Úřad pro ochranu osobních údajů

Směrnice č. 11/2018,

o systému řízení bezpečnosti informací

K provedení § 5 odst. 2 písm. c) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), § 3 písm. e) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), článku 7 odst. 3 směrnice č. 5/2016, o výboru pro řízení kybernetické bezpečnosti, na základě rozhodnutí výboru pro řízení kybernetické bezpečnosti č. R5, se stanoví:

Čl. 1

Bezpečnostní politika v oblasti systému řízení bezpečnosti informací

Bezpečnostní politika v oblasti systému řízení bezpečnosti informací je přílohou této směrnice.

Čl. 2

Zrušovací ustanovení

Rozhodnutí č. 7/2016, o celkové bezpečnostní politice, se zrušuje.

Čl. 3

Účinnost

Tato směrnice nabývá účinnosti dnem vyhlášení.

V Praze dne 15. listopadu 2018

JUDr. Ivana Janů
předsedkyně
(podepsáno elektronicky)

Příloha Bezpečnostní politika v oblasti systému řízení bezpečnosti informací

1. Úvod

1.1 Identifikace dokumentu

Dokument celkové bezpečnostní politiky je výchozí částí dokumentace pro řízení bezpečnosti informací a řeší oblast systému řízení bezpečnosti informací v rámci ÚOOÚ.

Bezpečnostní politika je zpracovávána v souladu s požadavky ČSN/ISO 27001:2014.

2. Vymezení pojmů a zkratek

2.1 Přehled použitých zkratek

Zkratka	Význam
AR	Analýza rizik
BF	Bezpečnostní fórum ÚOOÚ
BOZP	Bezpečnost a ochrana zdraví při práci
CBP	Celková bezpečnostní politika
ČSN	Česká technická norma (česká soustava norem)
DC	Datové centrum
EN	Evropská norma
HW	Hardware
ICT	Informační a komunikační technologie, pojem zahrnující komplexně oblast IT včetně informačních systémů
INF	Oddělení informatiky
IS	Informační systém je v podmínkách ÚOOÚ chápán jako celek obsahující procesy, uživatele, HW, data a aplikace
IS ORG	Informační systém, který spravuje a provozuje ÚOOÚ podle § 11 zákona č. 111/2009 Sb., o základních registrech
IS ÚOOÚ	Informační systém, který primárně zpracovává Registr zpracování OÚ a aplikaci Nevyžádaných obchodních sdělení (NOS) včetně integrace na navazující specifické systémy.
ISMS	*Information Security Management System* (Systém řízení bezpečnosti informací)
ISO	Mezinárodní organizace pro normalizaci (norma vydaná touto organizací)
IT	Informační technologie
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
NOS	Aplikace Nevyžádaná obchodní sdělení, součást IS ÚOOÚ
ORG	Oddělení základních identifikátorů
OÚ	Osobní údaj
PDCA	Metoda řízení rizik, z angl. *Plan – Do – Check – Act* = v překladu *Plánuj – Dělej – Kontroluj – Jednej*, tzv. Demingův cyklus, který je uplatněn pro hodnocení rizik, návrhu a zavedení bezpečnosti, management bezpečnosti a opětovné hodnocení bezpečnosti.
RA	Registr aktiv

RR	Registr rizik
SLA	Zkratka SLA (z angl. výrazu *Service Level Agreement*), je dohoda o úrovni poskytovaných služeb. SLA představuje formalizovaný popis služby, kterou poskytuje dodavatel zákazníkovi. SLA definuje rozsah, úroveň a kvalitu služby.
SW	Software, programové vybavení počítače
SZR	Správa základních registrů
ÚOOÚ	Úřad pro ochranu osobních údajů
TSC	Tesco SW, a.s., systémový integrátor
VKB	Výbor pro kybernetickou bezpečnost v rámci ÚOOÚ
VoKB	Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti
VPN	Virtuální privátní síť – způsob ochrany komunikace v nedůvěryhodném prostředí
ZKB	Zákon č. 181/2014 Sb. o kybernetické bezpečnosti
ZR	Systém základních registrů souhrnně
ZZR	Zákon č. 111/20029 Sb., o základních registrech

2.2 Vymezení pojmů

Zkratka, pojem	Význam
Administrátor aktiva	Fyzická osoba, která přichází do styku s aktivem v průběhu životního cyklu aktiva a vykonává správu aktiva v intencích pokynů a pověření garanta aktiva
AIFO	Agendový identifikátor fyzické osoby
Aktivum	Vše, co má pro organizaci nějakou hodnotu a je nutná ochrana z pohledu informační bezpečnosti (angl. *Asset*)
Analýza rizik	Proces identifikování bezpečnostních rizik, stanovující jejich závažnost a identifikující oblasti, které vyžadují ochranná opatření
Autentizace	Ověření platnosti identifikace s požadovanou mírou záruky, tj. akt zjištění, že proklamovaná identita je pravdivá.
Autorizace	Přidělení práv určitému subjektu k provádění definovaných operací v daném systému, autorizace obvykle probíhá na základě identifikace subjektu a ověření jeho identity (autentizace).
Bezpečnostní incident	Bezpečnostní incident je neočekávaná indikovaná bezpečnostní událost v IS, která způsobila narušení důvěrnosti, integrity, dostupnosti nebo neodmítnutelnosti informace v důsledku selhání bezpečnostních opatření nebo porušení bezpečnostní politiky
Bezpečnostní opatření	Praxe, postup, nebo mechanizmus, který snižuje riziko

