PODMÍNKY BEZPEČNOSTNÍHO AUDITU

Bezpečnostní audit budou provádět zástupci Objednatele (1–2 osoby) a je za Dodavatele vyžadována účast zaměstnance odpovědného za bezpečnost (bezpečnostní manažer nebo jím pověřená osoba). Audit bude proveden v souladu s normou ISO 19011:2019. Audit lze provést buď na místě, nebo pokud to situace nedovoluje, rovněž dálkovým auditem (tzn. videokonferencí v kombinaci se sdíleným uložištěm dokumentů).

Bezpečnostní audit bude zpravidla organizován do dvou dnů s následující agendou:

• 1. den – bezpečnostní politika, bezpečnostní dokumentace, řízení rizik, řízení kontinuity provozu, zajišťování bezpečnostních procesů, kontrola budovy,
• 2. den – dokončení kontroly budovy a kontrola nastavení bezpečnostních procesů, zpracování zápisu z bezpečnostního auditu, závěr.

Agendu vzdáleného auditu lze ve věcech časového harmonogramu upravit.

Dodavatel bude o bezpečnostním auditu informován minimálně **1 týden předem** v případě vstupního bezpečnostního auditu (kontaktní osoba uvedená v zadávacím řízení) a minimálně **30 dnů předem** v případě následných bezpečnostních auditů.

Dodavatel musí splňovat všechny následující požadavky, přičemž všechny níže uvedené požadavky vycházejí z požadavků ISO 14298 a CWA 15 374, a musí být vykládány ve smyslu ISO 14298 a CWA 15 374:

číslo	Požadavek	Bližší popis způsobu splnění požadavku
01	Musí být implementována bezpečnostní politika	**Minimální úroveň pro splnění požadavku:** Dokument "Bezpečnostní politika" musí být přijat a vydán vedením společnosti, dokument musí splňovat: (1) náležitosti normy ISO 27001, nebo (2) přiměřeně přílohy č. 5 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), nebo (3) musí obsahovat minimálně následující strukturu: • Cíle, • Priority, • Závazky v oblasti bezpečnosti **Způsob prokázání v případě fyzického auditu**: Předložení dokumentu „Bezpečnostní politika" **Způsob prokázání v případě vzdáleného auditu**: Předložení dokumentu „Bezpečnostní politika" formou vzdáleného přístupu, nebo zobrazení na sdílené obrazovce

číslo	Požadavek	Bližší popis způsobu splnění požadavku
02	U poddodavatelů, kteří se podílejí na zakázce pro Objednatele musí být provedena bezpečnostní kontrola	**Minimální úroveň pro splnění požadavku:** Musí existovat zápisy z bezpečnostních kontrol u dalších poddodavatelů, kteří se podílejí na dodávce služeb pro účastníka v rámci tohoto kontraktu. Bezpečnostní kontrolu u poddodavatelů je nutno provést minimálně v rozsahu tohoto dokumentu. V případě, že dodavatel nemá poddodavatele v rámci daného kontraktu, není tento bod auditován. **Způsob prokázání v případě fyzického auditu**: doložit zápisy se závěry z bezpečnostních kontrol **Způsob prokázání v případě vzdáleného auditu**: Předložení zápisů formou vzdáleného přístupu, nebo zobrazení na sdílené obrazovce
03	Musí být přijat systém uzavření dohody o mlčenlivosti s poddodavateli	**Minimální úroveň pro splnění požadavku:** Musí být přijata a podepsána smlouva o zachování důvěrnosti informací (NDA) mezi účastníkem a dalšími dodavateli, kteří se podílejí na zakázce pro Objednatele, která musí obsahovat minimálně tyto části: • Jména stran smlouvy, • Definice toho, co představuje důvěrné informace, • Zakazující jakékoliv vyloučení z důvěrnosti, • Prohlášení o vhodném použití informací, které mají být zveřejněny, • Příslušné časové období, • Pokuty a sankce v přiměřené výši **Způsob prokázání v případě fyzického auditu**: předložit písemný/é dokument/y případně vnitřní směrnici, která tuto oblast upravuje **Způsob prokázání v případě vzdáleného auditu**: Předložení písemných dokumentů formou vzdáleného přístupu, nebo zobrazení na sdílené obrazovce,
04	Musí být nastaveny a zdokumentovány bezpečnostní požadavky mezi Objednatelem a Dodavatelem	**Minimální úroveň pro splnění požadavku:** Dodavatel musí mít nastaveny a dokumentovány bezpečnostní postupy a pravidla pro výrobu a dodávku služeb či produktů pro Objednatele. Musí být popsán celý proces od nákupu surovin/polotovarů, výrobní cyklus až po expedici a přepravu výrobků odběrateli. Součástí dokumentu musí být evidence materiálů v průběhu výrobního cyklu a způsob likvidace neshodné výroby **Způsob prokázání v případě fyzického auditu**: předložit písemnou dokumentaci bezpečnostních pravidel a postupů při výrobě **Způsob prokázání v případě vzdáleného auditu**: Předložení písemných dokumentů formou vzdáleného přístupu, nebo zobrazením na sdílené obrazovce

