# Příloha č.4 – Technická specifikace

**Dílčí plnění 1:**

**A. Etapy projektu**

1. **Rozdílová analýza (identifikující úroveň plnění/neplnění standardů ISMS)**

V první kroku je třeba zjistit stav jednotlivých oblastí řízení bezpečnosti informací na úřadě (respektive úroveň/míru implementace ISMS), k čemuž budou provedeny následující kroky:

* Provedení auditu managementu rizik (posouzení míry implementace řízení rizik z hlediska):
* hodnocení, evidence a kontroly účinnosti řízení aktiv a rizik,
* klasifikace, evidence, ochrany aktiv, manipulace s nimi, způsobu jejich používání atd.
* Definice rozsahu, tj. upřesnění procesních skupin (interesovaných subjektů), které mají být zkoumány:
* posouzení úrovně zajištění organizační bezpečnosti,
* posouzení kompetencí a povinností osob zastávajících bezpečnostní role:
  1. vlastníků/garantů aktiv (primárních),
  2. technických garantů aktiv (podpůrných),
  3. členů fóra/výboru kro kybernetickou a informační bezpečnost,
* posouzení kompetencí a povinností administrátorů,
* posouzení kompetencí a povinností zaměstnanců,
* posouzení kompetencí a povinností dodavatelů,
* identifikace procesních skupin,
* posouzení provázanosti výše uvedených subjektů v rámci procesních skupin.
* Určení odpovědných osob pro konzultace:
* osob zastávajících bezpečnostní role (vlastníků/garantů aktiv),
* administrátorů,
* uživatelů (klíčových referentů),
* dodavatelů (zajišťujících podporu a provoz aktiv).
* Auditování bezpečnostních procesů z pohledu vyspělosti:
* existence procesu,
* existence procesního vlastníka,
* existence závazného standardu,
* dodržování standardu, bezpečnostní povědomí zaměstnanců,
* ověření v praxi pomocí auditních technik,
* ověření existence kontrolních mechanismů.

Rozdílová analýza bude provedena v souladu s normou ČSN ISO/IEC 27001. Na základě zjištění z rozdílové analýzy bude stanovena vyspělost jednotlivých oblastí a identifikuje se soubor nedostatků vůči požadovaným ISMS standardům.

**Výstupy etapy:**

* **Rozdílová analýza** 
  + Audit managementu rizik (řízení rizik a aktiv).
  + Matice procesních skupin a odpovědných osob.
  + Audit bezpečnostních procesů.
  + Souhrn naplněných a chybějících standardů ISMS.

1. **Stanovení rozsahu systému (předmět řešení bezpečnosti informací – ISMS)**

Definice rozsahu ISMS určuje, co bude předmětem řešení bezpečnosti informací (v úvahu se berou specifické rysy činností organizace, její struktura, umístění, aktiva a technologie apod.).

Jedná se o tzv. SCOPE (Co bude v rámci předmětu řešení bezpečnosti informací sledováno, de facto „jaké informace“ mají být chráněny a v „jakých systémech jsou obsaženy“).

Pro stanovení rozsahu ISMS je z hlediska „předmětu řešení ISMS“ nezbytné posouzení níže uvedených oblastí ISMS v návaznosti na kapitoly a s nimi souvisejí opatření dle ČSN ISO IEC 27001, a na jednotlivé § organizačních a technických opatření dle Vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti:

* systém řízení bezpečnosti informací,
* řízení rizik (aktiv),
* řízení organizační bezpečnosti (bezpečnostní role),
* bezpečnost lidských zdrojů,
* řízení přístupu,
* kryptografie,
* fyzická bezpečnost,
* řízení provozu a komunikací,
* akvizice vývoje a údržby systémů včetně dodavatelských vztahů,
* řešení kybernetických bezpečnostních událostí a incidentů,
* řízení kontinuity činností,
* řešení auditů a kontrol.

I přes obecné konstatování, že je potřeba chránit všechny informace, v praxi existuje řada omezení, která zaměří projekt na vybrané oblasti. Omezeními mohou být například investiční omezení, akutní potřeba řešit nejpalčivější problémy apod.

Pro stanovení priorit a omezení je potřeba definovat:

* Prioritní oblasti ISMS
* Omezující faktory z hlediska disponibilních prostředků:
  + finančních,
  + lidských zdrojů,
  + časových,
  + znalostních (odbornostních).

