

Ústřední evidence podnikatelů - Registr živnostenského podnikání



Provozní bezpečnostní dokumentace Bezpečnostní směrnice IS pro uživatele

Verze 1.6

1. 12. 2017

ICZ a.s.

Zpracoval: Realizační tým IS RŽP	Odpovídá: Ing. Martin Mikuškovíc	Schválil: Antonín Běhounek
Podpis:	Podpis:	Podpis:



Copyright © 2004, 2005, 2010, 2016, 2017 ICZ a.s.

Žádná část tohoto dokumentu nesmí být kopírována žádným způsobem bez písemného souhlasu majitelů autorských práv.

Autorská a jiná díla odvozená z tohoto díla podléhají ochraně autorských práv vlastníků.

Tento dokument slouží pouze pro vnitřní potřebu uživatelů pracujících s aplikačním vybavením IS RŽP.

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUzivatelel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

OBSAH

1	Úvod	4
2	Obecná bezpečnostní opatření na pracovištích IS RŽP5	
2.1	Fyzická bezpečnost	5
2.2	Personální bezpečnost	5
2.3	Režimová bezpečnost	5
2.4	Programová bezpečnost	6
2.5	Datová bezpečnost	6
2.6	Bezpečnost komunikačních cest	6
2.7	Realizace bezpečnostních opatření na pracovištích IS RŽP	7
3	Zvyšování bezpečnostního povědomí uživatelů IS RŽP8	
4	Kontaktní osoba a její povinnosti	9
4.1	Správa přístupových oprávnění	9
4.1.1	Přidělení přístupu k IS RŽP uživateli	10
4.1.2	Vypršení platnosti karty	11
4.1.3	Změny v přístupu k IS RŽP	11
4.1.4	Odebrání přístupu	12
4.2	Řešení kybernetických bezpečnostních událostí	13
4.2.1	Ztráta karty	13
4.2.2	Zničení, poškození, trvalé zablokování karty	13
4.2.3	Zneužití přístupu k IS RŽP	13
5	Uživatel IS RŽP, jeho práva a povinnosti	15
5.1	Postupy při používání IS RŽP	15
5.1.1	Zásady používání čipové karty	15
5.1.2	Přihlášení k IS RŽP	20
5.1.3	Přerušení práce s IS RŽP a odhlášení	20
5.1.4	Zálohování a obnova funkčnosti	20
5.1.5	Vstup / výstup datových souborů z / na nosiče informací	21
5.2	Řízení přístupu k IS RŽP	21
5.2.1	Získání přístupu k IS RŽP	21
5.2.2	Vypršení platnosti karty	22
5.2.3	Změny v přístupu k IS RŽP	22
5.2.4	Odebrání přístupu	23
5.2.5	Řešení bezpečnostních událostí	23
6	PŘÍLOHY	24
6.1	Seznam použitých zkratk	24
6.2	Seznam pojmů	24

Bezpečnostní směrnice IS pro uživatele

Zpracoval: Realizační tým IS RŽP

Utajení: -

Stav: Finální

Výtisk: 001

ID: RZP_DOC_PBD-BSUživatel

Změna: 1. 12. 2017

Verze: 1.6

Stran: 024

1 ÚVOD

Dokument je součástí provozní bezpečnostní dokumentace a skládá se ze čtyř částí:

- Obecná bezpečnostní opatření na pracovištích IS RŽP – popis požadavků na bezpečnostní opatření na ŽÚ a na pracovištích externích uživatelů IS RŽP.
- Zvyšování bezpečnostního povědomí - popis doporučeného způsobu poučování o bezpečnostních opatřeních a důsledcích vyplývajících z porušení těchto opatření.
- Kontaktní osoba – popis této role a jejích povinností.
- Uživatel IS RŽP - popis zásad používání IS RŽP.

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

2 OBECNÁ BEZPEČNOSTNÍ OPATŘENÍ NA PRACOVÍŠTÍCH IS RŽP

IS RŽP je významným informačním systémem dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „kybernetický zákon“), a vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, a vztahují se k němu povinnosti vyplývající z těchto právních norem.

Jednotlivé živnostenské úřady (obecní a krajské) jsou pak podle zákona č. 570/1991 Sb., o živnostenských úřadech, ve znění pozdějších předpisů, a zákona č. 455/1991 Sb., o živnostenském podnikání (živnostenský zákon), ve znění pozdějších předpisů, provozovateli živnostenského rejstříku. Vzhledem k tomu, že živnostenské úřady, které vykonávají činnosti podle živnostenského zákona v přenesené působnosti, jsou součástí městských úřadů, úřadů městských částí hl. města Prahy, krajských úřadů a magistrátů (dále jen „úřady“), jsou i tyto úřady subjekty, na něž se vztahují určité povinnosti podle zákona o kybernetické bezpečnosti.

2.1 Fyzická bezpečnost

Požadavkem je, aby prostředky výpočetní a komunikační techniky (dále jen ICT) pracovišť IS RŽP nebyly volně přístupné veřejnosti.

2.2 Personální bezpečnost

Přístup k IS RŽP mohou mít pouze pracovníci úřadů, kteří ho používají pro výkon státní správy. Rozsah přístupových oprávnění musí odpovídat zastávané funkci. O přidělení a odebrání přístupových oprávnění k IS RŽP rozhoduje vedoucí ŽÚ nebo jím pověřená osoba (dále jen kontaktní osoba).

Rozsah oprávnění externího uživatele je stanoven v rámci písemné dohody mezi MPO a externím subjektem o poskytnutí přístupu k IS RŽP.

Na správě prostředků ICT používaných pro IS RŽP se může podílet pouze osoba k tomu určená vedením úřadu (dále jen informatik).

