**I N S T R U K C E**

**č. 5/2022**

**Ministerstva spravedlnosti**

**ze dne 30. června 2022, č. j. 115/2022-OI-SP/1**

**o zajištění bezpečnosti informací v prostředí informačních a komunikačních technologií resortu spravedlnosti**

Ministerstvo spravedlnosti (dále jen „ministerstvo“) stanoví:

**ČÁST PRVNÍ**

**ÚVODNÍ USTANOVENÍ**

§ 1

**Působnost instrukce**

1. Tato instrukce stanoví cíle, principy, pravidla a postupy pro řízení bezpečnosti informací v prostředí informačních a komunikačních technologií v resortu Ministerstva spravedlnosti České republiky (dále jen „resort spravedlnosti“), a to v následujících organizačních složkách státu nebo státních příspěvkových organizacích:

* ministerstvo,
* Nejvyšší správní soud,
* Nejvyšší soud,
* vrchní soudy,
* krajské soudy a Městský soud v Praze,
* okresní (obvodní) soudy a Městský soud v Brně,
* Nejvyšší státní zastupitelství,
* vrchní státní zastupitelství,
* krajská státní zastupitelství a Městské státní zastupitelství v Praze,
* okresní (obvodní) státní zastupitelství a Městské státní zastupitelství v Brně,
* Vězeňská služba České republiky,
* Zotavovny Vězeňské služby České republiky,
* Rejstřík trestů,
* Justiční akademie,
* Probační a mediační služba,
* Institut pro kriminologii a sociální prevenci,

dále jen „justiční složka“.

1. Tato instrukce platí i pro organizační složky resortu spravedlnosti, které budou zřízeny po datu účinnosti této instrukce, nestanoví-li vnitřní předpis jinak.
2. Za plnění povinností vyplývajících z této instrukce odpovídají a právní jednání činí následující osoby:

* ministr spravedlnosti,
* předsedové:
* Nejvyššího správního soudu,
* Nejvyššího soudu,
* vrchních soudů,
* krajských soudů a Městského soudu v Praze,
* okresních (obvodních) soudů a Městského soudu v Brně,
* nejvyšší státní zástupce,
* vrchní státní zástupci,
* krajští státní zástupci a městský státní zástupce v Praze,
* okresní (obvodní) státní zástupci a městský státní zástupce v Brně,
* generální ředitel Vězeňské služby České republiky;
* ředitelé:
* Rejstříku trestů,
* Justiční akademie,
* Probační a mediační služby,
* Zotavovny Vězeňské služby České republiky,
* Institutu pro kriminologii a sociální prevenci,

(dále jen „vedoucí justiční složky“).

1. Prostředím informačních a komunikačních technologií (dále jen „ICT“) resortu spravedlnosti se rozumí informační systémy, výpočetní technika včetně mobilních zařízení a přídavných zařízení, veškeré počítačové sítě, komunikační infrastruktura, nosiče informací a programové vybavení justičních složek, a schválené služby technologií, které nejsou pod plnou kontrolou resortu spravedlnosti (jedná se například o služby cloud computingu). Prostředí ICT dále zahrnuje dokumentaci ICT, správu ICT, bezpečnostní správu ICT a práci uživatelů využívajících prostředků ICT.

§ 2

**Vymezení pojmů**

Pro účely této instrukce se rozumí:

