Zpracování osobních údajů

(nakládání s osobními údaji v rámci IS Krizkom)

IS Krizkom je „základním“ nástrojem informační podpory procesu vyžadování věcných zdrojů a jeho provozování je začleněno do systému informační podpory komunikace mezi orgány krizového řízení. IS Krizkom provozuje SSHR. Je zajištěna trvalá dostupnost systému pro všechny určené orgány krizového řízení, jeho odolnost, odpovídající bezpečnost systému a jeho obnova. S ohledem na rozvoj technologií ICT a nové kybernetické hrozby je nezbytné v dalším období řešit i nadále jeho technologický rozvoj a reagovat na tyto změny a hrozby.

1. Úvod a identifikace IS

Správa státních hmotných rezerv (SSHR) je ústředním orgánem státní správy (ÚSÚ) v oblastech hospodářských opatření pro krizové stavy (HOPKS) a státních hmotných rezerv (SHR) podle § 1 zákona č. 97/1993 Sb. Věcný obsah a oprávnění plnění HOPKS po vyhlášení krizových stavů a v období přípravy je vymezen § 2, 3 a další zákona č. 241/2000 Sb. Povinnosti a oprávnění pro orgány krizového řízení k zajištění připravenosti na řešení krizových situací, včetně zpracování dokumentů, poskytování podkladů, poskytování údajů z informačních systémů veřejné správy (ISVS) apod., jsou vymezeny § 9 a další zákona č. 240/2000 Sb. Pro orgány krizového řízení je stanoveno při plánování krizových opatření a při řešení krizových situací využívat informační systémy krizového řízení § 26 zákona č. 240/2000 Sb. IS Krizkom naplňuje určující kritéria pro „Významné informační systémy“ podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, a je do nich zahrnut vyhláškou č. 317/2014 Sb., (Příloha 1 vyhlášky). Postupy a procesy při přípravě a vyžadování věcných zdrojů za krizových stavů a mimořádných událostí, vymezené zejména zákonem č. 97/1993 Sb., a zákonem č. 241/2000 Sb., informačně podporované IS Krizkom jsou podrobně specifikovány „Metodikou vyžadování věcných zdrojů za krizových situací“ (Metodika) schválenou Usnesením vlády ČR ze dne 4. ledna 2012 č. 14/2012. Tato Metodika stanoví, že IS Krizkom je „základním“ nástrojem informační podpory procesu vyžadování věcných zdrojů a jeho provozování je začleněno do systému informační podpory komunikace mezi orgány krizového řízení.

2. Popis zpracování OÚ v IS

K fyzickým osobám a k fyzickým podnikajícím osobám (dále jen „fyzické osoby“) jsou v IS Krizkom vedena osobní data:

a) **Převzatá z jiných IS** (IS Argis, IS KISKAN SSHR). Popis těchto dat, jejich charakteristika a vymezení mandátu pro jejich pořizování (na základě zákona nebo souhlasu) bude obsahem samostatné analýzy těchto systémů.

b) **Vkládaná přímo do IS Krizkom uživateli tohoto systému**, kteří vkládají data s rolí

- uživatelů, za svoji osobu nebo za osobu, kterou byli pověřeni (starostu, hejtmana, vedoucího správního úřadu, apod.).
  - Žadatelé o poskytnutí věcných zdrojů za krizového stavu a za mimořádných událostí při uplatňování požadavků za orgán krizového řízení,
  - Řešitelé na jednotlivých stupních krizového řízení a u ochraňovatelů SHR,
- administrátorů (centrálních i lokálních), za skupinu zaměstnanců svého úřadu na základě rozhodnutí zaměstnavatele a se souhlasem dotčeného zaměstnance se zařazením mezi uživatele systému (v rámci stanovených nezbytných údajů k uživatelskému účtu – metadata účtu).

Charakteristika (obsah) údajů vkládaných uživateli o osobních datech fyzických osob: Jedná se o tato osobní data:

- jméno, příjmení, popř. akademický titul
- telefonní spojení (mobilní a pevná linka)
- e-mailová adresa
- fax

Uvedená data jsou vkládána do IS Krizkom a zpracovávána zpravidla v návaznosti na adresu sídla právnické osoby, tj. žadatele o věcný zdroj – správního úřadu, dodavatele věcného zdroje (dodavatele nezbytné dodávky (DND), ochraňovatele státních hmotných rezerv (SHR), řešitele požadavku – orgánu krizového řízení (správního úřadu)).

