Úřad vlády České republiky

Odbor Rady pro výzkum, vývoj a inovace

PŘÍRUČKA ISMS

Zpracoval:	kolektiv RELSIE
Schválil:	Marek Jan
Verze:	1.0
Datum:	28. listopadu 2018

Obsah

1 ÚVOD

1.1 Účel dokumentu

Dokument „Příručka ISMS“ je základním dokumentem systému řízení bezpečnosti informací (ISMS) pro informační systém pro výzkum, vývoj a inovace (IS VaVaI).

Informace o systému řízení ISMS jsou uvedeny:

- v této příručce
- v Politice bezpečnosti informací IS VaVaI
- v procesním modelu „Systém řízení bezpečnosti informací“
- v dalších dokumentech nebo směrnicích, a dále
- v záznamech vznikajících v rámci fungování systému řízení ISMS.

Všechny procesy systému řízení bezpečnosti informací, které plynou z požadavků normy ČSN ISO/IEC 27001, jsou zachyceny ve výše zmíněném procesním modelu „Systém řízení bezpečnosti informací“. Tento model je vedle Příručky ISMS a Politiky bezpečnosti informací nedílnou součástí celkové dokumentace k ISMS.

Tato příručka slouží jakožto „rozcestník“ směrem na ostatní dokumenty obsahující informace o systému řízení ISMS.

1.2 Působnost

Dokument „Příručka ISMS“ je určen pro vnitřní potřebu Odboru Rady pro výzkum, vývoj a inovace.

Tato příručka ISMS je závazná pro všechny pracovníky Odboru Rady pro výzkum, vývoj a inovace.

1.3 Použité zkratky

Zkratka	*Vysvětlení*
IS VaVaI	Informační systém výzkumu, vývoje a inovací
ÚV ČR	Úřad vlády České republiky
RVVI	Rada pro vědu, výzkum a inovace, poradní orgán Vlády České republiky
KB	Kybernetická bezpečnost
ISMS / SŘBI	Information Security Management System / Systém řízení bezpečnosti informací
ISO	International Organization for Standardization - mezinárodní organizace zabývající se tvorbou norem

2 DEFINICE A POPIS ISMS

2.1 Cíl ISMS

Účelem zavedení ISMS je zajištění a kontrola bezpečnosti informací, v souladu s obecně závaznými předpisy a doporučeními příslušných norem pro oblast bezpečnosti informací. **Cílem je stanovení zásad, pravidel, kompetencí a odpovědností v oblasti řízení a zajištění bezpečnosti informací.**

Hlavním záměrem je důsledná ochrana informací obsažených v IS VaVaI v rozsahu stanoveným příslušnými ISO normami a právními normami. Právní normy vyplývají ze skutečnosti, že IS VaVaI je klasifikován jako významný informační systém dle zákona o kybernetické bezpečnosti.

2.2 Kontext ISMS

Účelem stanovení kontextu je zaznamenání všech vlivů, které mají být zohledněny při stanovení přiměřených opatření a adekvátního přístupu v rámci systému ISMS. Tyto vlivy působí na bezpečnost informací, a proto je třeba neustále sledovat jejich případné změny a tyto promítnout do systému řízení bezpečnosti informací.

Stanovení kontextu ISMS:

- Účel IS VaVaI:
  IS VaVaI je definován § 30 zákona č. 130/2002 Sb., o podpoře výzkumu, experimentálního vývoje a inovací z veřejných prostředků a o změně některých souvisejících zákonů (zákon o podpoře výzkumu, experimentálního vývoje a inovací) ve znění pozdějších předpisů a nařízením vlády č. 397/2009 Sb., o informačním systému výzkumu, experimentálního vývoje a inovací.
- Zajištění financování IS VaVaI (zajišťováno Úřadem vlády ČR)
- Zajištění ochrany informací proti neoprávněnému pozměňování údajů obsažených v IS VaVaI
- Zajištění ochrany osobních údajů uložených v IS VaVaI

2.3 Rozsah ISMS

Rozsah ISMS je definován v příloze č. 1 „Rozsah ISMS pro IS VaVaI“.