**Výstupy etapy:**

* **Předmět řešení ISMS (souhrn informačních systémů ISMS)**
* Seznam vybraných provozních systémů ISMS.
* Seznam vybraných agendových systémů ISMS.
* Poskytované služby v rámci vybraných systémů ISMS.
* Evidované a zpracovávané informace (+osobní údaje) u vybraných systémů ISMS.
* **Stanovení rozsahu systému** (v kontextu)
* Bezpečnosti informací.
* Organizace bezpečnosti informací.
* Bezpečnosti lidských zdrojů.
* Řízení aktiv.
* Řízení přístupu.
* Kryptografie.
* Fyzické bezpečnosti a bezpečnosti prostředí.
* Bezpečnosti provozu.
* Bezpečnosti komunikací.
* Akvizice, vývoje a údržby systémů.
* Vztahů s dodavateli.
* Řízení incidentů bezpečnosti informací.
* Aspektů řízení kontinuity činností organizace z hlediska bezpečnosti informací.
* Souladu s požadavky (předpisy, politiky, postupy, směrnice).
* **Procesní schéma rozsahu ISMS**
* Prováděné činnosti
* Role zúčastněných všech zúčastněných subjektů:
  + osob zastávajících bezpečnostní role,
  + fóra, výboru kybernetické bezpečnosti,
  + administrátorů,
  + zaměstnanců,
  + institucí (NÚKIB, ÚOOÚ, CERT).
* **Stanovení priorit a omezení**
* Seznam prioritní oblasti ISMS
* Seznam omezujících faktorů, „omezení“ pro implementaci ISMS:
  + finanční,
  + personální,
  + časové,
  + znalostní,
  + legislativní.

1. **Definice Politiky ISMS, cílů a odpovědností**

Politika ISMS je vrcholným dokumentem. Deklaruje vůli a chuť managementu úřadu se bezpečností informací zabývat, a také cíle, kterých chce organizace v této oblasti dosáhnout. Při vytváření Politiky ISMS je proto nezbytná úzká součinnost s managementem, tento dokument musí být jednomyslně přijat vrcholným vedením a následně se stát obecně závazným napříč celou organizací.

**Seznam požadovaných bezpečnostních politik:**

1.1. Politika systému řízení bezpečnosti informací

1. Cíle, principy a potřeby řízení bezpečnosti informací.
2. Rozsah a hranice systému řízení bezpečnosti informací.
3. Pravidla a postupy pro řízení dokumentace.
4. Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací.
5. Pravidla a postupy pro provádění auditů kybernetické bezpečnosti.
6. Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací.
7. Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací.

1.2. Politika řízení aktiv

1. Identifikace, hodnocení a evidence primárních aktiv.
2. Identifikace, hodnocení a evidence podpůrných aktiv.
3. Pravidla ochrany jednotlivých úrovní aktiv.
4. Způsoby spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií.

1.3. Politika organizační bezpečnosti

1. Určení bezpečnostních rolí a jejich práv a povinností.
2. Požadavky na oddělení výkonu činností jednotlivých bezpečnostních rolí.
3. Požadavky na oddělení výkonu bezpečnostních a provozních rolí.

1.4. Politika řízení dodavatelů

1. Pravidla a principy pro výběr dodavatelů.
2. Pravidla pro hodnocení rizik souvisejících s dodavateli.
3. Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti.
4. Pravidla pro provádění kontroly zavedení bezpečnostních opatření.
5. Pravidla pro hodnocení dodavatelů.

1.5. Politika bezpečnosti lidských zdrojů

1. Pravidla rozvoje bezpečnostního povědomí a způsoby jeho hodnocení.
2. Bezpečnostní školení nových zaměstnanců.
3. Pravidla pro řešení případů porušení bezpečnostní politiky systému řízení bezpečnosti informací.
4. Pravidla pro ukončení pracovního vztahu nebo změnu pracovní pozice.

1.6 Politika řízení provozu a komunikací

1. Pravomoci a odpovědnosti spojené s bezpečným provozem.
2. Postupy bezpečného provozu.
3. Požadavky a standardy bezpečného provozu.
4. Pravidla a omezení pro provádění auditů kybernetické bezpečnosti a bezpečnostních testů.

