

# **Pravidla kybernetické bezpečnosti**

## **ZKRATKY A ZNAČKY**

Níže uvedený seznam obsahuje zkratky a značky použité v tomto dokumentu. V seznamu se neuvádějí legislativní zkratky, zkratky a značky obecně známé, zavedené právními předpisy, uvedené v obrázcích, příkladech nebo tabulkách.

DSP Dokumentace pro stavební povolení

eDAP.....elektronická knihovna dokumentů a předpisů

IS SŽ .....informační systém Správy železnic, státní organizace

NÚKIB.....Národní úřad pro kybernetickou a informační bezpečnost

SŽ .....Správa železnic, státní organizace

ÚKB .....Úsek kybernetické bezpečnosti, Správa železniční telematiky

VoKB.....prováděcí vyhláška 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)

ZoKB.....zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů

## **VÝKLAD POJMŮ**

**Administrace řízení** – zajištění celého výběrového či zadávacího řízení, včetně vypracování zadávací dokumentace, zajištění procesních úkonů, zajištění splnění oznamovací povinnosti zadavatele, archivace veškeré související dokumentace apod. administrátorem nebo zpracovatelem.

**Akceptační řízení** – postupné provedení akceptačních procesů a podepsání Akceptačního/ch protokolu/ů pro část Plnění dle Smlouvy, spočívající v dodávce, vývoji, implementaci a/nebo servisu Informačního či komunikačního systému, nebo pokud má Plnění dopad na Informační či komunikační systém. Podkladem musí být Technická dokumentace.

**Bezpečnostní opatření** – rozumí se soubor opatření, která zajistí požadavky kybernetické bezpečnosti v souladu s požadavky vyplývající ze ZoKB, VoKB popřípadě z norem ISO/IEC 27000 nebo ČSN EN IEC 62443. (best practice) (např. standardy NIST).

**Dostupnost** - vlastnost přístupnosti a použitelnosti na žádost oprávněné entity.

**Důvěrnost** - vlastnost, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům.

**Objednatel** - je osoba, entita, v tomto případě SŽ, která udělala příkaz na dodávku zboží, služby nebo vykonání nějaké práce na, kterou zadává a specifikuje své požadavky.

**Hardware (HW)** - veškeré hmotné součásti počítačových systémů a veškeré související vybavení hmotné povahy spolu se vším příslušenstvím, a včetně veškeré související dokumentace.

**Informační systém Správy železnic, státní organizacei (IS SŽ)** - informační či komunikační systém kritické informační infrastruktury Objednatel ve smyslu § 2 b) ZOKB nebo jiný informační či komunikační systém, na který se vztahuje ZOKB.

**Integrita** - vlastnost přesnosti a úplnosti.

**Kybernetický bezpečnostní incident** - narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací podle § 7 ZoKB, v důsledku Kybernetické bezpečnostní události.

**Kybernetická bezpečnostní událost** - událost podle § 7 ZoKB, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.

**Maintenance** – modifikace produktu k nápravě chyb, zlepšení výkonu nebo jiných atributů.

**Multifaktorová autentizace** – ověřování uživatele pomocí dvou nebo více faktorů.

**Smlouva** – smlouva, uzavřená mezi Zhotovitelem a Objednatelem na základě zadávacího nebo výběrového řízení vedeného Objednatelem, jejíž součástí jsou Zvláštní technické podmínky, jichž je tato příloha součástí.

**Oprávněné entity** – je osoba nebo odborný orgán, který rozhoduje o přístupovém oprávnění do určitého fyzického místa či informačního nebo komunikačního systému.

**Odborný útvar** – je útvar GR nebo OJ na úrovni odboru (odbor, kancelář ředitele OJ, odborná správa).

**Penetrační testování** – je penetračním testováním myšleno jakékoliv zkoumání informačního/počítačového systému s cílem najít slabá místa (zranitelnosti) dodávaného řešení.

**Pododavatel** – fyzická osoba, podnikající fyzická osoba nebo právnická osoba vykonávající externě činnost pro SZ na základě platné smlouvy.

**Produkční prostředí** - představuje fázi vývojového cyklu, ve které je hotový software nebo aplikace nasazen do ostrého provozu a používán reálnými uživateli. Je navrženo tak, aby poskytovalo stabilní a spolehlivé podmínky pro běh softwaru, a to často na skutečných zařízeních, serverech nebo v cloudu. V produkčním prostředí jsou prováděny všechny operace a transakce, které jsou součástí běžného uživatelského prostoru. To zahrnuje interakci uživatelů s aplikací, zpracování dat, zajištění bezpečnosti a výkonu, monitorování a zálohování

**Provozovatel** - je osoba nebo entita, která je odpovědná za provoz a správu určitého systému, zařízení, služby nebo podniku.

