# Bezpečnostní audit

## 1. Stanovení předmětu bezpečnostního auditu

Tento dokument je relevantní a popisuje podmínky a požadavky všech bezpečnostních auditů definovaných v Rámcové dohodě, tj.:

a) počáteční bezpečnostní audit, tj. audit před podpisem Rámcové dohody s vybraným dodavatelem v rámci zadávacího řízení;
b) všechny následné pravidelné bezpečnostní audity a mimořádné bezpečnostní audity prováděné po podpisu Rámcové dohody.

## 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 jakýkoli subjekt, který bude zajišťovat plnění předmětu Rámcové dohody jako poddodavatel/poddodavatelé dodavatele. Dodavatel zůstává odpovědný za plnění těchto povinností a je povinen zajistit spolupráci na straně poddodavatele/poddodavatelů.

## 3. Účast / personální složení

Bezpečnostní audit 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. (kde „o.p.s“ znamená „společnost zájmového společenství“ forma nebo právnická osoba uznávaná českým právem) nebo jiný orgán podle právního řádu dané země.

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

Ze strany dodavatele je vyžadována účast pracovníka odpovědného za bezpečnost, tj. bezpečnostní manažer nebo jím pověřená osoba. Další osoby se mohou účastnit podle uvážení dodavatele.

## 4. Způsob provedení bezpečnostního auditu:

Bezpečnostní audit bude proveden v souladu s ISO 19011:2019. Bezpečnostní audit bude proveden buď fyzicky na místě, nebo pokud to současná situace neumožňuje, bude proveden na dálku (tj. prostřednictvím videokonference v kombinaci s využitím úložiště sdílených dokumentů) (dále jen „**vzdálený audit**“).

## 5. Časový průběh:

Bezpečnostní audit bude obvykle organizován ve dvou dnech s následujícím programem:

• Den 1 - bezpečnostní politika, bezpečnostní dokumentace, řízení rizik, řízení kontinuity provozu, zajištění bezpečnostních procesů, inspekce budov,

• Den 2 - dokončení prohlídky budovy a kontrola nastavení bezpečnostních procesů, zpracování zápisu o bezpečnostním auditu, závěr.

Agendu vzdáleného auditu lze upravit z hlediska časového plánu.

**6. Termín bezpečnostního auditu:**

Kontaktní osoba dodavatele uvedená v zadávacím řízení bude informována o bezpečnostním auditu nejméně 5 dní předem v případě počátečního bezpečnostního auditu, tj. auditu před podpisem Rámcové dohody s vybraným dodavatelem v rámci zadávacího řízení, a nejméně 30 dní předem v následujících bezpečnostních auditech, tj. auditech prováděných po podpisu Rámcové dohody.

**7. Minimální požadavky, které mají podléhat bezpečnostnímu auditu:**

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 14298 a CWA 15374, a musí být interpretovány v souladu s ISO 14298 a CWA 15 374.**

**Základním dokumentem pro posouzení splnění následujících požadavků je analýza rizik zpracovaná Dodavatelem (viz požadavek 01 níže), na které je založen způsob plnění jednotlivých požadavků na základě ISO 14298 a CWA 15374:**

| číslo | Požadavek | Bližší popis způsobu splnění požadavku |
|---|---|---|
| 01 | Musí být zpracován a pravidelně aktualizován dokument o posouzení rizik a řízení rizik | **<u>Minimální úroveň pro splnění požadavku:</u>**<br>Dodavatel je povinen mít zpracovánu a pravidelně aktualizovánu (min. 1x ročně) analýzu rizik včetně stanovení řízení těchto rizik v rozsahu minimálně dle normy ISO 14298 - bod 4.4.<br><br>Dokument musí dále splňovat:<br>1) Náležitosti dle normy ISO 27001, nebo<br>2) musí obsahovat minimálně následující části:<br>• **identifikaci rizik** (risk identification)<br>• **analýzu rizik** (risk analysis)<br>• **zhodnocení rizik** (risk evaluation)<br>• **ošetření rizik** (risk mitigation)<br>• **zvládnutí rizik** (respektive jejich zmírnění)<br>• **monitoring rizik** (risk monitoring and review)<br><br>**<u>Způsob prokázání v případě fyzického auditu</u>**:<br>Předložení konkrétní písemné dokumentace obsahující analýzu rizik včetně řízení těchto rizik, která prokazuje splnění výše uvedených minimálních požadavků. |

