**Smernica riadenia kontinuity činností**



# Obsah

[Obsah 2](#_Toc122421273)

[1 Správa dokumentu 3](#_Toc122421274)

[2 Úvod 4](#_Toc122421275)

[2.1 Rozsah platnosti 4](#_Toc122421276)

[2.2 Použité skratky 4](#_Toc122421277)

[2.3 Cieľ riadenia kontinuity činností 4](#_Toc122421278)

[2.4 Cyklus riadenia kontinuity činností 4](#_Toc122421279)

[2.5 Metodika analýzy rizík a analýzy dopadov 5](#_Toc122421280)

[3 Požiadavky na zabezpečenie riadenia kontinuity činností 6](#_Toc122421281)

[4 Riadenie kontinuity činností 7](#_Toc122421282)

[4.1 Stratégia obnovy 7](#_Toc122421283)

[4.2 Krízové plány 8](#_Toc122421284)

[4.2.1 Plány kontinuity činností (BCP) 8](#_Toc122421285)

[4.2.2 Plány obnovy (DRP) 9](#_Toc122421286)

[4.3 Vyčlenenie zdrojov na zabezpečenie riadenia kontinuity procesov 11](#_Toc122421287)

[4.3.1 Finančné zdroje 11](#_Toc122421288)

[4.3.2 Materiálno-technické zdroje 12](#_Toc122421289)

[4.3.3 Personálne zdroje 12](#_Toc122421290)

[4.4 Komunikačný plán 12](#_Toc122421291)

[4.5 Určenie rolí a zodpovedností 13](#_Toc122421292)

[4.6 Spôsob testovania a vyhodnocovania procesov riadenia kontinuity 13](#_Toc122421293)

[4.7 Pravidlá pre realizáciu opatrení 15](#_Toc122421294)

[5 Postupy zálohovania 16](#_Toc122421295)

[6 Revízia dokumentu 17](#_Toc122421296)

[7 Prílohy 18](#_Toc122421297)

[7.1 Príloha 1: Osoby oprávnené aktivovať plán kontinuity činností (BCP) 18](#_Toc122421298)

[7.2 Príloha 2: Členovia tímu obnovy 19](#_Toc122421299)

[7.3 Príloha 3: Návrh obsahovej štruktúry plánu obnovy 20](#_Toc122421300)

# Správa dokumentu

Dokument „Politika riadenia kontinuity činností“ je vzorovým dokumentom slúžiacim pre potreby orgánov verejnej moci. Vytvorený vzor dokumentu nie je povinný na použitie a ani nie je záväzný. Dokument je poskytnutý voľne a bezplatne na využitie podľa potrieb konkrétnej organizácie.

Vytvorený dokument má aj svoj metodický rozmer, takže je ho 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. Dokument je potrebné upraviť na základe reálnych potrieb a špecifického prostredia 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).

Súčasťou každého dokumentu adaptovaného do prostredia organizácie je aj nasledovný zmenový list obsahujúci informácie minimálne v nasledovnom rozsahu:

|  |  |
| --- | --- |
| **Verzia** |  |
| **Garant dokumentu** |  |
| **Dátum poslednej revízie** |  |
| **Dátum vydania** |  |
| **Dátum účinnosti** |  |

# Úvod

Politika riadenia kontinuity činností (ďalej aj „BCM“) organizácie zdôrazňuje význam:

* porozumenia potrebám organizácie a nevyhnutnosť zabezpečenia kontinuity činností a cieľov,
* implementácie a vykonávania kontrol a opatrení na celkové riadenie schopnosti zvládať rušivé incidenty,
* monitorovanie a preskúmavanie výkonnosti a efektívnosti riadenia kontinuity procesov,
* neustále zlepšovanie založené na objektívnom meraní.

## Rozsah platnosti

Tento dokument sa vzťahuje na všetky informačné systémy organizácie, ktoré súvisia s poskytovaním základnej služby podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej aj „zákon o kybernetickej bezpečnosti“).

Tento dokument je záväzný pre všetkých zamestnancov organizácie a tretie strany zabezpečujúce prevádzku informačných systémov podliehajúcich zákonu o kybernetickej bezpečnosti.

## Použité skratky

|  |  |
| --- | --- |
| Skratka | Popis skratky |
| BCM | Business Continuity Management (Riadenie kontinuity činností) |
| BCP | Business Continuity Plan (Plán kontinuity činností) |
| CD | Compact Disc (Kompaktný disk) |
| DRP | Disaster Recovery Plan (Plán obnovy) |
| IKT | Informačné a komunikačné technológie |
| IS | Informačný systém |
| IT | Informačné technológie |
| USB | Universal Serial Bus (Univerzálna sériová zbernica) |
| Z. z. | Zbierka zákonov |

## Cieľ riadenia kontinuity činností

Cieľom riadenia kontinuity činností v organizácii je:

* zabezpečenie kontinuity prevádzky a poskytovaných služieb,
* zníženie rizík.