* 1. Aktivum – obecně cokoliv, co má pro organizaci hodnotu, která se dělí na primární aktiva a podpůrná aktiva a dále na informační a technická. Blíže je problematika upřesněna v dokumentu „Metodika určování aktiv a stanovování garantů“, který je přílohou této instrukce.
  2. *Architekt kybernetické bezpečnosti* – osoba zajišťující návrh a implementaci bezpečnostních opatření. V praxi je architekt odpovědný za návrh bezpečné architektury (např. od infrastruktury až po bezpečnost na aplikační úrovni) a její následnou implementaci.
  3. *Auditor kybernetické bezpečnosti* – osoba, provádějící audit kybernetické bezpečnosti všech informačních aktiv zahrnutých do systému řízení bezpečnosti informací resortu spravedlnosti.
  4. Bezpečnostní incident – jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, které kompromitovaly činnost organizace nebo ohrozily bezpečnost informací, či k této kompromitaci nebo ohrožení s vysokou pravděpodobností dojde.
  5. Bezpečnostní událost – identifikovaný stav systému, služby nebo sítě, který signalizuje možné porušení bezpečnostní politiky nebo selhání bezpečnostních opatření, popř. jinou předtím nepoznanou situaci, která může být významná z pohledu bezpečnosti informací. Bezpečnostní událost může být následně překvalifikována na bezpečnostní incident, např. pokud se porušení nebo selhání opatření prokáže.
  6. Dostupnost informací (aktiva) – informace musí být dostupné oprávněným osobám, a to tehdy, pokud je potřebují pro výkon své činnosti.
  7. Důvěrnost informací (aktiva) – informace mají být ve stanoveném rozsahu dostupné pouze osobě k tomu určené v daném rozsahu oprávnění nebo pověření vyplývající z výkonu činnosti.
  8. *Garant podpůrného aktiva* – fyzická osoba pověřená justiční složkou k zajištění rozvoje, použití a bezpečnosti podpůrného aktiva.
  9. *Garant primárního aktiva* – fyzická osoba pověřená justiční složkou k zajištění rozvoje, použití a bezpečnosti primárního aktiva.
  10. Hrozba – potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození informačního systému nebo organizace.
  11. Informační a komunikační technologie (ICT) – veškeré informační technologie používané pro komunikaci a práci s informacemi.
  12. Informační aktivum – jsou znalosti a data, která mají pro justiční složku hodnotu/význam (např. programová a bezpečnostní dokumentace, zálohy dat, plány obnovy apod.).
  13. Integrita informací (aktiva) – s informacemi musí být vždy nakládáno plně řízeným způsobem tak, aby nemohlo dojít k narušení správnosti a úplnosti dané informace.
  14. Klíčový informační systém – informační systém určený jako VIS nebo IS KII, nebo informační systém uvedený v příloze této instrukce; jedná se o informační systém nezbytný pro chod justiční složky.
  15. *Manažer kybernetické bezpečnosti* – osoba, odpovědná za systém řízení bezpečnosti informací (ISMS). V praxi je manažer kybernetické bezpečnosti mezistupněm mezi strategickou úrovní managementu a operativní úrovní.
  16. Oprávněná osoba – osoba oprávněná provádět definovanou činnost na základě povinností vyplývajících z pracovních smluv či pracovních náplní nebo na základě pokynů odpovědných osob.
  17. Opatření (bezpečnostní opatření) – ochranná opatření pro zajištění bezpečnostních požadavků kladených na systém. Mohou mít různý charakter.
  18. Pracovník – pracovník justiční složky nebo jakákoliv fyzická osoba v závislém vztahu odlišná od pracovníka justiční složky (např. zaměstnanec dodavatele).
  19. Pracovník justiční složky – fyzická osoba v pracovněprávním vztahu/služebním poměru s justiční složkou, včetně osoby ve výkonu funkce (např. soudce, státní zástupce) v justiční složce, která se účastní činností nebo procesů výkonu působnosti nebo správy dané justiční složky, např. uživatel nebo správce IS.
  20. Podpůrné aktivum – jakékoliv aktivum zajišťující správnou funkčnost a podporu primárního aktiva (hardware, software, počítačová síť, pracovníci, lokalita, organizace, apod.).
  21. Primární aktivum – informace nebo služba, kterou zpracovává nebo poskytuje klíčový informační systém. Zároveň se jedná o aktivum vysoké důležitosti, jehož narušení ohrožuje výkon působnosti a správy justiční složky (v prostředí justice jsou to např. data agendových informačních systémů ISAS, ISYZ, ISVKS atd.).
  22. Riziko – možnost, že určitá hrozba využije zranitelnosti informačního systému a způsobí poškození aktiva (blíže se této problematice věnuje „Metodika hodnocení a řízení rizik“, která je přílohou instrukce).
  23. Řízená dokumentace – dokumentace, u které jsou jednotlivé verze dokumentů a celý proces jejich uvolňování pod kontrolou, která prochází pravidelným přezkoumáním její aktuálnosti, a u které všichni uživatelé ví, která verze je platná.
  24. Technické aktivum – technické vybavení, komunikační prostředky a programové vybavení informačního systému a objekty, ve kterých je tento systém umístěn.
  25. Uživatel – fyzická nebo právnická osoba anebo orgán veřejné moci, který využívá primární aktiva; ve většině případů zahrnuje pracovníka justičních složek nebo pracovníka smluvního partnera, který má přístup k informačním službám, informacím nebo jiným aktivům justičních složek, přičemž má přidělený běžný rozsah oprávnění přístupu.
  26. Vedoucí justiční složky – vedoucí dané organizační složky resortu spravedlnosti.
  27. Vedoucí zaměstnanec (též vedoucí pracovník nebo představený) – je zaměstnanec, který je oprávněn na základě vnitřní organizace zaměstnavatele stanovit a ukládat podřízeným zaměstnancům pracovní/služební úkoly, organizovat, řídit a kontrolovat jejich práci a dávat jim k tomu účelu závazné pokyny/příkazy.
  28. Výbor pro řízení kybernetické bezpečnosti – poradní orgán ministra tvořený osobami, které jsou pověřeny celkovým řízením a rozvojem kybernetické bezpečnosti v resortu spravedlnosti.
  29. Zranitelnost – slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