Charakteristika (obsah) údajů vkládaných administrátory o uživatelských účtech:
Účet uživatele IS Krizkom obsahuje tyto údaje:

- Jméno
- Příjmení
- Titul
- E-mailová adresa
- Mobilní telefon
- Další telefon
- Poznámka
- Úřad KŘ
- Role

Správa účtů

Veškeré uživatelské účty v IS Krizkom jsou spravovány přes webové rozhraní. Není přípustný jakýkoliv jiný zásah nebo ruční změna údajů uložených v uživatelských účtech. Změny provedené v IS Krizkom se pomocí workflow zapisují do Active Directory (dále jen AD) v daném formátu a s potřebnými metadaty. Při vytvoření nového uživatelského účtu dojde k zapsání systémových položek do AD tak, aby účet mohl být používán v systému IS Krizkom.

Správa účtu je delegována z nejvyšší úrovně v hierarchii níže na všechny podřízené úrovně. Pro centrální správu účtů je zavedena skupina „Centrálních administrátorů“, jejíž členové mají

oprávnění definovat administrátorské účty pro všechny úrovně orgánů krizového řízení (dále jen „KŘ“). Administrátoři jednotlivých úrovní KŘ (Lokální administrátoři) mohou následně vytvářet uživatelské účty pro všechny uživatele IS na dané úrovni KŘ a mají také možnost definovat administrátorské účty pro všechny podřízené úrovně KŘ.

Spolupráce s externími IS

Do sjednocené databáze IS Krizkom jsou importována data ze zdrojových informačních systémů IS PCZ ARGIS a IS KISKAN SSHR v tomto rozsahu:

- z **IS ARGIS**
  - základní informace o nezbytných dodávkách (ND) a jejich potencionálních dodavatelích (DND),
  - mobilizačních rezervách (MR), místu skladování a ochraňovatelích těchto zásob,
  - majetku státu (MS), místu skladování a ochraňovatelích těchto zásob.

- **z IS KISKAN SSHR**
  - komplexní informace o pohotovostních zásobách (PZ), zásobách pro humanitární pomoc (ZHP), místu skladování a ochraňovatelích těchto zásob.

3. Řízení přístupu k OÚ

Z pohledu správy IS Krizkom jsou definovány následující skupiny a role:

Role		Oprávněné osoby do rolí určovat z úrovně							Poznámka
Skupina	Název	ÚKŠ (OPS)	SSHR	ÚSÚ	KÚ	JSÚ	ORP	Ochraňovatel	
Provozovatel			**A**						
Garanti	**Věcný garant IS**		**A**						**SSHR – Odbor příprav pro krizové stavy (dále jen „OPKS“)**
	Věcný garant za provoz IS		**A**						SSHR – Odbor informatiky (dále jen „OI“)
	Garant pro metodické řízení IS		**A**						SSHR – OPKS

Správci	Správce ICT		**A**						SSHR – OI
	Systémový správce IS		**A**						SSHR – OI
	Správce IS		**A**						**SSHR – OI**
	Správce číselníků		**A**						Věcná správa: SSHR – OPKS, SSHR – Odbor strategie a koordinace (dále jen „OSK“) Provozní správa: OI (dodavatel IS)
	Správce importu z KIS KD		**A**						SSHR – OPKS
	Bezpečnostní správce		**A**						SSHR – OI
Administrátoři	**Centrální administrátor**		**A**						**kumulovaná role se Správcem IS**
	Lokální administrátor		**A**	**A**	**A**				**SSHR (kumulovaná role s Centrálním administrátorem), Ústřední správní úřad (ÚSÚ),**
Uživatelé	**Manager**	**A**	**A**		**A**				**SSHR – OPKS, KÚ**
	Supervisor	**A**	**A**	**A**	**A**	**A**	**A**		
	Editor	**A**	**A**	**A**	**A**	**A**	**A**	**A**	
	Reader	**A**	**A**	**A**	**A**	**A**	**A**	**A**	

Pravomoci a odpovědnosti

Provozovatel IS - Provozovatelem IS Krizkom je Česká republika – Správa státních hmotných rezerv. Je garantem dostupnosti informačního systému. Odpovídá za bezpečnost, důvěryhodnost a aktuálnost dat v informačním systému. Vytváří finanční, materiální a personální zajištění, které je nutné k provozu a rozvoji IS po celou dobu jeho životního cyklu. Uvedené povinnosti jsou zabezpečovány jednotlivými odborně (věcně) příslušnými organizačními útvary Správy v souladu s Organizačním řádem Správy a Směrnicí předsedy Správy č. 13 ze dne 4. listopadu 2010.

