Politika bezpečnosti informací IS VaVaI

Politika naplňující povinnosti dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a vytvářející metodický základ systému řízení bezpečnosti informací informačního systému pro výzkum, vývoj a inovace (IS VaVaI)

Zpracoval: Tomáš Bezouška, garant aktiva IS VaVaI

Schválil: doplnit

Verze: 1.0

Datum: 23. června 2017

Obsah

Seznam zkratek a pojmů

Zkratka	Význam
KB	Kybernetická bezpečnost
ÚV ČR	Úřad vlády České republiky
RVVI	Rada pro vědu, výzkum a inovace, poradní orgán Vlády České republiky
IS VaVaI	Informační systém výzkumu, vývoje a inovací
ZKB	Zákon o kybernetické bezpečnosti
ISMS	Systém řízení bezpečnosti informací
Sb.	Sbírka zákonů České republiky
ČR	Česká republika
VIS	Významný informační systém
NCKB	Národní centrum kybernetické bezpečnosti
RACI	Matice odpovědností
IT	Informační technologie
EU	Evropská unie
ISO	Mezinárodní organizace pro standardizaci
IEC	International Electrotechnical Commission

1 Úvodní ustanovení

Úřad vlády České republiky s Radou pro výzkum, vývoj a inovace podporuje ustavení, zavedení, provoz, monitorování, přezkoumání, udržování a zlepšování systému řízení bezpečnosti informací v rámci Informačního systému výzkumu, vývoje a inovací.

S ohledem na zajištění stanovené úrovně bezpečnosti informací je prováděno monitorování a vyhodnocování bezpečnostních rizik a incidentů.

1.1 Vymezení působnosti

Úřad vlády České republiky byl zřízen zákonem č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů, jako ústřední orgán státní správy České republiky. Působnost Úřadu vlády České republiky je vymezena v § 28 citovaného zákona.

Rada pro výzkum, vývoj a inovace je odborným a poradním orgánem vlády České republiky, který byl zřízen zákonem 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.

Rada pro výzkum, vývoj a inovace **zabezpečuje úlohu správce a provozovatele informačního systému výzkumu, vývoje a inovací** podle § 30 zákona o podpoře výzkumu, experimentálního vývoje a inovací. Činnost Rady pro výzkum, vývoj a inovace zabezpečuje Sekce místopředsedy vlády pro vědu, výzkum a inovace, který je organizačně začleněn do Úřadu vlády České republiky. Sekce místopředsedy vlády pro vědu, výzkum a inovace mimo jiné zajišťuje provoz a rozvoj informačního systému výzkumu, experimentálního vývoje a inovací v souladu se zákonem o podpoře výzkumu, experimentálního vývoje a inovací, dalšími zvláštními právními předpisy a vládou schválenou koncepcí.

Tato Bezpečnostní politika informací je vypracovávána v souladu s požadavky definovanými v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti, v platném znění a jeho prováděcích předpisů, tj. zejména vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti, v aktuálním znění.

1.2 Závaznost

Tato Politika bezpečnosti informací je závazná pro všechny osoby, které IS VaVaI rozvíjejí, spravují nebo využívají.

1.3 Rozsah Bezpečnostní politiky informací

Politika bezpečnosti informací IS VaVaI je samostatnou politikou vztahující se k zajištění bezpečnosti informací spravovaných tímto systémem. K zajištění bezpečnosti informací a podpory bezpečnosti informací se touto politikou:

a) popisuje a vysvětluje zajištění bezpečnosti informací IS VaVaI,
b) stanovují bezpečnostní cíle IS VaVaI,
c) stanovuje rozsah a důležitost bezpečnosti informací IS VaVaI,
d) uvádí stručný výklad základních bezpečnostních zásad IS VaVaI,
e) stanovují kritéria, kterými bude hodnoceno riziko, a definuje struktura hodnocení rizik IS VaVaI.

1.4 Základní charakteristika bezpečnosti informací

Bezpečnost informací je charakterizována jako zachování důvěrnosti, integrity a dostupnosti informací, přičemž:

a) **důvěrnost** je zajištění toho, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům,
b) **integrita** je zabezpečení přesnosti a úplnosti informace a metod jejího zpracování,
c) **dostupnost** je zajištění toho, že jsou informace přístupné a použitelné na žádost oprávněného jednotlivce, entity nebo procesu.