2.4 Rozhodnutí o zavedení ISMS

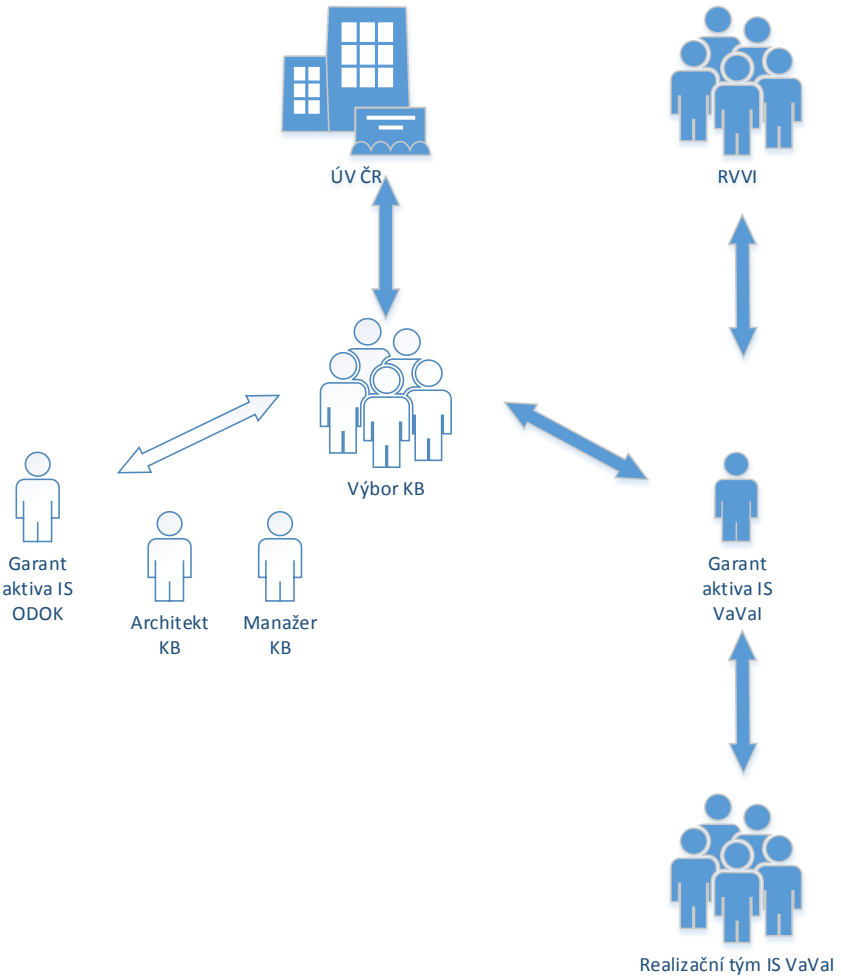
Přijetí rozhodnutí o zavedení ISMS je pro organizaci strategickým rozhodnutím. Toto rozhodnutí bylo provedeno na základě stanovení IS VaVaI jakožto významného informačního systému dle zákona o kybernetické bezpečnosti.

3 ORGANIZACE BEZPEČNOSTI INFORMACÍ

Na organizaci a řízení bezpečnosti informací se podílejí všichni pracovníci Oddělení informačních systémů, které je součástí Odboru Rady pro výzkum, vývoj a inovace. Konkrétní povinnosti pracovníků jsou stanoveny v dokumentaci ISMS a v popisu jejich pracovní náplně.

3.1 Odpovědnosti v ISMS

V úvodu této části je nezbytné definovat pozici IS VaVaI v rámci Úřadu vlády ČR a dokumentovat okolí ISMS v rámci ÚV ČR.



Obrázek 1 - Bezpečnostní role v rámci Úřadu vlády ČR

V rámci ISMS pro IS VaVaI vystupují tyto základní role:

- Manažer KB IS VaVaI
- Garant primárního aktiva IS VaVaI
- Garant podpůrného aktiva IS VaVaI
- Architekt KB IS VaVaI
- Uživatel IS VaVaI

Specifikace rolí je uvedena v příloze č. 2 „Bezpečnostní role v ISMS“, jejich použití je dokumentováno procesním modelem.

4 ŘÍZENÍ AKTIV

Řízení aktiv je v procesním modelu popsáno procesem **B 01 Řízení aktiv.**

4.1 Metodika hodnocení aktiv

Metodika hodnocení aktiv je řešena v dokumentu „Metodika identifikace a hodnocení aktiv IS VaVaI“, který je samostatným dokumentem, není součástí této příručky.

4.2 Provádění identifikace a hodnocení aktiv

Identifikace a následné hodnocení aktiv proběhne prostřednictvím řízených pohovorů s garanty aktiv. Postup identifikace a hodnocení je popsán dokumentu „Metodika identifikace a hodnocení aktiv IS VaVaI“, který je samostatným dokumentem, není součástí této příručky.

5 ŘÍZENÍ RIZIK

Řízení rizik je v procesním modelu popsáno procesem **B 02 Řízení rizik.**

5.1 Metodika posuzování rizik

Je definována metodika řízení rizik, která je popsána v dokumentu „Metodika řízení rizik kybernetické bezpečnosti IS VaVaI“. Tento dokument je samostatným dokumentem, není součástí této příručky.