Věcný garant IS - Věcným garantem IS Krizkom je ředitel Odboru příprav pro krizové stavy (dále jen „OPKS“) Správy, který v rámci svěřené působnosti vymezené Organizačním řádem Správy má věcnou (odbornou) odpovědnost za IS v průběhu celého jeho životního cyklu. Věcný garant IS zodpovídá zejména za formulaci zaměření informační podpory oblasti, zpracování věcného zadání na realizaci IS, návrhů na jeho úpravy nebo vyřazení z provozu a garantuje využitelnost daného IS pro stanovený okruh uživatelů.

Správce IS - pracovník OI jmenovaný ředitelem OI jako privilegovaný uživatel systému, jehož úlohou je především koordinace užívání IS.

Správce IS má oprávnění a odpovědnost za opatření v oblasti:

- Správy účtů, tj. za opatření v roli Centrálního administrátora a Lokálního administrátora na úrovni Správy.

- Provozní správy a udržování aktuálnosti číselníků, tj. za opatření k zajištění importů číselníků přebíraných z webových služeb IS ARGIS v pravidelných intervalech společně s importem dat a importů dalších číselníků a jejich aktualizovaných verzí na základě pokynu nebo souhlasu Věcného garanta IS.
- Správy importu z IS PCZ ARGIS.

Centrální administrátor - pracovník OI nebo OPKS jmenovaný ředitelem OI jako privilegovaný uživatel systému, který má svým účtem přístup pouze k nástrojům a datům nezbytným pro správu účtů, ale ne k nástrojům pro zpracování dat a databázi o věcných zdrojích.

Centrální administrátor:

- vytváří a spravuje administrátorské účty pro Lokální administrátory, vydává tyto účty Lokálním administrátorům na příslušných organizačních stupních (úrovních KŘ) k zajištění vytváření uživatelských účtů na těchto stupních a popř. na nižších stupních takto:
  - Lokálním administrátorům na ÚSÚ,
  - Lokálním administrátorům na KÚ,
- plní úkoly Lokálního administrátora Správy a
- zajišťuje centrální správu Systému notifikací (vyrozumívání) pomocí aktivních informačních kanálů (SMS, e-mail, WS), aktivaci a deaktivaci systému notifikací pro jednotlivé uživatele nebo skupiny uživatelů a nastavení parametrů vyrozumívání.

Lokální administrátor - pracovník ústředního správního úřadu (ÚSÚ), krajského úřadu (KÚ) nebo Správy státních hmotných rezerv jmenovaný jako privilegovaný uživatel systému, který má svým účtem přístup pouze k nástrojům a datům nezbytným pro správu účtů, ale ne k nástrojům pro zpracování dat a databázi o věcných zdrojích. Lokální administrátor vytváří uživatelské účty pro vymezený okruh uživatelů, provádí aktualizaci údajů o uživateli (kontaktních údajů, role, apod.) a deaktivaci uživatelských účtů.

Lokální administrátor Správy, vytváří a spravuje uživatelské účty pro:

- zaměstnance Správy určené do rolí Manager, Supervisor, Editor a Reader,
- ochraňovatele SHR určené do rolí Editor a Reader.

Lokální administrátor ÚSÚ, vytváří a spravuje uživatelské účty pro:

- zaměstnance vlastního ÚSÚ určené do rolí Supervisor, Editor a Reader a
- zaměstnance odborně řízených jiných správních úřadů (JSÚ) určené do rolí Supervisor, Editor a Reader.

Lokální administrátor KÚ, vytváří a spravuje uživatelské účty pro

- zaměstnance vlastního KÚ určené do rolí Manager, Supervisor, Editor a Reader a
- zaměstnance územně příslušných obecních úřadů obcí s rozšířenou působnosti (ORP) určené do rolí Supervisor, Editor a Reader.
-

Manager - pracovník Správy (SSHR) nebo kraje (KÚ) jmenovaný jako uživatel systému, který má svým účtem přístup k nástrojům pro změnu provozního stavu a druhu provozu IS

Krizkom. Spravuje datové procesy – založení, rozšíření, ukončení krize a změna metadat krize.

Supervisor - uživatel IS, který zastupuje v IS Krizkom statutární orgán a schvaluje důležité operace v rámci IS, zejména návrhy požadavků na věcné zdroje, návrhy řešení, rozhodnutí a postoupení požadavku nebo řešení na další orgán krizového řízení, popřípadě vrácení požadavku nebo řešení (k doplnění, zamítnutí). Supervisor má současně oprávnění Editora a Readera.

Editor - uživatel IS, který zpracovává návrhy požadavků na věcné zdroje a řešení (rozhodnutí). Editor má současně oprávnění Readera. Editor u ochraňovatele SHR je dále oprávněn schválit své řešení (údaje o vyskladnění SHR a další informace, které do IS vložil) a tím je zpřístupnit ostatním uživatelům.