1.5 Cíle a zásady bezpečnosti informací

Bezpečnostním cílem spojeným s bezpečností informací IS VaVaI je zajištění dostupnosti informačních aktiv jen oprávněným osobám, správnosti a kompletnosti informací, důvěrnosti a bezpečnosti jejich zpracování a ochrany informací proti náhodnému nebo neoprávněnému zničení nebo náhodné ztrátě, proti neoprávněnému přístupu, změnám nebo šíření, a to v souladu se zákony a jinými právními předpisy ČR.

Cílem ÚV ČR je udržovat přiměřenou ochranu informačních aktiv, včetně aktiv podpůrných (HW, SW, atd).

1.6 Revize Politiky bezpečnosti informací IS VaVaI

Revize Politiky bezpečnosti informací IS VaVaI se provádí nejméně jednou ročně. Za provedení revize dokumentu „**Politika bezpečnosti informací IS VaVaI**“ odpovídá Garant aktiva IS VaVaI, finální verzi dokumentu schvaluje Výbor pro řízení kybernetické bezpečnosti ÚV ČR a RVVI.

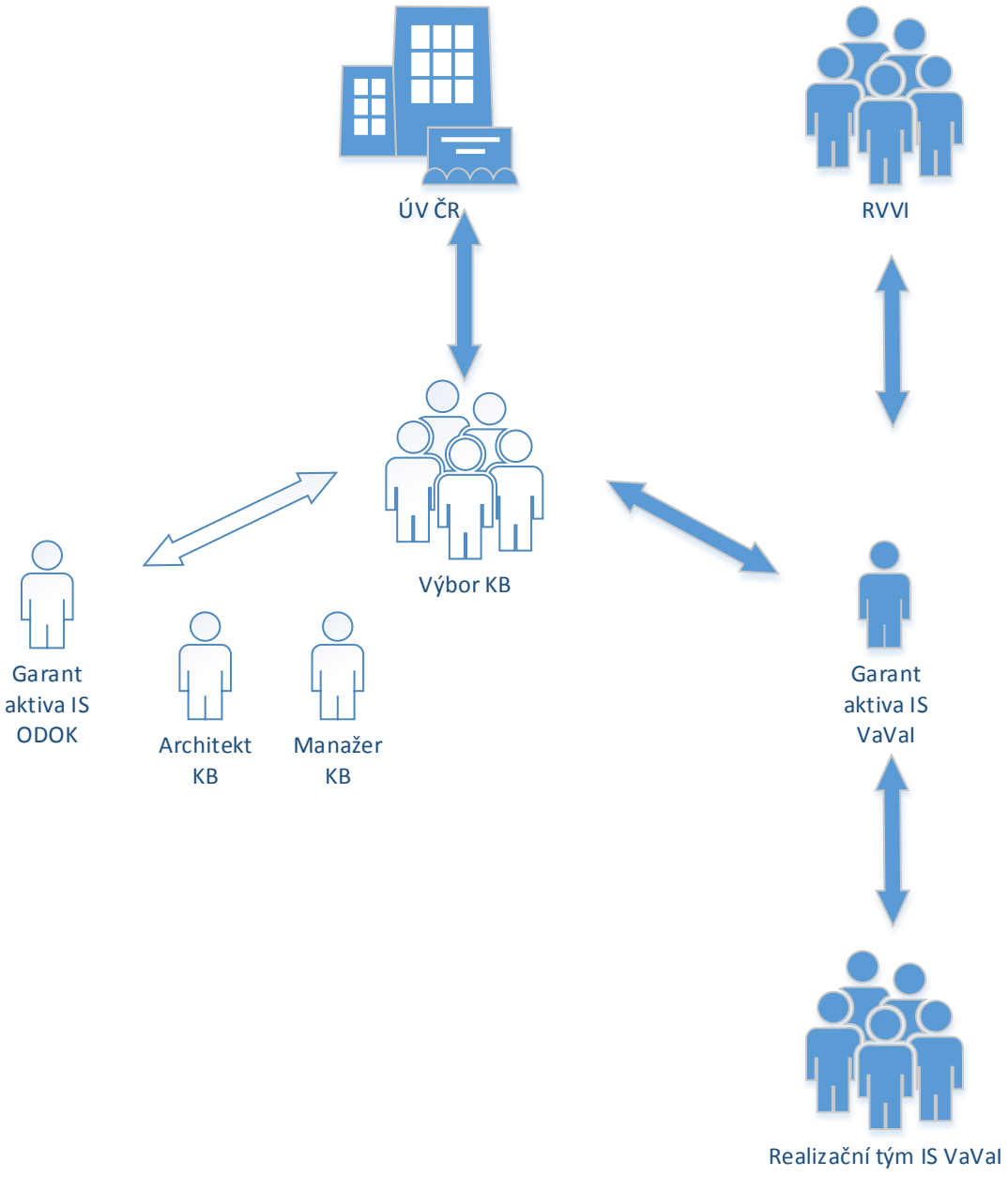
.

