujú určení členovia tímu obnovy (interní zamestnanci ako aj pracovníci dodávateľa). členovia tímu musia by s obsahom a formou testu dopredu oboznámení. Významným efektom vykonávania testov je tréning členov tímov obnovy a oboznámenie ich s rolami a úlohami, ktoré vykonávajú v pláne. Úlohou testu je preveriť funkčnosť testovaných komponentov plánu a identifikovať problémy. Pokiaľ sa v priebehu testu identifikujú problémy – test nie je neúspešný.

Po ukončení testu vypracúva koordinátor testu správu o priebehu a výsledkoch testu. S výstupom sú oboznámení všetci členovia tímu obnovy tak, aby mohli zhodnotiť jednotlivé kroky a vzniesť pripomienky k plánu obnovy. Na základe výstupu a podkladov od koordinátora a členov tímu obnovy hodnotí Správca DRP dosiahnutie cieľov testu a rozhoduje o ďalších krokoch v tvorbe plánu obnovy. V prípade nutnosti dodatočných testov upraví program testovania. Po ukončení plánovaných testov definovaných v programe testovania sa stáva plán obnovy platným.

5.7 Pravidlá pre realizáciu opatrení

Pravidlá pre realizáciu opatrení navrhuje manažér kybernetickej a informačnej bezpečnosti a predkladá na schválenie vedeniu organizácie.

Navrhované opatrenia sa prijímajú pre nasledovné domény informačnej a kybernetickej bezpečnosti:

- organizácia kybernetickej bezpečnosti a informačnej bezpečnosti,
- riadenie rizík kybernetickej bezpečnosti a informačnej bezpečnosti,
- personálna bezpečnosť,
- riadenie prístupov,
- riadenie kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,
- bezpečnosť pri prevádzke informačných systémov a sietí,
- hodnotenie zraniteľností a bezpečnostných aktualizácií,
- ochrana proti škodlivému kódu,
- sieťová a komunikačná bezpečnosť,
- akvizícia, vývoja a údržba informačných sietí a informačných systémov,
- zaznamenávanie udalostí a monitorovanie,
- fyzická bezpečnosť a bezpečnosť prostredia,
- riešenie kybernetických bezpečnostných incidentov,
- kryptografické opatrenia,
- kontinuita prevádzky,

- audit, riadenie súladu a kontrolných činností.

6 Postupy zálohovania

Organizácia má postupy zálohovania spracované v samostatnom dokumente, napr. v IT prevádzkovej smernici organizácie. Pri príprave takýchto postupov je možné vychádzať z nasledovnej smernice dostupnej na KB-K2_3-12-Bezpečná-prevádzka-IS-a-sietí.pdf (gov.sk)

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

8.1 Príloha 1 – Osoby oprávnené aktivovať havarijný plán

Meno a priezvisko	Pracovná pozícia	Kontaktné informácie

8.2 Príloha 2 – Členovia tímu obnovy

Meno a priezvisko	Pracovná pozícia	Mobil	Služobné tel. číslo	E-mail