Oblast působnosti:	Celá společnost		
Datum vydání:	1.7.2023		
Vypracováno:	1.7.2023	Účinnost od:	1.7.2023
Typ dokumentu:	Směrnice	Označení:	KB 06
Vypracoval:	Ing. Igor Prosecký	Funkce:	Manažer kybernetické bezpečnosti
Podpis:			
Ověřil správnost:	Ing. Jaroslav Kubínek	Funkce	Výrobní náměstek
Podpis:			
Schválil:	Ing. Martin Charvát	Funkce:	Místopředseda představenstva
Podpis:			

Revize:

Číslo změny	Datum provedení změny	Datum účinnosti změny	Obsah změny	Změnu provedl (jméno, podpis)	Změnu schválil (jméno, podpis)
R1					
R2					

R3					
R4					

Obsah

1. ÚVODNÍ USTANOVENÍ

1.1. Účel

Tato směrnice stanoví postupy obnovy poskytování služeb ICT u společnosti Vodovody a kanalizace Pardubice, a.s., v případě narušení jejich poskytování v důsledku mimořádné události. Cílem řízení kontinuity je zajistit dostupnost základní služby pro odběratele služeb a služeb ICT pro uživatele, minimalizovat výpadky ICT a minimalizovat škody způsobené výpadky ICT.

1.2. Závaznost

Tato směrnice je závazná pro všechny zaměstnance určené do bezpečnostních rolí dle VP **Organizace kybernetické bezpečnosti.**

2. VYMEZENÍ POJMŮ

2.1. Použité zkratky

BCM	Řízení kontinuity činností (Business Continuity Management)
BIA	Analýza dopadů (Business Impact Analysis)
ICT	Informační a komunikační technologie (Information and Communication Technologies). Označuje veškeré technologie používané pro komunikaci a práci s informacemi.
IS	Informační systém. Systém pro sběr, udržování, zpracování a poskytování informací a dat.
ISZS	Informační systém základní služby
IT	Informační technologie. Vše, co se týká fungování počítačů po technické stránce.
KB	Kybernetická bezpečnost
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
ON	Organizační norma
RPO	Bod obnovy dat (Recovery Point Objective)
RTO	Doba obnovy chodu (Recovery Time Objective)
SLA	Service level agreement = úroveň podpory služby
SŘBI	Systém řízení bezpečnosti informací
SW	software (programové vybavení) je v informatice sada všech počítačových programů v počítači. Software zahrnuje aplikační software (pracuje s ním uživatel), operační systém (zajišťuje běh programů) a další.
VAK	Vodovody a kanalizace Pardubice, a.s.
VP	Vnitřní předpis

2.2. Definice

2.2.1. *Aktivum*

Jakákoliv entita, která má pro jednotlivce nebo organizaci hodnotu a která může být zmenšena působením hrozby.

2.2.2. *Mimořádná událost*

Bezpečnostní incident v hranicích SŘBI, ISZS, technická porucha, útok, požár, živelná pohroma nebo jakákoli jiná závažná událost, kterou není možné řešit běžnými provozními postupy a která může způsobit přerušení nebo omezení poskytování základní služby či služeb IS SŘBI.

2.2.3. *Cíl obnovy činností – Recovery Point Objective (RPO)*

Ukazatel doby, po kterou lze akceptovat ztrátu informací, a přerušení služeb a dále pak, jak dlouho dokáže IS existovat bez přístupu k těmto údajům a službám. Ukazatel vyhodnocuje, o jaké množství dat lze přijít.
Časový interval je uváděn v minutách, hodinách, dnech, týdnech a měsících.

2.2.4. *Doba obnovy činností – Recovery Time Objective (RTO)*

Ukazatel času, do kterého je potřeba obnovit služby nebo přístup k informacím po či mimořádné události. Časový interval je uváděn v minutách, hodinách, dnech, týdnech a měsících.

3. ŘÍZENÍ KONTINUITY ČINNOSTÍ ICT

3.1. Aspekty řízení zachování kontinuity provozu

Řízení kontinuity činností (dále také Business Continuity Management nebo BCM) je nedílnou součástí systému řízení bezpečnosti informací. V rámci SŘBI a ISZS jsou identifikovány hlavní procesy, které je nutno zabezpečit proti případnému přerušení nebo výpadku poskytované služby. Identifikuje možnosti a dopady mimořádné události v rámci systému řízení bezpečnosti informací, vymezuje a zajišťuje základní rámec pro zvyšování schopnosti VAK rychle, správně a efektivně reagovat na mimořádné události. Standardizuje činnosti při přípravě na řešení mimořádné události a organizaci obnovy do původního stavu.