1.7. Politika řízení přístupu

1. Princip minimálních oprávnění/potřeba znát (need to know).
2. Požadavky na řízení přístupu.
3. Životní cyklus řízení přístupu.
4. Řízení privilegovaných oprávnění.
5. Řízení přístupu pro mimořádné situace.
6. Pravidelné přezkoumání přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách.

1.8. Politika bezpečného chování uživatelů

1. Pravidla pro bezpečné nakládání s aktivy.
2. Bezpečné použití přístupového hesla.
3. Bezpečné použití elektronické pošty a přístupu na internet.
4. Bezpečný vzdálený přístup.
5. Bezpečné chování na sociálních sítích.
6. Bezpečnost ve vztahu k mobilním zařízením.

1.9. Politika zálohování a obnovy a dlouhodobého ukládání

1. Požadavky na zálohování a obnovu.
2. Pravidla a postupy zálohování.
3. Pravidla a postupy dlouhodobého ukládání.
4. Pravidla bezpečného zálohování a dlouhodobého ukládání informací.
5. Pravidla a postupy obnovy.
6. Pravidla a postupy testování zálohování a obnovy.
7. Politika přístupu k zálohám, ukládaným informacím.

1.10. Politika bezpečného předávání a výměny informací

1. Pravidla a postupy pro ochranu předávaných informací.
2. Způsoby ochrany elektronické výměny informací.
3. Pravidla pro využívání kryptografické ochrany.

1.11. Politika řízení technických zranitelností

1. Pravidla pro omezení instalace programového vybavení.
2. Pravidla a postupy vyhledávání opravných programových balíčků.
3. Pravidla a postupy testování oprav programového vybavení.
4. Pravidla a postupy nasazení oprav programového vybavení.

1.12. Politika bezpečného používání mobilních zařízení

1. Pravidla a postupy pro bezpečné používání mobilních zařízení.
2. Pravidla a postupy pro zajištění bezpečnosti zařízení, která povinná osoba nemá ve své správě.

1.13. Politika akvizice, vývoje a údržby

1. Bezpečnostní požadavky pro akvizici, vývoj a údržbu.
2. Řízení zranitelností.
3. Politika poskytování a nabývání licencí programového vybavení a informací

1.14. Politika ochrany osobních údajů

1. Charakteristika zpracovávaných osobních údajů.
2. Popis přijatých a provedených organizačních opatření pro ochranu osobních údajů.
3. Popis přijatých a provedených technických opatření pro ochranu osobních údajů.

1.15. Politika fyzické bezpečnosti

1. Pravidla pro ochranu objektů.
2. Pravidla pro kontrolu vstupu osob.
3. Pravidla pro ochranu zařízení.
4. Detekce narušení fyzické bezpečnosti.

1.16. Politika bezpečnosti komunikační sítě

1. Pravidla a postupy pro zajištění bezpečnosti sítě.
2. Určení práv a povinností za bezpečný provoz sítě.
3. Pravidla a postupy pro řízení přístupů v rámci sítě.
4. Pravidla a postupy pro ochranu vzdáleného přístupu k síti.
5. Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů.

1.17. Politika ochrany před škodlivým kódem

1. Pravidla a postupy pro ochranu síťové komunikace.
2. Pravidla a postupy pro ochranu serverů a sdílených datových úložišť.
3. Pravidla a postupy pro ochranu pracovních stanic.

1.18. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí

1. Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí.
2. Provozní postupy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události.
3. Pravidla a postupy pro optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí.

1.19. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

1. Pravidla a postupy pro evidenci a vyhodnocení kybernetických bezpečnostních událostí.
2. Pravidla a postupy pravidelné aktualizace pravidel pro vyhodnocení kybernetických bezpečnostních událostí.
3. Pravidla a postupy pro optimální nastavení bezpečnostních vlastností nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí.

1.20. Politika bezpečného používání kryptografické ochrany

1. Úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu.
2. Pravidla kryptografické ochrany informací
3. Systém správy klíčů.

1.21. Politika řízení změn

1. Způsob a principy řízení významných změn v rámci povinné osoby, jejich procesech, informačních a komunikačních systémech.
2. Přezkoumávání dopadů významných změn.
3. Způsob vedení evidence a testování významných změn.