Bezpečnostní událost	Zjištění či identifikace nepředpokládaného stavu informačního systému, služby nebo počítačové sítě, jež potencionálně může narušit pravidla bezpečnostní politiky nebo selhání některého prvku či protiopatření, jež může ovlivnit bezpečnost.
Dodavatel	Smluvní partner ÚOOÚ, který poskytuje dohodnutý rámec služeb pro IS ÚOOÚ
Dopad rizika	Ohodnocení potenciální škody, která by mohla vzniknout realizací hrozby
Dostupnost	Vlastnost, že informace a s nimi spjatá aktiva jsou uživatelům přístupná v době, kdy je požadují, (angl. *Availability*)
Důvěrnost	Vlastnost, která zajišťuje, že informace je přístupná jen těm uživatelům, kteří jsou oprávněni mít přístup k této informaci, (angl. *Confidentiality*).
Garant aktiva	Fyzická osoba nebo role, která přichází do styku s aktivem v průběhu životního cyklu tohoto aktiva a nese odpovědnost za ochranu aktiva v daném okamžiku
Garant rizika	Osoba nebo odpovědnostní role, zodpovědná za řízení a zvládání konkrétního rizika ve smyslu novelizace ČSN/ISO 27001:2014
Hardware	Technická část počítače nebo komunikační infrastruktury
Hrozba	Vlastnost vnějšího prostředí, je definována jako potenciální příčina nechtěného incidentu, který může vyústit v poškození systému nebo organizace
Incident	Jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činností organizace a ohrožení bezpečnosti informací nebo jejich dostupnosti.
Integrita	Vlastnost, že data nebyla poškozena nebo neautorizovaným způsobem změněna (angl. *Integrity*).
Integrita informačního systému	Vlastnost, že systém vykonává svou zamýšlenou funkci nenarušeným způsobem, bez záměrné nebo náhodné neautorizované manipulace se systémem.
Kritéria rizik	Referenční hodnoty parametrů, podle kterých se vyhodnocuje závažnost rizika
Nepopíratelnost	Vlastnost, kdy veškeré operace v rámci informačních aktiv musí být jednoznačně přiřazeny konkrétnímu autorovi (osobě či AIS) a jsou jednoznačně ověřitelné
Neshoda	Stav, kdy je při kontrolní činnosti konstatováno nesplnění požadavku/ opatření.
Neveřejný údaj	Jedná se o údaj, který spadá do kategorie chráněných informací vyžadujících adekvátní ochranu
Normativní opatření	Opatření s označením začínajícím písmenem „A“ a číslem (ve tvaru A.n.n.n) jsou doslovně převzata z přílohy „A“ ČSN/ISO

	27001:2014 a číselné označení odpovídá zatřídění podle uvedené normy. Opatření převzatá nebo vytvořená na základě dokumentu NIST SP 800-53 jsou označena dvěma písmeny a pořadovým číslem (ve tvaru XX-n). Opatření interního charakteru, které doplňuje nebo upravuje formulaci katalogového opatření s ohledem na účel a zaměření, jsou nově zaváděná opatření označena zkratkou „ÚOOÚ“ a pořadovým číslem (ve tvaru ÚOOÚ.n). Opatření SZR, vycházející z metodických doporučení, jsou označena písmeny „SZR“ a pořadovým číslem (např. SZR.01)
Riziko	Potenciální možnost, že daná hrozba využije zranitelnosti aktiv nebo skupiny aktiv a způsobí tak ztrátu nebo zničení aktiv
Role	Souhrn vymezených činností a potřebných autorizací pro tyto činnosti v rámci informačního systému
Správce IS	Odpovědnostní role ve vztahu k provozovaným informačním systémům
Tesco SW	Společnost Tesco SW, a.s. se sídlem v Olomouci, systémový integrátor
Vlastník aktiva	Fyzická osoba nebo role, která přichází do styku s aktivem v průběhu životního cyklu tohoto aktiva a nese odpovědnost za ochranu aktiva v daném okamžiku
Vlastník rizika	Osoba nebo odpovědnostní role, zodpovědná za řízení a zvládání konkrétního rizika ve smyslu novelizace ČSN/ISO 27001:2014
Zaměstnanec	Osoba, která je v pracovním nebo služebním poměru v ÚOOÚ
Zbytkové riziko	Riziko, které zůstává po implementaci ochranných opatření, tzv. ošetření rizika.
ZIFO	Zdrojový identifikátor fyzické osoby
Zranitelnost	Vlastnost aktiva, je definována jako slabé místo aktiva nebo skupiny aktiv, které může být využito hrozbou
Zvládání rizik	Proces výběru, přijímání, implementace a kontroly opatření k ošetření rizika

3. Kontext ÚOOÚ

3.1 Rámec systému řízení bezpečnosti informací

Tato celková bezpečnostní politika ISMS ÚOOÚ vymezuje rámec řízení bezpečnosti informací pro provozované informační systémy v rámci činnosti ÚOOÚ v rozsahu:

3.1.1.1 IS ORG a
3.1.1.2 IS ÚOOÚ.

Celková bezpečnostní politika ISMS ÚOOÚ je prosazována jednotně v kontextu činnosti ÚOOÚ.

3.2 Rozsah a hranice ISMS pro účely certifikace

Pro účely certifikace dle ISO/IEC 27001 je rozsahem systému řízení ISMS IS ORG. Definované hranice ISMS jsou tvořeny:

3.2.1.1 oddělením základních identifikátorů ÚOOÚ,
3.2.1.2 perimetrem řídicího pracoviště a
3.2.1.3 datovými centry (primární, záložní, zálohovací lokalita 3L).

4. Specifikace provozovaných IS

4.1 IS ORG

4.1.1 Charakteristika IS ORG

IS ORG je samostatným informačním systémem, provozovaným podle zákona č. 111/2009 Sb., o základních registrech, jako nedílná součást systému základních registrů. Správcem IS ORG je podle § 11 ÚOOÚ.