2 Organizace bezpečnosti informací

2.1 Všeobecná organizace bezpečnosti informací

Organizace a řízení bezpečnosti je jednotné a je stanoveno vnitřními normami a bezpečnostní dokumentací.

Na organizaci a řízení bezpečnosti informací se podílejí všichni vedoucí zaměstnanci ÚV ČR, zaměstnanci zastávající role v systému řízení bezpečnosti informací, odborné orgány a organizační útvary a dodavatelé ÚV ČR. Jejich konkrétní povinnosti jsou stanoveny v bezpečnostní dokumentaci a v popisu pracovní náplně.



Obrázek 1 Hierarchie bezpečnostních rolí

Výchozí bezpečnostní předpisy:

- Strategie řízení bezpečnosti – rozhodnutí VÚ R-5/2017
- Bezpečnostní politika ochrany IS Úřadu – rozhodnutí VÚ R-8/2017
- Směrnice o zásadách využívání VT – 2/2017

ÚV ČR dále stanovil v „*Rozhodnutí vedoucího Úřadu vlády ČR č. 8/2017, kterým se vydává* Bezpečnostní *politika ochrany informačních systémů v Úřadu vlády ČR*" role v oblasti správy a podpory hlavních informačních systémů úřadu včetně rolí souvisejících se zajišťováním kybernetické bezpečnosti.

K naplnění cílů ÚV ČR v oblasti bezpečnosti informací byl ustanoven **Výbor pro řízení kybernetické bezpečnosti** ÚV ČR (dále jen „Výbor"), který je vrcholovým koordinačním orgánem kybernetické bezpečnosti ÚV ČR.

2.2 Definování odpovědností a vztahů í

Bezpečnostní politika IS VaVaI definuje vzájemné vztahy subjektů v rámci IS VaVaI.

V rámci IS VaVaI vystupují tyto subjekty:

- Garant aktiva IS VaVaI
- Garant podpůrného aktiva
- Uživatel IS VaVaI

2.2.1 Garant aktiva IS VaVaI

Pro potřeby IS VaVaI vykonává roli Manažera KB a Architekta KB Garant aktiva IS VaVaI.

Odpovědnost za zpracování koncepce bezpečnosti informací a za prosazení a zavedení systému řízení bezpečnosti informací IS VaVaI má **Garant aktiva IS VaVaI**. Jmenování Garanta aktiva IS VaVaI provádí vedoucí Úřadu vlády ČR.

Garant aktiva IS VaVaI zajišťuje koordinaci všech činností při ochraně primárního aktiva a všech dotčených podpůrných aktiv. V oblasti prosazování principů a zásad kybernetické bezpečnosti spolupracuje Garant aktiva IS VaVaI s Výborem a jednotlivými ustanovenými rolemi ÚV ČR, prostřednictvím Sekce pro vědu, výzkum a inovace ÚV ČR komunikuje s RVVI a zajišťuje koordinaci činností realizačního týmu IS VaVaI v rámci Sekce pro vědu, výzkum a inovace ÚV ČR.

2.2.2 Garant podpůrného aktiva IS VaVaI

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

2.2.3 Uživatel IS VaVaI

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.

2.3 Pravomoci a odpovědnosti Garanta aktiva IS VaVaI

Garant aktiva IS VaVaI vykonává pro potřeby IS VaVaI v přiměřeném rozsahu roli Manažera KB a Architekta KB.

Garant aktiva IS VaVaI zodpovídá 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. Role Garanta aktiva IS VaVaI působí jako kontaktní osoba pro kybernetickou bezpečnost, prosazuje a koordinuje úlohu systému řízení informační bezpečnosti v organizaci.