1.22. Politika zvládání kybernetických bezpečnostních incidentů

1. Definování kategorií kybernetického bezpečnostního incidentu.
2. Pravidla a postupy pro identifikaci, evidenci a zvládání jednotlivých kategorií kybernetických bezpečnostních incidentů.
3. Pravidla a postupy testování systému zvládání kybernetických bezpečnostních incidentů.
4. Pravidla a postupy pro vyhodnocení kybernetických bezpečnostních incidentů a pro zlepšování kybernetické bezpečnosti.
5. Evidence incidentů.

1.23. Politika řízení kontinuity činností

1. Práva a povinnosti zúčastněných osob.
2. Cíle řízení kontinuity činností
3. Politika řízení kontinuity činností pro naplnění cílů kontinuity.
4. Způsoby hodnocení dopadů kybernetických bezpečnostních incidentů na kontinuitu a posuzování souvisejících rizik.
5. Určení a obsah potřebných plánů kontinuity a havarijních plánů.
6. Postupy pro realizaci opatření vydaných Úřadem.

Nezbytnou součástí této fáze je také definování osoby/osob s primární zodpovědností za bezpečnost informací v rozsahu:

* osob zastávajících bezpečnostní role
* výboru kybernetické bezpečnosti
* administrátorů
* zaměstnanců

**Výstupy etapy:**

* **Zpracována bezpečnostní politika**

1. Politika systému řízení bezpečnosti informací
2. Politika řízení aktiv
3. Politika organizační bezpečnosti
4. Politika řízení dodavatelů
5. Politika bezpečnosti lidských zdrojů
6. Politika řízení provozu a komunikací
7. Politika řízení přístupu
8. Politika bezpečného chování uživatelů
9. Politika zálohování a obnovy a dlouhodobého ukládání
10. Politika bezpečného předávání a výměny informací
11. Politika řízení technických zranitelností
12. Politika bezpečného používání mobilních zařízení
13. Politika akvizice, vývoje a údržby
14. Politika ochrany osobních údajů
15. Politika fyzické bezpečnosti
16. Politika bezpečnosti komunikační sítě
17. Politika ochrany před škodlivým kódem
18. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí
19. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí
20. Politika bezpečného používání kryptografické ochrany
21. Politika řízení změn
22. Politika zvládání kybernetických bezpečnostních incidentů
23. Politika řízení kontinuity činností

* **Cíle ISMS**

Naplnění cílů ISMS, jejich specifikace a provázanost na bezpečnostní politiky z hlediska:

* zajištění bezpečnosti informačních a komunikačních systémů a služeb,
* zajištění kontinuity provozu informačních a komunikačních systémů a služeb,
* ochrany dat a informací, a dalších aktiv,
* řešení hrozeb, událostí a incidentů včetně prevence,
* zvyšování bezpečnosti informačních a komunikačních systémů a služeb,
* zvyšování obecného podvědomí uživatelů o bezpečnosti a bezpečnostních hrozbách (edukace),
* sdílení zkušeností s dalšími subjekty.
* **Jmenovací listina osoby/osob s primární zodpovědností za bezpečnost informací**
* osoby zastávající bezpečnostní role
* osoby v rámci fóra/výboru kybernetické bezpečnosti
* osoby / administrátoři

1. **Analýza rizik**

Analýza rizik je klíčovou aktivitou při budování bezpečnosti informací. Cílem je odpovědět na následující otázky:

* Jakými způsoby může být v naší organizaci porušena bezpečnost informací?
* Jaká je pravděpodobnost, že se to stane?
* Jaké budou dopady na organizaci (případně její okolí, nebudou-li informace chráněny?

V rámci analýzy rizik dojde k zaměření na hrubou analýzu procesů požadovaných normou ISO 27001 v součinnosti především s vlastníky procesů, resp. vedoucími pracovníky úřadu. Samotný proces analýzy rizik zahrnuje identifikaci a hodnocení aktiv a identifikaci a stanovení pravděpodobností hrozeb a identifikaci a stanovení síly zranitelností.

**a) Definice metodiky analýzy rizik**

Před vlastní analýzou rizik je nutné stanovit a vedením úřadu schválit metodiku pro provádění

analýzy rizik. Tato metodika musí primárně vycházet z požadavků normy ISO 27001.