číslo	Požadavek	Bližší popis způsobu splnění požadavku
05	Jsou prováděny pravidelné bezpečnostní audity	**Minimální úroveň pro splnění požadavku:** Účastník realizuje a eviduje pravidelné interní bezpečnostní audity vlastních postupů a pravidel (min. 1x ročně). **Způsob prokázání v případě fyzického auditu**: doložit zápisy z auditů a realizaci nápravných opatření v případě zjištěných nedostatků a program/plán interních auditů **Způsob prokázání v případě vzdáleného auditu**: doložit zápisy z auditů a realizaci nápravných opatření v případě zjištěných nedostatků a program/plán interních auditů formou vzdáleného přístupu, nebo zobrazením na sdílené obrazovce
06	Musí být implementovány a aktualizovány dokumenty o posouzení rizik a řízení rizik	**Minimální úroveň pro splnění požadavku:** Je zpracována a pravidelně aktualizována analýza rizik (min. 1x ročně). Dokument musí splňovat: (1) Náležitosti dle normy ISO 27001, nebo (2) musí obsahovat minimálně následující části: • identifikaci rizik (risk identification) • analýzu rizik (risk analysis) • zhodnocení rizik (risk evaluation) • ošetření rizik (risk mitigation) • zvládnutí rizik (respektive jejich zmírnění) • monitoring rizik (risk monitoring and review) **Způsob prokázání v případě fyzického auditu**: doložit dokument analýza rizik **Způsob prokázání v případě vzdáleného auditu**: doložit dokument analýza rizik formou vzdáleného přístupu, nebo zobrazením na sdílené obrazovce
07	Musí být zajištěna nepřetržitá dodávka výrobků nebo služeb	**Minimální úroveň pro splnění požadavku:** Existuje funkční a aktuální Business Continuity Plan k zajištění maximální ochrany s cílem zajistit provoz firmy a jejího fungování v situacích, kdy je firma ohrožena nebo čelí nějaké katastrofě. Dokument musí splňovat: (1) náležitosti normy dle ISO 22301, nebo (2) musí obsahovat minimálně následující části**:** • Analýza rizik a hrozeb • Analýza dopadů na business • Krizová opatření a organizační pokyny pro udržení chodu organizace v krizi • Plány a opatření na udržení kontinuity • Scénáře, plány a opatření na obnovy chodu • Techniky pro zajištění kvality, preventivní opatření jako jsou údržba, cvičení, audity • Kontaktní informace na členy managementu (zejména krizového)