5.2 Provádění posuzování rizik

Je definována metodika řízení rizik, která zahrnuje i jejich posuzování a která je popsána v dokumentu „Metodika řízení rizik kybernetické bezpečnosti IS VaVaI“. Tento dokument je samostatným dokumentem, není součástí této příručky.

Posuzování rizik je v procesním modelu popsáno procesem **B 02 Řízení rizik,** který obsahuje podproces na posuzování (hodnocení) rizik.

5.3 Ošetření rizik

Ošetření rizik je prováděno podle metodiky řízení rizik kybernetické bezpečnosti IS VaVaI, která není přílohou této příručky. Na základě provedených činností je zpracován plán opatření bezpečnosti informací (neboli plán opatření v rámci řízení bezpečnosti informací pro IS VaVaI). Formulář pro tento plán je uveden v příloze č. 4 „Plán opatření bezpečnosti informací“.

5.4 Cíle bezpečnosti informací

Cíle bezpečnosti informací jsou stanoveny v rámci prováděných činností dle metodiky řízení rizik kybernetické bezpečnosti IS VaVaI. Tato metodika tvoří samostatný dokument, není součástí této příručky.

6 PODPORA ISMS A ORGANIZAČNÍ OPATŘENÍ

6.1 Zdroje pro řízení a zajištění bezpečnosti

Úkolem zdrojů pro řízení a zajištění bezpečnosti je ustavení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací. Součástí tohoto systému je neustálé vzdělávání zaměstnanců v oblasti bezpečnosti. Podle platného organizačního řádu má řízení lidských zdrojů na starosti Odbor personální. Personální rozvoj zaměstnanců je konkrétně zajišťován Oddělením personálního rozvoje a péče o zaměstnance (jakožto součástí personálního odboru). Toto oddělení vytváří a spravuje plány vzdělávání, eviduje realizované vzdělávací akce, provádí vyhodnocení ročních plánů vzdělávání apod.

6.2 Bezpečnost lidských zdrojů

Pro bezpečnostní povědomí lidských zdrojů v organizaci, v souladu s § 9 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, jsou prováděna pravidelná školení, která jsou zahrnuta do plánu vzdělávání. Formulář na tento plán je obsažen v příloze č. 5 „Plán vzdělávání“.

6.3 Dokumentace ISMS (pravidla pro řízení dokumentovaných informací)

Na řízení těchto informací je aplikován cyklus P-D-C-A (tj. Plánuj-Dělej-Kontroluj-Jednej). Tato iterativní metoda, založená na čtyřech základních krocích, je využívána k neustálému zlepšování a zdokonalování procesů, služeb apod.

Řízení dokumentovaných informací je v procesním modelu popsáno procesem **C 08 Řízení dokumentů a záznamů.**

6.4 Řízení dodavatelů

Řízení dodavatelů je v procesním modelu popsáno procesem **A 05 Řízení dodavatelů**.

Je třeba uvést, že Úřad vlády ČR je pro IS VaVaI poskytovatelem všech nezbytných služeb. Žádné externí dodavatele IS VaVaI nemá.

7 KONTROLA A HODNOCENÍ ISMS

7.1 Monitorování a měření účinnosti

Monitorování je v procesním modelu popsáno procesem **B 03 Monitorování ISMS.**

7.2 Interní audit ISMS

Interní audit je v procesním modelu popsán procesem **C 04 Interní audit.** Dále je popsán metodikou interního auditu kybernetické bezpečnosti IS VaVaI. Tato metodika tvoří samostatný dokument, není součástí této příručky.

7.3 Přezkoumání ISMS vedením

Přezkoumání ISMS vedením je v procesním modelu popsáno procesem **A 03 Přezkoumání ISMS.** Výstupem z tohoto procesu je dokument „Zpráva z přezkoumání ISMS vedením“, jejíž struktura je obsažena v příloze č. 7 „Zpráva z přezkoumání ISMS vedením“.

8 ZLEPŠOVÁNÍ

Zlepšování je v procesním modelu popsáno procesem **A 04 Zlepšování ISMS**. Výstupem bude záznam „Rozhodnutí o návrhu“.

9 NESHODY A NÁPRAVNÁ OPATŘENÍ

Při výskytu neshody je třeba vždy přijmout opatření k řízení a nápravě neshody. Řešení neshod je v procesním modelu popsáno procesem **B 04 Řízení incidentů a problémů**. Jeho výstupem je záznam „Nápravné opatření“.

Dále je třeba vyhodnotit potřebu pro opatření k odstranění příčin neshody (aby se neshoda znovu nevyskytla) a tato nalezená opatření implementovat, včetně přezkoumání efektivnosti každého přijatého opatření.