V rámci této metodiky bude stanoveno, jakým způsobem budou hodnocena aktiva a stanoveny

míry rizika. Zároveň bude stanovena míra akceptace rizika, tedy od jaké hodnoty rizikovosti se

bude jednat o akceptovatelné riziko bez následných opatření a od jaké hodnoty jsou nezbytná

následná opatření směřující ke snížení rizika.

Stanovení přesné metodiky pro provádění analýzy rizik je předpokladem k tomu, aby analýza

rizik byla v budoucnu opakovatelná. To umožní sledovat vývoj rizik v čase dle jednotné a stejné

metodiky.

**b) Identifikace a hodnocení aktiv**

Hlavní pozornost bude věnována identifikaci a hodnocení jednotlivých aktiv (primárních a podpůrných). Hodnocení bude provedeno cestou interview s respondenty – odpovědnými představiteli uživatelů informačního systému (vedoucími pracovníky) formou ocenění následků ztráty dostupnosti, důvěrnosti a integrity podle předem připravených scénářů „Co se stane, když...“.

**c) Hodnocení hrozeb a zranitelnosti**

Hodnocení hrozeb a zranitelnosti je rovněž formální proces spočívající v zodpovězení sady předem připravených otázek vycházejících z požadavků norem ISO 27001 a ISO 27005.

**d) Hodnocení rizik a vytvoření souboru opatření**

Míra rizika bude stanovena pro jednotlivé prvky modelu aktiv (primární aktiva ve smyslu informací a služeb, podpůrná technická aktiva) jako součin hodnoty aktiv, pravděpodobnosti hrozeb a síly zranitelnosti. Vypočítaná míra rizika je vyjádřena v relativní stupnici. Zároveň je vygenerován soubor (organizačních a technických) bezpečnostních opatření. Jednotlivá bezpečnostní opatření jsou charakterizována bezpečnostní úrovní (ve stejné relativní stupnici jako míra rizika) a dalšími údaji, které umožní stanovit, na základě provedené analýzy rizik, prioritu (naléhavost) jejich realizace. Zjištěná rizika budou srozumitelně popsána, včetně jejich souvislostí s určitými aktivy, hrozbami a zranitelností.

**e) Návrhy a doporučení – aplikace analýzy**

V závěrečné fázi budou vytvořeny návrhy na bezpečnostní opatření, případně rozhodnutí o akceptaci rizika, jejichž potřeba vyplyne z analýzy rizik. V rámci této fáze projektu budou navržena opatření organizačního charakteru, která nebudou představovat investice, případně jiné finanční náklady a technická opatření, která mohou být předmětem „zadání“ projektů financovaných z Integrovaného regionálního operačního programu (IROP) v programovém období 2021–2027. Budou doporučeny priority a předložen návrh na další postup s ohledem na standardní etapy procesu řízení rizik a přijetí nezbytných manažerských rozhodnutí. Návrhy budou v dokumentu „Plán zvládání rizik“ a podle potřeby doplněny v přílohách.

**Výstupy etapy:**

* **Metodika pro provádění analýzy rizik**
* Metodika identifikace, klasifikace a hodnocení aktiv
  + Určení stupnice pro hodnocení primárních aktiv
    - určení stupnice pro hodnocení úrovní důvěrnosti aktiv,
    - určení stupnice pro hodnocení úrovní integrity aktiv,
    - určení stupnice pro hodnocení úrovní dostupnosti aktiv.
* Metodika identifikace a hodnocení rizik
  + Určení stupnice pro hodnocení rizik
    - určení stupnice pro hodnocení úrovní dopadu,
    - určení stupnice pro hodnocení úrovní hrozby,
    - určení stupnice pro hodnocení úrovní zranitelnosti,
    - určení stupnice pro hodnocení úrovní rizik.
* Metody a přístupy pro zvládání rizik
* Způsoby schvalování akceptovatelných rizik
* Proces hodnocení aktiv a rizik
* **Závěrečná zpráva z provedené analýzy rizik**
* Vyhodnocení opatření z předchozího přezkoumání systému řízení bezpečnosti informací (ISMS).
* Identifikace změn a okolností, které mohou mít vliv na ISMS.
* Zpětná vazba o výkonnosti řízení bezpečnosti informací
  + neshody a nápravná opatření,
  + výsledky monitorování a měření,
  + výsledky auditu,
  + naplnění cílů systému řízení bezpečnosti informací.
* Výsledky hodnocení rizik a stav plánu zvládání rizik.
* Identifikace možností pro neustálé zlepšování.
* Doporučení potřebných rozhodnutí, stanovení opatření a osob zajišťujících výkon jednotlivých činností.
* **Plán zvládání rizik**
* Seznam identifikovaných rizik.
* Zvládání rizik a návrh aplikovatelných opatření.
* Plán realizace navržených opatření.