Reader - uživatel IS, který je oprávněn prohlížet data vedená ve sjednocené databázi IS Krizkom, údaje o požadavcích na věcné zdroje a jejich řešení a další informace uvedené v S podle místa v systému krizového řízení. Reader nemá oprávnění k záznamu a editaci dat v IS Krizkom.

Pravomoci a odpovědnosti jednotlivých skupin a rolí uživatelů jsou podrobně popsány v Provozním řádu IS Krizkom.

Určení do rolí v IS Krizkom a přístup k datům

Uživatelé IS jsou určováni (jmenováni, pověřováni) do rolí v IS Krizkom na jednotlivých úrovních krizového řízení a u ochraňovatelských organizací příslušným vedoucím.

Určení zaměstnanců Správy do rolí garanta za metodické řízení, správců a administrátorů provádí Věcný garant IS a Věcný garant za provoz IS. Do ostatních rolí v IS jsou zaměstnanci Správy určování příslušným vedoucím organizačního útvaru.

V IS Krizkom jsou u jednotlivých operací a dokumentů zachovávána pole Vytvořil, Změnil (stejná pole jsou zachovávána také u dílčích verzí dokumentů obsahujících informace o Řešitelích nebo o Žadatelích). Tyto vazby jsou interně reprezentovány pomocí SID, které je jedinečné pro každý uživatelský účet. Při pokusu o vytvoření položky do jiného úřadu KŘ než má osoba oprávnění, dojde k jejímu automatickému smazání a v AD se účet vůbec nevytvoří.

V případě smazání účtu uživatele v AD je smazána i vazba SID ke všem položkám, které uživatel v IS Krizkom vytvořil nebo upravoval a nelze zpětně dohledat autora (nebo posledního editora) dokumentu. Celý IS je tvořen provázanými tabulkami, proto při smazání uživatele jsou pak veškeré vazby položek v IS s tímto uživatelem neplatné. Z uvedeného důvodu nejsou uživatelské účty mazány, ale dochází pouze k jejich zneplatnění (deaktivaci), v jejímž důsledku je uživateli znemožněn další přístup do IS Krizkom a OÚ uvedené v uživatelském účtu takového uživatele nelze standardním způsobem zobrazit.

Zodpovědnost za správu OÚ uživatelů IS Krizkom a za jejich aktuálnost nesou pro úroveň vlastního úřadu KŘ pověření pracovníci s rolí „Lokální administrátor“. Za spávu OÚ zbývajících uživatelů zodpovídají pověření pracovníci SSHR s rolí „Centrální administrátor“.

Veškerá činnost uživatelů v rámci IS Krizkom je automaticky zaznamenávána cestou Auditlogu. Vyhodnocení Auditlogu provádí Správce IS.

4. Fyzická bezpečnost a bezpečnost OÚ

IS Krizkom nabízí výstupní sestavy ve formě tiskových sestav nebo ve formě datových souborů typu „.doc“ resp. „.xls“. Získat některou z devíti typů základních sestav může pouze oprávněný uživatel IS Krizkom. Oprávnění přístupu je podmíněno absolvováním základního školení, jehož nedílnou součástí je poučení o ochraně osobních údajů v podmínkách Správy státních hmotných rezerv.

5. Účastník zpracování

5.1.Přijatelné použití OÚ Účastníkem zpracování

Charakteristika uživatelských a privilegovaných rolí z pohledu oprávnění vkládat respektive editovat data o OÚ:

V IS Krizkom jsou z pohledu oprávnění vkládat OÚ pro jednotlivé úrovně hierarchie definovány následující role a kompetence:

Role	Stupeň KŘ	Kompetence v rámci IS	Kompetence pro práci s OÚ
Centrální administrátor	SSHR	Vytváří administrátorské i uživatelské účty **pro všechny stupně KŘ**. Je oprávněn měnit hierarchii účtů, číselníky, apod. Nemá přístup k datům o VZ.	Vkládání dat o uživatelích IS Krizkom
Administrátor	SSHR, ÚSÚ, KÚ	Vytváří uživatelské účty **pouze v rámci úrovně působnosti vlastního stupně KŘ**. Nemá přístup k datům o VZ.	Vkládání dat o uživatelích vlastního úřadu KŘ
Supervizor	Všechny	Zastupuje v IS statutární orgán. Schvaluje důležité operace v IS v rámci úrovně působnosti vlastního stupně KŘ.	Vkládání dat o Žadatelích a Řešitelích
Editor	Všechny	Zpracovává návrhy požadavků, navrhuje řešení v rámci úrovně působnosti vlastního stupně KŘ.	Vkládání dat o Žadatelích a Řešitelích
Čtenář	Všechny	Má k dispozici data pouze pro čtení	