**Provozní technologie (OT)** – systémy detekují nebo způsobují přímou změnu prostřednictvím monitorování a/nebo řízení zařízení, procesů a událostí. Mezi provozní technologie patří např.: systémy dohledového řízení a sběru dat (SCADA), průmyslové , řídicí systémy a obdobné specifické systémy , programovatelné logické automaty (PLC), počítačová numerická zařízení (CNC) apod.

**Plnění** - tvoří součást předmětu Smlouvy a k němuž se váže povinnost Dodavatele toto plnění Objednateli poskytnout. Plnění je blíže specifikované ve Smlouvě a jejich přílohách.

**Software (SW)** - znamená veškeré programové vybavení a další Autorská díla, stejně jako další věci či jiné majetkové hodnoty, které s programovým vybavením souvisí a jsou určeny ke společnému užívání s tímto programovým vybavením, tj. zejména databáze, GUI, zvukové nahrávky, videa, obrázky, fotografie apod., včetně veškeré související dokumentace a updatů a upgradů tohoto programového vybavení, avšak s výjimkou Hardwaru, pokud není Smlouvou stanoveno jinak.

**Testovací prostředí** - je speciálně připravené prostředí, které je vytvořeno pro testování softwaru před jeho nasazením do produkčního prostředí. Toto prostředí je navrženo tak, aby napodobovalo produkční prostředí co nejvíce, ale zároveň umožňovalo bezpečné testování a ladění kódu. Testovací prostředí může obsahovat různé komponenty, jako jsou databáze, servery, hardware a další aplikace, které jsou potřebné pro běh testovaného softwaru. Toto prostředí je izolováno od produkčního prostředí, aby se předešlo jakýmkoli problémům nebo škodám, které by mohly vzniknout v důsledku testování.

**Technická dokumentace** - část specifikace IS SZ, která představuje jednotlivé dokumenty popisující IS SZ a zacházení s ním. Mezi tyto dokumenty patří uživatelská dokumentace, administrátorská dokumentace, bezpečnostní dokumentace, provozní bezpečnostní dokumentace (popisuje nezbytné bezpečnostní funkce dodávaného systému např. způsob aktualizace, možnosti logování apod) či jakákoliv jiná dokumentace vytváření anebo poskytovaná Zhotovitelem v rámci dodávky, vývoje, implementace

a/nebo servisu IS SŽ. Technická dokumentace je dodávána pokud má Plnění dopad na IS SŽ. Dokumentace musí být vždy vyhotovena a předána Objednateli v elektronické podobě.

**Významný dodavatel** – je dodavatel, který má přímý přístup k informacím a aktivům SŽ, která jsou klasifikovaná jako Diskrétní anebo Vysoce diskrétní. Kritická integrita nebo kritická dostupnost dat a informací má přímý vliv na poskytované služby informačních a komunikačních technologií (dále jen „ICT“) nebo řídicí systémy SŽ.

**Zdrojový kód** – je základním stavebním prvkem softwaru a umožňuje programátorům vytvářet různé aplikace, programy a systémy. Slouží jako lidsky čitelný zápis algoritmů a funkčnosti, kterou má program plnit. Zdrojový kód obsahuje deklarace proměnných, pokyny, funkce, smyčky a další příkazy, které programu říkají, jak má fungovat

**Zhotovitel – Dodavatel osoba, která nabízí poskytnutí dodávek, služeb či stavebních prací nebo i více těchto osob společně.**

**Zranitelnost** - úmyslná chyba nebo neúmyslný nedostatek či závada v software obecně nebo ve firmware zařízení komunikační infrastruktury, která může být zneužita potenciálním útočníkem pro škodlivou činnost. Tyto zranitelnosti jsou buď známé a publikované, ale výrobcem ještě neošetřené nebo skryté a neobjevené. V případě skrytých zranitelností je důležité, zda je objeví dříve útočník, výrobce, bezpečnostní analytik, či uživatel. Zranitelnosti jsou proto potenciálními hrozbami. Zranitelnosti lze eliminovat důsledným bezpečnostním záplatováním systémů.

**Zpracovatel** – příslušný odborný útvar, který administruje zadávací nebo výběrové řízení.

**ZZVZ** - zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů

**Vada** – v rámci tohoto pokynu je tím myšleno jeho nedodržení jako takové, nepředání technické dokumentace, dále pak nedostatky odhalené pomocí penetračního testování. Ty musí být opraveny před převzetím díla.

## **1 OBECNÉ POŽADAVKY**

1.1 Zhotovitel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:

1.1.1 Dodržovat požadavky vyplývající ze ZoKB a VoKB.

1.1.2 Nestanoví-li dohoda stran jinak, Zhotovitel jmenuje nejpozději do 15 dnů po uzavření Smlouvy odpovědnou kontaktní osobu pro potřeby zajištění plnění Bezpečnostních opatření vyplývajících ze Smlouvy (dále jen „Kontaktní osoba“). Kontaktní osobu sdělí Zhotovitel Objednateli písemně vtěže lhůtě. Případnou změnu Kontaktní osoby na straně Zhotovitele je Zhotovitel povinen Objednateli oznámit do 5 dnů od provedení změny.