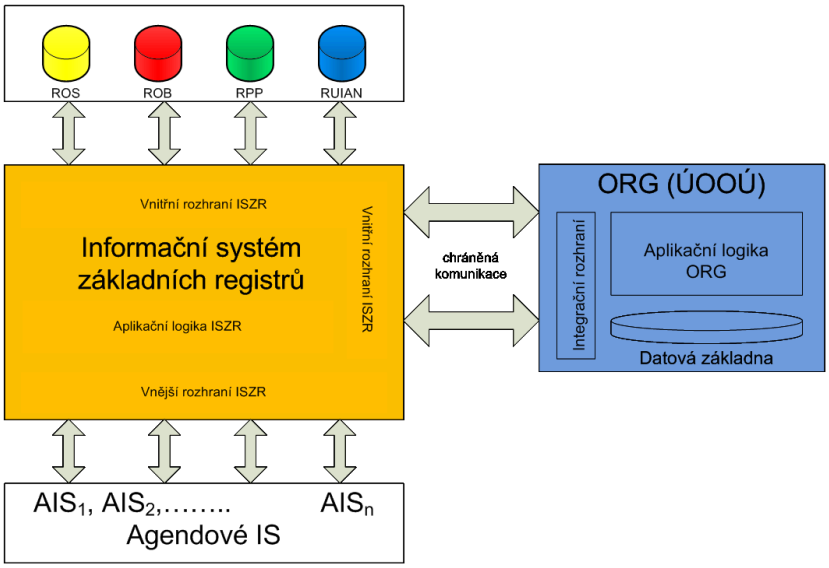
IS ORG byl vládním usnesením č. 390 ze dne 25. května 2015 ke 2. aktualizaci seznamu prvků kritické infrastruktury, jejichž provozovatelem je organizační složka státu (seznam je obsažen v přílohovém materiálu čj. 576/15 k tomuto usnesení v části III/3) zařazen jako systém kritické informační infrastruktury.

4.1.2 Kontext IS ORG v systému základních registrů

IS ORG je komponenta systému základních registrů (dále jen „ZR“). Základní registry jsou definovány v § 3 zákona o ZR. Základními registry jsou:

4.1.2.1 základní registr obyvatel, dále jen „ROB“, správcem je ministerstvo vnitra,
4.1.2.2 základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci, dále jen „ROS“, správcem je Český statistický úřad,
4.1.2.3 základní registr územní identifikace, adres a nemovitostí, dále jen „RÚIAN“, správcem je Český úřad zeměměřický a katastrální,
4.1.2.4 základní registr agend orgánů veřejné moci a některých práv a povinností, dále jen „RPP“, správcem je ministerstvo vnitra.

Další komponentou systému základních registrů z hlediska provozu je informační systém základních registrů – dále jen „ISZR“, věcným správcem je Správa základních registrů podle § 7 ZZR.



Obrázek 1: Blokové schéma základních registrů

4.1.3 Kontext IS ORG a ISMS

Z hlediska řízení bezpečnosti informací IS ORG:

4.1.3.1 obsahuje unikátní matici bezvýznamových identifikátorů fyzických osob ZIFO a AIFO, která se na jiném místě ZR nevyskytuje,

4.1.3.2 poskytuje identifikátory AIFO příslušným agendám, které je dále zpracovávají,

4.1.3.3 provádí on-line překlady AIFO mezi agendami, čímž je nezastupitelný v případě získávání referenčních údajů ze ZR,

4.1.3.4 neobsahuje jiné osobní údaje zpracovávaných fyzických osob, přičemž jednoznačný identifikátor identifikující subjekt údajů je rovněž osobním údajem,

4.1.3.5 je provozován nezávisle a odděleně od jiných informačních systémů ÚOOÚ,

4.1.3.6 jsou stanoveny SLA parametry pro dostupnost služeb a

4.1.3.7 správa IS ORG je organizačně vyčleněna do samostatného útvaru – oddělení základních identifikátorů.

4.1.4 Externí koordinace bezpečnosti informací IS ORG

Řízení bezpečnosti informací v rámci SZR je prováděno nezávisle na IS ORG. Požadavky na bezpečnost informací přesahující hranice SZR, které mají za cíl koordinovat dosažení přiměřeně shodné úrovně bezpečnosti informací v jednotlivých ZR je upraveno Rámcovou bezpečnostní politikou základních registrů.

Požadavky na bezpečnost informací, které vyplývají z Rámcové bezpečnostní politiky základních registrů, jsou posouzeny a nejsou-li v rozporu s legislativními a jinými požadavky na správce IS ORG, jsou přiměřeně zahrnuty do jednotlivých bezpečnostních politik IS ORG.

Pro koordinaci bezpečnosti informací v rámci ZR je ustaven bezpečnostní koordinační výbor, členové jsou zástupci správců jednotlivých registrů.

Ze strany SZR je monitorováno dodržování stanovených SLA parametrů pro všechny ZR, tedy včetně IS ORG.

4.2 IS ÚOOÚ

4.2.1 Charakteristika IS ÚOOÚ

IS ÚOOÚ je informačním systémem, který podporuje výkon kompetencí ÚOOÚ a řeší zejména:

4.2.1.1 dozor při šíření obchodních sdělení podle § 7 zákona č. 480/2004 Sb., o některých službách informační společnosti a

4.2.1.2 dozor nad dodržováním povinností stanovených při ochraně osobních údajů včetně správních procesů, souvisejících s předchozími povinnostmi.

IS ÚOOÚ byl zařazen vyhláškou č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, mezi významné informační systémy.

Aplikační rozsah IS ÚOOÚ:

4.2.1.3 registr zpracování OÚ, než bude zrušen,

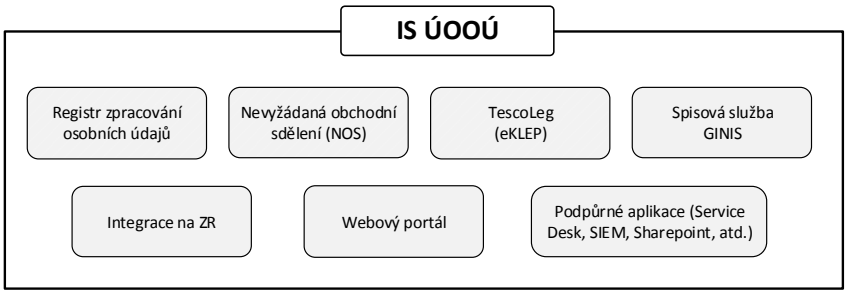
4.2.1.4 registr podání týkajících se nevyžádaných obchodních sdělení,

4.2.1.5 TescoLeg konektor na vládní aplikaci eKLEP,

4.2.1.6 výkon spisové služby v elektronické podobě v souladu se zákonem č. 499/2004 Sb., o archivnictví a spisové službě,

4.2.1.7 webový portál – podpora registru zpracování OÚ a NOS, publikace informací,

4.2.1.8 integrace na systém základních registrů (za účelem čerpání referenčních údajů).