2.3 Režimová bezpečnost

Přístup k prostředkům ICT mohou mít pouze oprávnění uživatelé a správci. Toto je nutno zabezpečit autentizací uživatelů minimálně heslem. Po autentizaci běžného uživatele (tj. přihlášení) není dovoleno ponechat prostředek ICT bez dozoru v nezabezpečené místnosti. Po autentizaci osoby s právy administrátora není dovoleno ponechat prostředek ICT nezabezpečený.

Zvláštní pozornost je potřeba věnovat čipovým kartám, které jsou v držení jednotlivých uživatelů IS RŽP. Není dovoleno:

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

Obecná bezpečnostní opatření na pracovištích IS RŽP

- kartu, PIN nebo PUK poskytnout jiné osobě,
- zapisovat si PIN,
- ponechávat kartu bez dozoru,
- kartu mechanicky poškozovat, ohýbat a vystavovat teplotám nad 50° C.

2.4 Programová bezpečnost

Programové vybavení pracovišť IS RŽP se skládá pouze ze systémového a standardního SW udržovaného v aktuálních verzích: z operačního systému (s ovladači pro HW), Adobe Readeru, internetového prohlížeče a kryptografických modulů pro čipové karty (SafeSign) a podepisovacích certifikátů.

Pro zajištění programové bezpečnosti je nezbytné:

- instalovat a aktualizovat programy pouze z důvěryhodných zdrojů - originální instalační CD, důvěryhodné servery na internetu,
- zajistit ochranu před škodlivým SW instalací spolehlivého antivirového prostředku, prostředku pro vyhledávání „spyware“,
- omezit poskytování síťových služeb pracovními stanicemi uživatelů instalací firewallu nebo vhodnou konfigurací operačního systému,
- chránit lokální síť před neoprávněným přístupem z veřejných sítí - internetu, bezdrátových sítí (WiFi), dial-up přístupu z JTS/GSM, atd.

Prostředky pro ochranu před škodlivým SW musí být trvale aktivovány (rezidentní ochrana) nebo automaticky periodicky spouštěny. Dále je nutno zajistit jejich periodickou aktualizaci - nejlépe automatizovaně.

2.5 Datová bezpečnost

Vzhledem k tomu, že data IS RŽP nejsou ukládána na pracovních stanicích uživatelů, je potřeba zabezpečit pouze konfiguraci prostředků výpočetní a komunikační techniky využívaných pro přístup k IS RŽP.

2.6 Bezpečnost komunikačních cest

Bezpečnost komunikačních cest se týká jednak IS RŽP a jednak správy uživatelů.

Protože IS RŽP používá protokol HTTPS, není potřeba používat další technická bezpečnostní opatření (IPSec, SSH tunely apod.). Protože pro funkčnost IS RŽP je životně důležité zabezpečení dostupnosti centra IS, je nutno zabezpečit odpovídající kvalitu komunikačních cest. Doporučené prostředky jsou:

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

Obecná bezpečnostní opatření na pracovištích IS RŽP

- vyhrazení potřebné kapacity linky pro potřeby IS RŽP,
- monitorování dostupnosti a vytížení komunikací s možností řízení vytížení jednotlivými subsítěmi, počítači nebo aplikacemi,
- existence záložního nebo zdvojeného spojení na centrum IS RŽP.

Pro správu uživatelů se kromě datového spojení společného pro IS RŽP používá i pošta, elektronická pošta a telefon. U těchto komunikačních cest je potřeba zabezpečit, aby příchozí zásilky, e-maily a hovory nemohly být zneužity.

2.7 Realizace bezpečnostních opatření na pracovištích IS RŽP

Realizace bezpečnostních opatření na jednotlivých ŽÚ je v kompetenci městských úřadů, úřadů městských částí, krajských úřadů a magistrátů. Za jejich realizaci je vůči IS RŽP odpovědný vedoucí ŽÚ.

Realizace bezpečnostních opatření na pracovištích externích uživatelů je v kompetenci příslušných externích subjektů, se kterými má MPO dohodu o poskytnutí přístupu do IS RŽP. Za jejich realizaci je vůči IS RŽP zodpovědný zástupce externího subjektu, který je oprávněn jednat s MPO o přístupu k IS RŽP, nebo jím pověřená osoba.

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

3 ZVYŠOVÁNÍ BEZPEČNOSTNÍHO POVĚDOMÍ UŽIVATELŮ IS RŽP

Jednou z hlavních povinností na úseku kybernetické bezpečnosti je zvyšování bezpečnostního povědomí uživatelů IS RŽP vycházející z požadavků zákona o kybernetické bezpečnosti. Vzhledem k tomu, že MPO nemá pravomoc ukládat úřadům všech úrovní povinnosti v oblasti kybernetické bezpečnosti, je na těchto úřadech, aby pro definici obsahu, formy, termínů poučení a ověření znalostí uživatelů IS RŽP zpracovaly a udržovaly vlastní plán zvyšování bezpečnostního povědomí vycházející z jejich bezpečnostní politiky a jim dostupné části bezpečnostní dokumentace IS RŽP. Pro registrované uživatele je dostupná část bezpečnostní dokumentace IS RŽP, sloužící pouze pro vnitřní potřebu ŽÚ, k dispozici na Infowebu RŽP a v Evidenci metodik MPO a dokumentů RŽP, který je přístupný pro přihlášeného uživatele IS RŽP.

Minimální doporučený obsah poučení o bezpečnostních opatřeních a důsledcích vyplývajících z porušení těchto opatření by měl zahrnovat:

- bezpečné používání výpočetní techniky,
- bezpečné používání internetu (zvláště e-mailů a webu),
- opatření v oblasti objektové (fyzické) bezpečnosti,
- ochranu osobních údajů a práce s dokumenty,
- význam údajů zapisovaných do Živnostenského rejstříku,
- povinnosti plynoucí z této Bezpečnostní směrnice IS pro uživatele.