## Cyklus riadenia kontinuity činností

Implementáciou riadenia kontinuity činností v organizácii sa zavádza pravidelne sa opakujúci cyklus, ktorý pozostáva z nasledovných krokov:

* analýza rizík, ktorá je zameraná na identifikáciu hrozieb a rizík spojených s dopadom hrozieb na aktíva organizácie,
* analýza dopadov, ktorá identifikuje kritickosť dopadu nedostupnosti procesov na organizáciu,
* implementácia nápravných opatrení na elimináciu rizík alebo ich zníženie na prijateľnú úroveň a identifikácia požiadaviek obnovy procesov,
* definícia základných predpokladov a princípov obnovy v stratégií obnovy,
* tvorba, testovanie a aktualizácia krízových plánov (plánov kontinuity činností a plánov obnovy),
* pravidelné reportovanie vykonaných aktivít.

## Metodika analýzy rizík a analýzy dopadov

Za účelom výkonu analýzy rizík a analýzy dopadov organizácia využíva „Metodiku analýzy rizík a analýzy dopadov. Cieľom tejto metodiky je poskytnúť návody a usmernenia pre správne vykonanie analýzy rizík a analýzy dopadov.

# Požiadavky na zabezpečenie riadenia kontinuity činností

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

* vypracovania stratégie a krízových plánov na zabezpečenie dostupnosti siete a informačného systému po narušení alebo zlyhaní v dôsledku bezpečnostného incidentu na základe vykonania analýzy dopadov bezpečnostného incidentu na základnú službu,
* vyčlenenia adekvátnych finančných, materiálno-technických a personálnych zdrojov na zabezpečenie riadenia kontinuity činností,
* určenia komunikačného plánu na plnenie plánov kontinuity činností a plánov obnovy spolu s kontaktnými údajmi, určeniami rolí a zodpovednosti na plnenie plánov kontinuity činností a plánov obnovy po 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 po bezpečnostnom incidente 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 základnej služby,
* testovania a vyhodnocovania jednotlivých procesov riadenia kontinuity činností a realizácie opatrení na zvýšenie odolnosti sietí a informačných systémov základnej služby,
* určenia plánov obnovy a postupov zálohovania na obnovu siete a informačného systému po jeho narušení alebo zlyhaní v dôsledku bezpečnostného incidentu,
* stanovenia práv a povinností administrátorov a osôb zastávajúcich bezpečnostné roly.

# Riadenie kontinuity činností

Riadenie kontinuity činností v organizácii je súbor aktivít zabezpečujúcich obnovu aktivít organizácie po ich narušení. V prípade narušenia aktivít a prieniku hrozby k aktívam organizácie (napr. personál, technologické prostriedky, budovy) by mohli byť organizácii spôsobené škody značného rozsahu narušením alebo úplným prerušením poskytovania služieb, narušením schopnosti plnenia legislatívnych povinností alebo ohrozením dobrého mena. Organizáciu ohrozujú rôzne typy hrozieb, ktoré je možné zatriediť do troch kategórií:

* technologické – napr. výpadok prúdu, únik plynu, nedostupnosť telekomunikačnej alebo dátovej infraštruktúry,
* prírodné – napr. povodeň, zemetrasenie,
* spoločenské – terorizmus, vydieranie, zdravotné ochorenia.

Cieľom riadenia kontinuity procesov je:

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

## Stratégia obnovy

Stratégia obnovy sa odvíja od určeného cieľového času obnovy (RTO) pre konkrétny informačný systém.

Účelom stratégie obnovy v organizácii:

* identifikovať kritické procesy prostredníctvom analýzy dopadov,
* identifikovať kritické informačné systémy nevyhnutné na chod kritických procesov,
* definovať predpoklady a princípy, podľa ktorých budú vykonávané činnosti v havarijnom stave,
* definovať spôsoby riadenia aktivít, ktoré zabezpečujú obnovu 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 rizík organizácie identifikuje rôzne možnosti obnovy a vybraný optimálny spôsob vzhľadom na implementované technológie a požiadavky.