2.3.1 Pravomoci a odpovědnosti role

Garant aktiva 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. Odpovídá za tvorbu a aktualizaci Strategie kybernetické bezpečnosti resortu IS VaVaI a aktualizaci Politiky bezpečnosti informací IS VaVaI.

Jako takový je i výkonným protějškem NCKB pro případy řešení kritických kybernetických bezpečnostních událostí týkajících se IS VaVaI.

Garant aktiva IS VaVaI odpovídá v za návrh a implementaci bezpečnostních opatření souvisejících s IS VaVaI, analýzu existujících opatření a vyhodnocení jejich účinnosti, za popis stávajícího stavu KB, formulování požadovaného stavu KB a identifikaci kroků vedoucích k jeho dosažení

Současně Garant aktiva IS VaVaI odpovídá za vyřešení všech neshod a závad v rozsahu systému řízení bezpečnosti informací IS VaVaI. Hlavní úlohou Garanta aktiva IS VaVaI je naplňovat Politiku bezpečnosti informací IS VaVaI schválenou Výborem pro řízení kybernetické bezpečnosti a RVVI.

2.3.1.1 Hlavní úkoly Garanta aktiva 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,
- vytváření a údržba modelu enterprise architektury kybernetické bezpečnosti (procesní model, organizační struktura, aplikační architektura, technologie apod.),
- 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 bezpečností událostí,
- ověření a vyšetření bezpečnostních incidentů,
- koordinace opatření ke zvýšení bezpečnostního povědomí v organizaci a školení kybernetické bezpečnosti,
- provádění činností stanovených plánem zvládání rizik 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 příslušnými státními orgány ve věcech kybernetické bezpečnosti.

Garant aktiva 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.

Garant aktiva 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.

3 Procesy a zásady řízení bezpečnosti informací

V rámci systému řízení bezpečnosti informací (ISMS) jsou definovány procesy a zásady řízení bezpečnosti informací. Vybrané oblasti popsané v této Politice bezpečnosti informací IS VaVaI jsou dále rozpracovány do metodických pokynů (viz seznam příloh).

3.1 Klasifikace a řízení informačních aktiv

Účelem procesu klasifikace a řízení informačních aktiv IS VaVaI je definovat a ohodnotit primární aktiva.

Při klasifikaci a řízení informačních aktiv jsou uplatňovány následující bezpečnostní zásady:

a) správce IS VaVaI vede evidenci primárních a podpůrných informačních aktiv, u nichž je určen garant
b) aktiva IS VaVaI jsou klasifikována tak, aby byla naznačena jejich potřebnost, důležitost,
c) klasifikaci stanoví garanti aktiv nebo vlastníci procesů, kteří odpovídají za periodické přezkoumávání této klasifikace a její aktualizaci,
d) klasifikace určuje způsob zacházení s informacemi s ohledem na jejich ochranu.

Postup identifikace, analýzy a klasifikace podpůrných aktiv IS VaVaI stanoví samostatný metodický dokument Metodika identifikace a správy informačních aktiv IS VaVaI.

3.2 Identifikace, hodnocení a řízení rizik

Analýza, hodnocení a řízení rizik a návrh a implementace bezpečnostních opatření jsou základním kamenem řízení kybernetické bezpečnosti.

Cíle řízení rizik v kontextu IS VaVaI jsou následující:

a) zajistit, že řízení rizik je jasně a konzistentně definovaný proces, integrovaný do procesů správy a rozvoje IS VaVaI, přičemž jeho výstupy jsou jednoznačně definované a evidované,
b) zajistit, že rizika jsou řízena v souladu se ZKB, Politikou bezpečnosti informací a relevantními metodikami a v souladu s nejlepší praxí,
c) zajistit, že proces řízení rizik brání škodám a vysokým nákladům na předcházení a eliminaci dopadů rizika,
d) zajistit, že rozhodování o požadavcích na rozvoj a provoz IS VaVaI je prováděno s ohledem na identifikovaná rizika a jejich pravděpodobné dopady,
e) zajistit nutnost řízení rizik všemi zainteresovanými stranami v rámci ÚV ČR a RVVI.

Postup identifikace, analýzy a řízení rizik IS VaVaI stanoví samostatný metodický dokument Metodika řízení rizik kybernetické bezpečnosti IS VaVaI.