| číslo | Požadavek | Bližší popis způsobu splnění požadavku |
|---|---|---|
| | | **<u>Způsob prokázání v případě vzdáleného auditu</u>**:<br>Předložení konkrétní písemné dokumentace obsahující analýzu rizik včetně řízení těchto rizik, která prokazuje splnění výše uvedených minimálních požadavků formou vzdáleného přístupu, nebo zobrazením na sdílené obrazovce. |
| 02 | Musí být nastaven a implementován systém pravidelných bezpečnostních kontrol poddodavatelů dodavatele, kteří mu dodávají vstupní bezpečnostní materiál pro výrobu a finalizaci produktů | **<u>Minimální úroveň pro splnění požadavku:</u>**<br>Dodavatel je povinen mít nastaven a implementován systém pravidelných (min. 1 x za období 3 let) bezpečnostních kontrol svých poddodavatelů, kteří mu dodávají vstupní bezpečnostní materiál pro výrobu a finalizaci produktů. Za bezpečnostní kontrolu je pro účely tohoto bezpečnostního auditu považována jakákoliv kontrola poddodavatele, která ověří splnění požadavků min. v rozsahu bodů 1-12 dle tohoto dokumentu, přičemž formou takové kontroly musí být bezpečnostní audit v osobní/fyzické či vzdálené formě, či ověření držení certifikátů ISO 14298 nebo CWA 15 374.<br><br>Rozsah a způsob provádění těchto bezpečnostních kontrol se může odlišovat od výše uvedeného, pokud bude tento odlišný postup v souladu s analýzou rizik dodavatele (tj. dokumentu dle požadavku 01 v tomto dokumentu).<br><br>**<u>Způsob prokázání v případě fyzického auditu</u>**:<br>Předložení konkrétní písemné dokumentace obsahující nastavení výše požadovaného systému bezpečnostních kontrol (tj. zejména interní dokumentace dodavatele) včetně doložení min. 1 vzorku ve smyslu prokázání provedení konkrétní bezpečnostní kontroly poddodavatele splňující výše uvedené požadavky v posledních min. 3 letech ode dne konání probíhajícího bezpečnostního auditu.<br><br>**<u>Způsob prokázání v případě vzdáleného auditu</u>**:<br>Předložení konkrétní písemné dokumentace obsahující nastavení výše požadovaného systému bezpečnostních kontrol (tj. zejména interní dokumentace dodavatele) včetně doložení min. 1 vzorku ve smyslu prokázání provedení konkrétní bezpečnostní kontroly poddodavatele splňující výše uvedené požadavky v posledních min. 3 letech ode dne konání probíhajícího bezpečnostního auditu formou vzdáleného přístupu, nebo zobrazením na sdílené obrazovce. |

| číslo | Požadavek | Bližší popis způsobu splnění požadavku |
|---|---|---|
| 03 | Musí být nastaven a implementován systém uzavírání dohod o mlčenlivosti s poddodavateli dodavatele | **<u>Minimální úroveň pro splnění požadavku:</u>**<br>Dodavatel je povinen mít nastaven a implementován systém uzavírání dohod o mlčenlivosti se svými poddodavateli, které obsahují minimálně následující části:<br><br>• Jména stran dané dohody,<br>• Definici toho, co představuje důvěrné informace,<br>• Ustanovení, zakazující jakékoliv vyloučení z důvěrnosti (kromě zákonných a jiných obecně závazných povinností informace uveřejňovat),<br>• Příslušné časové období závazku,<br>• Smluvní sankce v přiměřené výši v souladu s analýzou rizik<br><br>Konkrétní povinné náležitosti a konečná podoba těchto dohod o zachování mlčenlivosti se může odlišovat od výše uvedeného, pokud bude tento odlišný postup v souladu s analýzou rizik dodavatele (tj. dokumentu dle požadavku 01 v tomto dokumentu).<br><br>**<u>Způsob prokázání v případě fyzického auditu</u>**:<br>Předložení konkrétní písemné dokumentace obsahující nastavení výše požadovaného systému (tj. zejména interní dokumentace dodavatele) včetně doložení min. 1 vzorku ve smyslu prokázání uzavření konkrétní dohody o zachování mlčenlivosti s poddodavatelem splňující výše uvedené požadavky.<br><br>**<u>Způsob prokázání v případě vzdáleného auditu</u>**:<br>Předložení konkrétní písemné dokumentace obsahující nastavení výše požadovaného systému (tj. zejména interní dokumentace dodavatele) včetně doložení min. 1 vzorku ve smyslu prokázání uzavření konkrétní dohody o zachování mlčenlivosti s poddodavatelem splňující výše uvedené požadavky formou vzdáleného přístupu, nebo zobrazením na sdílené obrazovce. |
| 04 | Musí být nastaveny a implementovány bezpečnostní postupy | **<u>Minimální úroveň pro splnění požadavku:</u>**<br>Dodavatel je povinen mít zpracovány a implementovány bezpečnostní postupy a pravidla pro výrobu a dodávku bezpečnostních produktů. Musí být popsán celý proces od nákupu surovin/polotovarů, výrobní cyklus až po expedici a přepravu výrobků zákazníkovi. Součástí dokumentace musí být evidence materiálů v průběhu výrobního cyklu, tedy zajištění, že dodavatel zná (ví/dodavateli je známo) v každém okamžiku (při každém výrobním kroku), kde a kolik materiálu se nachází, přičemž stejný proces musí být nastaven také po ukončení výrobního kroku, a stejný postup musí být nastaven v případě likvidace neshodné výroby. |