1.1.3 Zajistit, aby Kontaktní osoba Zhotovitele nejpozději do 30 dnů od uzavření Smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování plnění, týkajícího se Informačního či komunikačního systému, této Smlouvy za Zhotovitele a/nebo jeho poddodavatelé byli prokazatelně seznámeni s tímto Pokynem.

1.1.4 Zajistit, aby předmět Plnění nebyl nevyhovující z hlediska informační bezpečnosti, přičemž za nevyhovující je považováno jakékoli plnění, které obsahuje technologie nebo klíčové prvky, vůči jejichž výrobcům příslušný správní orgán vydal opatření v souladu se ZoKB, a které dle analýzy rizik představují vysoké riziko.

1.1.5 Dodržovat příslušná ustanovení bezpečnostních politik, metodik a postupů Objednatele, resp. platné řídicí dokumentace Objednatele či její části, které jsou relevantní k předmětu plnění, pokud byl Zhotovitel s takovými dokumenty nebo jejich částmi seznámen, a to bez ohledu na způsob, jakým byl stakovou dokumentací Objednatele prokazatelně seznámen.

1.1.6 Provádět analýzu a hodnocení rizik předmětu Plnění Smlouvy, týkajícího se Informačního či komunikačního systému a na základě výsledků navrhopat a předkládat Objednateli ke schválení opatření na minimalizaci nebo odstranění zjištěných rizik. Jako vzorovou analýzu a hodnocení rizik lze využít podpůrný materiál, který vydal NÚKIB a který vychází z VoKB.

1.1.7 Pokud je technicky možné, zavést opatření pro ochranu zálohy dat a konfigurace systému, vztahujícího se k Informačnímu či komunikačnímu systému, který je součástí Plnění Smlouvy a pravidelně testovat funkčnost těchto záloh.

1.1.8 Zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost.

1.1.9 Dodávat Technickou dokumentaci.

1.1.10 Zajistit, aby dodávané řešení obsahovalo jen ty součásti, které jsou objektivně potřebné pro řádné provozování dodávaného Informačního či komunikačního systému a/nebo které jsou specifikovány výslovně ve Smlouvě, zejména, že SW ani HW nebude obsahovat žádné nepotřebné komponenty, které nejsou nezbytné pro provoz systému.

1.1.11 Zajistit, aby veškeré informace vyžadující vyšší míru ochrany<sup>1</sup> poskytnuté Objednatelům při poskytování plnění nebyly uchovávány v nešifrovaném tvaru a byly chráněny vůči neautorizovanému přístupu, pokud nebude mezi smluvními stranami v konkrétním případě dohodnuto jinak.

1.1.12 Provést před spuštěním systému v produkčním prostředí IS SŽ kontrolu souladu s bezpečnostními požadavky hardeningových bezpečnostních politik (best practice) a v případě zjištění nesouladu zajistit bez zbytečného odkladu nápravu.

1.1.13 Instalovat nový systém nebo nové verze systému pouze na základě Objednatelům předem schválených migračních postupů<sup>2</sup>.

1.1.14 Vytvořit seznam dodávaných součástí, verze jejich firmware a dále software verzi vztahených k životnímu cyklu produktů (Asset management).

1.1.15 Zhotovitel bere na vědomí, že veškerá jeho aktivita a jeho plnění realizované v systémovém prostředí Objednatelů budou Objednatelům průběžně a pravidelně monitorovány a vyhodnocovány s ohledem na obsah Smlouvy a interních dokumentů Objednatelů, se kterými byl Zhotovitel seznámen.

## **2 FYZICKÁ OCHRANA A BEZPEČNOST PROSTŘEDÍ**

2.1 Zhotovitel se zavazuje dodržovat opatření fyzické ochrany v objektech a prostorách Objednatelů (např. Provozní řád objektu), zejména pak v místech, ve kterých jsou umístěny komponenty IS SŽ anebo datové nosiče (dále také "Pracoviště").

2.2 V případě, že některé služby nebo procesy, které se vztahují k předmětu plnění, budou umístěny v prostorech Zhotovitele musí být požadavky fyzické ochrany zajištěny obdobně jako v bodě 2.1.

2.3 Zhotovitel se zavazuje, že na Pracovišti neponechá volně dostupná instalační, záložní nebo archivní média ani dokumentaci k systému IS SŽ, který je předmětem plnění Smlouvy.

2.4 Zhotovitel musí zajistit ochranu řadičů pomocí mechanických zábranných systémů (úroveň dle standardů ČSN P CEN/TS 14383) tak, aby nemohlo dojít k neautorizovaným zásahům v dodávaných systémech.