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

4 KONTAKTNÍ OSOBA A JEJÍ POVINNOSTI

Kontaktní osobou pro ŽÚ je zpravidla vedoucí nebo jím pověřená osoba. Kontaktní osoba pro externí subjekty a její pravomoci jsou stanoveny dohodou mezi MPO a externím subjektem. Kontaktní osoba se podílí na správě přístupových práv a na řešení kybernetických bezpečnostních událostí.

Kontaktní osoba je odpovědná vůči správci IS RŽP za dodržování této Bezpečnostní směrnice IS pro uživatele jednotlivými uživateli. Každý uživatel proto musí být před přidělením přístupu k IS RŽP prokazatelným způsobem:

- vyškolen v používání IS RŽP v rozsahu odpovídajícímu jeho funkčnímu zařazení,
- seznámen s uživatelskou dokumentací,
- seznámen s touto Bezpečnostní směrnicí IS pro uživatele,
- poučen o bezpečnostních opatřeních a důsledcích vyplývajících z porušení těchto opatření.

4.1 Správa přístupových oprávnění

V oblasti správy přístupových oprávnění existují 3 druhy procesů:

- založení nového uživatele (nový uživatel),
- odebrání přístupu uživateli (odebrání uživatele),
- změna údajů, oprávnění a způsobu autentizace uživatele (změna uživatele).

Procesy správy přístupových oprávnění vznikají na základě žádosti oprávněného žadatele. Žadatelem může být:

- vedoucí ŽÚ nebo jím pověřená osoba,
- pracovník Helpdesku RŽP,
- správce uživatelů v hostingovém centru RŽP,
- odpovědný pracovník MPO.

Kontaktní osoby externích subjektů žádají o přidělení, odebrání a změnu přístupových oprávnění prostřednictvím odpovědného pracovníka MPO (dále jen "správce externích přístupů").

Žadatel vyplňuje žádost vždy elektronicky a odesílá ji e-mailem opatřeným zaručeným el. podpisem na Helpdesk RŽP. Elektronická žádost je automaticky uložena v IS Helpdesku RŽP

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

a její zpracování je předáno odpovědnému pracovníkovi ICZ a.s., poskytovatele služby IS RŽP (dále jen "správě uživatelů").

U externích organizací veškerou komunikaci zprostředkovává správce externích subjektů, který současně schvaluje žádosti a všechny požadované změny. Pro kontakt s uživateli (a žadateli) se používá poštovní adresa úřadu a e-mailové adresy uživatelů. Pro ověření žádosti používá správa uživatelů telefonní číslo daného úřadu/kontaktní osoby/žadatele.

Obsahem komunikace je:

- E-mailová žádost v elektronické podobě opatřená zaručeným el. podpisem kontaktní osoby,
- informace o přidělení přístupu,
- předávací protokol – seznam „informací o přidělení přístupu“ a čipová karta v jedné zásilce na úřad,
- podepsaný předávací protokol – předávací protokol z předchozího bodu podepsaný jednotlivými uživateli a
- obálka s PIN s PUK.

4.1.1 Přidělení přístupu k IS RŽP uživateli

Pro přidělení přístupu uživatele k IS RŽP musí žadatel vyplnit elektronickou žádost. Formulář pro jednotlivé úrovně úřadů je dostupný na infowebeu IS RŽP - sekce Dokumenty - Vydání nové karty. K vyplnění žádosti musí žadatel znát a do žádosti uvést:

- jméno, příjmení a tituly uživatele,
- e-mailovou adresu uživatele,
- označení živnostenského úřadu uživatele,
- telefonní číslo uživatele,
- iniciály uživatele,
- osobní číslo uživatele,
- zastávanou funkci,
- požadovanou úroveň oprávnění (vyplývá z funkce) a
- datum, ke kterému má být přístup uživateli zřízen.

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

Formulář pro žádost o přístup uživatelů externích organizací jejich kontaktním osobám poskytuje správce externích subjektů, který pak žádost schválí a předá správě uživatelů ke zpracování.

Standardně je přihlašování do IS RŽP nastaveno použitím čipové karty. O přijetí a vyřízení žádosti je žadatel informován správou uživatelů prostřednictvím Helpdesku RŽP e-mailem.

Standardně do 2 týdnů správa uživatelů žádost o přidělení přístupu zpracuje a doručí čipovou kartu (chráněnou PIN) uživatele a obálku s PIN a PUK na ŽÚ, příp. prostřednictvím správce externích subjektů na externí organizaci. Kontaktní osoba předá uživateli kartu a obálku s PIN a PUK a nechá uživatelem podepsat předávací protokol (je součástí zásilky). Uživatel má povinnost obálku s PIN a PUK pečlivě uschovat pro příp. použití při nesprávné manipulaci s kartou (např. zablokování karty nesprávným zadáním PINu).

Podepsaný předávací protokol žadatel doručí zpět správě uživatelů poštou nebo elektronicky. Protože předávací protokol může obsahovat řádky pro více uživatelů, je možno jej odesílat zpět i částečně podepsaný. Není nutno čekat, až protokol podepíše všechny osoby.

O aktivování uživatelského účtu je žadatel informován (stejně jako uživatel) e-mailem nebo telefonicky. Přihlášení k aplikaci není možné okamžitě po převzetí karty a PIN z bezpečnostních důvodů. Uživatelský účet je aktivován poskytovatelem služby IS RŽP až po doručení podepsaného předávacího protokolu zpět správě uživatelů.

4.1.2 Vypršení platnosti karty

Před vypršením platnosti čipové karty poskytovatel služby IS RŽP každému aktivnímu uživateli automaticky vyrobí novou kartu a doručí prostřednictvím kontaktní osoby na ŽÚ či prostřednictvím správce externích subjektů do externí organizace. Při „plánované“ výměně karty není potřeba vyplňovat žádost o vydání nové karty. Kontaktní osoba předá karty uživatelům a zajistí od dotčených uživatelů podpis předávacího protokolu (je součástí zásilky). Podepsaný předávací protokol žadatel doručí zpět správě uživatelů poštou nebo elektronicky. O okamžiku, od kterého je možno (i nutno) používat pouze novou kartu, je informován e-mailem uživatel a kontaktní osoba. Po ověření funkčnosti nové karty je uživatel nebo kontaktní osoba za úřad povinna zajistit fyzickou likvidaci původní karty uživatele. Zničit kartu lze pomocí skartovacího stroje k takovému účelu určeného nebo přestřížením karty v místě čipu.