Charakteristika uživatelských a privilegovaných rolí z pohledu oprávnění zobrazovat data o OÚ:

V IS Krizkom jsou z pohledu oprávnění zobrazovat OÚ pro jednotlivé úrovně hierarchie definovány následující role a kompetence:

Role	Stupeň KŘ	Kompetence v rámci IS	Kompetence pro práci s OÚ
Centrální administrátor	SSHR	Vytváří administrátorské i uživatelské účty **pro všechny stupně KŘ**. Je oprávněn měnit hierarchii účtů, číselníky, apod. Nemá přístup k datům o VZ.	Zobrazování dat o uživatelích IS Krizkom
Administrátor	SSHR, ÚSÚ, KÚ	Vytváří uživatelské účty **pouze v rámci úrovně působnosti vlastního stupně KŘ**. Nemá přístup k datům o VZ.	Zobrazování dat o uživatelích vlastního úřadu KŘ
Supervizor	Všechny	Zastupuje v IS statutární orgán. Schvaluje důležité operace v IS v rámci úrovně působnosti vlastního stupně KŘ.	Zobrazování dat o uživatelích vlastního úřadu KŘ; Zobrazování dat o Žadatelích a Řešitelích
Editor	Všechny	Zpracovává návrhy požadavků, navrhuje řešení v rámci úrovně působnosti vlastního stupně KŘ.	Zobrazování dat o uživatelích vlastního úřadu KŘ; Zobrazování dat o Žadatelích a Řešitelích
Čtenář	Všechny	Má k dispozici data pouze pro čtení	Zobrazování dat o uživatelích vlastního úřadu KŘ; Zobrazování dat o Žadatelích a Řešitelích

5.2. Čistý stůl a čistý displej

Politika bezpečnosti informací definuje základní strategii a zásady týkající se managementu zabezpečení informací v souladu s ČSN ISO/IEC 27001, určuje základní bezpečnostní pravidla pro provoz, používání a údržbu informačních a komunikačních technologií s cílem zajistit požadovanou dostupnost a ochranu informací a minimalizaci škod vzniklých v důsledku možných bezpečnostních incidentů. Základní zásadou je prosazování politiky bezpečného pracoviště: čistý stůl, prázdná obrazovka a prázdný odpadkový koš.

Bezpečnostní požadavky pro centrální instalaci IS Krizkom

- Bezpečnost provozu IS Krizkom je realizována podle zásad stanovených v platném znění Směrnice předsedy Správy státních hmotných rezerv č. 19 ze dne 20. června 2014.
- Opatření k zajištění bezpečnosti centrální instalace IS v oblasti počítačové a komunikační bezpečnosti, administrativní bezpečnosti a organizačních opatření, personální bezpečnosti a fyzické bezpečnosti jsou uvedena v bezpečnostní dokumentaci IS, která je vedena, spravována a uložena na Odboru informatiky Správy (u Bezpečnostního správce IS Krizkom).
- Vnitřní část datové sítě Správy je chráněna proti vniknutí nežádoucího škodlivého SW tzv. bezpečnostní bránou (firewall).
- Pro zajištění fyzické bezpečnosti je nezbytnou podmínkou řízení přístupu, tj. zajištění řízení přístupu do serverovny a zajištění ostrahy budovy, kde se toto pracoviště nachází.
- Ukládání archivních médií a nosičů informací je zabezpečeno mimo objekt Správy, ve kterém je umístěna centrální instalace IS Krizkom

Bezpečnostní pravidla pro vzdálený přístup do IS Krizkom

- Vzhledem k riziku zanesení škodlivého SW na pracovní stanici po připojení na infikovaný Web server a následnému sekundárnímu efektu zneužití dat jsou uživatelé povinni zachovávat obezřetnost a dodržovat stanovené bezpečnostní politiky a pokyny pro uživatele výpočetní techniky pro oblast bezpečnosti provozu ICT.
- Pro přístup do IS Krizkom je používán zabezpečený protokol https.
- Na pracovních stanicích musí být nainstalován aktualizovaný antivirový program.