3.3 Řízení lidských zdrojů

Účelem procesu řízení bezpečnosti lidských zdrojů je snížení rizika lidské chyby, krádeže, podvodu nebo zneužití prostředků IS VaVaI a zajištění bezpečnostního povědomí uživatelů. Bezpečnostní cíle v oblasti řízení lidských zdrojů zahrnují zajištění:

a) vhodných postupů v rámci přijímacího řízení,
b) povědomí zaměstnanců o bezpečnosti informací,
c) vhodných postupů v rámci změny pracovní pozice,
d) vhodných postupů v rámci ukončení pracovního poměru.

Pro oblast personální bezpečnosti jsou v rámci IS VaVaI stanoveny následující bezpečnostní zásady:

a) posuzování uchazečů o zaměstnání z hlediska personální bezpečnosti je součástí výkonu personálních činností dle Pracovního řádu a v souladu s obsahem pracovněprávních dokumentů v personálních šablonách,
b) zaměstnanci podepisují prohlášení o mlčenlivosti formou závazku zaměstnance ve smyslu zákonem uložené povinnosti,
c) zaměstnanci jsou povinni zachovávat mlčenlivost o skutečnostech, se kterými se seznámili při plnění svých pracovních úkolů nebo v přímé souvislosti s nimi a tato povinnost trvá i po skončení pracovního vztahu, pokud zvláštní právní předpis nestanoví jinak,
d) seznámení zaměstnanců s Politikou bezpečnosti informací IS VaVaI, (vstupní školení a periodická školení),
e) nedodržení bezpečnostních zásad může být kvalifikováno jako porušení povinností zaměstnance příp. porušení pracovní kázně s příslušnými důsledky pro zaměstnance, ve smyslu zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, pokud se nejedná o přestupek podle § 44 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů nebo trestný čin podle § 178 zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů,
f) šetření bezpečnostních incidentů v ISVaVaI zajišťuje Garant aktiva IS VaVaI včetně zpracování protokolů o bezpečnostních incidentech, jejich evidence a předložení návrhů opatření ÚV ČR k zajištění bezpečnosti.

3.4 Řízení fyzické bezpečnosti

Účelem řízení fyzické bezpečnosti a bezpečnosti prostředí je předcházet neoprávněnému a neautorizovanému přístupu k informacím, poškození a narušení informací a podpůrných informačních aktiv.

Bezpečnostním cílem je zajištění fyzické ochrany informací, technických informačních aktiv a prostředí, ve kterém se informace nacházejí:

a) vymezením a využíváním zabezpečených oblastí, zahrnujících kontrolu vstupu a upřesněním způsobu práce osob v těchto oblastech, zabezpečením kanceláří,

místností a zařízení, ochranou proti hrozbám působícím z vnějšího prostředí, zejména tam, kde se informace nacházejí, zpracovávají a uchovávají,

b) zabezpečením zařízení proti odcizení a zničení, poškození, zahrnujícím bezpečné umístění zařízení, zajištěním podpůrných služeb pro provoz zařízení (dodávky energie, klimatizace atd.), zabezpečením kabeláže a zajištěním pravidelné a bezpečné údržby zařízení,

c) zajištěním bezpečnosti informací mimo objekty ÚV ČR.

3.5 Personální bezpečnost

Pro oblast personální bezpečnosti pro IS VaVaI platí následující bezpečnostní zásady:

a) stanovení režimu vstupu a výstupu osob včetně zajištění zabezpečených oblastí a definování fyzického bezpečnostního perimetru je stanoveno samostatnou politikou a společnou dokumentací ÚV ČR,

b) zajištění požární bezpečnosti podle zákonů a jiných právních předpisů je upraveno zvláštní vnitřní organizační politikou,

c) vstup do budov oprávněným orgánům ke zdolání požáru nebo k provedení jiných záchranných prací dle rozhodnutí velitele zásahu stanovuje dokumentace zdolávání požáru a navazující dokumentace požární ochrany,

d) uplatnění zásad čistého stolu a čisté obrazovky spadá do kompetence vedoucích zaměstnanců.

