České dráhy

Bezpečnostní pravidla pro dodavatele v rámci systému řízení bezpečnosti informací

OBSAH

ČÁST PRVNÍ – ZÁKLADNÍ USTANOVENÍ
KAPITOLA I – ÚVODNÍ USTANOVENÍ

1. Cílem tohoto dokumentu je stanovení povinností a odpovědností dodavatelů ke snižování kybernetických rizik a zvyšování účinnosti bezpečnostních opatření chránících aktiva společnosti České dráhy, a.s. (dále jen „**ČD**“), ke kterým mají přístup dodavatelé dle ustanovení § 4 odstavce 4 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, v platném znění, (dále jen „**zákon o kybernetické bezpečnosti**“), resp. s účinností od 1.11.2025 ustanovení § 13 odst. 5 zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „**zákon**“), ve spojení s § 8 odstavce 1 a) vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (dále jen „**vyhláška o kybernetické bezpečnosti**“) resp. s účinností od 1.11.2025 ve spojení s § 9 odst. 1 písm. a) vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „**vyhláška**“). Níže uvedený text navazuje zejména na relevantní aktuální legislativu účinnou od 1.11.2025.

2. Dodavatel dle výše uvedeného bodu (dále jen „**Dodavatel**“) bere na vědomí, že ČD má zaveden systém řízení bezpečnosti informací a je zároveň povinnou osobou dle § 3 písm. f) zákona o kybernetické bezpečnosti, resp. poskytovatelem regulované služby v režimu vyšších povinností dle § 4 odst. 1 písm. a) body 2. a 8. ve spojení s § 8 odst. 1 zákona a vyhlášky č. 408/2025 Sb., o regulovaných službách, a je povinen naplnit požadavky tohoto zákona a související legislativy.

3. Dodavatel musí při plnění smluvního vztahu (dále jen „**předmět plnění**“) pro ČD dodržovat níže uvedená pravidla (dále také jako „**bezpečnostní pravidla**“). Pokud jsou tato obecná bezpečnostní pravidla v rozporu s ustanovením smlouvy uzavírané mezi Dodavatelem a ČD nebo zadávací dokumentací na veřejnou zakázku či jejich jinou přílohou nebo bezpečnostní politikou ČD předanou Dodavateli, má přednost ustanovení smlouvy, zadávací dokumentace nebo jejich jiná příloha nebo bezpečnostní politika.

ČÁST DRUHÁ – BEZPEČNOSTNÍ PRAVIDLA PRO DODAVATELE
KAPITOLA II – SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

1. Dodavatel je v rozsahu předmětu plnění povinen:

   1.1. aktivně se podílet na dodržování, provozu a rozvoji bezpečnostních opatření ČD;

   1.2. postupovat v souladu s platnými a účinnými právními předpisy, zejména pak v souladu s požadavky vyplývajícími pro ČD, jakožto provozovatele regulované služby v režimu vyšších povinností, ze zákona a vyhlášky a reflektovat případné novely uvedených právních předpisů či novou právní úpravu;

   1.3. plnit své řešení/dodávku/správu tak, aby respektovalo požadavky na bezpečnost ČD, zabránilo kybernetickým bezpečnostním incidentům a krizovým situacím a odpovídat za dodávku a implementaci řešení v požadované kvalitě i z pohledu bezpečnosti;

   1.4. vytvořit a schválit bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Dodavatele při poskytování předmětu plnění, a to v případě, že Dodavatel dosud nemá zaveden systém řízení bezpečnosti informací (SŘBI) a/nebo bezpečnostní politiku pokrývající předmět plnění. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací;

1.5. stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky;

1.6. prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Dodavatele při poskytování předmětu plnění a vést záznamy o vytváření a zpracování těchto dat;

1.7. řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění a provádět analýzu a hodnocení rizik informační infrastruktury, která je součástí předmětu dodávaného řešení a na základě výsledků navrhovat a předkládat ČD ke schválení opatření na minimalizaci nebo odstranění zjištěných rizik;

1.8. zavést na základě bezpečnostních potřeb a výsledků hodnocení rizik příslušná bezpečnostní opatření v rozsahu poskytovaného předmětu plnění, monitorovat je a vyhodnocovat jejich účinnost;

1.9. zajistit adekvátní dodržování těchto bezpečnostních pravidel rovněž se svými poddodavateli;

1.10. zabezpečit veškerý přenos dat a informací z pohledu bezpečnostních požadavků na jejich důvěrnost, integritu a dostupnost během poskytování plnění pro ČD minimálně dle vyhlášky či jiným interním řídícím aktem ČD (pokud byl poskytnut). Přičemž, pokud není určena klasifikace aktiva, bude použit způsob pro úroveň aktiva – kritická;

1.11. trvale zachovat mlčenlivost všech svých pracovníků i po ukončení smluvního vztahu s ČD;

1.12. podepsat závazek mlčenlivosti (tj. podpisu NDA – Non Disclosure Agreement) před vlastním přístupem k datům a informacím ČD.