1. **Bezpečnostní standardy (bezpečnostní dokumentace)**

Bezpečnostní standardy (bezpečnostní dokumentace) navazují na bezpečnostní politiku (co, jak, proč a pro koho chránit atd.) a provedenou analýzu rizik.

Zahrnují kontrolní mechanismy jak technické, tak procedurální povahy. Jsou obvykle (v závislosti na zvoleném přístupu) zaměřeny na:

* Směrnice a postupy pro uživatele
* Směrnice a postupy pro správce IT/IS
* Postupy pro zachování kontinuity
* Postupy a směrnice pro monitorování systémů

**a) Směrnice a postupy pro uživatele IS a správce IS**

Formalizované dokumenty zahrnující postupy pro práci uživatelů a správců (administrátorů) tak, aby bylo dosaženo v bezpečnostní politice definovaných cílů. Je známo, že lidský faktor představuje potenciálně největší hrozbu pro bezpečnost informací. Lidé tedy nikdy nemohou být ve funkčním systému opomenuti.

Součástí zavádění standardů (dokumentace) v této oblasti nezbytně musí být provedeno seznámení dotčených subjektů (uživatelů a správců) s jednotlivými výstupy dokumentace (navazujících politik).

Standardy pro uživatele obvykle obsahují zásady pro používání a změny hesel, ochranu přenosných médií a počítačů, pravidla pro vynášení informací mimo úřad, pravidla pro přístup k informačním systémům z prostředí veřejného internetu, povinnosti související se zjištěním bezpečnostních incidentů apod.

Směrnice a postupy pro uživatele navazují na konkrétní bezpečnostní politiky (stanovující povinnosti a pravidla zejména v oblasti bezpečného chování uživatelů, používání kryptografické ochrany a mobilních zařízení, zvládání kybernetických bezpečnostních incidentů atd.)

Směrnice a postupy pro správce IS (administrátory) navazují na konkrétní bezpečnostní politiky (definující povinnosti a pravidla zejména v oblasti zajištění bezpečnosti z hlediska řízení provozu a komunikací, řízení přístupu, zálohování a obnovy, akvizice a vývoje IS, komunikační sítě, fyzické bezpečnosti, ochrany před škodlivým kódem, zvládání kybernetických bezpečnostních incidentů atd.)

**b) Směrnice pro plánování kontinuity**

Tato směrnice bude obsahovat závazná pravidla pro to, jakým způsobem předcházet vzniku

nepříznivých situací, které by mohly ovlivnit chod organizace a bude definovat pravidla pro tvorbu havarijních plánů na základě provedené detailní analýzy rizik a analýzy dopadů.

**c) Monitorování systémů**

Postupy a směrnice pro monitorování systémů definují, které informace, ukazatele, výstrahy

systémů apod. je potřeba monitorovat, jak často a jakým způsobem. Úkolem je podchytit indikace možných výpadků, nelegální činnosti v informačním systému atd. a umožnit tak rychlé řešení potenciální hrozby.