4.1.3 Změny v přístupu k IS RŽP

Požadavky na změny v přístupu k IS RŽP vyplývají jednak z běžných změn na ŽÚ - změna funkce uživatele, změna údajů o uživateli (příjmení, telefon, e-mail), jednak z nestandardních situací - ztráta karty, zablokování karty, apod. Řešením nestandardních situací se zabývá kapitola 4.2 Řešení kybernetických bezpečnostních událostí

Standardně je možno provádět následující změny:

- změna údajů o uživateli – jméno, příjmení, tituly, jednoznačný e-mail, zaměstnanecké (osobní) číslo, telefonní spojení, iniciály uživatele,

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

- změna oprávnění - při změně funkce,
- změna stavu uživatele - pozastavení přístupu a obnovení přístupu např. při mateřské dovolené, dlouhodobé nemoci, apod.

V jedné žádosti lze požadovat provedení několika změn současně. Dále je možno zadat datum, ke kterému mají být změny provedeny (při zadání aktuálního data budou změny provedeny neprodleně).

Postup vyřízení změny přístupových práv uživatele:

1. Žadatel vyplní elektronickou žádost - napíše a odešle na Helpdesk RŽP el. podepsaný e-mail obsahující veškeré potřebné informace. Pro pozastavení přístupu se použije „žádost o odebrání přístupu uživatele“, pro ostatní změny se použije identický formulář jako pro vydání nové karty, ve kterém se vyznačí, že se jedná o změnu nastavení pro stávajícího uživatele.
2. O přijetí žádosti je žadatel informován správou uživatelů e-mailem prostřednictvím Helpdesku RŽP.

Pokud nebylo požadováno vydání nové karty, správa uživatelů informuje o vyřízení žádosti žadatele i uživatele e-mailem a proces změny je ukončen. Pokud bylo požadováno vydání nové karty, je další postup shodný jako při vypršení platnosti karty: karta je správou uživatelů odeslána na úřad kontaktní osobě, která ji vydá uživateli proti podpisu předávacího protokolu. Podepsaný protokol žadatel odešle zpět správě uživatelů a po obdržení protokolu správa uživatelů informuje žadatele i uživatele e-mailem o provedení změn.

Při pozastavení přístupu je nutno kartu a obálku s PIN a PUK uživateli odebrat a uschovat na bezpečném místě (např. v trezoru úřadu). Odebrání karty s obálkou s PIN a PUK provede kontaktní osoba. Obojí kontaktní osoba vrátí uživateli při obnovení jeho přístupu.

Přechod pracovníka na jiný úřad je řešen odebráním přístupu k IS RŽP na jednom ŽÚ, zničením jeho čipové karty (viz kapitola 4.1.4) a přidělením přístupu na novém ŽÚ současně s vydáním nové čipové karty (viz kapitola 4.1.1).

4.1.4 Odebrání přístupu

Pokud uživatel „přestal mít nárok“ na přístup k IS RŽP, kontaktní osoba zajistí odebrání jeho přístupu k IS RŽP. Žadatel vyplní „Žádost o odebrání přístupu“. Lze požadovat odebrání přístupu k určitému datu anebo co nejdříve. Po vyplnění žádosti ji žadatel formou e-mailu podepsaného zaručeným el. podpisem odešle na Helpdesk RŽP. O přijetí žádosti je žadatel Helpdeskem RŽP informován e-mailem.

O vyřízení žádosti je prostřednictvím Helpdesku RŽP informován žadatel e-mailem. V případě žádosti o odebrání přístupu k určitému datu dojde k vyřízení žádosti nejdříve k požadovanému datu.

Po odebrání přístupu uživateli, stejně jako v případě přechodu uživatele na jiný živnostenský úřad, kontaktní osoba zajistí odebrání čipové karty uživateli a její prokazatelné zničení. Zničit

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

kartu lze pomocí skartovacího stroje k takovému účelu určenému nebo přestřížením karty v místě čipu.

4.2 Řešení kybernetických bezpečnostních událostí

V rámci správy přístupových oprávnění k IS RŽP mohou vzniknout nestandardní situace, které musí řešit kontaktní osoba ve spolupráci s uživateli. Jedná se o:

- ztrátu karty,
- zničení, poškození, trvalé zablokování karty,
- zneužití přístupu k IS RŽP.

U nestandardních situací, které uživatel mohl vyřešit a vyřešil sám (vyzrazení PIN ke kartě), kontaktní osoba pouze předává zpětně prostřednictvím Helpdesku RŽP informaci o nestandardní situaci poskytovateli služby IS RŽP. Ostatní nestandardní situace je nutno řešit podle pokynů poskytovatele služby IS RŽP.

4.2.1 Ztráta karty

Prvním krokem při řešení ztráty karty je pozastavení přístupu uživatele k IS RŽP (jako např. při dlouhodobé nemoci). O pozastavení přístupu žádá okamžitě po zjištění bezpečnostní události žadatel žádost o „Odebrání přístupu“. Žádost je třeba zaslat na Helpdesk RŽP a v takovém případě je vhodné prostřednictvím Call Centra (telefonní spojení na Helpdesk RŽP) upozornit poskytovatele služby IS RŽP na tuto žádost a potřebu okamžitého zablokování přístupu. Žádost lze rovněž realizovat přímo prostřednictvím Call Centra RŽP. V takovém případě si pracovník Call Centra RŽP oprávněnost žádosti ověří zpětným voláním na „oficiální telefonní kontakt“ žadatele. O přijetí žádosti je žadatel informován e-mailem. Další postup řešení ztráty karty je obdobný jako řešení zničení, poškození nebo trvalého zablokování karty. Rozdíl spočívá v tom, že je následně nutno požádat i o obnovení přístupu uživatele k IS RŽP.