KAPITOLA III – PROVÁDĚNÍ AUDITU KYBERNETICKÉ BEZPEČNOSTI

1. Dodavatel je povinen ČD umožnit provedení zákaznického auditu kybernetické bezpečnosti u Dodavatele v rozsahu kontroly zajištění plnění požadavků ČD dle smlouvy a těchto bezpečnostních pravidel vč. zejména kontroly způsobu plnění dohodnutých bezpečnostních opatření (dále jen „**Audit**“).

2. ČD oznámí konání Auditu nejpozději 30 dnů předem (s výjimkou uvedenou dále v tomto bodě), přičemž uvede nejméně složení auditního týmu a v jakém rozsahu bude Audit proveden. V případě kybernetického bezpečnostního incidentu nebo jiné mimořádné situace je ČD oprávněna provést Audit kdykoliv (mimo plán Auditů), přičemž termín pro konání auditu oznámí Dodavateli nejpozději 10 dní předem.

3. Dodavatel je povinen poskytnout ČD k provedení Auditu nezbytnou součinnost (např. umožní a zajistí přístup do prostor).

4. Audit může za ČD provést pověřený zaměstnanec ČD nebo jiná pověřená osoba. ČD je oprávněna pověřit provedením Auditu třetí stranu.

5. Zjistí-li ČD v rámci Auditu jakákoliv pochybení či nedostatky, Dodavatel se zavazuje vyvinout veškerou součinnost ke sjednání nápravy dle návrhu ČD a v přiměřené lhůtě.

6. Dodavatel je povinen ČD zpřístupnit veškerou potřebnou dokumentaci pro účely Auditu a je povinen určit svého zástupce, který bude po dobu provádění Auditu přítomen.

7. Dodavatel je povinen umožnit provedení Auditu ze strany dozorových orgánů. Dodavatel je povinen umožnit provedení Auditu u svých případných významných poddodavatelů, a to ze strany ČD i dozorových orgánů, a to ve lhůtách stanovených v bodě 2 této kapitoly.

KAPITOLA IV – ZAJIŠTĚNÍ SOULADU S PCI DSS

1. Pokud se předmět plnění Dodavatele týká informačních systémů, sítí, aplikací, infrastruktury nebo jiných aktiv ČD, která jsou součástí rozsahu Cardholder Data Environment (CDE), je Dodavatel povinen dodržovat požadavky standardu Payment Card Industry Data Security Standard (PCI DSS), a to v aktuálně účinné verzi, ledaže by související konkrétní smlouva stanovila jinak.

2. Pokud Dodavatel poskytuje služby jako poskytovatel služeb ve smyslu PCI DSS, je povinen:

   2.1. udržovat vlastní soulad s PCI DSS,

   2.2. mít platné potvrzení o souladu (např. Attestation of Compliance, pokud je relevantní),

   2.3. na vyžádání ČD předložit doklad o aktuálním souladu.

3. Dodavatel nesmí provést žádnou změnu v architektuře, konfiguraci nebo zabezpečení systému, která by mohla negativně ovlivnit soulad CDE s PCI DSS, bez předchozího písemného souhlasu ČD.

KAPITOLA V – BEZPEČNOST LIDSKÝCH ZDROJŮ

1. Dodavatel je v rozsahu předmětu plnění povinen:

   1.1. zajistit seznámení všech osob, které se podílí na plnění předmětu smlouvy s těmito bezpečnostními pravidly a dalšími upřesňujícími bezpečnostními informacemi prokazatelně předanými ze strany ČD. Za prokazatelné seznámení se považuje školení osob podílejících se na plnění Dodavatele zajištěné ČD, protokolární či elektronické předání příslušné dokumentace a/nebo zajištěný přístup na sdílené úložiště ČD obsahující příslušné dokumenty, a zároveň čestné prohlášení o zajištění seznámení osob a subjektů v rámci plnění Dodavatele s těmito bezpečnostními pravidly a dalšími upřesňujícími bezpečnostními informacemi podepsané Dodavatelem;

   1.2. využívat pro poskytování předmětu plnění pouze oprávněných osob, které byly řádně seznámeny s těmito bezpečnostními pravidly a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu plnění;

   1.3. dodržovat příslušná ustanovení bezpečnostních politik ČD či jiných interních řídících aktů ČD (dále také jako „**bezpečnostní politika a bezpečnostní dokumentace**“) v rozsahu, v jakém byl s těmito akty prokazatelně seznámen.

