BEZPEČNOSTNÍ PRAVIDLA PRO VÝZNAMNÉ DODAVATELE UPLATŇOVANÁ V OBLASTNÍ NEMOCNICI NÁCHOD

Tato dokument popisuje bezpečnostní požadavky, projektu Zavedení nástroje pro správu logů zejména pro naplnění požadavků vyplývajících ze zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZoKB“), a 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 (dále jen „VoKB“), pro významný informační systém Oblastní nemocnice Náchod (dále jen „ONN“).

1. ŘÍZENÍ INFORMAČNÍ A KYBERNETICKÉ BEZPEČNOSTI

1.1. Dodavatel má povinnost ve svých interních procesech realizovat minimálně tato opatření:

1.1.1. má stanoven plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí v následující formě, obsahu a rozsahu:

a) poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice;

b) potřebná teoretická i praktická školení uživatelů, administrátorů a osob zastávajících bezpečnostní role;

1.1.2. má určeny osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny;

1.1.3. v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení se zaměřením na kybernetickou bezpečnost a její aktuální trendy;

1.1.4. pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje pravidelná odborná školení, přičemž vychází z aktuálních potřeb v oblasti kybernetické bezpečnosti a ve zdravotnictví;

1.1.5. v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje pravidelné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní;

1.1.6. zajišťuje kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;

1.1.7. v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajišťuje předání odpovědností;

1.1.8. vede o provedených školení přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

1.2. Využívá-li dodavatel při poskytování předmětu plnění subdodavatele, je povinen zajistit adekvátní dodržování těchto bezpečnostních pravidel rovněž ve smluvních vztazích se svými subdodavateli.

1.3. ONN si vyhrazuje právo vést záznamy a prověřovat činnosti dodavatele, vést záznamy o

1.4. incidentech a nestandardních činnostech zaměstnanců a dalších osob působících ve prospěch dodavatele (dále jen „zaměstnanci dodavatele“).

1.5. Na základě těchto záznamů má oprávnění vyhodnocovat důvěryhodnost a spolehlivost zaměstnanců dodavatele. V případě identifikovaného rizika oznámí ONN nesoulad dodavateli a obě strany vejdou v jednání pro řešení této situace.

2. PERSONÁLNÍ BEZPEČNOST

2.1. Dodavatel se zaváže zajistit dostatečnou míru zastupitelnosti pro veškeré aspekty řešení (zajištění kontinuity dodávky, zastupitelnost pracovníků, zejména Kontaktní osoba pro bezpečnost na straně dodavatele).

2.2. Osoby, účastnící se plnění zakázky musí mít prokazatelné potřebné kvalifikační předpoklady, zkušenosti a znalosti.

3. ŘÍZENÍ PŘÍSTUPU

Každý zaměstnanec dodavatele podílející se na plnění smlouvy výpočetními prostředky dodavatele, musí mít v rámci své ICT infrastruktury evidován a veden svůj vlastní jedinečný uživatelský účet, kterému jsou v jednotlivých systémech, modulech nebo aplikacích přiřazeny specifické role. Každý zaměstnanec dodavatele musí být veden s platnými identifikačními a aktuálními kontaktními údaji.

4. ŘÍZENÍ ZMĚN

4.1. Změny na straně dodavatele musí být řízeny s ohledem na kritičnost informací, systémů, procesů a opětovným posuzováním rizik.

4.2. Dodavatel se zavazuje:

a) řídit a evidovat smluvní změny;
b) řídit a evidovat změny v poskytovaných službách v souladu s požadavky VoKB a doporučeními technických norem řady ISO/IEC 27000

5 KYBERNETICKÉ BEZPEČNOSTNÍ UDÁLOSTI / INCIDENTY

Dodavatel má za povinnost hlásit veškerá podezření na kybernetické bezpečnostní události resp. incidenty manažerovi kybernetické bezpečnosti ONN v termínu bezprostředně (bez prodlení) po zjištění kybernetické bezpečnostní události / incidentu prostřednictvím emailu, telefonicky se zajištěním evidence hovoru na obou stranách, nebo osobně s popisem:

a) data a času zjištění;
b) povahy události;
c) zdroje události;
d) cíle / oběti události;
e) potencionálního dopadu