## **3 ŘÍZENÍ PŘÍSTUPU A PŘÍSTUP ZHOTOVITELE K TECHNOLOGIÍ**

3.1 Práce Zhotovitele v souvislosti s instalací, konfigurací, modifikací, správou licencí a údržbou dodávaného i stávajícího hardwarového a softwarového vybavení bude probíhat na technických prostředcích (např. PC, notebook, Jumpserver atp.) v majetku Objednatelů, metodou a způsobem práce, který stanoví Objednatel. Takto stanovené metody a způsob práce jsou pro Zhotovitele závazné po celou dobu plnění zakázky.

---

<sup>1</sup> Za důvěrné informace vyžadující vyšší míru ochrany se ve smyslu této přílohy považují zejména identifikační údaje certifikátu, hesla, přístupová oprávnění, konfigurační soubory, systémové programy, kritické knihovny, obnovovací procedury apod.

<sup>2</sup> Migrační postup – soubor kroků definující převod dat mezi dvěma nebo více systémy IS SŽ

3.2 V případě, že součástí plnění je přístup zaměstnanců SŽ k externím webovým službám, musí být dodrženy následující požadavky:

- Přihlašovací údaje nesmí být uloženy v čitelné podobě, ale musí být chráněny kryptografickými prostředky doporučenými NÚKIBem.
- Systém, ke kterému zaměstnanci SŽ přistupují, musí být pravidelně testován, aktualizován a být dostatečně odolný tak, aby byla zajištěna bezpečnost informací a dat.

3.3 Objednatel si vyhrazuje možnost provedení pravidelného penetračního testování nebo testování zranitelností v průběhu trvání Smlouvy. Zhotovitel je povinen neprodleně přijmout dodatečná, účinná nápravná opatření k odstranění kritických zranitelností, které byly zjištěny v průběhu penetračního testování předmětu plnění.

3.4 Při realizaci penetračního testování nebo testování zranitelností řešení, poskytne Zhotovitel Objednateli veškerou potřebnou součinnost.

3.5 V případě, že výsledkem penetračního testování nebo testování zranitelností jsou kritická zjištění zranitelností, je Zhotovitel povinen neprodleně informovat Objednatele o těchto skutečnostech a přijmout dodatečná, účinná nápravná opatření.

3.6 Zhotovitel bere na vědomí, že přístup k IS SŽ je možné povolit pouze fyzické identitě zaměstnance Zhotovitele (popřípadě Poddodavatele), zaevidované v registru identit Objednatele, a to na základě požadavku Zhotovitele na přístup.

3.7 Zhotovitel bere na vědomí, že jeho zaměstnanec musí poskytnout své osobní údaje Objednateli, a to v rozsahu nutném pro zřízení přístupu. Zaměstnanec Zhotovitele s přiděleným přístupem (fyzickým, logickým) k systému IS SŽ, bere na vědomí, že dochází ke zpracování osobních údajů, a to po dobu nezbytně nutnou pro plnění smlouvy, během vyhodnocování údajů o pohybu a prováděných aktivitách v prostorách Objednatele (např.: monitoring pomocí řešení Security Information and Event Management).

3.8 Zhotovitel bere na vědomí, že přidělení oprávnění zaměstnanci Zhotovitele musí být řízeno principem nezbytného minima a není nárokové.

3.9 Zhotovitel se zavazuje, že udělený přístup nesmí být sdílen více zaměstnanci Zhotovitele nebo Poddodavatele.

3.10 Zhotovitel se zavazuje, že vzdálený přístup do IS SŽ bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN s využitím multifaktorové autentizace.

3.11 Zhotovitel se zavazuje, že před připojením koncového zařízení, mobilního koncového zařízení nebo aktivního síťového prvku jako síťové switche, Wi-Fi access pointy, routery či huby do počítačové sítě zažádá o schválení připojení kontaktní osobu na straně Objednatele.

3.12 Zhotovitel se zavazuje, že bez zbytečného odkladu deaktivuje všechny nevyužívané zakončení sítě anebo nepoužívané porty aktivního síťového prvku.

3.13 Zhotovitel se zavazuje, že nebude instalovat a používat zejména typy nástrojů Keylogger, Sniffer, Analyzátor zranitelností a Port Scanner, Backdoor, rootkit a trojský kůň nebo jinou podobu malware.

3.14 Zhotovitel se zavazuje, že všechny jeho informační systémy, které se připojují do síťové infrastruktury Objednatele – jsou a budou chráněny, v reálném čase, proti malware.

3.15 Zhotovitel se zavazuje, že nebude vyvíjet, kompilovat a šířit v jakékoliv části systému IS SŽ programový kód, který má za cíl nelegální ovládnutí, narušení, nebo diskreditaci systému IS SŽ nebo nelegální získání dat a informací.

3.16 Zhotovitel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli v IS SŽ:

- a) Neukládaly, nesdílely, data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele.
- b) Nestahovaly, nesdílely, neukládaly, nearchivovaly a/nebo neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.
- c) Nezasílaly řetězové emaily.

3.17 Zhotovitel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě nebo IS SŽ Objednatele měly v externím zařízení typu notebook/počítač aplikovány bezpečnostní záplaty a nainstalovanou, spuštěnou a pravidelně aktualizovanou antivirovou ochranu.