Další zkratky a pojmy jsou uvedeny v příloze č. 1, části III „Seznam dalších zkratek a pojmů“

§ 3

**Rozsah a hranice systému řízení bezpečnosti informací**

1. Řízení bezpečnosti informací v prostředí ICT se týká:
   1. veškerého hardwaru a softwaru,
   2. uložených zpracovávaných nebo přenášených informací,
   3. dokumentace prostředí ICT,
   4. veškerých činností spojených s užitím služeb a prostředků prostředí ICT, jeho provozní správou, bezpečnostní správou a používáním nosičů informací (včetně služeb zajišťovaných dodavatelským způsobem),
   5. veškerých etap životního cyklu prostředí ICT.
2. Tato instrukce se nevztahuje na systémy obsahující nebo zpracovávající utajované informace podle zákona o ochraně utajovaných informací[[1]](#footnote-2).

**ČÁST DRUHÁ**

**POLITIKA SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ**

§ 4

**Cíle řízení bezpečnosti informací**

1. Cílem činností v oblasti bezpečnosti informací v prostředí ICT resortu spravedlnosti je podporovat plnění úkolů justičních složek, zajistit jejich kontinuitu a ochránit dobré jméno justičních složek tím, že omezuje možná narušení jejich činností, následky bezpečnostních incidentů a zajišťuje potřebnou důvěrnost, integritu a dostupnost informací v prostředí ICT.
2. Základní strategické cíle řízení bezpečnosti informací jsou:
   1. zajištění bezpečného a důvěryhodného provozu justičních složek a ochrany jejich dobrého jména tím, že omezuje možná narušení činností justičních složek a následky bezpečnostních incidentů,
   2. splnění právních a dalších regulačních a smluvních požadavků na bezpečnost,
   3. maximálně efektivní zajištění bezpečnosti odpovídající hodnotě relevantních částí chráněného ICT prostředí.
3. Specifické cíle řízení bezpečnosti informací vycházejí ze strategických cílů a naplňují následující povinnosti, za jejichž splnění zodpovídají vedoucí justičních složek:
   1. zajištění ochrany informací – ochrana informací justičních složek před hrozbami vnějšími i vnitřními, úmyslnými či neúmyslnými,
   2. zajištění důvěrnosti informací – informace mají být dostupné pouze osobě k tomu určené, a to v rozsahu jejího oprávnění nebo pověření vyplývající z výkonu její činnosti; současně je třeba zajistit přiměřenou úroveň jejich ochrany před neoprávněným přístupem k nim nebo jejich zneužití,
   3. zajištění integrity informací – s informacemi musí být vždy nakládáno plně řízeným způsobem tak, aby nemohlo dojít k narušení správnosti a úplnosti dané informace; informace mohou být měněny pouze odpovědnými osobami nebo oprávněnými osobami na základě povinností vyplývajících z pracovních smluv či pracovních náplní nebo na základě pokynů odpovědných osob, a to vždy řízeným způsobem; správnost a úplnost informací nesmí být narušena neoprávněnými ani neúmyslnými změnami,
   4. zajištění dostupnosti informací – informace musí být dostupné oprávněným osobám, a to tehdy, pokud je potřebují pro výkon své činnosti,
   5. dodržování požadavků právních norem a dalších předpisů, se zvláštním zřetelem na zákon o kybernetické bezpečnosti[[2]](#footnote-3), platné právní předpisy týkající se zpracování a ochrany osobních údajů[[3]](#footnote-4), zákon o informačních systémech veřejné správy[[4]](#footnote-5) a platné právní předpisy týkající se elektronického podpisu[[5]](#footnote-6),
   6. hlášení a vyšetření každého narušení bezpečnosti informací, podezření na toto narušení nebo na zjištěné slabiny a následné informování příslušných pracovníků složky,
   7. efektivnost a přiměřenost opatření chránících informace vzhledem k riziku – opatření (včetně mechanismů systému řízení bezpečnosti informací) musí odpovídat významu chráněných informací, hrozbám, kterým jsou tyto informace vystaveny, a identifikovaným potřebám v oblasti bezpečnosti informací,
   8. zvyšování bezpečnostního povědomí o bezpečnosti informací – poskytnutí informací o požadavcích a postupech při zajišťování bezpečnosti informací všem osobám přistupujícím k informacím a informačním systémům justičních složek,
   9. řízení a zajištění bezpečnosti informací při přístupu třetích stran k informacím a informačním systémům. Přístup k informacím, které nejsou veřejné, musí být upraven v příslušném smluvním vztahu,
   10. realizace služeb v oblasti ICT dodávaných třetími stranami musí být zajištěna na základě smluvního vztahu, který zajistí soulad s požadavky na zajištění bezpečnosti a nápravu případných nedostatků.

