Příloha č. 1. Požadavky na zavedení ISMS v organizaci Moravskoslezské datové centrum, příspěvková organizace

Cíl projektu:

Cílem projektu je zavedení systému řízení bezpečnosti informací (ISMS - Information Security Management System), dále jen „ISMS", v souladu s normou ČSN ISO/IEC 27001:2014, a nastavení řízení procesů spojených se zachováním dostupnosti, integrity a důvěrnosti informací v organizaci Moravskoslezské datové centrum, příspěvková organizace (dále jen „MSDC").

Popis zadání jednotlivých etap projektu:

1) **Harmonogram realizace**

Harmonogram bude obsahovat popis dílčích aktivit nezbytných pro realizaci díla (viz body 2 až 7 „Zavedení systému ISMS v organizaci Moravskoslezské datové centrum, příspěvková organizace") s upřesněním času plnění. **Úvodní přezkoumání připravenosti MSDC na zavedení systému ISMS a stanovení jeho rozsahu**

Cílem úvodního přezkoumání je zjistit míru připravenosti MSDC na zavedení systému ISMS. Z úvodního přezkoumání bude vypracována zpráva popisující mimo jiné stav bezpečnosti informací v MSDC a návrh na realizaci doporučení (opatření) vedoucích k dosažení shody s požadavky normy ČSN ISO/IEC 27001:2014 a zákona č. 181/2014 Sb., zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „zákon o kybernetické bezpečnosti" nebo „ZoKB"). Dalším výstupem úvodního přezkoumání bude formalizovaný dokument obsahující definovaný rozsah zaváděného systému ISMS včetně zvolené strategie a cílů.

Součástí úvodního přezkoumání bude:

- Zpracování rozdílové analýzy připravenosti MSDC na požadavky zákona o kybernetické bezpečnosti.
- Zhodnocení stávající situace v oblasti správy informačních rizik, řízení rizik a ICT bezpečnosti.
- Identifikace průnikových parametrů a procesů mezi již zavedenou normou ČSN EN ISO 9001, ČSN EN ISO14001, zákonem o kybernetické bezpečnosti a návrhu procesů v souladu s normou ČSN ISO/IEC 27001:2014.
- Zapracování stanovení návrhu rozsahu a hranice ISMS, definování kontextu včetně externího a interního aspektu ISMS (dle kap. 4 ČSN ISO/IEC 27001) tak, aby bylo reálné ISMS implementovat v podmínkách MSDC. Kontext musí být v souladu s požadavky ISO 27001 a také s požadavky kybernetického zákona.
- Přezkoumání bezpečnostních politik, kontrola nastavení stávající metodiky pro vyhledávání a hodnocení rizik, sledování konzistence odpovědností a pravomocí v oblasti informační bezpečnosti.
- Přezkoumání evidence informačních aktiv včetně podpůrných aktiv dle zákona o kybernetické bezpečnosti a jejich vlastníků (garantů) a jejich zdokumentování včetně určení významnosti aktiv.
- Přezkoumání existujících hrozeb pro informační aktiva a zranitelnosti, které by mohly být hrozbami využity, přezkoumání zmapování dopadů na aktiva z hlediska ztráty důvěrnosti, integrity a dostupnosti.
- Přezkoumání posouzení pravděpodobnosti selhání bezpečnosti včetně následků na ztrátu důvěrnosti, integrity a dostupnosti aktiv.

- Přezkoumání odhadu úrovně rizik a analýza, zdali jsou bezpečnostní rizika akceptovatelná nebo vyžadují opatření pro jejich minimalizaci.
- Přezkoumání stavu identifikace variant pro zvládání rizik.
- Přezkoumání rizikových scénářů a možných souvisejících hrozeb.
- Přezkoumání, zda rámce řízení informačních rizik odpovídají standardu ZoKB.
- Zpracování analýzy a doplnění cílů a opatření dle přílohy A normy ČSN ISO/IEC 27001:2014 včetně Prohlášení o aplikovatelnosti.
- Přezkoumání existence souhlasu vedení MSDC se zbytkovými riziky.
- Přezkoumání způsobu přidělování hesel a přihlašování do systému.
- Přezkoumání dokumentace a nastavení procesů u technické vybavenosti, technické shody a identifikace technických zranitelností v IT infrastruktuře MSDC, IT specialistů pro bezpečnost HW dle ZOKB.
- Zdokumentování postupu pro včasnou detekci pokusů o narušení bezpečnosti z oblasti IT včetně přezkoumání nastavení tohoto postupu.
- Přezkoumání dokumentovaného hodnocení rizik včetně zbytkových rizik s ohledem na případné změny kontextu organizace, identifikované hrozby a účinnost zavedených opatření.
- Přezkoumání způsobu zaznamenávání bezpečnostních incidentů a zpracovaného bezpečnostního plánu.
- Přezkoumání povinných dokumentovaných postupů dle ČSN ISO/IEC 27001:2014.