3.18 Zhotovitel se zavazuje zajistit, aby osoby podílející se na poskytování plnění Objednateli, kteří přistupují do interní sítě a/nebo systému IS SŽ Objednatele, chránily autentizační prostředky a údaje k systémům IS SŽ Objednatele.

3.19 Zhotovitel bere na vědomí, že v případě neúspěšných pokusů autentizaci uživatele může být příslušný účet zablokován a řešen jako kybernetická bezpečnostní událost a mohou být uplatněny příslušné postupy zvládání kybernetické bezpečnostní události (např. okamžité zrušení přístupu k informačním aktivům fyzických osob externího subjektu).

3.20 Zhotovitel bere na vědomí, že postup zvládáním kybernetické bezpečnostní události či jiný důsledek porušení Bezpečnostních opatření nebude posuzován jako okolnost vylučující odpovědnost Zhotovitele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Zhotovitel či jiné osobě ze strany Objednatele.

3.21 Zhotovitel nesmí ponechat v dodávaných systémech tovární přístupová hesla.

3.22 Dodávané řešení musí využívat nástroj pro centrální správu přístupových účtů.

3.23 Dodávané řešení musí využívat procesy pro ověřování identity uživatelů a administrátorů, která je založena na autentizačním mechanismu využívajícího multifaktorovou autentizaci s nejméně dvěma různými typy faktorů.

3.24 Dodávané řešení přidělí každému uživateli a administrátorovi přístupujícímu k IS SŽ přístupová práva i oprávnění a jedinečný identifikátor.

3.25 Přístupová oprávnění musí být šifrována pomocí silných kryptografických prostředků doporučených NÚKIBem.

3.26 Body 3.1 – 3.25 jsou přiměřeně plněny podle toho, zda se jedná o Informační a komunikační technologii a nebo Provozní technologii.

## **4 PŘEDÁNÍ A PŘEVZETÍ PLNĚNÍ**

4.1 Zhotovitel bere na vědomí, že nedodržení Bezpečnostních opatření Objednatele, včetně požadavku na předání kompletní Technické dokumentace, je Vadou bránící převzetí předmětu Smlouvy, přičemž Objednatel není do doby odstranění příslušné Vady plnění povinen dané plnění převzít.

4.2 Vadou bránící převzetí plnění jsou i kritické zranitelnosti zjištěné při penetračním nebo akceptačním testování.

4.3 Zhotovitel odpovídá za to, že systémy dodávané do IS SŽ budou obsahovat nejnovější, stabilní, bezpečné a řádně odzkoušené bezpečnostní aktualizace (patche).

## **5 VÝMĚNA INFORMACÍ**

5.1 Zhotovitel se zavazuje, že veškerý přenos dat a informací musí být dostatečně zabezpečen pomocí aktuálně odolných kryptografických algoritmů a kryptografických klíčů.

5.2 Zhotovitel se zavazuje, že on-line transakce realizované prostřednictvím webových technologií budou chráněny SSL certifikáty.

## **6 PODDODAVATELÉ**

6.1 Zhotovitel nezapojí do poskytování plnění dle Smlouvy žádného dalšího Poddodavatele bez předchozího souhlasu Objednatele.

6.2 Zhotovitel se zavazuje, že se bude řídit požadavky Objednatele na řízení bezpečnosti informací a poskytne Objednateli veškerou nezbytnou součinnost v otázkách řízení bezpečnosti informací a pokud využívá při poskytování plnění Poddodavatele, zajistí, že bude Objednateli poskytnuta veškerá nezbytná součinnost v otázkách řízení bezpečnosti informací také od těchto Poddodavatelů.

6.3 Pokud Zhotovitel využívá za účelem plnění předmětu Smlouvy Poddodavatele, musí být tomuto Poddodavateli uloženy na základě smlouvy se Zhotovitelem stejné povinnosti k dodržování smluvních ujednání, jaká jsou sjednaná touto Přílohou mezi Objednatelem a Zhotovitelem.

## **7 LIKVIDACE DAT**

7.1 Pokud v rámci plnění předmětu Smlouvy má Zhotovitel povinnost k mazání dat a k likvidaci technických nosičů a/nebo provozních údajů a/nebo informací a jejich kopií, postupuje vždy v souladu s pokyny Objednatele. V případě, že Objednatel nepožaduje specifickou likvidaci, je Zhotovitel povinen při likvidaci postupovat v souladu s VoKB.



7.2 Objednatel stanovuje, že příslušným způsobem likvidace technických nosičů a/nebo provozních údajů a/nebo informací a jejich kopií v rámci plnění předmětu Smlouvy může být, v souladu s Vyhláškou, odstranění, přepsání či fyzická likvidace nosiče informace.

## **8 KONTROLA A AUDIT ZHOTOVITELE**

8.1 Toto ustanovení se zároveň použije přiměřeně po dobu trvání smluvního vztahu v případě, že bude navazovat servisní smlouvou.