Obrázek 2: Blokové schéma IS ÚOOÚ

4.2.2 Kontext IS ÚOOÚ a ISMS

IS ÚOOÚ je provozován fyzicky i organizačně odděleně od IS ORG a pro dostupnost služeb nejsou stanoveny SLA parametry.

5. Definice cílů v oblasti bezpečnosti informací

ÚOOÚ podporuje níže stanovené cíle a postupy k trvalému zajištění bezpečnosti informací ve spravovaných informačních systémech a specifikovaných v kapitole 3.1. Bezpečnost informací je chápána jako celek složený z jednotlivých prvků organizační a technické bezpečnosti, trvalé zajištění ochrany aktiv oblastech důvěrnosti, dostupnosti, integrity a nepopiratelnosti informací.

Společnými cíli pro IS ORG a IS ÚOOÚ jsou:

A. zajištění kontinuálního plnění účelu, pro který byl ÚOOÚ zřízen a souvisejících činností uložených zákonnými a podzákonnými předpisy a normami,

B. ustavení řídicí struktury pro oblast bezpečnosti informací a její podpora, stanovení odpovědnosti pro tuto oblast včetně sdílení informací mezi jednotlivými stupni řízení,

C. zajištění stavu, kdy bezpečnost informací je trvale a účinně prosazována a že řízení informační bezpečnosti je nedílnou součástí řídicích procesů ÚOOÚ,
D. plánování a efektivní vynakládání prostředků na zajišťování bezpečnosti,
E. minimalizace dopadů bezpečnostních opatření na činnosti ÚOOÚ, uživatelů a provozní parametry informačních systémů,
F. zajištění prevence a proaktivního předcházení bezpečnostním incidentům a
G. zájem na trvalém udržení prestiže a dobrého jména ÚOOÚ.

Vzhledem k tomu, že ÚOOÚ plní funkci nezávislé dozorové autority pro kontrolu nakládání s osobními údaji jejich zpracovateli je jakékoliv selhání nebo poškození důvěryhodnosti autority nežádoucí a může mít dopad na kredibilitu a společenskou prestiž ÚOOÚ.

Specifickými cíli pro IS ORG jsou:

a) zabezpečení provozu IS v parametrech daných SLA,
b) zjištění informovanosti, součinnosti a realizace oprávněných požadavků SZR, jakožto garanta za provoz základních registrů jako celku v oblasti bezpečnosti informací,
c) zabezpečení shody s požadavky ZKB v oblasti bezpečnosti informací,
d) zajištění certifikace IS ORG v oblasti ISMS a její udržování v dlouhodobém horizontu.

Specifickými cíli pro IS ÚOOÚ jsou:

e) zajištění oprávněných zájmů ÚOOÚ v souladu s platnými právními předpisy,
f) zabezpečení shody s požadavky ZKB v oblasti bezpečnosti informací.

5.1 Plánování krátkodobých cílů

Pro realizaci průběžných cílů ISMS musí být vytvářeny Plány dílčích cílů ISMS pro kalendářní rok, které musí být schváleny a následně vyhodnocovány. Za zpracování plánu dílčích cílů odpovídá MKB.

Podkladem pro sestavení plánu dílčích cílů jsou zejména:

5.1.1.1 plán zvládání rizik,
5.1.1.2 návrhy ke zlepšování jako zpětná vazba vyplývajících z hodnocení incidentů,
5.1.1.3 požadavky legislativy nebo normativní požadavky,
5.1.1.4 detekované neshody nebo příležitosti z auditů a
5.1.1.5 požadavky na změny řízení ISMS.

5.1.2 Vyhodnocování plánů dílčích cílů

Zpráva o vyhodnocení plánu dílčích cílů pro kalendářní rok je projednána ve Výboru pro KB a předložena předsedovi.

5.2 Nástroje cílů politiky

Programy a dílčí cíle ISMS uváděné v prováděcích dokumentech pro řízení bezpečnosti informací nižší úrovně jsou základním nástrojem pro plnění cílů bezpečnostní politiky a jsou zaměřené na konkrétní základní oblasti ochrany, jejich specifikace vzniká na základě:

5.2.1.1 strategických cílů stanovených bezpečnostní politikou,
5.2.1.2 výsledků analýzy rizik,
5.2.1.3 klasifikace informací,

5.2.1.4 rozhodnutí manažera kybernetické bezpečnosti nebo výboru pro kybernetickou bezpečnost,
5.2.1.5 návrhů bezpečnostních konzultantů,
5.2.1.6 návrhů architekta kybernetické bezpečnosti,
5.2.1.7 nařízených reaktivních opatření NÚKIB,
5.2.1.8 doporučených opatření vydaných SZR,
5.2.1.9 návrhů vedoucích zaměstnanců ÚOOÚ,
5.2.1.10 fyzické ochrany a
5.2.1.11 personální ochrany.