Cílem řízení kontinuity činností je zejména:

a) stanovit na základě výstupů hodnocení rizik a analýzy dopadů minimální rozsah úrovně a kvality poskytované základní služby a dalších služeb poskytovaných VAK;
b) zajistit bezpečnost a kontinuitu poskytování služeb ICT i v podmínkách vzniku kybernetických bezpečnostních incidentů, událostí, mimořádné události;
c) zahájit kroky směřující k zajištění obnovy služeb na požadovanou úroveň;
d) minimalizovat škody na majetku nebo aktivech, které VAK vlastní a vzniklé v důsledku mimořádné události.

Procesy kontinuity činností jsou řízeny a dokumentovány.
Struktura (životní cyklus) BCM zahrnuje:

a) Porozumění činnostem VAK:
   - identifikace kritických činností (procesů) a zdrojů;
   - analýza dopadů stanovující jaké dopady by mělo narušení klíčových služeb a činností;
   - posouzení rizik – ve vztahu k aktivům a zdrojům, využívaným v kritických činnostech.
b) Určení celkové strategie BCM:
   - stanovení strategie obnovy procesů a zdrojů;
   - vývoj a implementace plánů BCM;
   - testování a udržování plánů BCM.
c) Vytvoření a upevňování kultury BCM a bezpečnostního povědomí zaměstnanců.

3.2. Cíle BCM

Základní cíle BCM VAK jsou:

a) stanovit na základě výstupů hodnocení rizik a analýzy dopadů minimální rozsah a úroveň poskytované základní služby a služeb zajišťujících interní agendy VAK;
b) zajistit, že informace a služby musí být v definované kvalitě a v požadované úrovni dostupné tomu, kdo je k nim oprávněn a v době, která je k tomu určená;
c) zajistit bezpečnost a kontinuitu poskytování služeb ICT i v podmínkách vzniku kybernetických bezpečnostních incidentů, kybernetických bezpečnostních událostí, mimořádné události nebo v případě narušení poskytování služeb ICT s cílem minimalizovat škody na majetku a aktivech VAK;
d) pravidelné ověřování aktuálnosti dokumentovaných postupů a procesů;
e) zajištění povědomí o řízení kontinuity provozu.

3.3. Řízení systému BCM

Za řízení systému BCM odpovídá Výbor pro řízení kybernetické bezpečnosti a za jeho plánování a implementaci odpovídá Manažer KB.
Mezi základní práva a povinnosti všech bezpečnostních rolí patří:

a) každý zaměstnanec VAK, který zjistí bezpečnostní událost, která může způsobit přerušení činností a zajišťovaných služeb v rámci SŘBI a ISZS, musí postupovat podle procesů zvládání kybernetických bezpečnostních událostí a incidentů, v souladu s VP **Zvládání kybernetických událostí a incidentů**;
b) Manažer KB je odpovědný za posouzení rizik a analýzu dopadů v rámci celého SŘBI, včetně ISZS;
c) Manažer KB, v součinnosti s Architektem KB a Garanty aktiv, je odpovědný za implementaci reaktivních opatření vydaných NÚKIB, s cílem minimalizovat vliv těchto opatření na kontinuitu činností;
d) Garanti aktiva jsou odpovědní za určení základních požadavků na dostupnost aktiva;
e) Manažer KB ve spolupráci s Architektem KB a Garanty aktiv, je odpovědný za vypracování Havarijních plánů ICT a Plánů obnovy. K tomu je oprávněn vyžádat potřebnou součinnost odpovědných zaměstnanců VAK.

3.4. Strategie řízení kontinuity činností

Rozsah kontinuity činností odpovídá rozsahu a hranicím SŘBI, včetně ISZS.

Posouzení rizik je základním východiskem BCM. Je koordinováno a řízeno Manažerem KB v souladu s metodickým pokynem **Metodika analýzy rizik kybernetické bezpečnosti**.

Posouzení rizik dále zahrnuje hodnocení dopadů bezpečnostních událostí a incidentů a současně dopady opatření, vydaných Národním úřadem pro kybernetickou bezpečnost, na kontinuitu činností VAK.

3.5. Analýza dopadů

Při analýze dopadů se vychází z informací a hodnot získaných při identifikaci a hodnocení aktiv, zejména z požadavků na dostupnost jednotlivých aktiv.