Bezpečnostní pravidla pro práci v IS Krizkom

- Uživatelé jsou povinni dodržovat „Zásady pro tvorbu a používání silného hesla“:
  - Heslo musí mít délku minimálně 8 znaků,
  - heslo musí obsahovat minimálně 3 ze 4 markantů (velká písmena, malá písmena, číslice, speciální znaky),
  - heslo nesmí být snadno uhodnutelné,
  - heslo nesmí obsahovat mnohonásobné opakování jednoho znaku,
  - při prvním přihlášení nového uživatele do IS Krizkom musí být změněno heslo přidělené Administrátorem,
  - změna hesla vždy při jeho vyzrazení nebo podezření na jeho vyzrazení,
  - pravidelná změna hesla (minimálně 1x za rok),
  - heslo nesmí být zapisováno do písemných dokumentů, pokud není zajištěno jeho bezpečné uložení,
  - heslo nesmí být zapisováno do jakýchkoli přihlašovacích skriptů.

Bezpečnostní pravidla pro nakládání s výstupními sestavami v papírové podobě

- Uživatelé jsou povinni dodržovat „Zásady čistého stolu a prázdného koše“:
  - výstupní přehledové sestavy jsou tištěny výhradně pro konkrétní použití, konkrétního oprávněného Žadatele,
  - sestavy musí být neprodleně bezpečným způsobem předány oprávněnému Žadateli,
  - nepotřebné sestavy musí být bez prodlení skartovány, nesmí být vyhazovány do koše na odpadky.

Bezpečnostní pravidla pro nakládání s výstupními sestavami v elektronické podobě

- Uživatelé jsou povinni dodržovat „Zásady prázdné obrazovky, vyprázdněného koše“:
  - výstupní přehledové sestavy v elektronické podobě jsou vytvářeny výhradně pro konkrétní použití, pro konkrétního oprávněného Žadatele,
  - sestavy musí být neprodleně bezpečným způsobem předány oprávněnému Žadateli,
  - je přísně zakázáno bez příkazu oprávněného Žadatele vytvářet kopie výstupních sestav v elektronické formě,
  - nepotřebné datové soubory obsahující OOÚ musí být bez prodlení smazány.

5.3. Mobilní zařízení a práce na dálku s OÚ

K přístupu do IS Krizkom prostřednictvím mobilního zařízení jsou třeba následující komponenty:

- Funkční přístup do internetu.
- Použití některého z níže popsaných internetových prohlížečů.
- Použití protokolu zabezpečeného https.
- Platný uživatelský profil s uživatelským heslem.
- Níže uvedený podpůrný software.

5.4. Omezení nebo požadavky týkající se instalací a použití softwaru, který je vyžadován pro speciální práci s OÚ

IS Krizkom je vytvořen jako webová aplikace. Prostředí, ve kterém je realizována prezentace dat na koncových stanicích používá pouze internetový prohlížeč ve verzi MS IE 8 až 11 (kompatibilní zobrazení od verze 8) a MS Windows 7 a výše. Další podporované prohlížeče

a jejich omezení jsou uvedeny v následující tabulce (pro editaci dokumentů v IS je plně podporován pouze Internet Explorer).

Prohlížeč	Podporovaný	Kompatibilní zobrazení
Internet Explorer verze 8,9	Ano	Ano
Internet Explorer verze 10,11	Ano	Ano
Microsoft Edge	Ano	-
Google Chrome (nejnovější)	Ano	-
Mozilla Firefox (nejnovější)	Ano	-
Apple Safari (nejnovější)	Ano	-

Pro práci s dokumenty je nutná instalace MS Office Word 2007 32bit a vyšší. Pro práci s přehledovými obrazovkami je nutná instalace MS Office Excel 2007 32bit a vyšší. Pro práci s dokumenty ve formátu .pdf je třeba PDF Reader 11.0 a vyšší. Maximální velikost přílohy, kterou lze vložit do IS Krizkom, je omezena na 50MB.

Podrobné informace o software potřebném k provozu IS Krizkom jsou uvedeny v uživatelské dokumentaci.

6. Zálohování OÚ

Zálohování probíhá podle platného harmonogramu následujícím způsobem:

- V průběhu dne probíhají opakované replikace na záložní hardware (záložní server s kompletní instalací IS Krizkom).
- Jedenkrát denně probíhá kompletní zálohování vytvořením záložního souboru nejprve na disk a následně na magnetickou pásku.
- Magnetické pásky jsou ukládány v budově BDO, Olbrachtova 5, Praha 4.

Podrobný popis zálohování uvádí platná verze Provozního řádu IS Krizkom.

Nedílnou součástí zálohování OOÚ je funkcionalita IS Krizkom nazvaná „Archivace“. Pomocí této funkcionality mohou uživatelé s oprávněním „Centrální administrátor“ archivovat ukončené krize včetně uplatněných požadavků a jejich řešení. „Ostré krize“ (řešení skutečně vyhlášených krizových stavů) jsou archivovány v souladu s Metodikou vyžadování věcných zdrojů na dobu deseti let. „Cvičné krize“ jsou archivovány pouze v případě, že je jejich archivace vyžádána, zpravidla na dobu tří let.