10 BEZPEČNOSTNÍ UDÁLOSTI A INCIDENTY

Řešení bezpečnostních událostí a incidentů je v procesním modelu popsáno procesem **B 04 Řízení incidentů a problémů.** Výstupem tohoto procesu je dokument „Záznam o incidentu nebo problému“, který je určen pro Manažera KB Úřadu vlády. Jeho forma je určena vyhláškou č. 82/2018 Sb.

V příloze č. 8 této příručky („Záznam incidentu“) je uložen návrh šablony pro interní záznam o způsobu vyřešení incidentu.

11 ŘÍZENÍ KONTINUITY ČINNOSTI IS VAVAI

Řízení kontinuity činnosti informačního systému je v procesním modelu popsáno procesem **C 06 Řízení kontinuity**. Podrobnější informace k této problematice jsou uvedeny v příloze č. 11 „Řízení kontinuity“.

12 ŘÍZENÍ ZMĚN, AKVIZICE, VÝVOJ, ÚDRŽBA

Řízení změn, akvizice, vývoj, údržba je v procesním modelu popsáno procesem **C 05 Řízení změn IS VaVaI, akvizice, vývoj.**

13 ZÁVĚREČNÁ USTANOVENÍ

13.1 Seznam příloh dokumentu

Uvedené přílohy jsou součástí této příručky.

Příloha č.	*Název*
1	Rozsah ISMS pro IS VaVaI
2	Bezpečnostní role v ISMS
3	Prohlášení o aplikovatelnosti
4	Plán opatření bezpečnosti informací
5	Plán vzdělávání
6	Cíle bezpečnosti informací
7	Zpráva z přezkoumání ISMS vedením
8	Záznam incidentu
9	Oznámení o provedení reaktivního a ochranného opatření
10	Přehled právních a smluvních požadavků
11	Řízení kontinuity

13.2 Historie změn dokumentu

Verze	*Autor*	*Datum*	*Stručný popis změn*
1.0	Kolektiv RELSIE	23.11.2018	Vypracování dokumentu
1.1	Kolektiv OIS	11.1.2019	Úpravy formulací

14 PŘÍLOHY

Příloha č. 1

Rozsah ISMS pro IS VaVaI

Systém řízení bezpečnosti informací pro IS VaVaI pokrývá všechna aktiva tohoto systému.

K zajištění bezpečnosti informací, se kterými je nakládáno na pracovištích IS VaVaI, je implementován „Systém řízení bezpečnosti informací (ISMS) pro IS VaVaI“, jehož hranice ISMS jsou definovány:

1) z hlediska organizační struktury Oddělení pro informační systémy,
2) z hlediska pracoviště Oddělení pro informační systémy,
3) z hlediska informační infrastruktury a IS VaVaI a
4) z hlediska služeb externích subjektů

Rozsah z hlediska organizační struktury

ISMS zahrnuje Oddělení informačních systémů, které je součástí Odboru Rady pro Výzkum, vývoj a inovace. Organizační struktura pracovních pozic včetně vykonávaných rolí je znázorněna v procesním modelu.

Rozsah z hlediska pracovišť týkajících se IS VaVaI

Pro stanovení výčtu všech pracovišť, tedy míst, kde se pracuje s IS VaVaI a odkud se k němu přistupuje, je třeba uvést tyto lokality:

- Interní pracoviště (pracoviště Oddělení informačních systémů), kde se nachází obsluha IS VaVaI (programátoři, systémoví administrátoři apod.). Toto pracoviště se nachází v 5. patře budovy Ministerstva dopravy ČR (servrovna se nachází v suterénu budovy Úřadu vlády ve Strakově akademii),
- Pracoviště uživatelů, majících přístup do IS VaVaI, tj. veřejnosti, která systém používá,
- Pracoviště členů Rady pro výzkum, vývoj a inovace, kteří přistupují k IS VaVaI prostřednictvím VPN.

Rozsah z hlediska informační infrastruktury a IS VaVaI

IS VaVaI je tvořen čtyřmi provázanými částmi, kterými jsou Evidence veřejných soutěží ve výzkumu, vývoji a inovacích, Centrální evidence aktivit výzkumu, vývoje a inovací, Centrální evidence projektů a Rejstřík informací o výsledcích. IS VaVaI je doplněn o již neaktivní modul Centrální evidence výzkumných záměrů.

ISMS pro IS VaVaI zahrnuje všechny čtyři zmíněné části systému.

Rozsah z hlediska služeb externích subjektů

Odbor informatiky Úřadu vlády ČR poskytuje pro IS VaVaI službu zálohování. Nicméně Úřad vlády se tu nevyskytuje v roli externího dodavatele.