4.2.2 Zničení, poškození, trvalé zablokování karty

Tuto situaci řeší žadatel žádostí o vydání nové karty. Opět je nutno vyplnit žádost a standardním způsobem odeslat tak, jak je uvedeno v kapitole 4.1 této příručky. Vyřízení takovéto žádosti je delší s ohledem na nutnost kartu vyrobit a doručit kontaktní osobě.

4.2.3 Zneužití přístupu k IS RŽP

V rámci běžného provozu i přes všechna přijatá opatření může dojít ke zneužití přístupu k IS RŽP a tím poškození důvěrnosti, resp. důvěryhodnosti dat. Jedná se např. o:

- úmyslný zápis chybných dat do živnostenského rejstříku,

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

Kontaktní osoba a její povinnosti

- získání neoprávněného výpisu informací o subjektu či osobě evidované v IS RŽP,
- zneužití přístupu k IS RŽP jinou osobou na základě opuštění pracoviště uživatelem a ponechání čipové karty bez dozoru.

Tyto události je kontaktní osoba povinna okamžitě nahlásit Helpdesku RŽP a řídit se dále jeho pokyny.

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

5 UŽIVATEL IS RŽP, JEHO PRÁVA A POVINNOSTI

5.1 Postupy při používání IS RŽP

Při používání IS RŽP je uživatel povinen řídit se uživatelskou dokumentací, touto Bezpečnostní směrnicí IS pro uživatele a pokyny svého nadřízeného.

Všichni uživatelé systému jsou odpovědní za obsahovou správnost, úplnost a ochranu jimi vytvořených, přijatých a zpracovávaných dat a jsou povinni ihned hlásit jakékoliv odchylky svému nadřízenému. Dále jsou uživatelé povinni:

- dodržovat požadavky této Bezpečnostní směrnice IS pro uživatele,
- zachovávat mlčenlivost o datech, zejména osobních, s nimiž se seznámí při práci s IS RŽP, dále o přijatých bezpečnostních opatřeních, s nimiž jsou seznamováni,
- dokumenty, které obsahují osobní údaje a údaje z neveřejné části živnostenského rejstříku, bezpečně ukládat, aby nemohla být narušena jejich důvěrnost,
- absolvovat akreditovaný Vzdělávací program IS RŽP (platí pouze pro uživatele z řad ObŽÚ),
- používat pouze schválené programové vybavení a řádně evidovaná média,
- hlásit všechna podezření na bezpečnostní incidenty a neobvyklé události pozorované během provozu kontaktní osobě,
- dodržovat požadavky na tvorbu a změnu PIN ke kartě (viz kap. 5.1.1).

Uživateli není povoleno:

- sdílet účet s jakoukoliv jinou osobou / uživatelem,
- usilovat o získání přístupových práv nebo privilegovaného stavu, který nebyl uživateli přidělen,
- šířit, instalovat, nebo používat takový software a data, k jejichž šíření, instalaci nebo používání nemá uživatel oprávnění a/nebo jehož provozování není schváleno správcem IS.

5.1.1 Zásady používání čipové karty

Čipovou kartu je možno používat pouze pro přihlašování k IS RŽP a podepisování dokumentů v IS RŽP. Není dovoleno:

- kartu, PIN nebo PUK poskytovat jiné osobě,

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

- zapisovat si PIN,
- používat triviální PIN - např. 1111, 1234,
- ponechávat kartu bez dozoru,
- kartu mechanicky poškozovat, ohýbat a vystavovat teplotám nad 50° C.

Zásady práce s čipovou kartou jsou následující:

- po vypršení platnosti karty je uživatel nebo kontaktní osoba povinna kartu fyzicky zlikvidovat, platnost karty končí také s ukončením pracovního poměru / funkce uživatele na ŽÚ; kartu lze fyzicky zlikvidovat použitím skartovacího stroje k tomu určeného nebo přestřížením karty v místě elektronického čipu,
- v každém okamžiku existuje pro daného uživatele pouze jedna platná karta; výjimkou je pouze obměna karty, kdy až do vypršení platnosti původního certifikátu mohou být v platnosti dvě karty současně. Po ověření funkčnosti nově vydané karty je uživatel nebo kontaktní osoba povinna původní kartu fyzicky zlikvidovat,
- při dočasném odebrání přístupu (např. dlouhodobá nemoc, odchod na MD) uloží uživatel kartu u vedoucího ŽÚ (PIN mu nesděluje); vedoucí ŽÚ nahlásí správě uživatelů změnu v přístupu uživatele k IS RŽP; při obnovení přístupu dostane uživatel kartu zpět,
- pokud uživatel ukončí pracovní poměr na daném ŽÚ a nastoupí do pracovního poměru na jiném ŽÚ, bude mu stará karta zničena a na novém pracovišti vydána žadatelem karta nová,
- karty jsou z centra (poskytovatelem služby IS RŽP) odeslány na úřad, který je přiděluje pracovníkům; zpět se vrací podepsaný protokol o převzetí neporušené obálky s PIN a kartou,
- obálky s PIN a PUK posílá správa uživatelů odděleně od obálek s čipovými kartami,
- pokud došlo k prozrazení PIN a existuje podezření na zneužití karty, uživatel je povinen to ohlásit vedoucímu ŽÚ pro kontrolu toho, co bylo provedeno v IS RŽP jménem uživatele. Dále je uživatel povinen změnit si PIN a poté kartu opět používat,
- při zablokování PIN si uživatel odblokuje PIN pomocí SW SafeSign a znalosti PUK; pokud existuje podezření, že zablokování karty je důsledkem pokusu o zneužití karty, je uživatel povinen to nahlásit vedoucímu ŽÚ (pro kontrolu toho, co bylo provedeno v RŽP jménem uživatele),
- při nezvratném zablokování karty (zablokování PUK) vedoucí ŽÚ požádá o vydání nové karty. Pokud se jedná o kartu vedoucího ŽÚ a pokud je tento vedoucí zároveň kontaktní osobou, žádá o vydání nové karty správce externích přístupů,