Oblast fyzické bezpečnosti ve vztahu k IS VaVaI a k technickým aktivům ÚV ČR stanoví samostatný metodický dokument Směrnice vedoucího Úřadu vlády ČR č. 2/2017 o zásadách užívání výpočetní a kancelářské techniky, případně další interní řídící akty ÚV ČR, a dále Směrnice vedoucího Úřadu vlády ČR č. 3/2015, kterou se vydávají provozní řády objektů Úřadu vlády ČR a Směrnice vedoucího Úřadu vlády ČR č. 13/2015 k organizaci a zabezpečení požární ochrany (PO) v Úřadu vlády ČR.

3.6 Řízení bezpečnosti komunikací a provozu

Účelem procesu řízení bezpečnosti komunikací a provozu je zajistit správný a bezpečný provoz prostředků pro zpracování informací, minimalizovat riziko selhání systému, minimalizovat negativní dopady havárie systému, chránit integritu a dostupnost programů, dat a informačních systémů, chránit důvěrnost informací a zajistit ochranu počítačových sítí.

Pro oblast řízení bezpečnosti komunikací a provozu jsou v rámci dotčených organizací v resortu ÚV ČR stanoveny následující bezpečnostní zásady, prvky a činnosti:

a) je využívána ochrana proti škodlivým a automaticky spouštěným programům a škodlivému kódu,

b) je prováděno zálohování, které umožní obnovu dat a systémů ve vazbě na zachování základních funkcí IS VaVaI,

c) jsou zpracovány postupy obnovy po selhání nebo výpadku IS VaVaI,

d) je prováděno zajišťování bezpečnosti komunikační infrastruktury,

e) je zajištěna dostupnost informací a služeb dle definované požadované úrovně dostupnosti stanovené v rámci klasifikace aktiv,
f) je zajištěna důvěrnost informací při jejich přenosu pomocí kryptografické ochrany,
g) je zajištěna ochrana před neautorizovanými zásahy dodržováním principu oddělení povinností a odpovědností při přidělování uživatelských práv,
h) je prováděno monitorování provozu a zaznamenávání událostí,
i) jsou přijata opatření pro zajištění bezpečnosti elektronické pošty,
j) je vymáháno dodržování bezpečnosti při zacházení s paměťovými médii.

Stanovení a vymáhání pravidel bezpečnosti komunikací a provozu zajišťuje odbor informatiky ÚV ČR.

3.7 Řízení přístupu

Účelem procesu řízení přístupu k informacím a prostředkům IS VaVaI je zajistit, aby k nim měli přístup pouze oprávnění uživatelé. Pro přístup k těmto informacím a prostředkům jsou stanovena pravidla, která určují postupy pro autorizaci, zřizování, změny a odebírání přístupových práv, systém správy přístupu zajišťuje definovaný postup přidělování, změny a odebírání přístupu, správu hesel a kontrolu přístupových práv.

V rámci IS VaVaI jsou využívány následující **uživatelské role**, pro které jsou nastavena speciální aplikační oprávnění:

Role[1]	Rozsah činností a oprávnění
Administrátor – Úřad vlády	Přihlášení do rozhraní IS VaVaI pro Administrátory, správa všech číselníků, administrace a správa uživatelů všech úrovní, správa definic oprávnění, zálohování databáze, správa webu a verzí SW, správa všech oblastí IS VaVaI (CEP, CEA, RIV, VES).
Administrátor – Správce rady	Přihlášení do rozhraní IS VaVaI pro Administrátory, správa všech oblastí IS VaVaI (CEP, CEA, RIV, VES), schvalování nových a editovaných veřejných soutěží, schvalování nových a editovaných aktivit.
Uživatel - Poskytovatel	Přihlášení do rozhraní IS VaVaI pro Poskytovatele, založení a editace záznamů vlastní organizace, změna přístupového hesla
Uživatel - Příjemce	Přihlášení do rozhraní VaVER pro vytváření XML souborů pro předávání dat v požadované a předepsané struktuře.

[1] Administrátorem je v kontextu tohoto přehledu myšlena uživatelská role s rozšířenou sadou oprávnění v rámci aplikace IS VaVaI, nikoliv osoba s oprávněními nutnými pro administraci technických systémů zajišťujících provoz IS VaVaI

Role[1]	Rozsah činností a oprávnění
	Nicméně funkcionalita je udělaná tak, že ti lidé jsou administrátorem spravování a mají účty s přístupem na provozní server IS VaVaI.
Anonymní uživatel	Prohlížení záznamů ve veřejné části IS VaVaI

Zakládání účtů Uživatel – Poskytovatel a přidělování oprávnění provádí Administrátor – Úřad vlády na základě písemné žádosti schválené vedoucím Oddělení informačních systémů Odboru podpory Rady pro výzkum, vývoj a inovace.

