ČESKÝ STATISTICKÝ ÚŘAD

Pravidla pro přístup k IAIS ROS

1. Použité zkratky a pojmy

IAIS ROS	Integrovaný agendový informační systém ROS
IS	Informační systém
ISZR	Informační systém základních registrů
JIP/KAAS	Jednotný identitní prostor / Katalog autentizačních a autorizačních služeb
ČSÚ	Český statistický úřad
GUI	Grafické uživatelské rozhraní
OVM	Orgán veřejné moci
OS	Operační systém
ROB	Registr obyvatel
ROS	Registr osob
RÚIAN	Registr územní identifikace, adres a nemovitostí
SZR	Správa základních registrů
ZR	Základní registry
Bezpečnostní událost	Pozorovatelný stav systému, který má negativní dopady na provoz a bezpečnost informačního systému (např. pád systému, zneužití oprávnění, neoprávněný přístup). Za bezpečnostní událost se nepovažují události většího rozsahu způsobené externími vlivy, jako například přírodní katastrofy nebo výpadky napájení.
Bezpečnostní incident	Jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, porušení (nebo podezření na porušení) bezpečnostních politik nebo bezpečnostních směrnic, porušení SLA nebo události většího rozsahu způsobené externími vlivy, jako například přírodní katastrofy nebo výpadky napájení.

2. Integrovaný agendový informační systém ROS

Integrovaný agendou informační systém ROS (dále jen IAIS ROS) je informační systém sloužící jako centrální agendový systém pro evidenci osob. Je využíván agendami, které nemají vlastní agendový systém integrovaný se systémem základních registrů. IAIS ROS obsahuje množinu referenčních údajů, které jsou obsaženy v IS ROS, IS ROB a RÚIAN. IAIS ROS obsahuje osobní údaje z IS ROB v rozsahu podmnožiny údajů podle paragrafu 28a) zákona o ZR.

IAIS ROS je významným informačním systémem podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (podle vyhlášky č. 317/2014 Sb.). V IAIS ROS tak musí být splněny požadavky na bezpečnostní opatření dané navazující vyhláškou č. 316/2014 Sb.

Správcem IAIS ROS je ČSÚ, který zajišťuje věcnou správu a rozvoj IAIS ROS a prosazování a podporu dodržování bezpečnostních opatření. Podporu provozu poskytuje Správa základních registrů (SZR).

K IAIS ROS přistupují uživatelé z jednotlivých agend přímo přes WWW rozhraní aplikace IAIS. WWW rozhraní je přístupné ze sítě Internet. Komunikace IAIS ROS s ROS není přímá, ale probíhá skrze informační systém základních registrů (ISZR) využitím webových služeb.

3. Pravidla přístupu k IAIS ROS

Orgán veřejné moci (dále jen OVM), jehož zaměstnanci používají aplikaci IAIS ROS (dále i Provozovatel), musí splnit níže uvedené povinnosti. Tyto povinnosti musí být závazné (smluvně, pomocí všeobecně platných pravidel používání IAIS nebo obdobným způsobem). Provozovatel (vedoucí pracovník v organizaci nebo osoba odpovědná za smluvní vztah) odpovídá za odsouhlasení oprávněnosti obsazení pracovníka do konkrétní role a za informování o ukončení potřeby pracovníka přistupovat k informačnímu systému nebo jeho aktivům. Všechny tyto žádosti musí být dokumentovány.

Provozovatel musí zajistit seznámení všech uživatelů přistupujících k IAIS ROS s těmito závaznými podmínkami a proškolit je v oblasti bezpečnosti podle interních pravidel provozovatele.

Provozovatel musí:

a) zajistit, aby všem uživatelům byla pověřenými pracovníky provozovatele schválena pouze taková přístupová oprávnění k IAIS ROS, která vyplývají z náplně jejich práce.

b) uchovávat záznamy o skutečné identitě uživatelů a jim přidělených uživatelských identifikátorech.

c) v případě odchodu pracovníka, změny pracovní pozice nebo ukončení potřeby přístupu k IAIS ROS zajistit bezodkladné ukončení přístupu pracovníka k IAIS ROS.

d) minimálně jednou ročně provést kontrolu uživatelů přistupujících k IAIS ROS a zrušení přístupu uživatelů, kteří již nepotřebují do IAIS ROS přistupovat.

e) zajistit bezpečnost pracovních stanic určených pro přístup k IAIS ROS (minimálně aktuálnost OS, lokálně instalovaného software, instalovaný antivirus),

f) stanovit správci IAIS ROS postupy pro hlášení narušení bezpečnosti nebo podezření na ně formou závazných interních přepisů a zajistit dodržování následujících povinností ze strany uživatelů přistupujících k IAIS ROS.