8.2 Zhotovitel je povinen Objednateli zpřístupnit veškerou potřebnou dokumentaci pro účely kontroly či auditu, zejména výčet technických a organizačních opatření.

8.3 Zhotovitel má povinnost určit svého zástupce (případně své zástupce), který bude po dobu provádění kontroly či auditu přítomen.

8.4 Kontrola nebo audit mohou být provedeny v prostorách Zhotovitele nebo jeho Poddodavatele a Zhotovitel má povinnost tyto kontroly nebo audity Objednateli či Objednatelem pověřené osobě umožnit či možnost jejich provedení v prostorách poddodavatele zajistit, přispět k nim a poskytnout Objednateli (či Objednatelem pověřené osobě) k jejich provedení maximální možnou součinnost, kterou lze po Zhotoviteli rozumně požadovat. Počet a frekvence kontrol ani auditů nejsou nijak omezeny.

8.5 Objednatel má povinnost písemně oznámit Zhotoviteli provedení kontroly či auditu, a to nejméně 14 dnů před provedením kontroly či auditu. Součástí oznámení bude i seznam osob, které jsou pověřeni ze strany Objednatele k provedení kontroly či auditu.

8.6 Výstupem provedené kontroly či auditu je auditní zpráva; s jejími výsledky bude Zhotovitel seznámen a může se k nim vyjádřit.

8.7 Body 8.2 až 8.6 se neuplatní v případě, že Zhotovitel provádí pravidelné audity dodržování bezpečnostních požadavků uvedených v tomto pokynu, alespoň v ročních intervalech. Zhotovitel neprodleně informuje Objednatele v případě vysokého rizika nebo Zhotovitel předloží, na vyžádání, výsledky auditu.

8.8 Zhotovitel je dále povinen umožnit provedení kontroly či auditu i ze strany dozorových orgánů.

8.9 Zhotovitel se zavazuje poskytnout Objednateli veškeré informace potřebné k doložení toho, že byly splněny povinnosti vyplývající z tohoto pokynu, jakož i ZoKB a VoKB, a za tímto účelem se zavazuje umožnit Objednateli provedení kontrol, včetně auditů prováděných Objednatelem či auditorem, kterého Objednatel k auditu pověří, a poskytne k těmto kontrolám a auditům veškerou potřebnou součinnost.

## **9 OCHRANA DŮVĚRNÝCH INFORMACÍ**

9.1 Strany se zavazují zachovat mlčenlivost o veškerých informacích, osobních údajích, datech či zprávách, o nichž se dozvěděly v souvislosti s přípravou či plněním této Smlouvy (dále jen „důvěrné informace“), a to včetně předmětu Smlouvy, vlastní spolupráce a vnitřních záležitostí Stran.

9.2 Důvěrné informace ve smyslu tohoto pokynu nepředstavují utajované informace klasifikované stupněm „důvěrné“ ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

9.3 Strany se zavazují, že zajistí, aby se všechny osoby oprávněné zpracovávat důvěrné informace zavázaly k mlčenlivosti, nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti. Závazek mlčenlivosti a ochrany důvěrných informací zůstává v platnosti i po ukončení této Smlouvy.

## **10 POVINNOSTI PŘI UKONČENÍ SMLOUVY**

10.1 Zhotovitel se zavazuje poskytnout Objednateli veškerou potřebnou součinnost, dokumentaci a informace, účastnit se jednání s Objednatelem a popřípadě třetími osobami za účelem plynulého a řádného převedení všech činností spojených s provozem, maintenance a rozvojem předmětu Smlouvy na Objednatele a/nebo nového dodavatele, ke kterému dojde po skončení účinnosti Smlouvy, a to vše dle pokynů Objednatele (dále jen „Ukončení smlouvy“).

10.2 Zhotovitel se zavazuje za tímto účelem vypracovat a nejpozději spolu s provozní dokumentací ke každému předávanému dílčímu plnění předat Objednateli dokumentaci, která bude stanovovat postup při Ukončení smlouvy (dále jen „Plán“). Zhotovitel se zavazuje Plán po dobu trvání Smlouvy průběžně aktualizovat a Objednateli vždy při změně jakékoliv skutečnosti uvedené v Plánu předat aktualizovanou verzi Plánu zohledňující tuto změnu.

10.3 Zhotovitel je povinen poskytnout plnění nezbytná k realizaci tohoto Plánu za přiměřeného použití vhodných ustanovení Smlouvy. Závazek dle tohoto ustanovení platí i po ukončení Smlouvy.

10.4 Strany se dohodly, že cena za vypracování Plánu a poskytnutí plnění nezbytného k realizaci Plánu je součástí ceny dle Smlouvy.

## **Provozní technologie (OT)**

### **A.1 PROVOZNÍ TECHNOLOGIE (OT)**

12.1 Zhotovitel se při poskytování plnění pro Objednatele zavazuje plnit následující povinnosti:

12.1.1 Postupovat v souladu s platnými právními předpisy, zejména pak v souladu s požadavky vyplývajícími z požadavků souboru norem ČSN EN IEC 62443.