| číslo | Požadavek | Bližší popis způsobu splnění požadavku |
|---|---|---|
| | | Musí být dodržováno pravidlo dohledatelnosti - **schopnost vysledovat historii, použití nebo umístění toho, co je posuzováno.**<br><br>Konkrétní bezpečnostní postupy a pravidla musí vycházet a být v souladu s analýzou rizik dodavatele (tj. dokumentu dle požadavku 01 v tomto dokumentu).<br><br>**Způsob prokázání v případě fyzického auditu**:<br>Předložení konkrétní písemné dokumentace obsahující výše požadované bezpečnostní procesy a pravidla (tj. zejména interní dokumentace dodavatele) včetně doložení min. 1 vzorku ve smyslu prokázání implementace daných procesů a pravidel splňující danou dokumentaci.<br><br>**Způsob prokázání v případě vzdáleného auditu**:<br>Předložení konkrétní písemné dokumentace obsahující výše požadované bezpečnostní procesy a pravidla (tj. zejména interní dokumentace dodavatele) včetně doložení min. 1 vzorku ve smyslu prokázání implementace daných procesů a pravidel splňující danou dokumentaci formou vzdáleného přístupu, nebo zobrazením na sdílené obrazovce. |
| 05 | Musí být nastaven a implementován systém pravidelných interních bezpečnostních auditů | **Minimální úroveň pro splnění požadavku:**<br>Dodavatel je povinen mít nastaven systém pravidelných (min. 1 x ročně) interních bezpečnostních auditů vlastních postupů a pravidel v rozsahu minimálně dle normy ISO 14298 - bod 9.2. Provádění bezpečnostních auditů může být součástí interních auditů.<br><br>**Způsob prokázání v případě fyzického auditu**:<br>Předložení konkrétní písemné dokumentace obsahující nastavení výše požadovaného systému interních bezpečnostních auditů (tj. zejména interní dokumentace dodavatele) včetně doložení min. 1 vzorku ve smyslu prokázání provedení konkrétního interního bezpečnostního auditu splňujícího výše uvedené požadavky v posledním roce od dne konání probíhajícího bezpečnostního auditu. Dodavatel je dále povinen doložit zápis z takového auditu a informace o realizaci nápravných opatření v případě zjištěných nedostatků, je-li relevantní, a dále aktuální program/plán interních auditů, je-li zpracován.<br><br>**Způsob prokázání v případě vzdáleného auditu**: Formou vzdáleného přístupu, nebo zobrazením na sdílené obrazovce předložení konkrétní písemné dokumentace obsahující nastavení výše požadovaného systému interních bezpečnostních auditů (tj. zejména interní dokumentace |