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

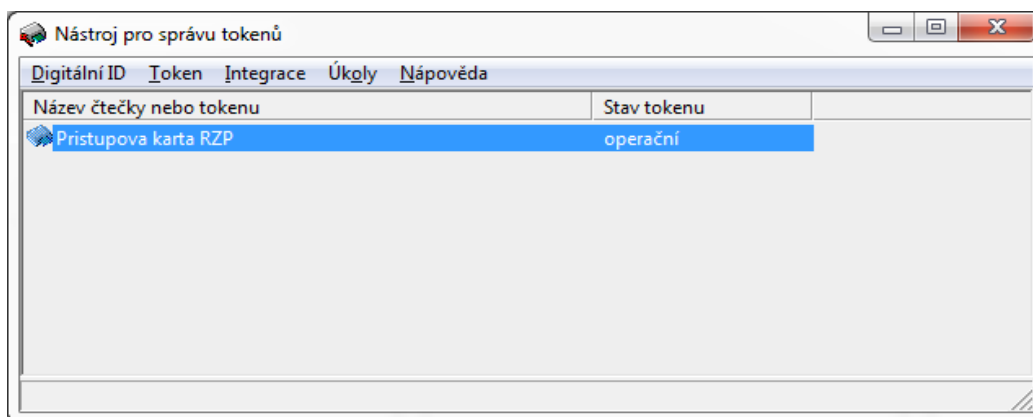
- při ztrátě karty provede poskytovatel služeb IS RŽP odebrání přístupu uživateli bez odebrání vazeb, a to na základě elektronické nebo telefonické žádosti kontaktní osoby na Helpdesk RŽP, a následně žadatel požádá správu uživatelů o vydání nové karty.

Uživatelé externích organizací

Pro uživatele externích organizací platí předchozí ustanovení obdobně. Komunikaci mezi kontaktní osobou externí organizace a poskytovatelem služby IS RŽP zajišťuje správce externích přístupů na MPO, který poskytuje formulář pro vydání nové karty. Tento správce také schvaluje žádosti o přístup uživatelů externích organizací a zprostředkovává distribuci karet.

5.1.1.1 Pokyny pro změnu PIN a PUK

Změna PIN a PUK se provádí pomocí programu „Správa tokenů“, který se spouští z menu volbou: Start / Programy / SafeSign Standard / Řízení Tokenů (doporučujeme provést ve spolupráci s informatikem úřadu) :



Obr. 1

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

Vlastní změna PIN, resp. PUK se provádí volbou Token / Změnit kód (Change) PIN ... (resp. Token / Změnit kód (Change) PUK ...) následujícím dialogem:

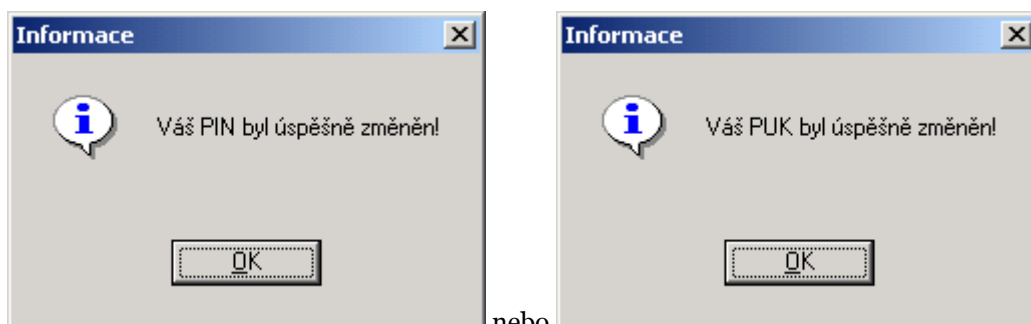
Obr. 2

resp.

Obr. 3

V dialogu je potřeba vyplnit původní PIN (resp. PUK) a zadat 2x nový PIN (resp. PUK) a stisknout tlačítko OK. Úspěšná změna je potvrzena dialogem:

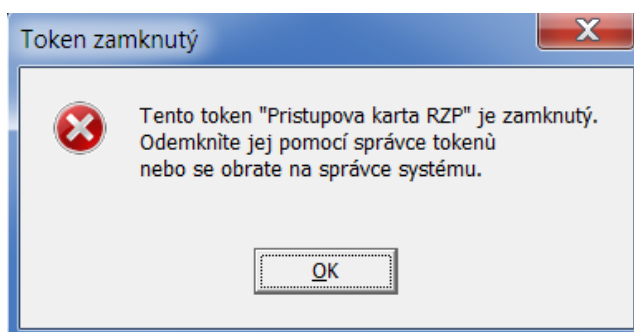
Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RŽP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024