6. Politika systému řízení bezpečnosti informací

6.1 Principy uplatňované v oblasti řízení bezpečnosti informací

Celkové pojetí bezpečnosti informací v ÚOOÚ a úsilí k dosažení cílů je založeno na základních principech:

- **Zajištění bezpečnosti informací je trvalé úsilí**
  Přijatá bezpečnostní opatření pro zajištění informační bezpečnosti musí být vždy přiměřeně účinná a musí být uplatňována nepřetržitě.
- **Princip znalosti a uvědomění**
  Všechny osoby a subjekty participující na správě a provozování informačních systémů musí být v přiměřené míře seznámeny se zásadami bezpečnosti informací stanovené bezpečnostními politikami, průběžně doškolovány a předepsaná bezpečnostní opatření musí být schopny aplikovat a plnit.
- **Princip nejlepší praxe** („*best practices*“)
  Přijaté postupy a bezpečnostní opatření jsou aplikovány na základě ověřených praktik definovaných normou ISO/IEC 27002 Informační technologie – Soubor postupů pro řízení informační bezpečnosti, a dalšími standardy ze skupiny norem ISO 27k.
- **Princip prevence**
  Bezpečnostní opatření musí být navrhována, přijímána a realizována jako proaktivní s cílem vytvořit předcházet narušení důvěrnosti, integrity či dostupnosti a předcházet škodám.
- **Princip odpovědnosti**
  Prosazení stanovených cílů, zásad, pravidel a postupů informační bezpečnosti je vždy spojeno s individuální jednoznačně určenou odpovědností konkrétních osob na straně vlastníka, garanta, správce, poskytovatele, uživatele nebo dodavatele.
  Na zajištění bezpečnosti informací se podílí všichni, kdo se podílejí na návrhu, implementaci, provozu, užívání, údržbě, rozvoji a likvidaci informačních systémů.
- **Princip formalizace**
  Prosazování a řízení bezpečnosti informací v rámci ÚOOÚ je spojeno s formalizovanými, jednoznačně definovanými a náležitě popsanými postupy, jejichž uplatňování je řádně dokumentováno. Nedílnou součástí řízení jsou nástroje kontroly a nezávislého auditu, které důsledně ověřují míru a kvalitu skutečné realizace všech přijatých opatření.

- **Princip kontroly**

  Zavádění a dodržování zásad, pravidel a postupů bezpečnosti informací na všech úrovních musí být pravidelně kontrolováno. Zjištěné nedostatky musí být předepsaným způsobem dokumentovány, komunikovány a odstraněny.

- **Princip soustavného rozvoje**

  Bezpečnostní opatření musí reagovat na vývojové trendy v oblasti kybernetické kriminality, zejména na nové hrozby, které mohou ovlivnit užívání spravovaných informačních systémů a jejich okolí a proto musí být pravidelně přezkoumávána.

- **Princip regulace rozhodování**

  Co není výslovně povoleno, je zakázáno.

6.2 Závaznost dokumentu politiky

6.2.1.1 Tato celková bezpečnostní politika, jakož i navazující dílčí bezpečnostní politiky jsou závazné pro všechny zaměstnance v ÚOOÚ; adekvátní požadavky pak rovněž pro všechny smluvní dodavatele služeb.

6.2.1.2 Zaměstnanci jsou seznámeni s bezpečnostními politikami a řídí se jimi.

6.2.1.3 Bezpečnostní politika je přiměřená potřebám ÚOOÚ pro naplnění požadavků na řízení bezpečnosti informací.

6.2.1.4 Zaměstnancům za každé závažné porušení stanovených pravidel bezpečnosti hrozí sankce a postihy v souladu předpisy.

6.2.1.5 Konkrétní postih je stanoven na základě posouzení závažnosti, míry zavinění a konkrétního rizika, případně míry dopadu a následků bezpečnostního incidentu.

Normativní opatření:

A.5.1.1	Soubor politik pro bezpečnost informací musí být definován, schválen vedením organizace, vydán a dán na vědomí všem zaměstnancům a relevantním externím stranám.

6.3 Závazek ÚOOÚ směrem k bezpečnosti informací

Předseda svým souhlasem vyjadřuje podporu ustaveným bezpečnostním politikám, deklarovaným cílům ISMS a strategiím v nich uvedených a vyjadřuje závazek k zajišťování bezpečnosti a ochrany informací a vytváření zdrojů pro její podporu.

Normativní opatření jsou podle předchozího opatření A.5.1.1.

6.4 Kontrolní činnost předsedy

Předseda vyvíjí kontrolní činnost ve vztahu k bezpečnosti informací:

6.4.1.1 Vyžaduje pravidelné předkládání roční zprávy o přezkoumání stavu bezpečnosti informací a plnění bezpečnostních politiky.

6.4.1.2 Vyžaduje průběžné zprávy při významných bezpečnostních událostech.

6.5 Dokumentace pro řízení bezpečnosti informací

Pro řízení bezpečnosti informací v ÚOOÚ musí být zpracována, komunikována a schválena dokumentace, která hierarchicky tvoří ucelený soubor. Jednotlivé úrovně dokumentace jsou následující:

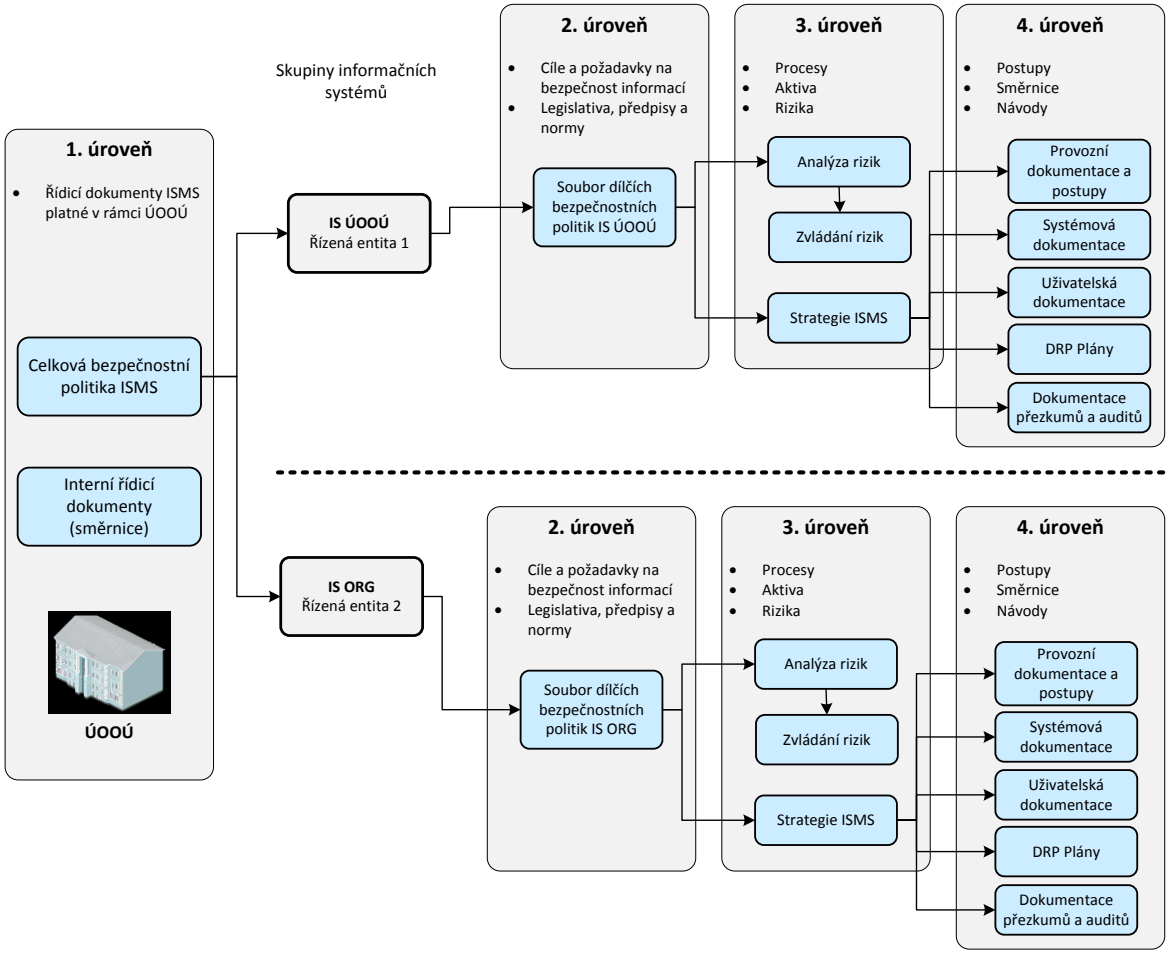
6.5.1 Struktura dokumentace pro IS podléhající dikci ZKB

Dokumentace pro řízení bezpečnosti informací v rámci ÚOOÚ je rozčleněna do 4 základních úrovní:

Úroveň	Podúroveň	Popis, charakteristika
1	Celková bezpečnostní politika ÚOOÚ	Řeší hlavní cíle v oblasti bezpečnosti informací a způsob řízení bezpečnosti informací v rámci ÚOOÚ jako celku bez ohledu na jednotlivé specifické oblasti. Celkovou bezpečnostní dokumentací je tento dokument.
	Řídicí dokumenty a normy platné v rámci ÚOOÚ	Obecné řídící dokumenty a směrnice, které řeší i část problematiky týkající se bezpečnosti informací, např. organizační řád, služební řád, spisový řád, přístupy do perimetrů atd.
2	Dílčí bezpečnostní politiky IS ORG a IS ÚOOÚ	Bezpečnostní politiky definují cíle, kterých má být v jednotlivých oblastech řízení bezpečnosti informací dosaženo. Dílčí bezpečnostní politiky jsou zpracovány odděleně pro IS ORG a IS ÚOOÚ. Důvodem je rozdílná kategorizace uvedených IS podle ZKB a tím i rozdílná úroveň požadavků na bezpečnost informací.
3	Analýza rizik	Analýza rizik je výchozím dokumentem pro zmapování aktiv v daném informačním systému a rizik, která mohou na aktiva působit. Pro IS ORG a IS ÚOOÚ jsou zpracovány oddělené analýzy rizik s ohledem na odlišné zaměření IS a odlišnými požadavky vyplývajícími ze zařazení informačních systémů a jejich definovaných hranic.
	Strategie řízení bezpečnosti informací	Strategie jsou zpracovány pro vybrané procesy řízení bezpečnosti informací, odpovídající specifikám jednotlivých IS. Strategie řeší popis procesů v metodice ITIL v oblasti zajištění bezpečnosti informací. Strategie jsou zpracovány samostatně pro IS ORG, a IS ÚOOÚ. Výčet zpracovávaných strategií je uveden v následujícím schématu.
4	Provozní dokumentace a postupy	Dokumenty typu formalizovaných pravidel a postupů, záznamy o činnostech, záznamy o incidentech, plány změn v IS, provozní deníky, knihy návštěv v perimetrech apod.
	Systémová dokumentace	Dokumentace návrhu systému, dokumentace výrobců SW a HW prvků a návody k instalaci.
	Uživatelská dokumentace	Dokumentace s návody pro obsluhu a podporu IS.

	DRP plány	Návody a postupy pro řešení krizových situací.
	Zprávy z přezkumů a auditů	Kontrolní dokumenty zajišťující zpětnou vazbu o úrovni a účinnosti řízení bezpečnosti informací. Zpracovávají se odděleně pro jednotlivé sledované informační systémy.

Schéma struktury dokumentace pro řízení bezpečnosti



6.5.2 Distribuce politik a řídících dokumentů

Pokud je kterákoliv z bezpečnostních politik nebo řídicích dokumentů pro oblast bezpečnosti informací distribuována mimo ÚOOÚ, je třeba dbát na to, aby nebyly prozrazeny citlivé informace.

Bezpečnostní politiky a řídicí dokumenty pro oblast bezpečnosti informací musí být sdělovány zaměstnancům a externím třetím stranám ve formě, která je relevantní a pochopitelná vzhledem k zamýšlenému příjemci informace.