Uživatelská oprávnění pro správu virtualizační platformy, operačních systémů, databází a aplikačních serverů jsou omezena na definované pracovníky Úřadu vlády ČR, kteří dané úkony vykonávají:

Role	Rozsah činností a oprávnění
Systémový administrátor	Administrátorská oprávnění ke správě virtualizační platformy a operačního systému serverů, k nástrojům pro zálohování a dalším technologickým SW
Databázový administrátor	Administrátorská oprávnění k databázovému systému
Administrátor aplikace	Administrátorská oprávnění k aplikačnímu serveru, správa kódu aplikace, správa verzí a release management

Zakládání uživatelů a přidělování oprávnění provádí vedoucí Oddělení informačních systémů Odboru podpory Rady pro výzkum, vývoj a inovace nebo jím pověřený administrátor.

3.8 Vývoj a údržba systémů

Účelem řízení bezpečnosti v oblasti vývoje a údržby systémů je prosadit bezpečnost informací do celého životního cyklu provozovaných informačních systémů od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu. Implementace a změny IS VaVaI jsou spojeny se stanovením vhodných bezpečnostních požadavků.

V oblasti vývoje a údržby IS VaVaI je zajištění kybernetické bezpečnosti zajištěno především prostřednictvím opatření v následujících oblastech:

a) analýza a specifikace bezpečnostních požadavků – určení bezpečnostních požadavků v klíčových fázích životního cyklu informačního systému zajistí, aby bezpečnost byla nedílnou součástí informačních systémů,

b) zajištění přesnosti a spolehlivosti zpracování dat v aplikacích a kryptografická opatření – validace a kontrola dat má spolu s kryptografickými opatřeními za cíl předcházet ztrátě, neoprávněné modifikaci nebo zneužití dat v aplikacích,
c) bezpečnost systémových souborů a procesu vývoje a podpory – je nutné zabezpečit systémové soubory a zdrojový kód a kontrolovat postupy vývoje a podpory, včetně formalizovaného postupu řízení změn,
d) správa zranitelností – je nutné vhodnými opatřeními omezit rizika vyplývající ze zneužití publikovaných zranitelností.

Vývoj a údržba IS VaVaI je z pohledu požadavků na bezpečnost informací koordinována Garantem aktiva IS VaVaI ve spolupráci s jejich pracovníky zajišťujícími vývoj a testování IS VaVaI a případnými dodavateli, a to včetně zajišťování implementace Politiky bezpečnosti informací IS VaVaI.

3.9 Řízení dodavatelů

Požadavky bezpečnosti informací na snížení rizik spojených s přístupem dodavatelů k aktivům organizace musí být projednány s dodavateli a dokumentovány. Obecná pravidla stanoví Rozhodnutí vedoucího Úřadu vlády ČR č. 8/2017, kterým se vydává Bezpečnostní politika ochrany informačních systémů v Úřadu vlády ČR.

Bezpečnostní cíle stanovené pro oblast řízení dodavatelů zahrnují:

a) zajištění ochrany aktiv organizace, ke kterým mají dodavatelé přístup,
b) udržování dohodnuté úrovně bezpečnosti informací a dodávky služeb ve shodě s dodavatelskými dohodami.

Pro oblast řízení dodavatelů jsou v rámci IS VaVaI stanoveny následující bezpečnostní zásady:

a) každý dodavatel, který může přistupovat k informacím, zpracovávat je, ukládat, komunikovat nebo je zajišťovat prvky IT infrastruktury, je zavázán k dodržování všech relevantních požadavků bezpečnosti informací,
b) dohody s dodavateli zahrnují požadavky na řízení rizik bezpečnosti informací spojených s dodavatelským řetězcem služeb a produktů informačních a komunikačních technologií,
c) změny v poskytování služeb dodavateli, včetně změn v udržování a zlepšování existujících politik, postupů a opatření bezpečnosti informací, jsou řízeny s ohledem na kritičnost informací, systémů a procesů organizace, které jsou součástí těchto změn, a s ohledem na opakované posouzení rizik.

