Postup auditu ISO 27001

Audit bezpečnosti informací

1. Stanovení předmětu auditu

Tento dokument je relevantní a popisuje podmínky a požadavky všech auditů bezpečnosti informací definovaných ve Smlouvě, tj.:

a) vstupní audit bezpečnosti informací, tj. audit před podpisem Smlouvy s vybraným dodavatelem v rámci zadávacího řízení;
b) všechny následné pravidelné audity bezpečnosti informací či vyhrazené a mimořádné audity bezpečnostní informací prováděné po podpisu Smlouvy, které budou prováděny zadavatelem nejméně jednou za 3 roky s výjimkou vyhrazených a mimořádných auditů bezpečnosti informací, které mohou být zadavatelem provedeny nad rámec takto stanovené periodicity.

2. Určení stran

Pro účely tohoto dokumentu se používají obecná označení smluvních stran, kde je jako zadavatel určen Státní tiskárna cenin, s. p., IČ: 0001279, a jako dodavatel Zhotovitel. Dodavatel zůstává odpovědný za plnění těchto povinností a je povinen zajistit dodržování shodných povinností i na straně poddodavatele/poddodavatelů a ve vztahu ke všem místům, kde bude plněno.

3. Účast / personální složení

Audit bezpečnosti informací budou provádět zástupci zadavatele (obvykle 1–2 osoby) a fakultativně s podporou zástupců nezávislého auditora, kterým je osoba akreditovaná Českým institutem pro akreditaci, o.p.s. nebo jiný orgán podle právního řádu dané země.

Pokud vznese dodavatel výhrady k průběhu, způsobu provedení nebo výsledku auditu bezpečnosti informací, který byl proveden pouze zadavatelem, bude následně zajištěn a proveden další audit bezpečnosti informací nezávislým auditorem definovaným v předchozím odstavci.

Ze strany dodavatele je vyžadována účast pracovníka odpovědného za bezpečnost informací, tj. bezpečnostního manažera, manažera bezpečnosti informací, manažera kybernetické bezpečnosti či materiálně obdobné pozici nebo jimi pověřené osoby. Další osoby se mohou účastnit podle uvážení dodavatele.

4. Způsob provedení auditu bezpečnosti informací:

Audit bezpečnosti informací bude proveden v souladu s ISO 19011:2019. Audit bezpečnosti informací bude proveden u dodavatele fyzicky na místě. Zadavatel může audit bezpečnosti informací provést rovněž na dálku (tj. prostřednictvím videokonference v kombinaci s využitím úložiště sdílených dokumentů) (dále jen „**vzdálený audit**“).

5. Časový průběh:

Audit bezpečnosti informací bude obvykle organizován v jeden den s následujícím programem:

- bezpečnostní politika, bezpečnostní dokumentace, řízení rizik, řízení kontinuity provozu, zajištění procesů bezpečnosti informací, inspekce infrastruktury dodavatele a kontrola nastavení procesů bezpečností informací, zpracování zápisu o auditu bezpečnosti informací, závěr.

Agendu vzdáleného auditu lze upravit z hlediska časového plánu.

6. Termín auditu bezpečnosti informací:

Kontaktní osoba dodavatele uvedená v zadávacím řízení bude informována o auditu bezpečnosti informací nejméně 5 kalendářních dní předem v případě vstupního auditu bezpečnosti informací, tj. auditu před podpisem Smlouvy s vybraným dodavatelem v rámci zadávacího řízení, a nejméně 30 dní předem v následujících auditech bezpečnosti informací, tj. auditech prováděných po podpisu Smlouvy.

7. Minimální požadavky, které mají podléhat auditu bezpečnosti informací:

Všechny informace, termíny a požadavky v tomto dokumentu musí být interpretovány v kontextu příslušných standardů a obecných bezpečnostních zásad (zejména podle mezinárodních standardů řady 27000 a výkladu Národního úřadu pro kybernetickou a informační bezpečnost), správy systému (podle mezinárodních standardů systému řízení) a procedurálních postupů (podle obecných zásad procedurálního přístupu).

Dodavatel musí zajistit soulad se všemi následujícími požadavky, z nichž všechny vycházejí z požadavků zejména ISO/IEC 27001 a zákona č. 264/2025 Sb., o kybernetické bezpečnosti.

Požadavky uvedené níže (01-04) musí být splněny všechny kumulativně.

Základním dokumentem pro posouzení splnění následujících požadavků je analýza rizik zpracovaná dodavatelem (vizte bližší požadavky níže), na které je založen způsob plnění jednotlivých požadavků bezpečnosti informací:

Část	Požadavek	Bližší popis způsobu splnění požadavku
01	Musí být zavedena základní opatření řízení bezpečnosti informací	**<u>Minimální úroveň pro splnění požadavku:</u>** Management rolí a odpovědnosti managementu k řízení bezpečnosti informací. Dodavatel je povinen mít zpracovánu a pravidelně aktualizovánu (min. 1x ročně) analýzu rizik bezpečnosti informací včetně stanovení řízení těchto rizik. Oblasti bezpečnosti informací, u kterých musí být zavedena základní opatření řízení bezpečnosti informací:

Část	Požadavek	Bližší popis způsobu splnění požadavku
		• Klasifikace aktiv • Ochrana informací proti prozrazení, zničení, narušení důvěrnosti, integrity a dostupnosti • Ochrana osobních dat • Identifikace a autentizace uživatelů • Přístup k informacím a dat na základě rolí • Řízení privilegovaných přístupů • Ochrana koncových stanic • Ochrana mobilních zařízení a vzdáleného přístupu • Ochrana e-mailu a vnitrofiremní komunikace • Ochrana přístupu do internetu • Ochrana médií • Procesy řízení změn • Ochrana bezdrátových sítí a komunikace • Fyzická bezpečnost informačních aktiv • Bezpečnostní školení koncových uživatelů a administrátorů • Ochrana proti škodlivému softwaru • Ochrana při výměně dat • Procesy zvládání bezpečnostních anebo kybernetických incidentů • Procesy řízení rizik dodavatelů • Bezpečnost lidských zdrojů • Bezpečnostní audity a analýzy • Řízení kontinuity činností a havarijního plánování **<u>Způsob prokázání v případě fyzického auditu</u>**: Předložení konkrétních důkazů a dokumentovaných informací, která prokazuje splnění výše uvedených minimálních požadavků. **<u>Způsob prokázání v případě vzdáleného auditu</u>**: Předložení konkrétních důkazů a dokumentovaných informací, která prokazuje splnění výše uvedených minimálních požadavků formou vzdáleného přístupu, nebo zobrazením na sdílené obrazovce.
02	Musí být nastaven a implementován systém řízení bezpečnostní technologie organizace dodavatele provozovaných s cílem předcházet	**<u>Minimální úroveň pro splnění požadavku:</u>** Dodavatel musí mít stanovena technologická opatření v analýze rizik s cílem minimalizovat rizika a předcházet bezpečnostním hrozbám.

Část	Požadavek	Bližší popis způsobu splnění požadavku
	bezpečnostním hrozbám ve vztahu k datům a informačním systémům	Příkladný výčet jednotlivých možných opatření ve vztahu k ochraně dat a informačních systému jsou: • Antivirový software na pracovních stanicích • Antivirový software na mobilních zařízeních • Pravidelné aktualizace softwaruřízení privilegovaných účtů a oprávnění • Více-faktorová autentizace • Pravidelné zálohování dat a testování obnovy, • Nástroj pro řízení přístupu k síti • Nástroj pro ochranu před útoky • Šifrovací nástroje a techniky • ochrana před malwarem a kybernetickými útoky např. • Vyhodnocování bezpečnostních událostí **<u>Způsob prokázání v případě fyzického auditu</u>**: Předložení analýzy rizik, resp. aplikaci nástrojů bezpečnostních technologií organizace dodavatele s cílem předcházet bezpečnostním hrozbám ve vztahu k datům a informačním systémům. **<u>Způsob prokázání v případě vzdáleného auditu</u>**: Předložení analýzy rizik, resp. aplikaci nástrojů bezpečnostních technologií organizace dodavatele s cílem předcházet bezpečnostním hrozbám ve vztahu k datům a informačním systémům.
03	Musí být nastaven a implementován systém zvládání bezpečnostních anebo kybernetických incidentů	**<u>Minimální úroveň pro splnění požadavku:</u>** Dodavatel je povinen mít nastaven a implementován systém zvládání bezpečnostních anebo kybernetických incidentů: • zaveden proces zvládání bezpečnostních anebo kybernetických incidentů • všichni zaměstnanci organizace dodavatele pravidelně (min. 1× ročně) vzdělávání v identifikaci bezpečnostních anebo kybernetických incidentů **<u>Způsob prokázání v případě fyzického auditu</u>**: Předložení konkrétních důkazů a dokumentovaných informací včetně vzdělávání v identifikaci bezpečnostních anebo kybernetických incidentů **<u>Způsob prokázání v případě vzdáleného auditu</u>**:

Část	Požadavek	Bližší popis způsobu splnění požadavku
		Předložení konkrétních důkazů a dokumentovaných informací včetně vzdělávání v identifikaci bezpečnostních anebo kybernetických incidentů
04	Musí být nastaveny a implementovány způsoby komunikace, vzdělávání a zvyšování povědomí zaměstnanců o bezpečnosti informací	**Minimální úroveň pro splnění požadavku:** Dodavatel je povinen mít zpracovány a implementovány způsoby povolené komunikace, vzdělávání a zvyšování povědomí zaměstnanců o bezpečnosti informací: • zavedení procesu vzdělávání a zvyšování povědomí zaměstnanců o bezpečnosti informací • školení lidských zdrojů v oblasti bezpečnosti informací dříve, než získají přístup k datům a informačním systémům **Způsob prokázání v případě fyzického auditu**: Předložení konkrétních důkazů a dokumentovaných informací včetně vzdělávání a zvyšování povědomí zaměstnanců o bezpečnosti informací **Způsob prokázání v případě vzdáleného auditu**: Předložení konkrétních důkazů a dokumentovaných informací včetně vzdělávání a zvyšování povědomí zaměstnanců o bezpečnosti informací