4. Uživatelé IAIS ROS

Uživatel IAIS ROS je pro účely tohoto dokumentu zaměstnanec OVM, který má oprávnění využívat IAIS ROS pro vedení své agendy v roli čtenáře resp. editora této agendy.

Správa uživatelů je řízena v rámci externího systému JIP/KAAS (správu zajišťuje lokální administrátor - odpovědná osoba příslušného OVM).

Právo agendy editovat v ROS (prostřednictvím IAIS ROS) ohlašuje správci ROS gestor (ohlašovatel) dané agendy, zároveň stanoví, které OVM budou agendu využívat. Poté příslušné OVM ohlásí působnost v dané agendě. Následně je možné, aby lokální administrátor daného OVM nastavil v JIP pro konkrétní uživatele příslušné oprávnění v IAIS ROS (GestorEditor nebo Uživatel). Běžný uživatel má pouze právo číst údaje zapsané do ROS. Uživatel typu GestorEditor má právo i zapisovat nebo měnit údaje v ROS.

Uživatelé IAIS ROS přistupují k IAIS ROS pouze prostřednictvím definovaného GUI.

5. Povinnosti uživatele IAIS ROS

a) Je zakázáno přistupovat do prostředí informačního systému IAIS ROS z veřejně přístupných zařízení nebo zařízení, které nemá provozovatel pod svou výhradní kontrolou.
b) Uživatel IAIS ROS nesmí sdělovat nebo půjčovat přístupové údaje (sdělovat heslo) další osobě, ani jiným způsobem umožnit jiné osobě přístup k IAIS ROS s jeho uživatelskou identifikací a to ani v případě, kdy tato osoba má také zřízen přístup do IAIS ROS.

c) Uživatel nesmí přístupové údaje, které mu byly přiděleny z JIP/KAAS, použít v informačních systémech, kde není přístup řízen JIP/KAAS.

d) Uživatel nesmí přístupové údaje k IAIS ukládat nebo zapisovat tak (např. na papírek), aby k němu mohly získat přístup (a to ani za mimořádných okolností) jiné osoby.

e) Uživatel je povinen:
- při přidělení nového přístupového údaje, při prozrazení přístupového údaje nebo podezření na jeho prozrazení, okamžitě provést změnu tohoto přístupového údaje.

- okamžitě hlásit postupem, který určil provozovatel, narušení bezpečnosti nebo podezření na ně (například prozrazení hesla, hlášení antivirového programu atd.).
- při každém opuštění počítače se odhlásit z IAIS ROS a zavřít všechna okna prohlížeče nebo uzamknout klávesnici, myš a obrazovku tak, že pro obnovení přístupu bude vyžadováno jeho opětovné přihlášení.
- zachovávat mlčenlivost o údajích a datech, se kterými se v rámci výkonu přidělené role seznámí. Tato povinnost nezaniká ukončením výkonu role spojené s přístupem k IAIS ROS ani ukončením pracovního poměru uživatele u provozovatele.

6. Bezpečnostní událost a incident

Za hlášení bezpečnostních událostí, incidentů nebo podezření na ně odpovídají všichni uživatelé přistupující k IAIS ROS. Hlášení se provádí na kontaktní e-mailovou adresu **ros@czso.cz**, případně jiným způsobem, který určí provozovatel na základě dohody se správcem IAIS ROS.

Hlášení incidentu, události nebo podezření na ně musí obsahovat:

- jméno, příjmení a kontaktní údaje osoby podávající hlášení;
- datum a čas zjištění a případné další údaje o času výskytu a postupu události / incidentu;
- stručný a výstižný popis zjištěné události / incidentu včetně případného popisu dat, zařízení nebo médií, kterých se zjištění týká;
- jména osob, které byly přítomny nebo kterým bylo zjištění již oznámeno.

Obecně platí, že výše uvedeným způsobem musí být ohlašovány:

- okolnosti, jejichž důsledkem bylo nebo může být narušení bezpečnosti informací (důvěrnost nebo integrita) či dostupnosti poskytovaných služeb (např. prozrazení přístupových údajů, …);
- podezřelé aktivity nebo děje, které mohou vést k úniku, narušení nebo zničení informací;
- zjištěné bezpečnostní slabiny systémů nebo služeb.