Příloha č.1
Specifikace Předmětu plnění

(1) Předmětem plnění je provedení auditu souladu systému řízení bezpečnosti informací u Objednatele s požadavky:

a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti (zákon o kybernetické bezpečnosti)
b) vyhlášky č. 82/2018 Sb.
c) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
d) dalších souvisejících právních norem.

(2) Auditovanou organizační složkou Objednatele bude odbor sociálních věcí a odbor kancelář hejtmana.

(3) Požadovaný rozsah auditu je pokrytí všech paragrafů vyhlášky č. 82/2018 Sb., ověřované v následujících blocích:

(4) Porozumění kontextu organizace,

(Zejména: Rozsah, hranice a popis systému řízení bezpečnosti informací (ISMS), Bezpečnostní politika a strategie, Bezpečnostní role v oblasti řízení, správy a kontroly ICT (organizační bezpečnost)

(5) Řízení aktiv a rizik,

(Zejména: Metodiky hodnocení aktiv a rizik, Zpráva o hodnocení aktiv a rizik, Proces řízení aktiv a rizik, Plán zvládání rizik – RTP, Prohlášení o aplikovatelnosti – SoA, Pravidelné přezkoumání)

(6) Řízení dodavatelů,

(Zejména: Řízení rizik s dodavateli, Pravidla pro dodavatele, Smlouvy, dodržování SLA)

(7) Technická bezpečnost vybraného významného informačního systému č.1,

(Zejména: Popis a architektura systému (HW, SW, OS, komponenty, jejich popis a umístění v síti a souvisejícími procesy v rámci celé organizace), Ukázka logického a fyzického schématu sítě (způsob propojení systémů), Bezpečnost komunikačních sítí, řízení síťového provozu a komunikací, Správa a ověřování identit, autentizační mechanismy, Ochrana před škodlivým kódem, Logování, Detekce kybernetických bezpečnostních událostí, Aplikační bezpečnost, Kryptografické prostředky, Zálohování)

(8) Technická bezpečnost vybraného významného informačního systému č.2,

(viz předchozí)

(9) Řízení provozu a změn,

(Zejména: Řízení provozu a komunikací, Řízení změn, Akvizice, vývoj a údržba)

(10) Řízení kontinuity činností,

(Zejména: Politika řízení kontinuity činností, Analýza dopadů (BIA), Plány kontinuity činností a havarijní plány)

(11) Fyzická bezpečnost,

(Zejména: serverovna, DC,)

(12) Bezpečnost lidských zdrojů, personální bezpečnost,

(Zejména: Zaměřeno na životní cyklus zaměstnance, jejich vzdělání a rozvoj, Plán rozvoje bezpečnostního povědomí zaměstnanců, Řízení identit)

(13) Proces zvládání kybernetických bezpečnostních incidentů,

(Zejména: Oznamování kybernetických bezpečnostních incidentů, Zvládání kybernetických bezpečnostních incidentů, Ukázka systému pro evidenci kybernetických bezpečnostních incidentů)

(14) Interní audit a penetrační testování.

(Zejména: Proces a pravidla interního auditu, Zprávy z auditu, Proces a pravidla penetračních testů, Výsledky penetračních testů, Rozsah a způsob provádění skenů zranitelností a pracování s výsledky)

(15) Zhotovitel je odpovědný za návrh osoby vedoucího auditora kybernetické bezpečnosti.

(16) Vedoucí auditor kybernetické bezpečnosti musí:

a) vybrat auditní tým a určit jednotlivé auditory, kteří se budou na auditu kybernetické bezpečnosti podílet,
b) připravit detailní plán auditu kybernetické bezpečnosti v požadované struktuře,
c) projednat plán auditu kybernetické bezpečnosti s auditovanými, a to nejméně dva týdny před plánovaným termínem auditu,
d) koordinovat všechny činnosti během auditu kybernetické bezpečnosti,
e) shromažďovat nálezy od jednotlivých auditorů kybernetické bezpečnosti a tyto nálezy kategorizovat v souladu s RŘ/102/REDI Bezpečnostní politika systému řízení bezpečnosti informací,
f) objasnit nálezy a výsledky auditu kybernetické bezpečnosti na závěrečném setkání s představiteli auditovaných,
g) připravit zprávu z auditu kybernetické bezpečnosti a předložit ji představitelům auditovaných,
h) předat schválenou zprávu z auditu kybernetické bezpečnosti představitelům auditovaných a manažerovi kybernetické bezpečnosti.