§ 5

**Principy řízení bezpečnosti informací**

Mezi základní principy bezpečnosti informací, které systém řízení bezpečnosti zohledňuje, patří:

* 1. zavedení jednoho systému řízení bezpečnosti informací v rámci justičních složek,
  2. zajištění bezpečnosti informací jako trvalého procesu zahrnujícího jednorázové, opakované i soustavné činnosti,
  3. přidělení odpovědností konkrétním osobám (např. na konkrétní pracovní/služební pozici nebo v konkrétní uživatelské roli), nikoliv skupině osob,
  4. princip, kdy může systém řízení bezpečnosti informací v rámci svého rozsahu pokrývat více prostředí; každé z uvedených prostředí může mít vlastní seznam bezpečnostních opatření (politiku bezpečnosti informací), avšak základní procesy řízení bezpečnosti jsou však společné,
  5. výběr bezpečnostních opatření může být pro každé z prostředí zmíněných v předchozím bodě prováděn samostatně a za použití různých strategií,
  6. v rámci systému řízení jsou pro všechna prostředí zavedeny mechanismy kontroly souladu mimo posloupnost přímých nadřízených,
  7. vedoucí justičních složek jsou informováni o stavu bezpečnosti informací v resortu spravedlnosti.

§ 6

**Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací**

1. Pravidla a postupy zajišťující provoz systému řízení bezpečnosti informací, uvedené v příloze č. 1, části II-2 „Příručka řízení bezpečnosti“, vedou ke splnění požadavků řízení bezpečnosti informací a implementaci identifikovaných opatření.
2. Vedoucí justiční složky musí zajistit, že pravidla a postupy systému řízení bezpečnosti informací, uvedené v příloze č. 1, části II-2 „Příručka řízení bezpečnosti“, jsou pravidelně kontrolovány, hodnoceny a upravovány za účelem neustálého zlepšování.
3. Vedoucí justiční složky musí zajistit, že pravidla a postupy systému řízení bezpečnosti informací, stejně jako opatření vybraná k implementaci, uvedená v příloze č. 1, jsou dokumentovány ve formě řízené dokumentace a jsou dostupné a prezentované všem koncovým uživatelům.
4. Plánování systému řízení bezpečnosti informací a bezpečnostních opatření pro konkrétní informační systémy je prováděno na základě posouzení bezpečnosti informací. Pravidla a postupy posouzení bezpečnosti informací jsou uvedeny v příloze č. 1, části II-2 „Příručka řízení bezpečnosti“ a části II-1 „Metodika hodnocení a řízení rizik“, čímž je zajištěno, že opakovaná posouzení bezpečnosti informací produkují konzistentní, opodstatněné a porovnatelné výsledky. Za zajištění dodržování těchto pravidel a postupů v justiční složce odpovídá vedoucí dané justiční složky.
5. *Manažer kybernetické bezpečnosti* zajistí, že minimálně jednou ročně je provedena revize systému řízení bezpečnosti informací a aktualizace dokumentace systému řízení bezpečnosti informací a bezpečnostních opatření. Podrobnosti jsou stanoveny v příloze č. 1, části II-2 „Příručka řízení bezpečnosti“.
6. *Manažer kybernetické bezpečnosti* minimálně jednou ročně vytvoří zprávu o stavu bezpečnosti informací v resortu spravedlnosti a tu předloží výboru pro řízení kybernetické bezpečnosti. Podrobnosti jsou uvedeny v příloze č. 1, části II-2 „Příručka řízení bezpečnosti“.