   1.4. zajistit, aby osoby podílející se na poskytování plnění v prostředí nebo s prostředky ČD, a to i tehdy, pokud jsou prostředky ČD používány mimo jeho prostředí:

1.4.1. pro uložení a sdílení dat a informací ČD využívaly pouze k tomu schválené prostředky;

1.4.2. neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno ČD;

1.4.3. nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo autorským zákonem;

1.4.4. nenavštěvovaly internetové stránky s eticky nevhodným obsahem;

1.4.5. nerealizovaly pokusy o neautorizovaný přístup ke zdrojům ČD ani ke zdrojům jiných subjektů;

1.4.6. nerealizovaly pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků ČD, a to ani v případě, kdy jim byl prostředek ČD svěřen do správy;

1.4.7. nepodílely se s prostředky ČD na šíření spamu ani škodlivého softwaru.

1.5. stanovit plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí ve formě poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice ČD v souladu s odst. 1.1.

KAPITOLA VI – ŘÍZENÍ PROVOZU A KOMUNIKACÍ

1. Dodavatel je v rozsahu předmětu plnění povinen:

1.1. zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění;

1.2. poskytnout ČD na vyžádání přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře;

1.3. bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu plnění a je ve správě Dodavatele;

1.4. zajistit, že pro poskytování předmětu plnění budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky a zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, v platném znění.

1.5. realizovat bezpečnostní opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě.

KAPITOLA VII – ŘÍZENÍ PŘÍSTUPU A BEZPEČNÉ CHOVÁNÍ UŽIVATELŮ

1. Dodavatel je v rozsahu předmětu plnění povinen:

1.1. přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům ČD;

1.2. uskutečnit vzdálený přístup do systémů ČD pouze prostřednictvím zabezpečeného a schváleného připojení přes VPN;

1.3. zajistit, aby osoby, které se podílejí na poskytování plnění předmětu, a které přistupují do interní sítě nebo informačního systému ČD, měly v externím zařízení typu notebook/počítač aplikovány bezpečnostní záplaty a nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu;

1.4. průběžně kontrolovat a vyhodnocovat oprávněnost přístupu, jak fyzického, tak logického, u všech zaměstnanců Dodavatele, kteří přistupují do prostředí ČD;

1.5. neinstalovat a nepoužívat zejména typy nástrojů Keylogger, Sniffer, Analyzátor zranitelností a Port Scanner, Backdoor, rootkit a trojský kůň nebo jinou podobu malware s výjimkou prostředí a počítačů, které jsou určeny k provádění penetračních testů v rámci konkrétního předmětu plnění souvisejícího s provedením penetračních testů. V případě nutnosti nasazení a instalace podobných nástrojů na prostředí nebo počítače ČD je toto možné jedině s písemným schválením ČD;

1.6. nepoužívat a neinstalovat žádné další nástroje, které nejsou součástí předmětu plnění bez vědomí ČD;

1.7. nesdílet udělený přístup s více zaměstnanci Dodavatele nebo poddodavatele. Každý zaměstnanec Dodavatele podílející se na předmětu plnění musí mít evidován a veden svůj vlastní jedinečný uživatelský účet, kterému jsou v jednotlivých systémech, modulech nebo aplikacích přiřazeny specifické role související výhradně s plněním smlouvy. Každý zaměstnanec Dodavatele musí být veden s platnými identifikačními a aktuálními kontaktními údaji;

1.8. zajistit, aby osoby podílející se na poskytování předmětu plnění a mající přístup k informačním aktivům ČD chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám;

1.9. využívat v rámci ICT infrastruktury ČD k jednoznačné identifikaci privilegovaných uživatelů (privilegovaný uživatel disponuje vyššími právy a oprávněními, než mají běžní uživatelé a jeho činnost na technickém aktivu tudíž může mít významný dopad na bezpečnost regulované služby) systémů více faktorovou autentizaci nebo ověření heslem – pokud není možné použít jednoznačnou identifikaci privilegovaných uživatelů více faktory, je použita autentizace pomocí kryptografických klíčů se zaručením obdobné úrovně bezpečnosti nebo použití hesla s definovanými pravidly.