Smluvní třetí strany musí být ve vztahu k dokumentům pro řízení bezpečnosti informací zavázány k mlčenlivosti

6.5.3 Přístupnost dokumentace

Přístupnost dokumentů pro řízení bezpečnosti informací je uvedena v úvodní kapitole každého dokumentu nebo na samostatném listu *Excelu*. Způsob označování dokumentů a jejich přístupnost je popsána v Politice klasifikace aktiv.

6.6 Řízení zdrojů a provozu systému řízení bezpečnosti informací

Cílem je plánování a zabezpečení potřebných zdrojů (finančních, personálních) pro realizaci opatření pro zajištění bezpečnosti informací, pro akvizici a změny v aplikacích a technické infrastruktuře a dále k provádění auditů a školení. Do této oblasti jsou rovněž zahrnuty i požadavky NÚKIB v oblasti nařízených reaktivních opatření, vyžadující finanční zdroje pro realizaci.

Za zpracování plánu požadavků na finanční zdroje jejich předložení k projednání poradou vedení ÚOOÚ zodpovídá manažer kybernetické bezpečnosti.

Normativní opatření:

SA-2	Organizace v rámci přidělování zdrojů: a) Určuje požadavky informační bezpečnosti pro informační systém nebo systémové služby pro plánování účelu / podnikových procesů; b) Určuje, dokumentuje a přiděluje zdroje potřebné pro ochranu bezpečnosti informačního systému jako součást svého plánovacího procesu (rozpočet)

6.7 Pravidla a postupy pro provádění auditů kybernetické bezpečnosti

Cílem je ustanovit pravidla pro provádění auditů za účelem efektivní a účinné kontroly dodržování nastavených pravidel v oblasti bezpečnosti informací.

Audit bezpečnosti je zaměřen na následující oblasti:

a) analýzu a kontrolu auditních záznamů automaticky vytvářených systémem,
b) provádění interních auditů ISMS v rámci ÚOOÚ a stanovení požadavků na interní audity prováděné dodavateli služeb a
c) provádění periodických externích auditů ISMS (v případě certifikace IS ORG).

Pravidla a postupy pro provádění auditů bezpečnostních událostí z bezpečnostního monitoringu by měla řešit minimálně následující oblasti:

6.7.1.1 seznam auditovatelných událostí a jeho údržbu,
6.7.1.2 seznamy auditních logů, které jsou předmětem kontroly a jejich umístění,
6.7.1.3 požadavky auditu na přístup k logům,
6.7.1.4 způsob a periodicitu provádění kontrol auditních záznamů,
6.7.1.5 odpovědnost za kontrolu auditních záznamů,
6.7.1.6 pořizování záznamů o provedených auditech,
6.7.1.7 uchovávání a archivace auditních záznamů jako důkazů,
6.7.1.8 způsob hlášení a reportování zjištěných odchylek a nesrovnalostí a
6.7.1.9 postupy vypořádání zjištění auditu.

6.7.2 Provádění auditů ISMS

K provádění interních auditů a jejich organizaci musí být stanovena odpovědná osoba/role.

K provádění externích auditů musí být vybrána vhodný poskytovatel, nezávislý na provozu hodnoceného IS.

Normativní opatření k dané oblasti:

A.12.7.1	Požadavky auditu a činnosti zahrnující verifikaci provozních systémů musí být pečlivě naplánovány a schváleny, aby se minimalizovalo narušení procesu organizace.
A.16.1.7	Organizace musí definovat a aplikovat postupy pro identifikaci, sběr, získání a uchování informací, které mohou sloužit jako důkazy.
A.15.2.1	Organizace musí pravidelně monitorovat, přezkoumávat a auditovat dodávky služeb dodavatelů.
AU-2 (3)	Seznam auditovatelných událostí musí být přezkoumáván a aktualizován jednou ročně nebo po větší změně informačního systému.
AU-6	Musí být zajištěno pravidelné prohlížení auditních záznamů.

6.8 Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací

Cílem je zajistit, že přezkoumání bezpečnosti informací v informačních systémech budou prováděna systematicky a v požadovaném rozsahu. K naplnění cíle musí být zpracována a udržována formální pravidla a postupy.

Přezkoumání provádí pověření odborníci v rámci přidělené gesce. Přezkoumání řídí a kontroluje manažer kybernetické bezpečnosti podle plánu schváleného Výborem pro kybernetickou bezpečnost.

Pokud při přezkumech jsou zjištěny závažné skutečnosti či odchylky, jsou závěry přezkumů projednány ve Výboru pro kybernetickou bezpečnost a se závěry seznámen předseda.

Normativní opatření k dané oblasti:

A.5.1.2	Pro zajištění neustálé vhodnosti, přiměřenosti a efektivnosti musí politiky pro bezpečnost informací přezkoumávány v plánovaných intervalech a vždy když nastane významná změna.
A.18.2.1	Přístup organizace k řízení a implementaci bezpečnosti informací (tj. cílů opatření, jednotlivých opatření, procesů a postupů bezpečnosti informací) musí být nezávisle přezkoumáván v plánovaných intervalech, nebo když nastane významná změna.
A.18.2.2	Vedoucí pracovníci musí pravidelně přezkoumávat shodu zpracování informací a postupů v rozsahu jejich odpovědnosti s odpovídajícími bezpečnostními politikami, normami a dalšími požadavky na bezpečnost.
A.18.2.3	Informační systémy musí být pravidelně přezkoumávány, zda jsou v souladu s politikami a normami bezpečnosti informací ÚOOÚ.

6.8.1 Výstupy z přezkoumání

Výbor pro kybernetickou bezpečnost iniciuje a koordinuje provedení přezkoumání ISMS. Výsledek přezkoumání:

6.8.1.1 projedná a zaznamená do zápisu z jednání a
6.8.1.2 informuje předsedu o stavu a trendech vývoje bezpečnosti informací v rámci IS ORG.