§ 7

**Odpovědnost za bezpečnost**

1. Odpovědnost za řízení bezpečnosti informací v resortu spravedlnosti má ministr. Jako poradní orgán ministra pro tyto účely slouží výbor pro řízení kybernetické bezpečnosti.
2. Výstupy výboru pro řízení kybernetické bezpečnosti v rámci systému řízení bezpečnosti slouží jako podklady pro rozhodování ministra.
3. Ředitel odboru informatiky ministerstva:
   1. je zpracovatelem závazných předpisů k provozu prostředí ICT,
   2. je oprávněn posuzovat projekty akvizice informačních systémů s ohledem na zajištění bezpečnosti informací ICT resortu spravedlnosti,
   3. je odpovědný za průběžnou kontrolu činností osob využívajících služeb ICT resortu spravedlnosti.
4. Vedoucí justičních složek:
   1. jsou odpovědni za uplatňování této instrukce a na ni navazující předpisy upravující provoz a bezpečnost prostředí ICT,
   2. jsou oprávněni předkládat odboru informatiky ministerstva připomínky a návrhy změn v oblasti bezpečnosti prostředí ICT,
   3. jsou odpovědni za zajištění dodržování postupů stanovených platnou provozní a bezpečnostní dokumentací informačního systému smluvními partnery dané justiční složky.
5. Pracovníci odboru informatiky a IT oddělení justičních složek jsou odpovědni za soulad správy a provozu prostředí ICT justiční složky s předpisy upravujícími provoz a bezpečnost prostředí ICT.
6. Každý pracovník justiční složky je při výkonu role ve správě a/nebo užití informačního systému odpovědný za dodržování postupů stanovených platnou provozní a bezpečnostní dokumentací informačního systému.
7. Porušení zásad řízení bezpečnosti informací při výkonu role ve správě a/nebo užití informačního systému je chápáno jako bezpečnostní incident a může být postiženo jako porušení pracovních/služebních povinností, resp. porušení právních předpisů.

§ 8

**Bezpečnostní role**

1. Za účelem zajištění výše uvedených povinností ministr určuje osoby do role *manažer kybernetické bezpečnosti*, *architekt kybernetické bezpečnosti* a *auditor kybernetické bezpečnosti*. Tyto osoby převezmou odpovědnosti, práva a povinnosti uvedené v politice organizační bezpečnosti, která je součástí přílohy č. 1 této instrukce.
2. Do role *garanta primárního aktiva* určuje ministr pracovníka na návrh ředitele odboru zodpovídajícího za výkon věcné agendy, resp. vedoucího justiční složky. Tento *garant primárního aktiva* se společně s *garanty podpůrného aktiva* podílí na zajištění vývoje, provozu, použití a údržby jednotlivých částí informačního systému. Jeho další práva a povinnosti jsou uvedeny v dokumentu „Politika organizační bezpečnosti“ (příloha č. 1 této instrukce).
3. Určení/jmenování osob do ostatních bezpečnostních rolí/funkcí uvedených v této dokumentaci je v rámci dané justiční složky v pravomoci vedoucího justiční složky.

§ 9

**Pravidla a postupy pro řízení dokumentace**

K naplnění této politiky systému řízení bezpečnosti informací jsou vytvořeny potřebné procesy a navazující předpisy, které jsou obsaženy v příloze č. 1 této instrukce.

§ 10

**Pravidla a postupy pro řízení rizik**

1. Návrh bezpečnostních opatření je pro systémy spadající do oblasti působnosti zákona o kybernetické bezpečnosti prováděn v rámci procesu řízení rizik na základě hodnocení rizik.
2. Návrh bezpečnostních opatření je pro systémy nespadající do oblasti působnosti zákona o kybernetické bezpečnosti prováděn na základě nejlepší běžné praxe nebo na základě hodnocení rizik.
3. Pro zajištění jednotného přístupu k hodnocení rizik je definována jednotná metodika hodnocení a řízení rizik, která bude použita pro všechny dotčené informační systémy. Tato metodika je uvedena v příloze č. 2, část II, odstavec 2 této instrukce.
4. Systém řízení rizik musí zajišťovat, že rizika jsou nejenom identifikována, ale je rozhodováno i o jejich zvládání a následně jsou v průběhu celého životního cyklu informačního systému nadále monitorována a přehodnocována.