3) Informační seminář pro vedení MSDC, pro vedoucí zaměstnance a zaměstnance

Provedení informačního semináře v oblasti ISMS, který bude zaměřen svým obsahem a rozsahem pro vedení MSDC a zaměstnance. Semináře budou probíhat v objektu MSDC za pomoci vizualizace (např. VT, dataprojektor apod.). Součástí informačního semináře bude osvědčení o účasti.

V rámci tohoto bodu bude vypracována osnova semináře a harmonogram realizace semináře, včetně zpracování pozvánky pro jednotlivé účastníky. Součástí semináře budou také praktické příklady a řešení jednotlivých vzorových situací z řízení ISMS v MSDC.

Minimální obsah semináře:

- Přínosy implementace systémů řízení, včetně ISMS
- Právní a technická regulace bezpečnosti informací v oblastech:
    - systému řízení bezpečnosti informací (ISMS) ve smyslu ISO 27001:2014
    - Zákon 365/2000 Sb., o informačních systémech veřejné správy (dále jen „zákon o ISVS")
    - Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
    - Přehled bezpečnostních opatření ISMS

a) Informační seminář pro zaměstnance

- Předpokládaný rozsah semináře 2 hodiny: 1 hodina výklad, 1 hodina řízená diskuze k dotazům účastníků
- Vytvoření prezentace, která bude sloužit jako podklad pro informační seminář pro zaměstnance.

b) **Informační seminář pro vedoucí zaměstnance**
   - Rozsah semináře 2 hodiny: 1 hodina výklad, 1 hodina řízená diskuze k dotazům účastníků

2) Přezkoumání a doplnění dokumentace dle požadavku normy ČSN ISO/IEC 27001:2014

V rámci této etapy bude provedeno přezkoumání, zhodnocení stávající dokumentace MSDC s požadavky normy a zpracování relevantní dokumentace ISMS ve spolupráci s odpovědnými zaměstnanci MSDC. Součástí této etapy projektu je i zapracování případných připomínek ze strany MSDC do jednotlivých dokumentů a grafické zpracování a vydání dokumentace MSDC v elektronické a tištěné podobě (min. ve dvou vyhotoveních ve formátu *.pdf. a *.docx).

Požadovaný minimální rozsah:

- Zapracování příručky ISMS do stávající příručky řízení objednavatele
- Prohlášení o aplikovatelnosti a souvisejících dokumentů

A.5	Politiky informační bezpečnosti informací
A.6	Organizace bezpečnosti informací
A.7	Bezpečnost lidských zdrojů
A.8	Management aktiv
A.9	Opatření k přístupu a řízení přístupových práv
A.10	Technologie kryptování
A.11	Fyzická bezpečnost pracovišť a zařízení
A.12	Bezpečnost provozu
A.13	Bezpečná komunikace a přenos dat
A.14	Bezpečná akvizice, vývoj a podpora informačních systémů
A.15	Bezpečnost pro dodavatele a třetí strany
A.16	Management incidentů
A.17	Kontinuita podnikání s ohledem na informační bezpečnost
A.18	Shoda s interními i externími požadavky

- Politika a cíle ISMS
- Metodika pro řízení rizik a plány zvládání rizik
- Řízení informačních aktiv
- Plán kontinuity
- Řízení dokumentace a záznamů ISMS
- Řízení auditů ISMS
- Řízení nápravných opatření ISMS včetně zlepšování
- Řízení bezpečnostních incidentů
- Registr právních a jiných požadavků
- Zpracování bezpečnostních standardů a tvorby bezpečnostních dokumentů a směrnic, v rámci realizace směrnice budou vypracovány směrnice pro práci uživatelů s informačním systémem/informacemi a směrnice pro správu systému). Součástí tvorby bezpečnostních standardů je úprava potřebných dokumentů MSDC, a její integrace do celkové koncepce MSDC.
- Proces a směrnice ošetření přístupu třetích stran k informacím MSDC.