| číslo | Požadavek | Bližší popis způsobu splnění požadavku |
|---|---|---|
| | | dodavatele) včetně doložení min. 1 vzorku ve smyslu prokázání provedení konkrétního interního bezpečnostního auditu splňujícího výše uvedené požadavky v posledním roce od dne konání probíhajícího bezpečnostního auditu. Dodavatel je dále povinen doložit zápis z takového auditu a informace o realizaci nápravných opatření v případě zjištěných nedostatků, je-li relevantní, a dále aktuální program/plán interních auditů, je-li zpracován. |
| 06 | Musí být zpracován tzv. Business Continuity Plan dodavatele | **<u>Minimální úroveň pro splnění požadavku:</u>**<br>Dodavatel je povinen mít zpracován tzv. Business Continuity Plan dodavatele za účelem zajištění nepřetržité dodávky výrobků nebo služeb a k zajištění maximální ochrany s cílem zajistit provoz společnosti a jejího fungování v situacích, kdy je společnost ohrožena nebo čelí nějaké katastrofě, přičemž tento dokument musí splňovat následující minimální požadavky:<br><br>1) náležitosti normy dle ISO 22301, nebo<br>2) musí obsahovat minimálně následující části:<br>• Analýza rizik a hrozeb<br>• Analýza dopadů na business<br>• Krizová opatření a organizační pokyny pro udržení chodu organizace v krizi<br>• Plány a opatření na udržení kontinuity<br>• Scénáře, plány a opatření na obnovy chodu<br>• Techniky pro zajištění kvality, preventivní opatření jako jsou údržba, cvičení, audity<br>• Kontaktní informace na členy managementu (zejména krizového)<br>• Pokyny pro zaměstnance v případě krizové situace<br>• Alokace lidí, nástrojů a dalších zdrojů<br><br>Konkrétní povinné náležitosti a konečná podoba tohoto plánu se může odlišovat od výše uvedeného, pokud bude tento odlišný postup v souladu s analýzou rizik dodavatele (tj. dokumentu dle požadavku 01 v tomto dokumentu).<br><br>**<u>Způsob prokázání v případě fyzického auditu</u>**:<br>Předložení konkrétní dokumentace, která prokazuje splnění výše uvedených minimálních požadavků.<br><br>**<u>Způsob prokázání v případě vzdáleného auditu</u>**:<br>Předložení konkrétní dokumentace, která prokazuje splnění výše uvedených minimálních požadavků formou vzdáleného přístupu, nebo zobrazením na sdílené obrazovce. |

| číslo | Požadavek | Bližší popis způsobu splnění požadavku |
|---|---|---|
| 07 | Výrobní a skladovací prostory dodavatele musí být zabezpečeny prostřednictvím následujících systémů:<br>PZTS (poplachový zabezpečovací a tísňový systém),<br>EPS (elektrická požární signalizace),<br>CCTV (kamerový systém),<br>ACS (přístupový systém) | **Minimální úroveň pro splnění požadavku:**<br>Dodavatel je povinen zajistit a vybavit výrobní a skladovací prostory dodavatele definovanými bezpečnostními systémy (PZTS, EPS, CCTV, ACS) s napojením na dohledové centrum (interní či externí), přičemž musí být splněny následující minimální požadavky:<br><br>- CCTV musí být se záznamem, a musí monitorovat celý výrobní prostor a perimetr bez mrtvých úhlů.<br>- ACS musí být minimálně nainstalován na všech vstupech do výrobních prostor.<br>- PZTS musí plně pokrývat minimálně všechny výrobní prostory, přípravu výroby a skladové prostory.<br>- EPS není povinný, pokud je tato skutečnost uvedena v „Požárně bezpečnostním řešení“ nebo obdobném dokumentu.<br><br>Konkrétní podoba a nastavení těchto systémů se může odlišovat od výše uvedeného, pokud bude tento odlišný postup v souladu s analýzou rizik dodavatele (tj. dokumentu dle požadavku 01 v tomto dokumentu).<br><br>**Způsob prokázání v případě fyzického auditu**:<br>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, a které prokazují splnění výše uvedených minimálních požadavků.<br><br>**Způsob prokázání v případě vzdáleného auditu**:<br>Předložení konkrétních dokumentů „Popis fyzického a logického perimetru, nebo „Bezpečnostní projekt“ nebo směrnici „Fyzická ochrana“ nebo obdobných dokumentů, které popisují instalované bezpečnostní technologie, které prokazují splnění výše uvedených minimálních požadavků, formou vzdáleného přístupu nebo zobrazením na sdílené obrazovce (součástí uvedené dokumentace musí být fotografie instalovaných technologií, popř. doložit nainstalované bezpečnostní prvky kamerou v rámci on-line přenosu, které budou dokumentovat splnění minimálních požadavků). |
| 08 | Musí být určen prostor pro nakládku a vykládku zboží a materiálu | **Minimální úroveň pro splnění požadavku:**<br>Dodavatel je povinen mít označený prostor pro nakládání či vykládání zboží a materiálu a tento prostor musí být provozován v bezpečnostním režimu (tj. min. PZTS, ACS a CCTV se záznamem, který monitoruje celý prostor bez mrtvých úhlů). V době nakládky/vykládky se v prostoru musí |