Norma STN ISO/IEC 27031 Informačné technológie. Bezpečnostné metódy. Návody pre pripravenosť informačných a komunikačných technológií na zabezpečenie kontinuity činnosti – predstavuje nasledovné rôzne prístupy k príprave stratégie obnovy:

* tzv. Hot standby – IKT infraštuktúra je replikovaná na dvoch nezávislých lokalitách,
* tzv. Warm standby – obnova prebieha v alternatívnej/sekundárnej lokalite, kde je IKT infraštruktúra čiastočne pripravená,
* tzv. Cold standby – IKT infraštuktúra je postavená od počiatku v alterntívnej/sekundárnej lokalite,
* tzv. Ship-in – dodávateľ je plne zodpovedný za dodanie hardvéru,
* tzv. High availability – cieľom je získať nepretržitú dostupnosť výpočtových služieb a zdrojov tak, že vzniknutý výpadok systému bude mať na užívateľov minimálny dopad,
* zmiešaný prístup, ktorý pozostáva z prvkov obsiahnutých v prístupoch zmienených vyššie.

|  |
| --- |
| **Bližší popis zvolenej stratégie obnovy a tiež relevantnej internej dokumentácie bude doplnený zo strany organizácie podľa aktuálne implementovanej stratégie obnovy.** |

## Krízové plány

Súčasťou riadenia kontinuity činností je tvorba plánov kontinuity činností a plánov obnovy, ktorých cieľom je riešiť už vzniknuté incidenty v prípade, že závažnosť ich dopadov na činnosť organizácie presahuje štandardné pracovné postupy.

Stratégia riadenia zahŕňa tvorbu krízových plánov, ktorých cieľom je riešiť obnovu v prípade nedostupnosti:

* pracovísk,
* kritických záznamov (papierové alebo elektronické),
* kritických dodávateľov,
* IT infraštruktúry,
* informačných systémov.

Cieľom krízových plánov je:

* koordinovať aktivity obnovy,
* definovať zodpovednosti počas krízovej situácie
* minimalizovať straty,
* vykonať návrat do štátnej prevádzky,
* pravidelne testovať a aktualizovať krízové plány.

Cieľom krízových plánov je poskytnúť návod 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.

### Plány kontinuity činností (BCP)

Plány popisujúce kontinuitu činností v organizácii obsahujú najmä:

* ustanovenie tímu obnovy,
* personálne obsadenie jednotlivých pozícií v rámci tímu obnovy,
* presne zadefinovaný súbor úloh pre členov tímu,
* kontakty na relevantné tretie strany (partneri, dodávatelia a pod.),
* 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.

Osoby oprávnené aktivovať plán sú súčasťou prílohy 1.

Osoby oprávnené aktivovať plán sa skontaktujú s Tímom obnovy a poskytnú mu príslušné pokyny.

Prehľad členov tímu obnovy je uvedený v prílohe 2.

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 (zaistiť, aby neboli poskytnuté žiadne interné informácie),
* 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,
	+ kritických aplikácií,
	+ kritických údajov,
	+ tretích strán,
	+ kritických záznamov,
	+ iného dôležitého materiálu,
	+ poskytnúť spätnú väzbu na už uskutočnené akcie.

### Plány obnovy (DRP)

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

* opravou škôd, ktoré vznikli počas kybernetického incidentu,
* premiestnením prevádzky z dočasných priestorov späť na hlavné miesto,
* presunom na nové miesto.

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

V rámci plánovania obnovy sú v organizácii definované nasledujúce role:

* sponzor DRP:
	+ sponzorom DRP je zástupca vedenia organizácie alebo iný poverený zamestnanec,
	+ presadzuje zámery organizácie,
	+ schvaľuje programy testovania.
* správca DRP:
	+ rolu správcu DRP v organizácii vykonáva manažér kybernetickej a informačnej bezpečnosti
	+ 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:
	+ rolu koordinátora DRP v organizácii vykonáva osoba určená vedením organizácie,
	+ v prípade vyhlásenia krízového stavu aktivuje komplexný plán obnovy,
	+ zodpovedá za vypracovanie plánov obnovy ku konkrétnej technologickej službe/informačnému zdroju (DRP IS),
	+ 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 DRP,
	+ je informovaný o zmenách procedúr,
	+ zabezpečuje testovanie plánov obnovy pre dané služby,
	+ pri zmene technológií organizačne zabezpečuje zmenu plánov obnovy a ich otestovanie.
* vykonávateľ:
	+ člen tímu obnovy,
	+ zodpovedá za výkon jemu prislúchajúcich úloh v havarijnej procedúre,
	+ môže to by pracovník organizácie v roli administrátor IS alebo pracovník dodávateľa.