Příloha č. 2

Bezpečnostní role v ISMS

Systém řízení bezpečnosti informací (ISMS) IS VaVaI předpokládá výkon odborných bezpečnostních rolí, které bezprostředně souvisí s ISMS a se zajištěním bezpečnosti informací IS VaVaI. V této příloze je rozpracována působnost následujících rolí z pohledu potřeb řízení bezpečnosti informací:

1) Manažer KB IS VaVaI
2) Garant primárního aktiva IS VaVaI
3) Garant podpůrného aktiva IS VaVaI
4) Architekt KB IS VaVaI
5) Uživatel IS VaVaI

Působnost a povinnosti těchto rolí je uvedena níže. Jednotlivé role jsou též znázorněny v procesním modelu (část 02 Organizační struktura).

Manažer KB IS VaVaI

Působnost:

Manažer KB IS VaVaI řídí, koordinuje a vykonává činnosti související se zajištěním bezpečnosti informaci v IS VaVaI.

Jmenování:

Manažera KB IS VaVaI jmenuje ředitel Odboru Rady pro výzkum, vývoj a inovace.

Odpovědnost:

(1) Manažer KB IS VaVaI je osoba odpovědná za systém řízení bezpečnosti informací IS VaVaI od prevence přes průběžné testování až po eliminaci následků a vyhodnocení kybernetických incidentů.
(2) Odpovídá za tvorbu a aktualizaci Strategie kybernetické bezpečnosti IS VaVaI a aktualizaci Politiky bezpečnosti informací IS VaVaI.
(3) Odpovídá za plánování, organizování a řízení realizace opatření a projektů souvisejících s řízením bezpečnosti informací tak, aby bylo dosaženo cílů stanovených zákonem o kybernetické bezpečnosti a jeho prováděcími předpisy, a to ve stanoveném termínu a v rámci stanoveného rozpočtu.
(4) Manažer KB IS VaVaI působí jako kontaktní osoba pro kybernetickou bezpečnost, prosazuje a koordinuje úlohu systému řízení informační bezpečnosti v organizaci.
(5) Manažer KB IS VaVaI zajišťuje koordinaci všech činností při ochraně primárního aktiva a všech dotčených podpůrných aktiv.
(6) V oblasti prosazování principů a zásad kybernetické bezpečnosti spolupracuje Manažer KB IS VaVaI s Výborem kybernetické bezpečnosti Úřadu vlády ČR a s jednotlivými ustanovenými rolemi Úřadu vlády ČR prostřednictvím Odboru Rady pro vědu, výzkum a inovace. Úřad vlády ČR komunikuje s RVVI a zajišťuje koordinaci činností realizačního týmu IS VaVaI v rámci Odboru Rady pro vědu, výzkum a inovace Úřadu vlády ČR.

Hlavní úkoly Manažera KB IS VaVaI

- definice klíčových projektů, které vedou k naplnění bezpečnostní politiky a k dosažení cílového stavu modelu architektury kybernetické bezpečnosti, dohlížení na jejich realizaci a vyhodnocení,
- analýza architektury kybernetické bezpečnosti, definice metrik a identifikace existujících rizik včetně návrhu strategie na jejich zmírnění či eliminaci,
- příprava pravidel a standardů pro oblast kybernetické bezpečnosti,
- vedení realizačního týmu IS VaVaI (všichni pracovníci v definovaných rolích řízení kybernetické bezpečnosti) a koordinace jeho činností,
- prosazování bezpečnosti informací IS VaVaI,
- řízení systému bezpečnosti informací IS VaVaI a prosazování Politiky bezpečnosti informací IS VaVaI,
- aktualizace Politiky bezpečnosti informací IS VaVaI,
- tvorba a aktualizace Strategie kybernetické bezpečnosti IS VaVaI,
- koordinace tvorby bezpečnostního konceptu IS VaVaI, konceptu plánu obnovy a ostatních dílčích konceptů a systémových bezpečnostních pravidel, jakož i vydávání doplňujících pravidel a vodítek celkové kybernetické bezpečnosti,
- iniciace, sledování a vyhodnocování implementace opatření kybernetické bezpečnosti,
- informování Výboru a RVVI o bezpečnostních incidentech, zjištěných neshodách a nedostatečné efektivnosti bezpečnostních opatření,
- informování vedení ÚV ČR a RVVI o aktuálním stavu systému řízení informační bezpečnosti,
- koordinace projektů spojených s kybernetickou bezpečností,
- zvládání kybernetických bezpečnostních událostí,
- ověření a vyšetření bezpečnostních incidentů,
- koordinace opatření ke zvýšení bezpečnostního povědomí v organizaci a školení kybernetické bezpečnosti,
- provádění činností stanovených plánem opatření bezpečnosti informací a dohled nad splněním všech plánovaných úkolů,
- příprava podkladů pro přezkoumání systému řízení bezpečnosti informací, průběžné hodnocení aktuálního stavu úrovně bezpečnosti informací podle stanovených metrik,
- dokumentace systému řízení kybernetické bezpečnosti,
- komunikace s Manažerem KB Úřadu vlády.

