SMĚRNICE

Politika bezpečného chování dodavatelů IT technologií

Vypracoval: Manažer kybernetické bezpečnosti	**Schválil:** Technický ředitel
Ing. Jan Bareš	Ing. Jan Rais, MBA
Platnost dokumentu:	17.10.2024

1 Úvod

Tato politika stanovuje pravidla a pokyny pro bezpečné chování dodavatelů IT technologií, kteří poskytují služby nebo technologie do KNL. Cílem této politiky je zajistit ochranu citlivých informací, minimalizovat bezpečnostní rizika a zajistit, že všichni Dodavatelé dodržují bezpečnostní standardy.

2 Rozsah působnosti

Tato politika se vztahuje na všechny dodavatele IT technologií, kteří spolupracují s KNL, včetně jejich zaměstnanců, subdodavatelů a třetích stran.

3 Bezpečnostní požadavky

3.1 Ochrana informací

Důvěrnost: Dodavatelé musejí zajistit, že všechny informace, které získají při spolupráci s KNL, budou chráněny před neoprávněným přístupem, zneužitím nebo zveřejněním.

Integrita: Dodavatelé musejí zajistit, že všechny informace budou přesné a chráněny před neoprávněnou úpravou nebo zničením.

Dostupnost: Dodavatelé musejí zajistit, že informace budou dostupné oprávněným osobám v případě potřeby.

3.2 Řízení přístupu

Omezený přístup: Dodavatelé musejí zajistit, že přístup k systémům a informacím bude omezen pouze na oprávněné osoby.

Autentizace: Dodavatelé musejí používat silné autentizační mechanismy schválené KNL pro přístup k systémům a informacím.

Role a oprávnění: Dodavatelé musejí implementovat zásadu minimálních oprávnění, což znamená, že každý uživatel má pouze ta oprávnění, která jsou nezbytná pro výkon jeho pracovní činnosti.

4 Školení a povědomí

Školení: Dodavatelé musejí zajistit, že všichni jejich zaměstnanci jsou pravidelně školeni v oblasti kybernetické bezpečnosti a povědomí o bezpečnostních hrozbách.

Povědomí: Dodavatelé musejí propagovat povědomí o bezpečnostních hrozbách a zásadách mezi svými zaměstnanci.

5 Technické požadavky

5.1 Bezpečnostní aktualizace

Aktualizace: Dodavatelé musejí zajistit, že všechny systémy a aplikace, jejichž bezpečnost může mít dopad na KNL, jsou pravidelně aktualizovány a chráněny proti známým bezpečnostním zranitelnostem.

Záplaty: Dodavatelé musejí bez odkladu aplikovat bezpečnostní záplaty na všechny systémy a aplikace, jakmile jsou dostupné. Toto pravidlo je možné porušit v případě, kdy aplikace záplaty má dopad na funkčnost technologie. Takový případ musí být odůvodněn, schválen ze strany KNL a dokumentován.

5.2 Šifrování

Přenos dat: Dodavatelé musejí používat šifrování pro všechny citlivé informace přenášené mezi systémy a zařízeními.

5.3 Zálohování dat

Zálohy: Dodavatelé musejí pravidelně zálohovat všechny důležité informace a zajistit, že zálohy jsou bezpečně uloženy a chráněny před neoprávněným přístupem. Dodavatel koordinují zálohování dodaných či spravovaných technologií s IT KNL.

5.4 Konfigurace technologií

Výchozí konfigurace: Dodavatelé změní přednastavené konfigurace zařízení tak, aby nebylo možné zařízení ovládat přístupovými údaji od výrobce. Tzn. změna „default“ hesel, klíčů, přístupových kódů apod. Zařízení s přednastavenou konfigurací nesmějí být připojena k IT prostředí KNL.

Síťová izolace: KNL definuje omezený rozsah sítí, ve kterých se pracovníci dodavatele mohou pohybovat. Předávání významových dat do jiných systémů je konfigurováno na základě pravidla minimalizace propojení. Přístup k jiným systémům mimo předmět služby dodavatele je zakázán a je považován za porušení povinností dodavatele.

6 Komunikace a vzdálený přístup

Technické parametry pro připojení definuje gestor vzdáleného přístupu KNL.

Použije se jedna z následujících variant:

6.1 VPN na jméno

Uživatel přistupuje prostřednictvím přihlášení dvou-faktorovou autentizací. Sdílené použití přístupového účtu není přípustné.

6.2 Site-2- Site VPN

Propojení: Dodavatelé propojí svoji interní síť se síťovým segmentem KNL, ve kterém je připojena spravovaná technologie.

Autentizace: Dodavatelé řídí přístup svými prostředky v souladu s požadavky legislativy v oblasti kybernetické bezpečnosti.

Odpovědnost: Dodavatelé přebírají odpovědnost za zneužití, či ohrožení svěřeného segmentu sítě KNL.

7 Incident management

7.1 Hlášení incidentů

Oznamování: Dodavatelé musejí okamžitě hlásit všechny bezpečnostní incidenty a narušení, které by mohly ovlivnit bezpečnost KNL.

Odpovědnost: Dodavatelé musejí mít zavedené postupy pro rychlé a efektivní řešení bezpečnostních incidentů.

7.2 Vyšetřování

Analýza: Dodavatelé musejí provádět důkladné vyšetřování všech bezpečnostních incidentů a analyzovat jejich příčiny.

Zprávy: Dodavatelé musejí poskytovat KNL podrobné zprávy o všech bezpečnostních incidentech a navrhovat opatření k zabránění opakování incidentů.

8 Soulad a audit

8.1 Dodržování předpisů

Legislativa: Dodavatelé musejí dodržovat všechny platné zákony a předpisy týkající se ochrany informací a kybernetické bezpečnosti.

Standardy: Dodavatelé musejí dodržovat průmyslové standardy a nejlepší praxe v oblasti kybernetické bezpečnosti.

8.2 Audit

Kontroly: KNL si vyhrazuje právo provádět pravidelné audity a kontroly dodavatelů s cílem ověřit dodržování této politiky.

Spolupráce: Dodavatelé musejí plně spolupracovat při všech auditech a kontrolách a poskytovat veškeré požadované informace týkající se problematiky kybernetické bezpečnosti.

9 Závěr

Tato politika je základním vodítkem pro činnost dodavatelů. V oprávněných případech je tato politika doplněna dalšími konkretizujícími předpisy z předpisové základny KNL.