3.10 Řízení kontinuity činností

Záměrem ÚV ČR je zajistit připravenost IS VaVaI k řešení krizových situací a zachování základních funkcí VIS nejméně v rozsahu fungování definovaném zákonem.

Bezpečnostním cílem je zajištění přípravy, proškolení a připravenosti určených zaměstnanců ÚV ČR po odborné stránce k výkonu činností spojených s řešením krizových situací, ochranou zdraví a života zaměstnanců a ochranou majetku.

Pro oblast řízení kontinuity činností jsou v rámci ÚV ČR stanoveny následující bezpečnostní zásady:

a) rozhodnutí o zablokování komunikace IS VaVaI, případně jiném opatření omezujícím služby IS VaVaI, zavedeném na základě detekované bezpečnostní události, spadá do kompetence Garanta aktiva IS VaVaI, ten je oprávněn tuto kompetenci v definovaných případech delegovat na Manažera kybernetické bezpečnosti ÚV ČR,
b) realizace přechodu na krizové řízení spadá do kompetence Manažera kybernetické bezpečnosti ÚV ČR,
c) realizace opatření k zachování základních funkcí spadá do kompetence Garanta aktiva IS VaVaI.

3.11 Soulad s požadavky

Pro zabezpečení informací IS VaVaI jsou jednoznačně definovány a zdokumentovány všechny relevantní zákonné a smluvní požadavky. V rámci ÚV ČR je veden přehled platných právních norem a předpisů vztahujících se k problematice bezpečnosti informací IS VaVaI.

Pro oblast souladu s požadavky jsou v rámci ÚV ČR stanoveny následující bezpečnostní zásady:

a) ÚV ČR dodržuje ustanovení o autorském právu a podmínky licenčních ujednání dodavatelů programového vybavení,
b) ÚV ČR provádí posouzení shody Politiky bezpečnosti informací IS VaVaI a navazujících předpisů se skutečným stavem bezpečnosti informací a k zajištění souladu IS VaVaI s příslušnými technickými normami je prováděno posouzení shody,
c) ÚV ČR přijímá a provádí opatření k zajištění ochrany osobních údajů a citlivých údajů v souladu se zákony a jinými právními předpisy.

IS VaVaI je pravidelně podrobován posouzení shody nejméně s následujícími systémy:

a) Atestace dlouhodobého řízení informačních systémů veřejné správy ve smyslu § 6d zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů,
b) Systém řízení bezpečnosti informací dle normy ISO/IEC 27001.

3.12 Přezkoumávání a audity

Audity jsou zaměřeny na posouzení souladu dosaženého stavu bezpečnosti informací s požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a jeho prováděcích předpisů a s požadavky norem řady ISO/IEC 27000 na řízení systému bezpečnosti informací jakož i dalších předpisů a norem relevantních pro řízení bezpečnosti informací IS VaVaI. Cílem

provádění auditů je nezávislé prověření aktuálního stavu bezpečnosti informací. Rovněž viz kapitola 3.11 Soulad s požadavky.

Pro oblast přezkoumání a auditu kybernetické bezpečnosti jsou v rámci IS VaVaI stanoveny následující bezpečnostní zásady:

a) přístup ÚV ČR k řízení a implementaci bezpečnosti informací IS VaVaI (tj. cílů opatření, jednotlivých opatření, politik, procesů a postupů bezpečnosti informací) je nezávisle přezkoumáván v plánovaných intervalech, nebo když nastane významná změna,
b) vedoucí pracovníci musí pravidelně přezkoumávat shodu zpracování informací a postupů v rozsahu jejich odpovědnosti s odpovídajícími bezpečnostními politikami, normami a dalšími požadavky na bezpečnost,
c) informační systémy musí být pravidelně přezkoumávány, zda jsou v souladu s politikami a normami bezpečnosti informací organizace.

Metodiku auditu řízení kybernetické bezpečnosti IS VaVaI upravuje samostatná závazná Metodika pro výkon auditu kybernetické bezpečnosti IS VaVaI.

4 Seznam příloh

Příloha č. 1: Metodika identifikace a správy informačních aktiv IS VaVaI

Příloha č. 2: Metodika řízení rizik kybernetické bezpečnosti IS VaVaI

Příloha č. 3: Metodika pro výkon auditu kybernetické bezpečnosti IS VaVaI