<u>Nezbytná odbornost/znalosti:</u>

- získání certifikace „Certified Information Security Manager (CISM)“ nebo obdobné certifikace,
- alespoň 3 roky praxe v oboru informační nebo kybernetické bezpečnosti, nebo
- absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti.

Manažer KB IS VaVaI je zapojen ve všech důležitých projektech s dopadem na zpracování, přenos a ukládání informací, zavádění nových nebo změny existujících systémů a procedur s dopadem do informační bezpečnosti IS VaVaI ve fázi jejich přípravy a aplikace.

Manažer KB IS VaVaI je seznámen se všemi projekty s dopadem na zpracování, přenos a ukládání informací IS VaVaI, zavádění nových nebo změny existujících systémů a procedur s dopadem na bezpečnost informací. Cílem tohoto opatření je zajistit, že budou náležitě vzaty do úvahy veškeré aspekty kybernetické bezpečnosti ve fázích přípravy, realizace a implementace všech relevantních projektů.

Garant primárního aktiva IS VaVaI

Působnost:

Stanovuje základní požadavky na provoz a ochranu aktiv.

Jmenování:

Garanta primárního aktiva IS VaVaI jmenuje ředitel Odboru Rady pro výzkum, vývoj a inovace.

Odpovědnost:

- Garant primárního aktiva IS VaVaI odpovídá za zajištění rozvoje, použití a bezpečnosti aktiva.
- Garant primárního aktiva IS VaVaI odpovídá za stanovení parametrů aktiva, zejména požadavků na dostupnost, bezpečnost, integritu a akceptaci zbytkových rizik.

Znalosti/odbornost:

- Dobrá znalost aktiva, jehož je garantem,
- Dobrá znalost interních bezpečnostních politik a metodik.

Garant podpůrného aktiva IS VaVaI

Působnost:

Garant podpůrného aktiva IS VaVaI zajišťuje rozvoj, použití a bezpečnost svěřeného aktiva.

Jmenování:

Garanta podpůrného aktiva IS VaVaI jmenuje vedoucí Odboru Rady pro výzkum, vývoj a inovace.

Odpovědnost:

Garant podpůrného (technického) aktiva IS VaVaI odpovídá za správu a rozvoj svěřeného technického aktiva, v oblasti bezpečnosti postupuje v koordinaci s Garantem primárního aktiva IS VaVaI.

Nezbytná odbornost:

- Dobrá znalost aktiva, jehož je garantem,
- Dobrá znalost interních bezpečnostních politik a metodik.

Architekt KB IS VaVaI

Působnost:

Architekt KB IS VaVaI zajišťuje vytváření a udržování architektury IS VaVaI.

Jmenování:

Architekta KB IS VaVaI jmenuje ředitelí Odboru Rady pro výzkum, vývoj a inovace.

Odpovědnost:

- Architekt KB IS VaVaI odpovídá za vytváření a údržbu modelu enterprise architektury kybernetické bezpečnosti (procesní model, organizační struktura, aplikační architektura, technologie apod.).
- Architekt KB IS VaVaI odpovídá za návrhy implementace bezpečnostních opatření.

Nezbytná odbornost/znalosti:

- získání certifikace „Certified Information Security Manager (CISM)“, „Certified Ethical Hacker (CEH)“, nebo obdobné certifikace,
- alespoň 3 roky praxe v oboru informační nebo kybernetické bezpečnosti, nebo
- absolvování studia na vysoké škole a alespoň 1 rok praxe v oboru informační nebo kybernetické bezpečnosti.

Architekt KB IS VaVaI je seznámen se všemi projekty s dopadem na zpracování, přenos a ukládání informací IS VaVaI, zavádění nových nebo změny existujících systémů a procedur s dopadem na bezpečnost informací. Cílem tohoto opatření je zajistit, že budou náležitě vzaty do úvahy veškeré aspekty kybernetické bezpečnosti ve fázích přípravy, realizace a implementace všech relevantních projektů.

Uživatel IS VaVaI

Působnost:

Uživatel IS VaVaI užívá systém v souladu s přidělenou rolí a jejími oprávněními a možnostmi a s ohledem na stanovená provozní a bezpečnostní pravidla práce v IS VaVaI.

Odpovědnost:

Uživatel IS VaVaI je odpovědný za dodržování všech předepsaných pravidel pro užívání IS VaVaI.