7. Přenos informací, obsahující OÚ jiným účastníkům zpracování

IS Krizkom je vytvořen jako webová aplikace s účastníky zpracování uvnitř i vně SSHR. Procesy zpracování informací jsou podrobně popsány v uživatelské dokumentaci. Principielně jsou přednostně využívány doklady a informace přenášené v elektronické formě (jako součást IS Krizkom).

V případech, kdy jsou předepsány výstupy ve formě tiskových sestav, je vždy popsáno také nakládání s těmito sestavami (kdo je tiskne, na čí příkaz, komu jsou předávány, jakým způsobem ukládány).

Zabezpečení OOÚ je zajištěno principem poučených a řádně vyškolených uživatelů IS Krizkom, kteří jsou povinni dodržovat pravidla pro zacházení s OOÚ.

Uživatelům IS Krizkom je přísně zakázáno pořizování printscreenů obrazovek obsahujících OOÚ!

8. Dodavatelské vztahy

Dodavatelské vztahy byly ošetřeny Smlouvou o dílo č. 20160196 ze dne 20. 4. 2016 o zajištění technologického upgrade IS Krizkom. V článku XII, odstavci 3 jsou podrobně vymezeny podmínky mlčenlivosti. Smlouva zavazuje pracovníky Zpracovatele k dodržení uvedených podmínek. S ohledem na skutečnost, že dodavatel IS Krizkom je současně Zpracovatelem ve smyslu smlouvy č. 20160197 ze dne 20. 4. 2016 o zajištění uživatelské podpory a dalších služeb nutných k bezchybnému provozu IS Krizkom, je ošetření ochrany OÚ podrobněji rozvedeno v kapitole 9 Politiky zpracování osobních údajů IS Krizkom.

9. Vztah se Zpracovatelem

Dodavatel IS Krizkom je současně Zpracovatelem ve smyslu smlouvy č. 20160197 ze dne 20. 4. 2016 o zajištění uživatelské podpory a dalších služeb nutných k bezchybnému provozu IS Krizkom. V článku XI, odstavci 3 této smlouvy jsou podrobně vymezeny podmínky mlčenlivosti a podmínky pro nakládání s osobními údaji. Smlouva zavazuje Zpracovatele poučit veškeré osoby, které se na jeho straně budou podílet na jejím plnění. Smlouva zavazuje pracovníky Zpracovatele k dodržení uvedených podmínek.

Aktuální otázky týkající se vztahů s Dodavatelem, resp. Zpracovatelem IS Krizkom řeší jménem Správy státních hmotných rezerv Odbor informatiky (OI). Potřebné pokyny vydává Věcný garant IS Krizkom směrem k OI, které následně zajistí přenesení souvisejících povinností na Dodavatele resp. Zpracovatele.

10. Porušení zabezpečení OÚ

Pracovní postupy pro hlášení incidentů a pro nástroje zamezující neoprávněnému přístupu uvádí směrnice předsedy SSHR č.12 ze dne 23. prosince 2015 – bezpečnostní politika ICT Správy státních hmotných rezerv (dále jen BP).

1. Pokud uživatel IS Krizkom zjistí narušení bezpečnosti OÚ, je povinen o tom neprodleně informovat Garanta IS Krizkom.
2. Garant IS Krizkom předá nahlášený problém Řešiteli a informuje Koordinátora OÚ. Řešitel po odstranění problému zaznamená údaje o příčinách a řešení problému do databáze IT Dispečinku. Jedná-li se o bezpečnostní incident v oblasti ICT, informuje IT Dispečink bezpečnostního správce ICT, který vážná porušení bezpečnosti ICT hlásí řediteli OBKŘ.
3. Pro odvrácení bezpečnostního rizika, hrozby nebo již probíhajícího útoku je ředitel OI oprávněn nařídit na dobu nezbytně nutnou okamžité odpojení nebezpečného HW nebo SW (IS, serveru, počítače uživatele apod.) od sítě Správy, což může dočasně znepřístupnit některé služby sítě. O tomto opatření informuje ředitele OBKŘ, příslušného věcného garanta IS nebo vedoucího organizačního útvaru zaměstnance Správy, jehož počítač byl odpojen od sítě.
4. V případě rozsáhlé hrozby nebo útoku na síť Správy je ředitel OI oprávněn nařídit na dobu nezbytně nutnou vypnutí části nebo celé sítě Správy. O tomto opatření neprodleně informuje výbor KB a ředitele OBKŘ. Ředitel OBKŘ neprodleně informuje předsedu Správy.