Obr. 4

5.1.1.2 Pokyny pro odblokování zablokované karty

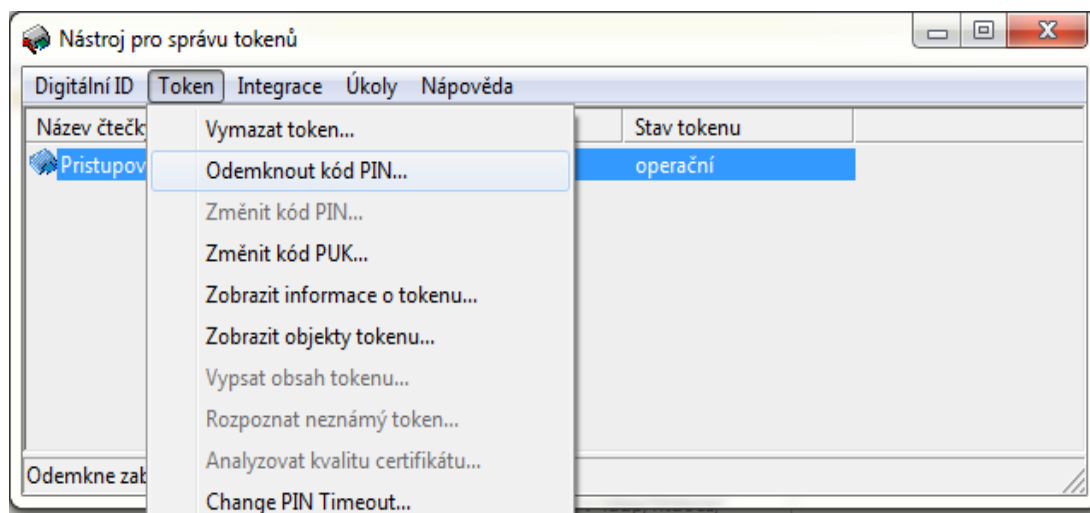
Pokud uživatel 3x zadá nesprávný PIN karty, karta (= token) se zablokuje a je uživateli zobrazeno informační okno:



Obr. 5

Kartu lze odblokovat zadáním PUK pomocí správy tokenů (z uschované obálky při převzetí karty). Aplikaci Správce tokenů lze spustit z hlavního menu „Start“ volbou „Programy“, „SafeSign Standard“ a „Řízení tokenů“.

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024



Obr. 6

5.1.2 Přihlášení k IS RŽP

Běžní uživatelé IS RŽP se mohou přihlásit na libovolné pracovní stanici, která je pro IS RŽP určena. Uživatel se přihlásí vložení karty do snímače před spuštěním aplikace a zadáním PINu po spuštění aplikace.

V případě, že uživatel zadá 3x nesprávný PIN karty, dojde k automatickému zablokování karty. Zablokovanou kartu je možno odemknout pomocí PUK – viz kapitola 5.1.1.2 Pokyny pro odblokování zablokované karty.

V případě, že si uživatel není vědom, že provedl tři chybné pokusy o zadání PIN, ohlásí to svému nadřízenému, případně vedoucímu živnostenského úřadu nebo kontaktní osobě, který za účelem eliminace tohoto rizika prověří, zda a jak mohla s kartou manipulovat třetí osoba.

5.1.3 Přerušení práce s IS RŽP a odhlášení

Při přerušení práce s IS RŽP, pokud uživatel potřebuje opustit pracoviště, a to i krátkodobě, je povinen:

- uzamknout pracovní stanici,
- vytáhnout ze snímače čipovou kartu a vhodným způsobem kartu zabezpečit, např. uložením do zásuvky pracovního stolu, nebo si vzít kartu s sebou.

Odhlášení od IS RŽP se provede uzavřením aplikace podle uživatelské dokumentace a vytažením čipové karty ze snímače.

5.1.4 Zálohování a obnova funkčnosti

Uživatel neprovádí zálohování a obnovu údajů.

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

5.1.5 Vstup / výstup datových souborů z / na nosiče informací

Při výstupu datových souborů z IS RŽP na nosiče informací (disketa, CD, flashdisk, ...) musí uživatel dodržovat následující zásady:

- výstup datových souborů na nosiče informací je povolen výhradně na podporu činnosti, kterou uživatel provádí v rámci výkonu státní správy,
- použitá média musí být uživatelem chráněna před zneužitím,
- po použití musí být data spolehlivým způsobem smazána.

Při vstupu datových souborů do IS RŽP z nosiče informací musí uživatel dodržovat následující zásady:

- vstupní média a data musí pocházet z důvěryhodného zdroje,
- po vložení média a před první akcí s daty musí být vždy provedena antivirová kontrola,
- vstup spustitelných kódů do IS RŽP je uživateli zakázán.

5.2 Řízení přístupu k IS RŽP

5.2.1 Získání přístupu k IS RŽP

Pokud pracovník živnostenského úřadu nebo externího subjektu (který má s MPO dohodu o přístupu k IS RŽP) potřebuje přístup k IS RŽP, získá ho prostřednictvím kontaktní osoby. Na základě údajů od (budoucího) uživatele vyplní kontaktní osoba žádost o přidělení přístupu. K vyplnění žádosti potřebuje uživatel znát a kontaktní osobě sdělit:

- jméno, příjmení a tituly uživatele,
- e-mailovou adresu uživatele,
- označení úřadu uživatele,
- telefonní číslo uživatele,
- iniciály uživatele,
- osobní číslo uživatele,
- zastávanou funkci,
- požadovanou úroveň oprávnění (vyplývá z funkce),
- datum, ke kterému má být přístup zřízen.

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

Standardně je přihlašování do IS RŽP nastaveno použitím čipové karty. O přijetí a vyřízení žádosti je žadatel informován správou uživatelů prostřednictvím Helpdesku RŽP e-mailem. Doručení žádosti správě uživatelů zajistí žadatel.

Standardně do 2 týdnů správa uživatelů žádost o přidělení přístupu zpracuje a doručí na ŽÚ čipovou kartu (chráněnou PIN) uživatele a obálku s PIN a PUK. Uživatel obdrží kartu a obálku s PIN a PUK od kontaktní osoby a podpisem předávacího protokolu potvrdí převzetí. Uživatel je povinen odmítnout podepsání protokolu v případě poškození obálky s PIN a PUK. Podepsaný předávací protokol předá uživatel kontaktní osobě, která doručí protokol zpět správě uživatelů poštou nebo elektronicky.

O aktivování uživatelského účtu informuje správa uživatelů uživatele (stejně jako žadatele) e - mailem nebo telefonicky. Přihlášení k aplikaci není možné okamžitě po převzetí karty a PIN z bezpečnostních důvodů. Uživatelský účet je aktivován až po doručení podepsaného předávacího protokolu zpět správě uživatelů.