Příloha č. 3

Prohlášení o aplikovatelnosti

Šablona ve formě tabulky je obsahem samostatného souboru s názvem „VaVaI_Prohlaseni o aplikovatelnosti_(sablona).xlsx“.

Příloha č. 4

Plán opatření bezpečnosti informací

Níže je zobrazena šablona pro plán opatření bezpečnosti informací pro IS VaVaI.

Plán opatření v rámci řízení bezpečnosti informací - na rok 2018

Id	Plánované opatření / oblast	Zdůvodnění potřeby	Předpokládaný způsob realizace	EXT / INT	Priorita	Odpovědnost / zdroje	Datum Plán / Realizace	Cílový stav / metriky účinnosti

Příloha č. 5

Plán vzdělávání

Níže je zobrazen formulář pro každoroční plán vzdělávání, který slouží k upevňování bezpečnostního povědomí zaměstnanců a pracovníků v obdobném vztahu.

Plán vzdělávání na rok …….

Jméno pracovníka	Název školení/kurzu č. 1	Název školení/kurzu č. 2	Název školení/kurzu č. 3	Název školení/kurzu č. 4	…..
Pracovník č. 1					
Pracovník č. 2					
Pracovník č. 3					
….					
Délka akce (dny)					
Předpokládané náklady					
Splněno dne					
Hodnocení (Ano/Ne)					

Poznámka k rubrice Hodnocení: Ano = součástí kurzu byl test/hodnocení, Ne = nebyl test.

Vypracoval:

Datum:

Schválil:

Datum:

Příloha č. 6

Cíle bezpečnosti informací

Je třeba stanovit cíle bezpečnosti informací, které musí být relevantní jednotlivým funkcím a úrovním řízení. Tyto cíle slouží k dosažení požadované úrovně bezpečnosti informací.

Při plánování jak dosáhnout cílů bezpečnosti informací je třeba konkrétně určit:

- čeho má být dosaženo (neboli co bude vykonáno),
- jaké jsou předpokládané zdroje k dosažení daného cíle,
- kdo bude odpovědný za dosažení cíle,
- plánovaný termín dosažení cíle a
- jakým způsobem budou hodnoceny výsledky, tj. jak bude posuzován splnění cíle.

Formulář pro stanovení cílů bezpečnosti je obsažen v příloze č. 9 dokumentu „Metodika řízení rizik kybernetické bezpečnosti IS VaVaI“.

Příloha č. 7

Zpráva z přezkoumání ISMS vedením

Šablona pro **Zprávu z přezkoumání ISMS vedením** není součástí této příručky. Tvoří jej samostatný dokument s názvem „VaVaI_Zprava z prezkoumani_(sablona)“.

Příloha č. 8

Záznam incidentu

FORMULÁŘ PRO ZÁZNAM O ZPŮSOBU VYŘEŠENÍ INCIDENTU – převzato z používané aplikace „Provozní deník“.

Záznam o způsobu vyřešení incidentu informačním systému VaVaI	
Datum zjištění	DD.MM.RRRR
Problém/úkol	
Priorita	
Datum splnění	DD.MM.RRRR
Osoba (jméno řešitele)	
Stav řešení	
Způsob řešení	
Vyjádření vedoucího	
Poznámka	

Poznámka: V současné době se pro IS VaVaI nepoužívá klasický HelpDesk se záznamy o událostech (incidentech). Pro zaznamenávání událostí je používána aplikace Provozní deník. Pro nahlášení události je používána speciální mailová schránka podpora.rvvi@vlada.cz, kde jsou všechny externí podněty evidovány a archivovány.

Příloha č. 9

Oznámení o provedení reaktivního a ochranného opatření

FORMULÁŘ PRO ZÁZNAM O OZNÁMENÍ O PROVEDENÍ REAKTIVNÍHO A OCHRANNÉHO OPATŘENÍ A JEHO VÝSLEDKU

Oznámení o provedení reaktivního a ochranného opatření a jeho výsledku	
Údaje o fyzické osobě, která provádí záznam	
Jméno, příjmení, titul	
Telefon	
Adresa elektronické pošty	
Pracovní zařazení, funkce	
Evidenční číslo reaktivního opatření	
Podrobnosti o realizaci reaktivního opatření	
Hodnocené negativní dopady reaktivního opatření a jejich možné negativní účinky	
Popis postupu možných negativních dopadů reaktivního opatření	
Problémy a negativní dopady, které se objevily během provedení reaktivního opatření	
Výsledek reaktivního opatření	
Datum a čas realizace reaktivního opatření	DD.MM.RRRR HH:MM
Datum a čas hodnocení výsledků reaktivního opatření	DD.MM.RRRR HH:MM
Poznámky	

Postup při provádění reaktivního opatření

Manažer KB IS VaVaI

a) posoudí očekávané dopady reaktivního opatření na informační a komunikační systém a na zavedená bezpečnostní opatření a vyhodnotí možné negativní účinky a

b) stanoví způsob rychlého provedení tohoto opatření, který minimalizuje jeho možné negativní účinky, a určí časový plán jeho provedení.