Cílem analýzy dopadů je stanovit pořadí obnovy aktiv, které zabezpečí efektivní obnovu funkčnosti IS v případě výskytu nepředvídané události a stanovení časů obnovy jednotlivých aktiv, které jsou základním parametrem pro plánování kontinuity.
Během analýzy dopadů je identifikována minimální úroveň/dostupnost zdrojů a služeb a jsou stanoveny další podmínky pro dosažení akceptovatelných parametrů. Úroveň těchto parametrů ovlivňuje ekonomickou náročnost na jejich zajištění a je stanovována tak, aby byla akceptovatelná jak pro VAK, tak pro okolí (zainteresované strany).
Analýza dopadů identifikuje dopady hrozby na SŘBI a ISZS. Určuje velikost ztrát v důsledku narušení nebo přerušení činnosti a škod na majetku VAK v případech, kdy nemohou být vykonávány kritické procesy, provozovány kritické zdroje, poskytovány kritické služby. Analýza dopadů identifikuje přijatelný časový úsek, ve kterém je nutné obnovit kritické a související procesy (RTO – Recovery Time Objective), včetně jejich obnovy na dohodnutou úroveň funkčnosti a použití v rámci VAK. Hodnoty RTO, doporučené časy pro obnovu jednotlivých aktiv, jsou stanoveny v rámci analýzy dopadů.

Analýza dopadů identifikuje současně maximální přípustnou ztrátu dat za definovaný čas (RPO – Recovery Point Objective). Tuto hodnotu určuje Garant podpůrného aktiva a její výsledek je zohledněn při návrhu příslušných opatření.

Vedoucí oddělení IT a Garant primárních aktiva ISZS vedou seznamy provozovaných IS, u kterých Garanti aktiv společně s Manažerem KB a Architektem KB stanoví RTO a RPO, tzn. RTO – maximální přípustnou dobu nedostupnosti provozovaných aplikací a služeb a RPO – maximální možnou ztrátu dat. Hodnoty RPO a RTO jsou evidovány v provozní dokumentaci pro každý IS zvlášť.
Na základě stanovených RPO, RTO jsou Garanty aktiv nastavovány mechanismy zálohování, obnovy dat a definování parametrů poskytované služby dodavatelem zahrnující minimálně:

a) reakční dobu;
b) dobu řešení;
c) garantovanou dobu dostupnosti služby a
d) nejdelší dobu výpadku služby.

Výše uvedené parametry vede vedoucí oddělení IT pro klíčové služby, které poskytuje uživatelům VAK oddělení IT.
Výstupy analýzy dopadů zpracovává Manažer KB v součinnosti s Architektem KB a následně zajišťují aktualizaci dokumentace BCM.
V případě ISZS jsou hodnoty RTO a RPO schvalovány Výborem pro řízení kybernetické bezpečnosti.

3.6. Havarijní plánování

Zachování kontinuity provozu SŘBI a ISZS je prvořadým cílem havarijního plánování. Jsou zpracovány plány pro řešení havarijních situací a plány obnovy, které jsou podrobně rozpracovány v dokumentech **Havarijní plán ICT**. Potřeba zajištění provozu je závislá na správném stanovení kritičnosti procesů, na hodnotě aktiv ISZS a dopadu havárií.

Havarijní plán ICT zpracovává Manažer KB ve spolupráci s vedoucím oddělení IT, Architektem KB a Garanty aktiv. V plánech je stanoven rozsah odpovědností a povinnosti osob zastávajících určené role pro řešení havárií.

Dokumentace BCM

Základní dokumentace BCM je zpracována v rozsahu:

a) Havarijní plán ICT, včetně plánu kontinuity provozu a komunikace;
b) Plán obnovy;
c) Plán záloh.