**Výstupy etapy:**

* **Struktura dokumentace**
* návrh jednotné struktury dokumentace, řízení dokumentace.
* **Směrnice a postupy pro uživatele IS**
* změny hesel,
* ochrana přenosných médií a počítačů,
* pravidla pro vynášení informací mimo úřad,
* pravidla pro přístup k informačním systémům z prostředí veřejného internetu,
* povinnosti související se zjištěním bezpečnostních incidentů atd.
* **Směrnice a postupy pro správce IS**
* řízení provozu a komunikací,
* řízení přístupu,
* pravidla pro zálohování a obnovu,
* povinnosti v rámci akvizice a vývoje IS,
* pravidla pro zajištění bezpečnosti komunikační sítě,
* povinnosti v rámci fyzické bezpečnosti,
* pravidla pro ochranu před škodlivým kódem,
* povinnosti související se zvládáním kybernetických bezpečnostních incidentů atd.
* **Směrnice pro plánování kontinuity**
* Plán kontinuity činností
  + cíle řízení kontinuity činností,
  + role zaměstnanců v procesu řízení kontinuity činností,
  + podíl dodavatelů v procesu řízení kontinuity činností,
  + plány řízení kontinuity činností,
  + implementace řízení kontinuity činností.
* Plán zálohy
  + vazba na bezpečnostní politiku
  + popis činností a postupů v procesu zálohování,
  + popis kontrolních mechanismů v procesu zálohování,
  + podíl zaměstnanců na procesu zálohování,
  + podíl správců na procesu zálohování,
  + podíl dodavatelů na procesu zálohování,
  + popis použití zálohy při obnově.
* Plán obnov
  + vazba na bezpečnostní politiku
  + popis činností a postupů v procesu obnovy,
  + popis kontrolních mechanismů v procesu obnovy,
  + podíl zaměstnanců na procesu obnovy,
  + podíl správců na procesu obnovy,
  + podíl dodavatelů na procesu obnovy.
* **Monitorování systémů**
* Směrnice pro řešení bezpečnostních událostí
  + navazující bezpečnostní politiky, metodiky,
  + definování pravidel a postupů pro:
    - detekci, evidenci bezpečnostních událostí,
    - zpracování záznamů vzniklých bezpečnostních událostí.
  + popis procesů řízení událostí v průběhu fází (sběru, ukládání, archivace, analýzy, posouzení dopadů na aktiva, aplikace vhodného bezpečnostního opatření, vyhodnocení a posouzení, zda jde o bezpečnostní incident)
* Směrnice pro zvládání bezpečnostních incidentů
  + navazující bezpečnostní politiky, metodiky
  + definování pravidel a postupů,
  + přijmutí opatření pro jejich odvrácení a zmírnění dopadu,
  + šetření a odstranění příčiny vzniku a následků,
  + hlášení NBÚ a zaznamenávání celého průběhu zvládání.
* **Prohlášení o aplikovatelnosti**
* Přehled vyloučených bezpečnostních opatření požadovaných touto vyhláškou včetně zdůvodnění, proč nebyla aplikována.
* Přehled zavedených bezpečnostních opatření včetně způsobu jejich implementace.

1. **Doporučení k aktualizaci a údržbě bezpečnostní dokumentace a politik**

Stanovení pravidel a definice nástrojů k ověřování trvalé kvality zavedeného systému managementu bezpečnosti informací za účelem trvalého a prokazatelného zajištění bezpečnosti informací.

**Výstupy etapy:**

* Předávací protokol o převzetí dokumentu s doporučeními, podepsaný Zadavatelem a Dodavatelem

1. **Implementace ISMS**

* Implementace jednotlivých opatření: V rámci této etapy budou do praxe zavedena organizační opatření definovaná v bezpečnostní dokumentaci, zejména v oblasti:
* klasifikování a označování zpracovávaných informací
* umístění (ukládání) důvěrných informací na bezpečné úložiště
* změny nastavení bezpečnostní politiky IT apod.
* Rozvoj bezpečnostního povědomí uživatelů, administrátorů a osob zastávajících bezpečnostní role v oblasti požadavků systému managementu bezpečnosti informací (ISMS) zahrnující:
* poučení pracovníků úřadu o bezpečnostní politice
* poučení pracovníků úřadu o jejich povinnostech
* poučení osob zastávajících bezpečnostní role o jejich odpovědnostech
* školení ochrany informací pro vedoucí pracovníky
* školení ochrany informací v rozsahu realizovaného projektu pro pracovníky

**Výstupy etapy:**

* Záznamy dokladující provedenou implementaci (vycházejí ze zavedené a schválené ISMS dokumentace/bezpečnostních standardů).
* Seznam proškolených uživatelů
* Seznam proškolených administrátorů
* Seznam proškolených osob zastávajících bezpečnostní role

1. **Ověření připravenosti k certifikačnímu auditu**

Prověření splnění povinností nutných k zahájení certifikačního auditu (formou výstupního auditu), v případě potřeby provedení nezbytných úprav v rozsahu výše uvedených plnění či jiných doporučení k dokončení připravenosti a poté vydání potvrzení o připravenosti k provedení certifikačního auditu.