3) Implementace požadavků ISMS

V rámci této etapy bude realizována implementační část, kdy budou zpracovány potřebné záznamy dle požadavků ISMS a k implementaci jednotlivých opatření vyplývajících z předchozí analýzy, zajišťujících dosažení požadovaného stupně informační bezpečnosti.
Dále bude provedena případná úprava zpracovaného harmonogramu pro implementaci ISMS, a to dle zjištění z úvodního přezkoumání připravenosti MSDC na zavedení systému ISMS.
V rámci realizace projektu zadavatel požaduje minimálně 10 kontrolních dnů, na kterých bude prováděna kontrola postupu a metodické vedení implementace ISMS.

Implementační část zahrnuje:

- Zpracování evidence a monitorování informačních aktiv (primárních i podpůrných aktiv) včetně jejich vlastníků (garantů) a jejich zdokumentování a určení významnosti aktiv.
- Definování a vytvoření vazeb mezi aktivy včetně zapracování těchto vazeb do procesů systému řízení aktiv a řízení rizik ISMS.
- Provedení identifikace a zdokumentování existujících hrozeb pro informační aktiva a zranitelnosti, které by mohly být hrozbami využity, analýza zmapování dopadů na aktiva z hlediska ztráty důvěrnosti, integrity a dostupnosti. Posouzení pravděpodobnosti selhání bezpečnosti včetně následků na ztrátu důvěrnosti, integrity a dostupnosti aktiv. Odhad úrovně rizik a analýza, zdali jsou bezpečnostní rizika akceptovatelná nebo vyžadují opatření pro jejich minimalizaci.
- Nastavení a monitorování identifikace variant pro zvládání rizik jako je aplikace vhodných opatření, vědomé a objektivní akceptování rizik, vyhnutí se rizikům či přenesení rizik spojených s činností MSDC na třetí strany.
- Nastavení, zdokumentováni a sledování cílů a opatření dle přílohy A normy ČSN ISO/IEC 27001:2014. Definice cílů s přímou vazbou na informační aktiva a stanovení parametrů pro vyhodnocování cílů.
- Zpracování existence souhlasu vedení MSDC se zbytkovými riziky včetně zpracování Prohlášení o aplikovatelnosti.
- Návrh variant pro zvládání rizik, ve kterém vedení MSDC vymezí odpovídající činnost vedení MSDC, zdroje, odpovědnosti a priority pro ISMS.
- Nastavení postupů pro monitorování v:
  - Zavedených bezpečnostních opatřeních sloužících jako nástroje pro zvládání rizik, definování, jakým způsobem bude probíhat měření účinnosti vybraných opatření.
  - Zavedených programů školení a zvyšování informovanosti ve vztahu k ISMS.
  - Zavedení systému u přidělování hesel a přihlašování do systému ze vzdálených lokací.
  - Pravidla „prázdného stolu".
  - Nastavení měření účinnosti zavedených opatření.
  - Nastavení zaznamenávání bezpečnostních incidentů.
  - Nastavení pravidelného přezkoumávání účinnosti ISMS s ohledem na výsledky bezpečnostních auditů, incidentů, výsledků měření účinnosti opatření, návrhů a podnětů všech zainteresovaných stran.
  - Nastavení a zdokumentování postupu pro včasnou detekci pokusů o narušení bezpečnosti z oblasti IT.
- Analýza procesů zvládání informačních incidentů s popisem slabých míst.
- Proškolení vybraných zaměstnanců, kteří následně budou provádět školení zaměstnanců MSDC a zaměstnanců externích společností.

4) Provedení kontrolních auditů s vazbou na kontrolu realizace nápravných a preventivních opatření a konečná kontrola projektu

Provedení kontrolních auditů pro odstranění neshod a realizace případných nápravných doporučení ve spolupráci se zaměstnanci MSDC. Následně bude provedena konečná kontrola projektu a zpracována zpráva o stavu ISMS.

5) Účast na certifikačním procesu

Dodavatel se zúčastní auditu prvního a druhého stupně v rámci certifikačního procesu ISMS a poskytne odbornou pomoc při obhajobě zavedeného systému ISMS. V případě zjištěných nedostatků vypracuje dodavatel ve spolupráci s objednavatelem potřebné náležitosti vyplývající z uskutečněného certifikačního procesu, a to bezodkladně.

6) Dokumentace poskytnutá zadavatelem

- Bezpečnostní politika.
- Relevantní vnitřní předpisy a další akty interního řízení.
- Výstupy relevantních rizikových analýz a další nezbytné podklady, pokud má zadavatel zavedeny.

Veškeré aktivity vč. školení budou probíhat v českém jazyce, rovněž všechny výstupy (dokumenty apod.) budou v českém jazyce.