číslo	Požadavek	Bližší popis způsobu splnění požadavku
		• Pokyny pro zaměstnance v případě krizové situace • Alokace lidí, nástrojů a dalších zdrojů **<u>Způsob prokázání v případě fyzického auditu</u>**: doložit dokument „Bussines Continuity Plan“. **<u>Způsob prokázání v případě vzdáleného auditu</u>**: doložit dokument „Bussines Continuity Plan“ formou vzdáleného přístupu, nebo zobrazením na sdílené obrazovce.
08	Budovy Dodavatele musí být zabezpečeny prostřednictvím: PZTS (poplachový zabezpečovací a tísňový systém), EPS (elektrická požární signalizace), CCTV (kamerový systém), ACS (přístupový systém)	**<u>Minimální úroveň pro splnění požadavku:</u>** Objekty a výrobní prostory Dodavatele musí být vybaveny definovanými bezpečnostními systémy s napojením na dohledové centrum (interní či externí). Kamerový systém musí být se záznamem, a musí monitorovat celý výrobní prostor a perimetr bez mrtvých úhlů. ACS musí být minimálně nainstalován na všech vstupech do výrobních prostor. PZTS musí plně pokrývat minimálně všechny výrobní prostory, přípravu výroby a skladové prostory. EPS není povinný, pokud je tato skutečnost uvedena v „Požárně bezpečnostním řešení“ nebo obdobné dokumentu. **<u>Způsob prokázání v případě fyzického auditu</u>**: fyzická kontrola nainstalované bezpečnostní techniky, návštěva dohledového centra, předložení dokumentu „Popis fyzického a logického perimetru,“ nebo „Bezpečnostní projekt“ nebo směrnici „Fyzická ochrana“ nebo obdobných dokumentů, které popisují instalované bezpečnostní technologie. **<u>Způsob prokázání v případě vzdáleného auditu</u>**: doložení dokumentů „Popis fyzického a logického perimetru, nebo „Bezpečnostní projekt“ nebo směrnici „Fyzická ochrana“ nebo obdobných dokumentů, které popisují instalované bezpečnostní technologie formou vzdáleného přístupu nebo zobrazení na sdílené obrazovce (součástí uvedené dokumentace musí být fotografie instalovaných technologií, popř. doložit nainstalované bezpečnostní prvky kamerou v rámci on-line přenosu).
09	Musí být určen prostor pro nakládku a vykládku zboží a materiálu	**<u>Minimální úroveň pro splnění požadavku:</u>** Prostory pro nakládání či vykládání produktů musí být vyznačeny a provozovány v bezpečnostním režimu (dveře musí být ve vazbě – nelze otevřít najednou). Musí se jednat o stavebně oddělený prostor, v době nakládky/vykládky se v prostoru musí zdržovat pouze obsluha provádějící manipulaci s materiálem a případně ostraha. Prostor musí být vybaven kamerovým systémem se záznamem, který monitoruje celý prostor bez mrtvých úhlů.

číslo	Požadavek	Bližší popis způsobu splnění požadavku
		Způsob prokázání v případě fyzického auditu: fyzická kontrola prostoru, předložení dokumentu „Popis fyzického a logického perimetru, nebo „Bezpečnostní projekt“ nebo směrnici „Fyzická ochrana“ nebo obdobných dokumentů, které popisují zabezpečení nakládacích/vykládacích prostor. **Způsob prokázání v případě vzdáleného auditu**: doložení dokumentů „Popis fyzického a logického perimetru, nebo „Bezpečnostní projekt“ nebo směrnici „Fyzická ochrana“ nebo obdobných dokumentů, které popisují zabezpečení nakládacích/vykládacích prostor formou vzdáleného přístupu nebo zobrazením na sdílené obrazovce (součástí uvedené dokumentace musí být fotografie instalovaných technologií).
10	Fyzickou ostrahu musí provádět vlastní zaměstnanci nebo externí firma s licencí	**Minimální úroveň pro splnění požadavku:** V objektech Dodavatele musí být organizována nepřetržitá fyzická ostraha (vlastními zaměstnanci, anebo externími kvalifikovanými subjekty). Objekty Dodavatele musí mít odpovídající zajištění perimetru (oplocení) a mechanické zabezpečení všech vstupů (mříže na oknech, zodolněné vstupy-dveře apod.) **Způsob prokázání v případě fyzického auditu**: fyzická kontrola prostoru ostrahy a mechanických systémů zabezpečení, předložení dokumentu „Popis fyzického a logického perimetru, nebo dokumentu „Bezpečnostní projekt“ nebo směrnice „Fyzická ochrana“ nebo obdobných dokumentů, které popisují stav fyzické bezpečnosti. V případě externího subjektu doložit smlouvu o zajištění fyzické ostrahy **Způsob prokázání v případě vzdáleného auditu**: předložení dokumentu „Popis fyzického a logického perimetru, nebo dokumentu „Bezpečnostní projekt“ nebo směrnice „Fyzická ochrana“ nebo obdobných dokumentů, které popisují stav fyzické bezpečnosti formou vzdáleného přístupu nebo zobrazením na sdílené obrazovce (součástí uvedené dokumentace musí být fotografie instalovaných technologií). Doložit fotografie ostrahy objektu a v případě externího subjektu doložit smlouvu o zajištění fyzické bezpečnosti.
11	Musí být implementován klíčový režim	**Minimální úroveň pro splnění požadavku:** Dodavatel provozuje transparentní klíčový režim – evidence, přidělení a bezpečné uložení klíčů. Není možno klíče vynášet mimo objekt Dodavatele. Minimálně jednou ročně musí být prováděna kontrola systému klíčového režimu. **Způsob prokázání v případě fyzického auditu**: kontrola evidence a úložných prostor pro klíče, doložení podkladů, že je prováděna minimálně jednou ročně kontrola evidence přidělených klíčů.