| číslo | Požadavek | Bližší popis způsobu splnění požadavku |
|---|---|---|
| | | zdržovat pouze obsluha provádějící manipulaci se zbožím nebo materiálem a případně ostraha.<br><br>Konkrétní podoba a nastavení těchto pravidel se může odlišovat od výše uvedeného, pokud bude tento odlišný postup v souladu s analýzou rizik dodavatele (tj. dokumentu dle požadavku 01 v tomto dokumentu).<br><br>**<u>Způsob prokázání v případě fyzického auditu</u>**:<br>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, které prokazují splnění výše uvedených minimálních požadavků, součástí uvedené dokumentace musí být fotografie instalovaných technologií, které budou dokumentovat splnění minimálních požadavků.<br><br>**<u>Způsob prokázání v případě vzdáleného auditu</u>**:<br>Předložení dokumentů „Popis fyzického a logického perimetru, nebo „Bezpečnostní projekt“ nebo směrnici „Fyzická ochrana“ nebo obdobných dokumentů, které popisují zabezpečení nakládacích/vykládacích prostor, které prokazují splnění výše uvedených minimálních požadavků, formou vzdáleného přístupu nebo zobrazením na sdílené obrazovce (součástí uvedené dokumentace musí být fotografie instalovaných technologií, které budou dokumentovat splnění minimálních požadavků). |
| 09 | Fyzickou ostrahu musí provádět vlastní zaměstnanci dodavatele nebo externí kvalifikovaný subjekt | **<u>Minimální úroveň pro splnění požadavku:</u>**<br>Dodavatel je povinen zajistit nepřetržitou fyzickou ostrahu svých objektů vlastními zaměstnanci, anebo externím kvalifikovaným subjektem, který je oprávněn k provádění dané fyzické ostrahy v souladu s daným právním řadem. Všechny výrobní a skladovací prostory dodavatele související s plněním dané veřejné zakázky musí být zabezpečeny proti vniknutí a vstupu neoprávněných osob, detailnímu nahlížení do vnitřních prostor zvenčí nebo přítomnosti neoprávněných osob. Např. musí mít odpovídající zajištění perimetru (oplocení) a mechanické zabezpečení všech vstupů (mříže na oknech, zodolněné vstupy-dveře apod.)<br><br>Konkrétní podoba a nastavení fyzické ostrahy dodavatele se může odlišovat od výše uvedeného, pokud bude tento odlišný postup v souladu s analýzou rizik dodavatele (tj. dokumentu dle požadavku 01 v tomto dokumentu).<br><br>**<u>Způsob prokázání v případě fyzického auditu</u>**: |