Manažer KB IS VaVaI oznámí způsob provedení reaktivního opatření a jeho výsledek **Manažerovi KB Úřady vlády.**

Příloha č. 10

Přehled právních a smluvních požadavků

Oblast bezpečnosti informací upravuje řada zákonů, vyhlášek a mezinárodních i národních standardů.

Jejich přehled je veden v samostatném dokumentu s názvem „Legislativa IS VaVaI“**.**

Manažer KB IS VaVaI má za úkol minimálně jedenkrát do roka zkontrolovat aktuálnost tohoto přehledu a v případě potřeby jej aktualizovat.

Příloha č. 11

Řízení kontinuity

Cíle řízení kontinuity:

Označ. cíle	Definice cíle	Hodnota cíle	Atribut bezpečnosti (D/I/D)	Poznámka
C01	Stanovení minimální úrovně poskytovaných služeb, která je přijatelná pro zajištění funkcionalit IS VaVaI.	Pouze jedna úroveň hodnocení: – IS VaVaI poskytuje služby v plném rozsahu, – IS VaVaI neposkytuje služby v plném rozsahu.	(1/0/0)	
C02	Stanovení doby obnovení chodu IS VaVaI, během které bude obnoven provoz IS VaVaI na definované minimální úrovni.	– do 5 následujících pracovních dní u havárie velkého rozsahu, – do následujícího pracovního dne u havárie malého rozsahu.	(1/0/0)	Havárie velkého rozsahu: HW závada, výpadek el. proudu na delší čas, výpadek rozvaděče na Úřadu vlády (není nastavena pohotovost). Havárie malého rozsahu: výpadek

				el. proudu na čas kratší než 1 hodina. Nedostatek paměti (přetečení logů), závada na databázovém serveru apod.
C03	Stanovení doby obnovy dat IS VaVaI, během které musí být zpětně obnovena data IS VaVaI po incidentu nebo selhání prostředků systému.	do následujícího pracovního dne	(1/1/1)	

Cíle řízení kontinuity IS VaVaI jsou stanoveny na základě vyhodnocení výsledků hodnocení rizik, analýzy dopadů možných incidentů a požadavků stanovených provozním řádem IS VaVaI.

Havarijní tým

Členové havarijního týmu jsou povinni včasně a přesně plnit činnosti předepsané plánem kontinuity resp. příslušnými postupy stejně jako činnosti uložené hlavním koordinátorem (Manažerem KB IS VaVaI). Zároveň je tým povinen přesně a včas informovat Manažera KB IS VaVaI o podstatných událostech a informacích v průběhu stavu ohrožení, které mohou ovlivnit jeho zvládání nebo jsou Manažerem KB IS VaVaI požadovány.

Seznam členů havarijního týmu

Seznam členů havarijního týmu je obsažen v samostatném dokumentu „VaVaI_Seznam clenu havarijniho tymu“, který vede a udržuje v aktuálním stavu Manažer KB IS VaVaI.

Seznam kontaktních osob (dodavatelé):

Třetí strana	Předmět spolupráce	Kontaktní informace			
		Kontaktní osoba	Telefon	Mobilní tel.	E-mail

Havarijní plány IS VaVaI

Jsou definovány plány kontinuity činnosti (havarijní plány) IS VaVaI, které obsahují postupy odezvy na nežádoucí („možné“) situace, postupy na udržení bezpečnosti informací IS VaVaI a odpovědnosti jednotlivých rolí.

Formulář na havarijní plán:

Hrozba	
Pravděpodobnost	
Dopad	
Pravděpodobný scénář	
Ohrožené činnosti / služby	
Opatření / postupy	
Odpovědnosti	
Prevence hrozby	
Zdroje	

Typy jednotlivých havarijních situací:

1) Požár
2) Povodeň
3) Zničení budovy (např. vlivem teroristického útoku)
4) Ztráta elektronických verzí dokumentů (větší množství)
5) Ztráta papírových verzí dokumentů (větší množství)
6) HW problémy
7) Výpadek dodávky elektrické energie
8) Výpadek připojení internetu
9) Výpadek personálních zdrojů
10) Změna lokality/sídla

Postup obnovy činnosti IS VaVaI

Tabulka obsahuje seznam kroků/činností, jejichž postupnou realizací bude dosaženo navrácení systému do normálního stavu.

Krok č.	Popis činnosti	Provádí	Zodpovídá	Doba ukončení činnosti	Poznámka
1					
2					
3					