5.2.2 Vypršení platnosti karty

Před vypršením platnosti čipové karty je uživateli poskytovatelem služby IS RŽP automaticky vyrobena a doručena nová karta prostřednictvím kontaktní osoby. Při „plánované“ výměně karty není potřeba vyplňovat žádost o vydání nové karty. Postup pro převzetí karty je stejný jako při přidělení přístupu: uživatel podpisem předávacího protokolu potvrdí převzetí karty a obálky s PIN a PUK a počká na e-mail od správy uživatelů, že novou kartu je možno používat. Po ověření funkčnosti nové karty uživatel nebo kontaktní osoba původní kartu fyzicky zlikviduje. Zničit kartu lze pomocí skartovacího stroje k takovému účelu určenému nebo přestřižením karty v místě čipu.

5.2.3 Změny v přístupu k IS RŽP

Uživatel může standardně žádat prostřednictvím kontaktní osoby o provedení následujících změn:

- změna údajů o uživateli – jméno, příjmení, tituly, jednoznačný e-mail, zaměstnanecké (osobní) číslo, telefonní spojení, iniciály uživatele,
- změna oprávnění - při změně funkce,
- změna stavu uživatele - pozastavení přístupu a obnovení přístupu, např. při mateřské dovolené, dlouhodobé nemoci, apod.

Je možno zadat datum, ke kterému mají být změny provedeny (při zadání aktuálního data budou změny provedeny neprodleně).

Postup vyřízení změny v přístupu uživatele (z pohledu uživatele):

- uživatel předá kontaktní osobě údaje potřebné pro vyplnění žádosti o změny v přístupu k IS RŽP. Kontaktní osoba vyplní elektronickou žádost - napíše a na Helpdesk RŽP odešle e-mail podepsaný zaručeným el. podpisem obsahující veškeré

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

potřebné informace. Pro pozastavení přístupu se použije „žádost o odebrání přístupu uživatele“, pro ostatní změny se použije „žádost o změnu uživatele“,

- po vyřízení žádosti je správou uživatelů uživatel (i kontaktní osoba) informován o provedené změně a proces je ukončen,
- v případě vydání nové karty obdrží uživatel od kontaktní osoby novou čipovou kartu, obálku s PIN a PUK a protokol, který uživatel podepíše a potvrdí tím převzetí nepoškozené karty a obálky s PIN a PUK. Následně je uživatel informován správou uživatelů o provedení změny přístupu do IS RŽP na novou kartu. Po ověření funkčnosti nové karty uživatel nebo kontaktní osoba původní kartu fyzicky zlikviduje. Zničit kartu lze pomocí skartovacího stroje k takovému účelu určenému nebo přestřížením karty v místě čipu.

Při pozastavení přístupu musí uživatel kartu a obálku s PIN a PUK odevzdat kontaktní osobě, karta bude uživateli vrácena při obnovení přístupu.

5.2.4 Odebrání přístupu

Pokud uživateli zanikne nárok na přístup k IS RŽP (např. z důvodu ukončení pracovního poměru), musí mu kontaktní osoba přístup k IS RŽP odebrat. Proces odebrání přístupu je zahájen opět vyplněním žádosti - „žádost o odebrání přístupu“ a odesláním této žádosti správě uživatelů, což zajistí kontaktní osoba. Odebrání přístupu lze požadovat k určitému datu nebo neprodleně.

Po odebrání přístupu uživateli, stejně jako v případě přechodu uživatele na jiný živnostenský úřad, uživatel odevzdá kontaktní osobě čipovou kartu a kontaktní osoba zajistí její prokazatelné zničení. Zničit kartu lze pomocí skartovacího stroje k takovému účelu určenému nebo přestřížením karty v místě čipu.

5.2.5 Řešení bezpečnostních událostí

Některé výjimečné situace (v souvislosti s přístupem k IS RŽP) může řešit uživatel sám a některé musí řešit ve spolupráci s kontaktní osobou. U situace, kterou může uživatel vyřešit sám, je povinen informovat o příčinách a způsobu řešení situace kontaktní osobu. Uživatel může sám řešit následující výjimečnou situaci:

- vyzrazení PIN ke kartě, kdy si uživatel změní PIN a kartu používá dále.

Pozn.: Zablokování karty (opakovaným chybným zadáním PIN) a její odblokování pomocí PUK není považováno za nestandardní situaci.

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024

6 PŘÍLOHY

6.1 Seznam použitých zkratk

GSM	Globální Systém pro Mobilní komunikaci
ICT	informační a komunikační technologie
IS	informační systém
JTS	jednotná telekomunikační síť
IS RŽP	informační systém Registru živnostenského podnikání
ObŽÚ	obecní živnostenský úřad
PIN	personal identification number
PUK	PIN unlock code
SW	software
WiFi	wireless fidelity, typ bezdrátové sítě
ŽÚ	živnostenský úřad

6.2 Seznam pojmů

poskytovatel služby IS RŽP	ICZ a.s.
správce externích přístupů	odpovědný pracovník MPO
kontaktní osoba	odpovědný pracovník ŽÚ (zpravidla vedoucí nebo jím pověřená osoba) nebo odpovědný pracovník externích subjektů (určeno dohodou mezi MPO a externím subjektem)
správa uživatelů	odpovědný pracovník ICZ a.s., poskytovatele služby IS RŽP
žadatel	vedoucí ŽÚ nebo jím pověřená osoba, pracovník Helpdesku RŽP, správce uživatelů v hostingovém centru RŽP, odpovědný pracovník MPO.

Bezpečnostní směrnice IS pro uživatele			
Zpracoval: Realizační tým IS RŽP	Utajení: -	Stav: Finální	Výtisk: 001
ID: RZP_DOC_PBD-BSUživatel	Změna: 1. 12. 2017	Verze: 1.6	Stran: 024