11. Změnové řízení

Při změně pracovních postupů IS Krizkom musí být vypracována Dokumentace změny.

Dokumentace musí obsahovat následující části:

a) Popis a důvod změny,

b) identifikaci subjektu, který změnu nařídil, nebo povolil,

c) identifikaci všech subjektů, kterých se změna dotkne a plán, jak tyto subjekty budou o změně v dostatečném časovém předstihu informovány,

d) identifikaci rizik spojených se změnou a metody řízení těchto rizik,

e) plán realizace změny (projekt),

f) plán testování změny,

g) postup obnovení do předchozího stavu a odpovědnou osobu za tuto činnost.

Za změnu je považována úprava konfigurace, funkcionality, nebo provozního prostředí. Změna systému může mít vliv na uživatele, administrátory, pracovníky podpory, monitoring systému včetně externích subjektů. Pro každý server v rámci IS musí existovat procedura, jejímž provedením se získá informace o základní konfiguraci počítače. Preferovanou formou takové procedury je vyvolání jednoho programu, který zobrazí požadované informace, ale může jít také o popis pracovního postupu.

Předepsaný postup při změnovém řízení:

1. Věcný garant definuje požadavky
2. Koordinátor schválí definice požadavků
3. Zadavatel (OI) zadá projekt
4. Zpracovatel zpracuje „Studii proveditelnosti“
5. Věcný garant ověří funkčnost a splnění podmínek
6. Zpracovatel zpracuje realizaci projektu

7. Věcný garant ověří funkčnost realizace
8. Proběhne školení uživatelů

12. Zvyšování a udržování odborné způsobilosti účastníků zpracování

Pravidelná školení nových i stávajících uživatelů IS Krizkom jsou předepsána v ročním Plánu zaměření HOPKS. Tato školení probíhají minimálně 1x za rok a jsou rozdělena podle okruhu zúčastněných Uživatelů IS Krizkom (dále jen „Uživatelé“) následujícím způsobem:

- Školení pro ochraňovatele PZ a ZHP (13 krajských ředitelství HZS, HZS Hlavního města Prahy, VIS. a.s., SOŽ a.s., SŽDC s. o., Státní veterinární správa, SUCHJBO, Neograph a.s. - SPM, Státní tiskárna cenin), pro pracovníky středisek SSHR Boletex, Polora, Soběslav, včetně jejich poboček, a Národního centra humanitární pomoci Olomouc-Holice.
- Školení pro ústřední správní úřady (MV, MZ, MD, MZV, MPO, MŽP, MF, MO, MMR, MV-GŘ HZS ČR, PP ČR, SÚJB).
- Školení pro Školitele ze 13 krajských úřadů a Magistrátu hlavního města Prahy. Školitelé krajských úřadů následně školí další zaměstnance vlastního krajského úřadu a uživatele z obecních úřadů obcí s rozšířenou působností (ORP) (resp. MHMP a městských částí hl. města Prahy)
- Školení pro jiné správní úřady (krajská ředitelství Policie České republiky, krajská ředitelství HZS ČR a Záchranný útvar HZS Praha).
- Školení pro SSHR – OPKS, OSK, OBKŘ, OLOG a OdKD, se speciálně zaměřenými školeními pro pracovní skupiny OCS (školení pro skupinu „Managers“, školení pro skupinu „Stálá služba“ a školení pro skupinu „Zabezpečení věcných zdrojů!).

Nedílnou součástí školení je poučení účastníků o OOÚ v souladu s pravidly předepsanými Směrnicí předsedy Správy státních hmotných rezerv č.5 ze dne 13. dubna 2018. Na základě tohoto poučení je všem Účastníkům školení předložen k podpisu Záznam o zpracování OÚ v IS Krizkom, uvedený v kapitole 14 Politiky pro zpracování OÚ v IS Krizkom. Svým podpisem se každý z Účastníků zavazuje k dodržování předepsaných pravidel pro OOÚ.

Shodná povinnost je předepsána také Školitelům z krajských úřadů během jimi pořádaných školení IS Krizkom. Účastníky školení podepsané Záznamy o zpracování OÚ v IS Krizkom zašlou Školitelé po provedeném školení k rukám ředitele OPKS. Tím je zajištěno, že noví uživatelé získají uživatelský přístup do IS Krizkom až poté, co byli prokazatelným způsobem seznámeni s pravidly pro OOÚ.

Datum účinnosti: 25. května 2018

Ing. Miloslav Novák
ředitel Odboru příprav pro krizové stavy