| číslo | Požadavek | Bližší popis způsobu splnění požadavku |
|---|---|---|
| | | 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, které prokazují splnění výše uvedených minimálních požadavků. Dodavatel musí předložit fotografie ostrahy objektu, které budou dokumentovat splnění minimálních požadavků, a v případě externího subjektu musí dodavatel doložit uzavřenou platnou smlouvu o zajištění fyzické bezpečnosti mezi dodavatelem a externím subjektem.<br><br>**Způsob prokázání v případě vzdáleného auditu**:<br>Předložení dokumentu „Popis fyzického a logického perimetru, nebo dokumentu „Bezpečnostní projekt“ nebo směrnice „Fyzická ochrana“ nebo obdobných dokumentů, které popisují stav fyzické bezpečnosti, které prokazují splnění výše uvedených minimálních požadavků, formou vzdáleného přístupu nebo zobrazením na sdílené obrazovce. Dodavatel musí předložit fotografie ostrahy objektu, které budou dokumentovat splnění minimálních požadavků, a v případě externího subjektu musí dodavatel doložit uzavřenou platnou smlouvu o zajištění fyzické bezpečnosti mezi dodavatelem a externím subjektem. |
| 10 | Musí být implementován klíčový režim | **Minimální úroveň pro splnění požadavku:**<br>Dodavatel je povinen mít implementovaný transparentní klíčový režim, který zajišťuje evidenci, přidělení a bezpečné uložení klíčů. Minimálně jednou ročně musí být prováděna kontrola systému klíčového režimu.<br><br>Konkrétní podoba a nastavení klíčového režimu dodavatele se může odlišovat od výše uvedeného, pokud bude tento odlišný postup v souladu s analýzou rizik dodavatele (tj. dokumentu dle požadavku 01 v tomto dokumentu).<br><br>**Způsob prokázání v případě fyzického auditu**:<br>Fyzická kontrola systému evidence a úložných prostor pro klíče, doložení konkrétní dokumentace, že je prováděna minimálně jednou ročně kontrola systému klíčového režimu, tj. dodavatel musí předložit alespoň zápis o kontrole v posledním roce ode dne konání probíhajícího bezpečnostního auditu.<br><br>**Způsob prokázání v případě vzdáleného auditu**:<br>Formou vzdáleného přístupu nebo zobrazením na sdílené obrazovce musí dodavatel doložit podklady, ze kterých je zřejmé, že je implementován klíčový režim (součástí musí být fotodokumentace prostor pro uložení klíčů) a doložit |

| číslo | Požadavek | Bližší popis způsobu splnění požadavku |
|---|---|---|
| | | konkrétní dokumentaci, že je prováděna minimálně jednou ročně kontrola evidence přidělených klíčů, tj. dodavatel musí předložit alespoň zápis o kontrole v posledním roce ode dne konání probíhajícího bezpečnostního auditu. |
| 11 | Musí být zpracovány a implementovány zásady přístupu k informačním systémům během a při ukončení pracovního poměru | **Minimální úroveň pro splnění požadavku:**<br>Dodavatel je povinen mít zpracovány a implementovány zásady řízeného přístupu k informačním systémům během a při ukončení pracovního poměru zaměstnanců dodavatele.<br><br>**Způsob prokázání v případě fyzického auditu**:<br>Předložení konkrétní písemné dokumentace obsahující nastavení výše požadovaných zásad (tj. zejména interní dokumentace dodavatele, např. výstupní list) včetně doložení min. 1 vzorku ve smyslu prokázání implementace daných zásad splňujících výše uvedené požadavky.<br><br>**Způsob prokázání v případě vzdáleného auditu**:<br>Předložení konkrétní písemné dokumentace obsahující nastavení výše požadovaných zásad (tj. zejména interní dokumentace dodavatele, např. výstupní list) včetně doložení min. 1 vzorku ve smyslu prokázání implementace daných zásad splňujících výše uvedené požadavky. formou vzdáleného přístupu nebo zobrazením na sdílené obrazovce |
| 12 | Dodavatel má vlastní zaměstnance pro zajištění výroby a skladování bezpečnostních produktů, nebo agenturní zaměstnance, kteří splňují další podmínky | **Minimální úroveň pro splnění požadavku:** Dodavatel je povinen zajišťovat výrobu a skladování bezpečnostních produktů vlastními zaměstnanci. V případě, že využívá agenturní zaměstnance, musejí mít podepsanou smlouvu o mlčenlivosti (v min. rozsahu bodu 03 tohoto dokumentu) a to jak s vlastní personální agenturou, tak i s dodavatelem. Současně musí existovat smlouva o mlčenlivosti (v min. rozsahu bodu 03 tohoto dokumentu) mezi dodavatelem a personální agenturou.<br><br>**Způsob prokázání v případě fyzického auditu**:<br>Předložení konkrétní písemné dokumentace prokazující splnění daného požadavku (tj. zejména personální evidence).<br><br>**Způsob prokázání v případě vzdáleného auditu**:<br>Předložení konkrétní písemné dokumentace prokazující splnění daného požadavku (tj. zejména personální evidence) formou vzdáleného přístupu nebo zobrazením na sdílené obrazovce. |