Výstupem z přezkoumání musí vždy být rozhodnutí a opatření vztahující se:

6.8.1.3 ke zlepšování efektivnosti integrovaného systému řízení a jeho procesů,
6.8.1.4 ke zlepšování IS ORG,
6.8.1.5 k činnosti dodavatelů služeb ve vztahu k pro IS ORG,
6.8.1.6 k aktualizaci hodnocení rizik a plánu zvládání rizik,
6.8.1.7 ke změnám postupů,
6.8.1.8 k potřebám zdrojů a
6.8.1.9 ke zlepšování efektivnosti opatření, která byla provedena.

6.9 Nápravná opatření a zlepšování systému řízení bezpečnosti informací

Pro odstranění příčin detekovaných provozních nebo bezpečnostních incidentů za účelem předcházení opakování incidentu musí být vypracována a dokumentována pravidla, která stanoví způsoby:

6.9.1.1 zadokumentování incidentu,
6.9.1.2 identifikace a klasifikace incidentu,
6.9.1.3 projednání příčin incidentu,
6.9.1.4 návrhy na zlepšení bezpečnosti zavedením doplňkových opatření organizačního nebo technického charakteru a
6.9.1.5 způsob předložení k projednání do výboru pro kybernetickou bezpečnost.

Provozní pravidla a dokumentované postupy pro činnosti systému musí být řízenými dokumenty s určením gestora a musí být schváleny.

V rámci procesu zlepšování musí být v rámci poučení z incidentu posuzovány zejména (nikoliv výlučně) následující úkony:

6.9.1.6 revize analýzy rizik – aktualizace registrů,
6.9.1.7 aktualizace bezpečnostních opatření za účelem předcházení podobné události,
6.9.1.8 zvýšení úrovně bezpečnostního povědomí – aktualizace plánu vzdělávání a výcviku a
6.9.1.9 zpětná vazba směrem k řízení lidských zdrojů – změna procesu prověřování a budování bezpečnostního povědomí.

6.9.2 Identifikace neshod

Cílem identifikace neshod je zaznamenat zjištěné nedostatky a nesplnění požadavků v oblasti řízení ISMS za účelem dokumentování stavu. Neshody obecně mohou být odhaleny během následujících procesů:

6.9.2.1 interní audit
6.9.2.2 externí audit
6.9.2.3 hodnocení dodavatelů
6.9.2.4 monitorování a přezkoumávání procesů v rámci IS ORG
6.9.2.5 revize dokumentace pro řízení bezpečnosti informací
6.9.2.6 testování
6.9.2.7 zkušebního provozu
6.9.2.8 výskyt incidentu

Neshody musí být zaznamenány, analyzovány a navržena opatření k nápravě.

6.9.3 Řešení neshod

Cílem řešení neshod je zjednání nápravy stavu věci a uvedení do souladu s požadavky. Výchozím podkladem pro řešení neshody je záznam o identifikované neshodě.

Normativní opatření k dané oblasti:

A.7.2.1	Vedení organizace musí po všech zaměstnancích a smluvních stranách požadovat dodržování bezpečnosti informací v souladu ustanovenými politikami a postupy v ÚOOÚ.
A.8.2.3	Pro manipulaci s aktivy musí být vytvořeny a implementovány postupy v souladu se schématem klasifikací informací přijatým ÚOOÚ.
A.12.1.1	Provozní postupy musí být dokumentovány a musí být dostupné všem uživatelům podle potřeby.
A.18.2.2	Vedoucí pracovníci musí pravidelně přezkoumávat shodu zpracování informací a postupů v rozsahu jejich odpovědnosti s odpovídajícími bezpečnostními politikami, normami a dalšími požadavky na bezpečnost.

6.10 Priority pro zvládání bezpečnostních událostí a incidentů

Cílem politiky je stanovit základní priority a principy, které musí být dodrženy při řešení incidentů bezpečnosti informací a havarijních stavů.

Hlavními prioritami, ze kterých vychází řešení bezpečnosti ÚOOÚ, jsou:

6.10.1.1 ochrana životů a zdraví zaměstnanců a všech osob nacházejících se v budově ÚOOÚ má vždy přednost před ochranou majetku,

6.10.1.2 ochrana informačních aktiv (s důrazem na data a osobní údaje) v kontextu trvalého udržení dobrého jména a prestiže ÚOOÚ,

6.10.1.3 ochrana technických aktiv a majetku,

6.10.1.4 bezpečnostní opatření musí respektovat potřeby bezkonfliktního zajišťování činnosti ÚOOÚ a minimalizovat dopady na oprávněné zájmy všech zúčastněných stran,

6.10.1.5 průběžné vyhodnocování hrozeb a analýza bezpečnostních rizik je rozhodujícím kritériem pro výběr konkrétních bezpečnostních opatření. Investice do bezpečnostních opatření musí být úměrné míře reálných rizik a finanční prostředky nebudou vynakládány v případech, kdy jsou rizika kryta pojistnými smlouvami,

6.10.1.6 výjimky stanoví předseda v případě vzniku mimořádné události nebo krizové situace při provádění záchranných a likvidačních prací.

6.10.1.7 průběžné zvyšování bezpečnostního povědomí zaměstnanců a

6.10.1.8 veškerá opatření chránící oprávněné zájmy ÚOOÚ jsou realizována v souladu s právními předpisy a respektují ochranu osobních údajů.

6.11 Proces monitorování

Monitorování výkonnosti a přezkoumání ISMS je hlavním nástrojem pro zajištění zpětné vazby a pravidelného sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací.

6.12 Proces zlepšování

Cílem je realizace možností zlepšování systému řízení bezpečnosti informací ať už soustavným zlepšování systému nebo odstraňování zjištěných slabin a nedostatků.

Každý zaměstnanec v ÚOOÚ nebo dodavatel služeb je povinen podle svých možností a schopností usilovat o trvalé zlepšování výkonu ISMS IS ORG.

Obsah