číslo	Požadavek	Bližší popis způsobu splnění požadavku
		Způsob prokázání v případě vzdáleného auditu: formou vzdáleného přístupu nebo zobrazením na sdílené obrazovce doložit podklady, že je implementován klíčový režim (součástí musí být fotodokumentace prostor pro uložení klíčů) a zápis o kontrole evidence přidělených klíčů (min. 1x ročně).
12	Data musí být bezpečně uložena, IT systémy pravidelně kontrolovány	**Minimální úroveň pro splnění požadavku:** Servery a datová uložiště musí být umístěna v samostatném prostoru vybaveném kamerovým systémem se záznamem, který monitoruje celý prostor bez mrtvých úhlů, zabezpečena před neautorizovaným přístupem – ACS a vybavena PZTS, EPS je doporučeno. Nad IT systémy musí být nastaven systémový audit **Způsob prokázání v případě fyzického auditu**: – fyzická kontrola prostoru se servery a datovými úložišti, doložení auditních záznamů, a logů včetně jejich analýzy a následné klasifikace nedostatků. Přehled bezpečnostních událostí a incidentů **Způsob prokázání v případě vzdáleného auditu**: formou vzdáleného přístupu nebo zobrazením na sdílené obrazovce předložit popis zabezpečení serveroven a datových úložišť, a předložení dokumentu, který popisuje způsob provedení systémového auditu.
13	IT specialisté jsou zaměstnanci Dodavatele	**Minimální úroveň pro splnění požadavku:** Dodavatel má vlastní IT zaměstnance, minimálně na úrovni bezpečnostní správy **Způsob prokázání v případě fyzického auditu**: – doložení/náhled do personální evidence **Způsob prokázání v případě vzdáleného auditu**: formou vzdáleného přístupu nebo zobrazením na sdílené obrazovce (náhled do personální evidence)
14	Je implementována politika oběhu a evidence materiálů a dokumentů	**Minimální úroveň pro splnění požadavku:** Dodavatel provozuje funkční systém pro evidenci, oběh a ukládání materiálu a dokumentů. Dodavatel musí mít vytvořeny skladové prostory a musí mít evidenci veškerého materiálu v průběhu výroby včetně odpadu. Musí být zaveden systém likvidace odpadu **Způsob prokázání v případě fyzického auditu**: předložení dokumentu, který popisuje systém evidence, oběhu a ukládání materiálů a dokumentů **Způsob prokázání v případě vzdáleného auditu**: formou vzdáleného přístupu nebo zobrazením na sdílené obrazovce doložit dokument, který popisuje systém evidence, oběhu a ukládání materiálů a dokumentů
15	Jsou implementovány zásady přístupu k informačním systémům	**Minimální úroveň pro splnění požadavku:** Dodavatel zajišťuje řízený přístup k informacím a má nastavený

číslo	Požadavek	Bližší popis způsobu splnění požadavku
	během a při ukončení pracovního poměru	systém pro ukončení přístupu do inf. systémů po ukončení pracovního poměru. **<u>Způsob prokázání v případě fyzického auditu</u>**: – doložit postupy – např dokument výstupní list **<u>Způsob prokázání v případě vzdáleného auditu</u>**: formou vzdáleného přístupu nebo zobrazením na sdílené obrazovce doložit např. dokument výstupní list
16	Dodavatel má vlastní zaměstnance pro zpracování dodávky	**<u>Minimální úroveň pro splnění požadavku:</u>** Pro zajištění výroby produktů Objednatele využívá dodavatel vlastní zaměstnance, nebo agenturní zaměstnance, kteří musejí mít podepsanou smlouvu o mlčenlivosti jak s vlastní agenturou, tak i s dodavatelem. Současně musí existovat smlouva o mlčenlivosti mezi Dodavatelem a personální agenturou. **<u>Způsob prokázání v případě fyzického auditu</u>**: doložení/náhled např do personální evidence **<u>Způsob prokázání v případě vzdáleného auditu</u>**: formou vzdáleného přístupu nebo zobrazením na sdílené obrazovce umožnit náhled do personální evidence.