**Výstupy etapy:**

* Potvrzení o připravenosti k provedení certifikačního auditu

1. **Součinnost při procesu certifikace až do splnění účelu předmětu veřejné zakázky – získání certifikátu dle normy ČSN ISO/IEC 27001**

Poskytnutí součinnosti nezbytné pro získání certifikátu dle připomínek a požadavků certifikující organizace, zahrnující zejména aktualizace dokumentů zpracovaných v rámci předmětu plnění, případně dopracování další požadované dokumentace, pomoc se zavedením stanoveného opatření, včetně provedení případných konzultací se zadavatelem.

**Výstupy etapy:**

* Předávací protokol obsahující seznam zapracovaných připomínek a požadavků certifikující organizace při aktualizaci dokumentů zpracovaných v rámci předmětu plnění, při dopracování potřebné dokumentace či zavedení opatření.

**Dílčí plnění 2:**

1. **Zajištění certifikačního auditu implementovaného systému managementu bezpečnosti informací**

Dodavatel v rámci předmětu plnění této dílčí části veřejné zakázky zajistí provedení certifikačního auditu implementovaného systému managementu bezpečnosti informací zadavatele od **nezávislého** **auditora** (který se nepodílel na dílčím plnění 1 - Zavedení systému ISO/ IEC 27001 - ISMS). Certifikačním auditem se pro účely této dílčí části veřejné zakázky rozumí všechny kroky certifikačního auditu, které je nezbytné absolvovat k získání platného certifikátu systému managementu bezpečnosti informací dle požadavků normy ČSN ISO/IEC 27001. Certifikát musí být vystaven certifikačním orgánem – procesním, akreditovaným národním akreditačním orgánem (pro Českou republiku ČIA) pro tuto oblast ověřování. Zadavatel stanovuje, že pro účely této zakázky vymezuje a požaduje provedení certifikace v lokalitě sídla Zadavatele.

**Výstupy etapy:**

* Doklad o zahájení certifikačního auditu osobou oprávněnou vystavit certifikát dle požadavků normy ČSN ISO/IEC 27001

1. **Certifikace dle normy ČSN ISO/IEC 27001**

Vystavení certifikátu shody s normou ČSN ISO/IEC 27001 certifikačním orgánem.

**Výstupy etapy:**

* Certifikát ČSN ISO/IEC 27001

**B. Harmonogram projektu**

**Dílčí plnění 1:**

|  |  |  |
| --- | --- | --- |
| **Fáze** | **Etapa** | **Termín**  **(T = termín uzavření smlouvy)** |
| Analytická část | 1. Rozdílová analýza | T + 10 kalendářních dní |
| Analytická část | 1. Stanovení rozsahu systému | T + 15 kalendářních dní |
| Analytická část | 1. Definice Politiky ISMS, cílů a odpovědností | T + 30 kalendářních dní |
| Analytická část | 1. Analýza rizik | T + 50 kalendářních dní |
| Návrhová část | 1. Bezpečnostní standardy, bezpečnostní dokumentace | T + 80 kalendářních dní |
| Návrhová část | 1. Doporučení k aktualizaci a údržbě bezpečnostních politik a dokumentace | T + 80 kalendářních dní |
| Realizační část | 1. Implementace ISMS | T + 110 kalendářních dní |
| Realizační část | 1. Ověření připravenosti k certifikačnímu auditu | T + 120 kalendářních dní |
| Realizační část | 1. Součinnost při certifikačním procesu | T + 150 kalendářních dní |

**Dílčí plnění 2:**

|  |  |  |
| --- | --- | --- |
| **Fáze** | **Etapa** | **Termín**  **(T = termín uzavření smlouvy)** |
| Realizační část | 1. Zajištění certifikačního auditu | T + 120 kalendářních dní |
| Realizační část | 1. Certifikace dle normy ČSN ISO/IEC 27000 | T + 150 kalendářních dní |