§ 11

**Pravidla a postupy pro provádění auditů kybernetické bezpečnosti**

1. Audit kybernetické bezpečnosti ověřuje správnost a účinnost zavedených bezpečnostních opatření a jejich soulad s právními předpisy, vnitřními předpisy, jinými předpisy a smluvními závazky. V resortu spravedlnosti jde o kontrolu bezpečnosti systémů ICT.
2. *Auditor kybernetické bezpečnosti* je v rámci resortu spravedlnosti organizačně zařazen jako kontrolor bezpečnosti ICT, příp. externí subjekt s odbornou způsobilostí k provádění auditů kybernetické bezpečnosti.
3. Výsledky auditu bezpečnosti informací jsou předávány výboru pro řízení kybernetické bezpečnosti, *manažerovi kybernetické bezpečnosti* a vedení resortu, nebo vedením resortu určenému zástupci, jako součást zprávy o stavu bezpečnosti informací v resortu.

§ 12

**Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací**

Systém bezpečnosti informací a bezpečnostní opatření jsou revidovány na základě výsledků prováděných kontrol souladu, výsledků auditů kybernetické bezpečnosti a analýz proběhlých bezpečnostních incidentů. Podrobnosti jsou uvedeny v příloze č.1, oddíl II, odstavec 3 (příručka řízení bezpečnosti).

§ 13

**Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací**

Výbor pro řízení kybernetické bezpečnosti minimálně jednou ročně přezkoumá a zhodnotí stav systému řízení bezpečnosti informací na základě předložené zprávy o stavu bezpečnosti informací a výsledků auditů kybernetické bezpečnosti.

**ČÁST TŘETÍ**

**BEZPEČNOSTNÍ DOKUMENTACE**

§ 14

Bezpečnostní dokumentace obsahující bezpečnostní politiky, bezpečnostní opatření, pravidla a postupy zajištění bezpečnosti informací je uvedena v příloze č. 2 a je pro resort spravedlnosti závazná.

**ČÁST ČTVRTÁ**

**ZÁVĚREČNÁ USTANOVENÍ**

§ 15

Zrušuje se instrukce Ministerstva spravedlnosti ze dne 1. dubna 2016, č.j.: MSP-53/2015-OI-SP o zajištění bezpečnosti informací v prostředí informačních a komunikačních technologií resortu spravedlnosti.

§ 16

**Účinnost**

Tato instrukce nabývá účinnosti dnem 1. 10. 2022.

ministr spravedlnosti

**JUDr. Pavel Blažek**

**Příloha č. 1 k instrukci č. 5/2022**

**BEZPEČNOSTNÍ DOKUMENTACE**

Tato příloha obsahuje bezpečnostní dokumentaci. Bezpečnostní dokumentace je rozdělena na bezpečnostní politiky, další bezpečnostní dokumentaci a zkratky a pojmy.

1. Bezpečnostní politiky
2. Politika akvizice a vývoje.
3. Politika organizační bezpečnosti.
4. Politika řízení dodavatelů.
5. Politika aktiv.
6. Politika bezpečnosti lidských zdrojů.
7. Politika řízení provozu a komunikací.
8. Politika řízení přístupu.
9. Politika bezpečného chování uživatelů.
10. Politika zálohování a obnovy.
11. Politika bezpečného předávání a výměny informací.
12. Politika řízení technických zranitelností.
13. Politika bezpečného používání mobilních zařízení.
14. Politika poskytování a nabývání licencí programového vybavení a informací.
15. Politika dlouhodobého ukládání a archivace informací.
16. Politika ochrany osobních údajů.
17. Politika fyzické bezpečnosti.
18. Politika bezpečnosti komunikační sítě.
19. Politika ochrany před škodlivým kódem.
20. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí.
21. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.
22. Politika bezpečného používání kryptografické ochrany.
23. Politika zvládání kybernetických bezpečnostních incidentů.
24. Politika auditu a kontroly souladu.
25. Politika řízení kontinuity činností.
26. Výčet další bezpečnostní dokumentace
27. Metodika určování aktiv a stanovování garantů.
28. Metodika hodnocení a řízení rizik.
29. Příručka řízení bezpečnosti.
30. Směrnice – Zajištění bezpečné infrastruktury prostředí ICT.
31. Seznam klíčových informačních systémů.
32. Seznam dalších zkratek a pojmů

1. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. [↑](#footnote-ref-2)
2. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů [↑](#footnote-ref-3)
3. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES a zákon č. 110/2019 Sb., o zpracování osobních údajů [↑](#footnote-ref-4)
4. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů. [↑](#footnote-ref-5)
5. Nařízení Evropského parlamentu a rady (EU) č. 910/2014 ze dne 23.července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES a zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů. [↑](#footnote-ref-6)