Plány musí být uloženy mimo systém tak, aby byla zajištěna jejich dostupnost i v případě havárie nebo kybernetického bezpečnostního incidentu. Za uložení a revize plánů odpovídají Garanti aktiv. Revize plánů a s ní související aktualizace plánů se provádí vždy při významné změně a současně minimálně jedenkrát za rok.

a) Havarijní plán ICT

Havarijní plán ICT zahrnuje:

- povinnosti a odpovědnosti rolí BCM;
- jednotlivé krizové situace, které mohou v rámci VAK nastat (dílčí havarijní scénáře);
- popis možných dopadů na procesy a služby VAK;

- oznamování bezpečnostních událostí;
- podmínky aktivace Havarijního plánu ICT;
- kontaktní údaje;
- komunikační plán – kdo s kým a co bude komunikovat, zejména kdo komunikaci schvaluje, kdo komunikuje vně organizace (např. směrem k médiím, zákazníkům, úřadům, dodavatelům apod.) a kdo dovnitř (např. směrem k zaměstnancům),
- havarijní tým;
- Plán zajištění kontinuity provozu:
  - krizová opatření a organizační pokyny pro udržení chodu organizace i v případě rozsáhlého kybernetického incidentu;
  - pokyny pro zaměstnance v případě krizové situace, včetně alokace lidí, nástrojů a dalších zdrojů.

b) Plán obnovy

Plán obnovy zahrnuje:

- povinnosti a odpovědnosti rolí BCM;
- konfigurační management;
- minimální úroveň poskytovaných služeb;
- doby obnovení chodu;
- obnova systémů, technologií a serverů;
- obnova lokality;
- obnova instalací SW a IS;
- postupy obnovy dotčené ICT infrastruktury (v podobě seznamů kroků, které je nezbytné provést, tak aby byl kompletní ale zároveň jednoduše interpretovatelný);
- obnova dat, definování bodu obnovení dat jako časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání IS;
- návrat do normálního provozu;
- kontaktní údaje na odpovědné osoby.

Odpovědnosti za plánování a realizaci Plánů obnovy jsou uvedeny ve VP **Bezpečnostní politika informací.**

c) Plán záloh

Plán záloh zahrnuje:

- povinnosti a odpovědnosti rolí BCM;
- stanovení systému zálohování;
- popis zálohovacího systému;
- obnova systému ze záloh.

Odpovědnosti za plánování a realizaci Plánů záloh jsou uvedeny ve směrnici VP **Bezpečnostní politika informací**.

Dokumentaci BCM pro ISZS schvaluje Výbor Pro řízení kybernetické bezpečnosti.

Za prokazatelné seznámení osob určených do bezpečnostních rolí, včetně dodavatelů, s jejich odpovědnostmi a povinnostmi v BCM, odpovídá vedoucí oddělení IT a Garant primárního aktiva ISZS, každý ve své působnosti.

3.7. Testování Havarijního plánu ICT

Manažer KB v součinnosti s Architektem KB a Garanty aktiv sestavuje Plán testování havarijních scénářů, ve kterém specifikuje termíny a způsoby testování jednotlivých scénářů Havarijního plánu ICT a dalších vybraných oblastí.
Předmětem testování jednotlivých scénářů je ověřit, že zaměstnanci v relevantních bezpečnostních rolích znají své povinnosti a nastavené postupy na sebe navazují tak, jak je v plánech uvedeno. Hlavním úkolem testování plánů je identifikace nedostatků, které je potřeba odstranit a zlepšit.
Účinnost Havarijního plánu ICT ověřuje Manažer a Architekt KB ve spolupráci s Garanty aktiv a dalšími pověřenými zaměstnanci teoretickou simulací testované havárie a praktickými testy tam, kde je to možné, účelné nebo se jedná o kritické systémy. Údržbu, přehodnocení a změny Havarijního plánu ICT zajišťuje Manažer KB, který úzce spolupracuje s Architektem KB, Garanty aktiv a zaměstnanci oddělení IT.
Testování Havarijního plánu ICT schvaluje Výbor pro řízení kybernetické bezpečnosti.
Testování Havarijního plánu ICT se provádí jedenkrát ročně.
Po každém testovaném scénáři musí Manažer KB v součinnosti s Architektem KB a Garanty aktiv vyhodnotit průběh a způsoby zvládnutí scénáře a na základě zjištěných informací rozhoduje o přijetí dodatečných opatření.
Z každého testu musí být Manažerem KB vypracován záznam, který je předkládán jako součást přezkoumání systémů řízení bezpečnosti informací.

4. SOUVISEJÍCÍ DOKUMENTY

4.1. Vnitřní předpisy

Bezpečnostní politika informací
Organizace kybernetické bezpečnosti
Bezpečné chování uživatele
Zvládání kybernetických bezpečnostních událostí a incidentů
Řízení dodavatelů
Řízení dokumentovaných informací
Pracovní řád

4.2. Metodické pokyny

Metodika analýzy rizik kybernetické bezpečnosti

4.3. Ostatní dokumenty

Aktuální zpráva z analýzy rizik