12.1.2 Provádět analýzu a hodnocení rizik Předmětu plnění a na základě výsledků navrhopvat Objednateli změny za účelem minimalizace dopadů identifikovaných rizik.

Realizovat bezpečnostní opatření v souladu s ČSN EN IEC 62443 Normou za účelem ochrany dat a informací vztahujícího se k Informačnímu či komunikačnímu systému, který je součástí Plnění Smlouvy.

### **A.2 PENETRAČNÍ TESTOVÁNÍ**

S výsledky penetračního testování mohou být seznámeny výhradně pověřené osoby Zhotovitele a Objednatele.

### **A.3 ZVLÁDÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ**

A.3.1 Zhotovitel má povinnost neprodleně informovat Objednatele o kybernetických bezpečnostních incidentech (došlo k narušení bezpečnosti informací), souvisejících s plněním předmětu Smlouvy (telefonicky na linku +420 972 235 333 a/nebo písemně na soc@spravazeleznice.cz). Součástí oznámení musí být popis povahy případu kybernetického bezpečnostního incidentu.

A.3.2 Pokud dojde ke kybernetické bezpečnostní události, popřípadě ke kybernetickému bezpečnostnímu incidentu, poskytne Zhotovitel požadovanou součinnost např.: poskytne logy a identifikační údaje (např. IP adresa, MAC adresa, HW typ, sériové číslo případně IMEI) dotyčného koncového zařízení nebo mobilního koncového zařízení k analýze obsahu, případně bez zbytečného odkladu zrealizuje opatření požadovaná Objednatelem).

### **A.4 ZRANITELNOSTI**

A.4.1 Zhotovitel do termínu stanoveného Objednatelem/ÚKB odstraní všechny relevantní zranitelnosti, které se vztahují k předmětu plnění smlouvy a které mají hodnocení Common Vulnerabilities and Exposures (CVE) stejné nebo vyšší než 8.0.

A.4.2 Detekované technické zranitelnosti musí být Zhotovitelem vyhodnoceny s ohledem na související riziko a musí podle povahy předmětu plnění dojít k nápravným opatřením ze strany Zhotovitele.

## **A.5 OPRAVNĚNÍ UŽÍVAT DATA**

- A.5.1 Zhotovitel je při poskytování plnění pro Objednatele oprávněn užívat data/informace předaná Zhotoviteli Objednatelem za účelem plnění předmětu Smlouvy, avšak vždy pouze v rozsahu nezbytném ke splnění předmětu Smlouvy.
- A.5.2 Zhotovitel se při poskytování plnění pro Objednatele zavazuje nakládat s daty pouze v souladu se Smlouvou a příslušnými právními předpisy.

## **A.6 ZDROJOVÝ KÓD A DOKUMENTACE**

- A.6.1 Zdrojový kód bude předáván Objednateli na datovém nosiči vždy na konci Akceptačního řízení, nebo za podmínek stanovených ve Smlouvě, zejména pokud bude smluvní vztah ukončen bez provedení Akceptačního řízení.
- A.6.2 Na datovém nosiči dat musí být viditelně označen „Zdrojový kód“ s označením části Modifikace a jeho verze a den předání Zdrojového kódu. O předání nosiče dat bude oběma Smluvními stranami sepsán a podepsán písemný předávací protokol.
- A.6.3 Povinnost Zhotovitele předávat Zdrojový kód se obdobně použije i pro jakékoliv opravy, změny, doplnění, upgrade nebo update Zdrojového kódu v rámci následného provádění Plnění anebo v rámci záručních oprav. Zdrojový kód musí obsahovat podrobný popis a komentář každého zásahu do Zdrojového kódu.
- A.6.4 Objednatel nebude v průběhu provádění Plnění sám anebo prostřednictvím jiných osob zasahovat do Zdrojového kódu nasazeného anebo fungujícího v Produkčním prostředí či Testovacím prostředí.
- A.6.5 Zhotovitel je povinen předat Objednateli příslušnou Dokumentaci a Zdrojový kód ve standardní podobě (to nejméně v kvalitě obvyklé pro open source projekty), vždy obsahující následující:
- A.6.5.1 Kompletní Zdrojové kódy celého díla.
- A.6.5.2 Administrátorskou příručku, popisující všechny parametry, které lze konfigurovat a popis dopadů změny konfigurace do systému.
- A.6.5.3 Technickou dokumentaci systému, pakliže se jedná o vícevrstvou architekturu, popis každé vrstvy zvlášť:
- (i) Datová vrstva – popis datové vrstvy, tj. tabulek v databázi včetně vazeb mezi tabulkami a včetně E-R schémat.
  - (ii) Aplikační vrstva – popis jádra systému, jeho funkcí, služeb a rozhraní. Technická dokumentace musí obsahovat kompletní popis architektury jádra systému, výčet a podrobný popis všech jeho funkcí, přehled a popis služeb, které jádro poskytuje dalším komponentám systému, modulům a knihovnám.
  - (iii) Prezentační vrstva – Technická dokumentace systému musí obsahovat drátové modely všech obrazovek uživatelského rozhraní včetně popisu funkcí prvků každé obrazovky.
- A.6.5.4 Popis konfigurace provozního prostředí systému (serverová strana i klientská strana).
- A.6.5.5 Technická dokumentace musí obsahovat soupis všech požadavků na nastavení hardwarových a softwarových komponent běhového prostředí jako jsou:
- (i) Mapování souborových systémů.