Návrh obsahovej štruktúry plánu obnovy je súčasťou prílohy č. 3

## Vyčlenenie zdrojov na zabezpečenie riadenia kontinuity procesov

Organizácia určuje nástroje a vyčleňuje zdroje na zabezpečenie riadenie kontinuity činností 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 činností,
* finančnými, logistickými a administratívnymi postupmi na podporu opatrení na zabezpečenie riadenia kontinuity činností pred, počas a po incidente
* cieľmi riadenia zdrojov pre časy odozvy, personál, vybavenie, školenie, financovanie, poistenie, kontrolu zodpovednosti, odborné znalosti, 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, komunikácie a strategickej aliancie medzi zainteresovanými stranami.

### Finančné zdroje

Organizácia určuje možnosti na zabezpečenie potrebných finančných prostriedkov počas a po kybernetickom incidente. Tieto možnosti zahŕňajú:

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

### Materiálno-technické zdroje

Organizácia identifikuje a udržiava zoznam hlavných dodávok, ktoré podporujú jej prioritné činnosti. V organizácii sú materiálno-technické zdroje určené na zabezpečenie riadenia kontinuity činností 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.

### 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.

## Komunikačný plán

Organizácia má ustanovený a implementovaný komunikačný plán, ktorý popisuje:

* odhalenie incidentu a varovanie zodpovedného personálu,
* pokračovanie v monitorovaní incidentu,
* internú komunikáciu medzi rôznymi úrovňami a funkciami 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,
* uľahčenie štruktúrovanej komunikácie s pohotovostnými jednotkami,
* zaznamenávanie dôležitých informácií o incidente, prijatých opatreniach a prijatých rozhodnutiach,
* prevádzku komunikačného zariadenia.

## Určenie rolí a zodpovedností

Pre proces riadenia kontinuity činností sú ustanovené nasledovné roly:

* správca,
* koordinátor,
* vykonávateľ.

Správca v procese BCM najmä:

* vytvára krízové plány,
* zúčastňuje sa obnovy a testov obnovy,
* hodnotí priebeh obnovy a testov obnovy,
* metodicky podporuje koordinátora a členov tímu pri plánovaní obnovy a testov obnovy.

Koordinátor v procese BCM najmä:

* vytvára detailný plán obnovy a testu obnovy,
* organizačne riadi členov tímu obnovy,
* riadi priebeh obnovy a testov obnovy,
* poskytuje informácie pre vyhodnotenie obnovy a testov obnovy.

Vykonávateľ v procese BCM najmä:

* zúčastňuje sa výkonu obnovy a testov obnovy,
* hodnotí a pripomienkuje priebeh obnovy a testov obnovy.

## 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.

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 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,
* 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.

## 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 kybernetickej a informačnej bezpečnosti:

* organizácia informačnej bezpečnosti,
* riadenie aktív, hrozieb a rizík,
* personálna bezpečnosť,
* riadenie dodávateľských služieb, akvizície, vývoja a údržby informačných systémov,
* technické zraniteľnosti systémov a zariadení,
* riadenie bezpečnosti sietí a informačných systémov,
* riadenie prevádzky,
* riadenie prístupov,
* kryptografické opatrenia,
* riešenie kybernetických bezpečnostných incidentov,
* monitorovanie, testovanie bezpečnosti a bezpečnostné audity,
* fyzická bezpečnosť a bezpečnosť prostredia,
* riadenie kontinuity procesov.

# Postupy zálohovania

Postupy zálohovania sa odvíjajú od určeného cieľového bodu obnovy (RPO) pre konkrétny informačný systém.

Organizácia má postupy zálohovania spracované ako súčasť nasledujúcich dokumentov:

* Bezpečnostná politika organizácie,
* iná interná dokumentácia.

|  |
| --- |
| **Bližší popis postupov zálohovania a tiež relevantnej internej dokumentácie bude doplnený zo strany organizácie podľa aktuálneho nastavenia zálohovania.** |

# Revízia dokumentu

Dokument „Riadenie kontinuity činností“ 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.

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

Tento dokument schvaľuje vedenie organizácie.

# Prílohy

## Príloha 1: Osoby oprávnené aktivovať plán kontinuity činností (BCP)

|  |  |  |
| --- | --- | --- |
| **Meno a priezvisko** | **Pracovná pozícia** | **Kontaktné informácie** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Príloha 2: Členovia tímu obnovy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Meno priezvisko** | **Pracovná pozícia** | **Mobil** | **Služobné tel. číslo** | **Email** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Príloha 3: Návrh obsahovej štruktúry plánu obnovy

