

Požadavky na kybernetickou bezpečnost – struktura dokumentů Dodavatele

Prokázání požadavků informační a kybernetické bezpečnosti

Tento dokument obsahuje doporučenou strukturu dokumentů, které Dodavatel zpracovává za účelem prokázání splnění požadavků informační a kybernetické bezpečnosti vyplývajících z dodatku *Požadavky na kybernetickou bezpečnost*, který je součástí smlouvy. Požadavky je vždy nutné vyhodnotit ve vztahu ke konkrétnímu předmětu plnění. Pokud příslušný požadavek není pro dané plnění relevantní, Dodavatel uvede tuto skutečnost v dokumentu včetně stručného odůvodnění. Pokud je možné požadavek splnit alternativní formou, Dodavatel popíše navržený způsob splnění.

Dokumenty Dodavatele

Konfigurační opatření a nastavení

Požadavek v dodatku:

V kapitole *Bezpečná konfigurace* je uveden požadavek, že Dodavatel předá Objednateli dokumentaci popisující provedená konfigurační opatření a nastavení.

Dodavatel zpracuje dokument *Konfigurační opatření a nastavení v oblasti kybernetické bezpečnosti*. V kontextu přílohy *Požadavky na kybernetickou bezpečnost* jde o výčet takových opatření a nastavení, která zajišťují plnění požadavků na kybernetickou bezpečnost implementovaného systému.

Dokument obsahuje minimálně následující kapitoly:

Kapitola	Obsah kapitoly
Účel dokumentu	Prohlášení, že jde o popis opatření a nastavení, která zajišťují plnění požadavků na kybernetickou bezpečnost implementovaného systému, a seznam odkazů na bezpečnostní požadavky, zejména smlouvu a její přílohu, relevantní legislativu, případně relevantní normy.
Komunikační matice	Kontakty pro nouzové situace, typicky service desk Odběratele a support Dodavatele.
Rozsah a architektura řešení	Seznam komponent tvořících předávaný nebo podporovaný systém a schéma architektury implementovaného řešení.
Řízení přístupů	Výchozí účty, autentizační mechanismy, pravidla pro hesla, předdefinované role a umožnění RBAC, případně informace o využití autentizačních a autorizačních mechanismů Objednatele.
Kryptografická opatření a ochrana dat	Ochrana dat v klidu, ochrana dat při přenosu, správa klíčů a secrets management, zejména ukládání a ochrana hesel, API klíčů a certifikátů.
Správa aktualizací	Stav aktualizací operačních systémů a knihoven k datu předání, způsob doručování aktualizací a způsob notifikace Odběratele o nových aktualizacích.
Logování	Seznam logovaných událostí, struktura údajů v jednom logu a podporované protokoly pro odesílání logů do centrálního SIEM Odběratele. Pokud logy sbírá a vyhodnocuje Dodavatel, uvede také směrování a retenci logů.
Ostatní bezpečnostní opatření	Seznam dalších konfiguračních opatření a nastavení zajišťujících odolnost systému, informační a kybernetickou bezpečnost systému a ochranu systému proti známým zranitelnostem.

Poznámky:

- Pokud je součástí plnění zálohování konfigurací anebo dat, mělo by být popsáno v samostatném dokumentu.
- Pokud některá kapitola není pro dané plnění relevantní, Dodavatel kapitolu zahrne do dokumentu a zdůvodní, proč není relevantní.

Zálohování a obnova dat

Požadavek v dodatku:

V kapitole *Zálohování a obnova dat* je uvedeno, že pokud součást plnění tvoří i provádění zálohování Dat Objednatele, předloží Dodavatel Objednateli ke schválení postupy zálohování a obnovy dat. Pokud je zajištění zálohování, případně obnovy dat, součástí plnění, Dodavatel zpracuje dokument *Postup zálohování a obnovy dat*.

Dokument obsahuje minimálně následující kapitoly:

Kapitola	Obsah kapitoly
Účel dokumentu	Prohlášení, že jde o zajištění kontinuity, ochranu před ztrátou dat, případně splnění legislativních požadavků, zejména pokud jde o regulovaný systém nebo jeho část.
Komunikační matice	Kontakty pro nouzové situace, typicky service desk Odběratele a support Dodavatele.
Rozsah	Výčet toho, co se zálohuje, například konfigurace aplikací, konfigurace virtuálních operačních systémů, konfigurace databázových strojů, data z databází nebo soubory.
Výjimky	Výslovný výčet toho, co se nezálohuje, i když je to součástí systému.
Parametry zálohování	Časy spouštění zálohovacích úloh včetně typu záloh, požadovaná doba uchování záloh, požadované RPO a RTO pro celý rozsah zálohování.
Popis architektury	Popis zálohovací infrastruktury, ideálně formou schématu a textového vysvětlení.
Zabezpečení záloh	Popis způsobu šifrování při přenosu a v klidu, řízení přístupu k zálohám a dalšího zabezpečení, například ochrany proti ransomware, pokud je implementována.
Postupy zálohování	Popis automatizovaných i manuálních kroků v procesu zálohování.
Postupy obnovy	Popis konkrétních kroků pro možné scénáře obnovy, od jednotlivého souboru po kompletní obnovu systému.
Testy obnovy	Popis procesu zajišťujícího pravidelné testování funkčnosti záloh.

Poznámky:

- Relevantní legislativní oporu lze uvést zejména ve vztahu k § 26 a příloze č. 1 „Hodnocení aktiv“, tabulce 3 „Stupnice pro hodnocení dostupnosti“ vyhlášky č. 409/2025 Sb., pokud je dokument zpracováván pro regulovaný systém nebo jeho část.

Plán ukončení spolupráce

Požadavek v dodatku:

Pokud je součástí dodatku kapitola *Plán ukončení spolupráce*, Dodavatel se zavazuje ve spolupráci s Objednatelem vypracovat a po dobu trvání smlouvy průběžně aktualizovat Plán ukončení spolupráce. Dodavatel zpracuje návrh relevantního dokumentu, který obsahuje výčet kroků nutných pro bezpečné opuštění implementovaného systému nebo pro bezpečnou změnu dodavatele.

Dokument obsahuje minimálně následující kapitoly:

Kapitola	Obsah kapitoly
Účel dokumentu	Prohlášení, že jde o plán ukončení spolupráce, který zajistí kontinuitu provozu a bezpečné opuštění implementovaného systému nebo bezpečnou změnu dodavatele.
Scénáře ukončení	Výčet relevantních scénářů ukončení podle typu plnění, například převod do interní správy Objednatele, přechod k jinému dodavateli, migrace dat do jiného řešení, bezpečné odstranění dat z původního prostředí nebo změna poskytovatele cloudových služeb.
Rizika ukončení	Výčet relevantních rizik pro jednotlivé scénáře ukončení a jejich mitigace. Cílem je řídit tato rizika během celého životního cyklu systému a snížit je na úroveň, která Objednatele nepoškodí, pokud na některý scénář ukončení dojde.
Kroky ukončení	Výčet nezbytných kroků pro každý scénář ukončení, například identifikace dat a konfigurací, formát a metoda předání, převod licencí, předání know-how, verifikace integrity předaných dat a likvidace nebo skartace dat u Dodavatele.

Poznámky:

- Scénář ukončení odsouhlasí Objednatel, který si může vyžádat jeho úpravu či doplnění. Při každé významné změně systému nebo smluvních ujednání je dokument přezkoumán a případně přizpůsoben změnám.