- (ii) Požadavky na operační paměť a procesory.
- (iii) Konfigurační parametry jednotlivých podpůrných Softwarových prostředků (např. specifika pro nastavení databáze, aplikačního serveru, webového serveru apod.).

A.6.5.6 Objednatel požaduje, aby tato Technická dokumentace byla ve formátech XML DocBook (zdrojové) a PDF (export z XML zdroje pro snadnou distribuci uživatelům) nebo případně v jiném formátu, který Objednatel schválí po vzájemné dohodě se Zhotovitelem. Všechny Technické dokumentace musí být označené verzí, opatřené seznamem autorů, přehledem změn jednotlivých verzí a musí být obsahově úplné pro tu část systému, kterou popisují.

A.6.6 V případě jakýchkoli pochybností o správnosti předání Zdrojového kódu se bude uvedené posuzovat podle svého účelu, tedy zejména následné možnosti provádět samostatně či prostřednictvím třetích osob opravy, změny, doplnění, upgrady nebo updaty Zdrojového kódu. Za nesprávné předání se přitom považuje takové předání, které v důsledku vede ke znemožnění či podstatnému ztížení práce se Zdrojovým kódem ve výše uvedeném smyslu.

## **A.7 ŘÍZENÍ ZMĚN**

A.7.1 Zhotovitel má povinnost přijmout účinná opatření ke snížení nepříznivých dopadů při zavádění změn.

A.7.2 Zhotovitel se zavazuje poskytnout Objednateli veškerou nezbytnou součinnost při analýze souvisejících rizik, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci Technické dokumentace, souvisejícím testováním a zajištění možnosti navrácení do původního stavu.

A.7.3 V případě realizace penetračního testování nebo testování zranitelnosti, které je v souladu s VoKB dodávaného řešení, poskytne Zhotovitel Objednateli veškerou potřebnou součinnost. Zhotovitel je povinen přijmout dodatečná účinná nápravná opatření kodstranění zranitelností, které byly zjištěny v průběhu penetračního testování.

## **A.8 AKTUALIZACE SW**

A.8.1 Pokud bude Zhotovitel v rámci poskytovaného předmětu plnění (dále také „Dodávané řešení“) provádět instalaci nebo aktualizaci SW, bude postupovat podle hardeningových bezpečnostních politik, které jsou určeny standardem Center for Internet Security (CIS) level (group) 1, dostupné z <https://www.cisecurity.org>, a v souladu s interními bezpečnostními standardy Objednatele a dále s dokumentem Platforma 2.0.

A.8.2 Zhotovitel odpovídá za to, že systémy dodávané do IS SŽ budou obsahovat nejnovější, stabilní, bezpečné a řádně odzkoušené bezpečnostní aktualizace (patche).

A.8.3 Veškerý SW musí splňovat požadavek na podporu od výrobce (podporovaný build).

## **A.9 INVENTARIZACE A KONTROLA HARDWAROVÝCH AKTIV**

A.9.1 Zhotovitel předá aktuální záznam veškerého uvedeného inventáře instalovaných aktiv OT, včetně aktuálních informací o fyzickém umístění zařízení, IP adresy, MAC adresy, modelového názvu zařízení, sériového čísla produktu, verzi FW řadiče, verzi SW, datum posledních provedených změn na zařízení včetně konkrétní informace o provedené změně.

## **A.10      ŘÍZENÍ KONTINUITY ČINNOSTÍ**

- A.10.1      Objednatel má oprávnění, pokud je s ním uzavřena servisní smlouva, zapojit Zhotovitele do řízení kontinuity činností, a to zejména oprávnění k zahrnutí Zhotovitele do plánu kontinuity činností, který souvisí s předmětem plnění a souvisejících služeb a/nebo zahrnutí Zhotovitele do havarijního plánu Objednatele.
- A.10.2      Objednatel má povinnost informovat Zhotovitele o způsobu zapojení dle čl. 20. 1.
- A.10.3      Zhotovitel předloží Objednateli příslušnou dokumentaci ohledně zálohování a obnovy dat v rozsahu, jak ji stanovuje VoKB.
- A.10.4      Musí být prováděno v souladu se směrnicí SŽ SM094 – Směrnice ve věci systému řízení kontinuity procesů ve státní organizaci Správa železnic