1.10. využívat v systémech ČD privilegovaná oprávnění jen v přiměřené míře a jen po dobu nezbytně nutnou pro vykonávání činností v souladu s předmětem plnění. Zaměstnanci Dodavatele nesmí používat účty s privilegovanými oprávněními pro běžnou práci nesouvisející se správou informačního systému.

2. Dodavatel bere na vědomí, že přidělení oprávnění zaměstnanci Dodavatele musí být řízeno principem nezbytného minima a není nárokové.

3. Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu Dodavatele) může být příslušný účet zablokován a řešen jako bezpečnostní incident a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu.

KAPITOLA VIII – MONITOROVÁNÍ ČINNOSTÍ

4. Přístup zaměstnanců Dodavatele k interním informacím ČD je nepřetržitě zaznamenáván, monitorován a vyhodnocován. Události jsou zaznamenávány do logů dle vyhlášky.

5. Dodavatel je v rozsahu předmětu plnění povinen:

   5.1. umožnit přístup k auditním údajům (systémové a aplikační logy) v takové podobě a formátu, který je možné dále zpracovávat;

   5.2. zajistit sběr informací o provozních a bezpečnostních činnostech v rozsahu předmětu plnění a ochranu získaných informací před jejich neoprávněným čtením nebo změnou;

   5.3. zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu plnění a v souladu s požadavky platné české a evropské legislativy;

   5.4. poskytnout na vyžádání report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu předmětu plnění, a to po celou dobu trvání smlouvy a do 2 let po jejím ukončení.

6. Dodavatel je povinen průběžně monitorovat v rámci své ICT infrastruktury zveřejněné a známé bezpečnostní chyby, které mohou ovlivnit hladký a bezpečný provoz systémů souvisejících s jím poskytovanými službami. Jedná se například o zranitelnosti v operačních systémech, software třetích stran, webové komponenty apod.

KAPITOLA IX – APLIKAČNÍ BEZPEČNOST

1. Dodavatel je v rozsahu předmětu plnění povinen:

   1.1. užívat technická aktiva, která jsou jejich výrobcem, dodavatelem nebo jinou osobou podporována a zajistit aplikování schválených bezpečnostních aktualizací vydaných pro tato aktiva;

   1.2. zavést bezpečnostní opatření, která zaručí obdobnou nebo vyšší úroveň bezpečnosti těchto technických aktiv do doby plnění podle odstavce 1.1 této kapitoly;

   1.3. evidovat technická aktiva, která již nejsou výrobcem, dodavatelem nebo jinou osobou podporována a na která není možné aplikovat poslední schválenou bezpečnostní aktualizaci;

   1.4. v rámci aplikační bezpečnosti zajistit trvalou ochranu aplikací, informací, transakcí a přenášených identifikátorů relací před neoprávněnou činností a popřením provedených činností;

   1.5. pravidelně skenovat zranitelnosti technických aktiv a provádět penetrační testování technických aktiv dle požadavků vyhlášky;

   1.6. zohlednit výsledky skenování zranitelností technických aktiv a výsledky penetračního testování v rámci řízení rizik a zavádět bezpečnostní opatření na základě zjištěných výsledků;

   1.7. provést opětovné otestování nálezu zjištěného na základě provedeného skenování zranitelností nebo penetračního testování za účelem ověření funkčnosti zavedených bezpečnostních opatření.

KAPITOLA X – UŽÍVÁNÍ KRYPTOGRAFICKÝCH PROSTŘEDKŮ

1. Dodavatel je povinen zajistit, že veškerý přenos dat a informací musí být dostatečně zabezpečen pomocí aktuálně odolných kryptografických algoritmů a kryptografických klíčů.

2. Kryptografické prostředky musí být používány v souladu s dokumentem Minimální požadavky na kryptografické algoritmy (doporučení kryptografické ochrany v oblasti kybernetické bezpečnosti) vydaným Národním úřadem pro kybernetickou a informační bezpečnost v posledním platném znění (dále „**NÚKIB**“).

KAPITOLA XI – ZAJIŠŤOVÁNÍ DOSTUPNOSTI REGULOVANÉ SLUŽBY

1. Dodavatel je v rozsahu předmětu plnění povinen:

   1.1. přijmout taková technická a organizační opatření, aby byla zajištěna dostupnost aktiv, která jsou součástí regulované služby ČD v rozsahu odpovídajícím jejich významu pro regulovanou službu;

   1.2. zajistit odpovídající úroveň redundance aktiv, které mají vliv na dostupnost regulované služby ČD;

   1.3. zajistit navržení redundance aktiv tak, aby selhání jednoho prvku nevedlo k nedostupnosti regulované služby;

   1.4. pravidelně vytvářet zálohy konfigurací a nastavení technických aktiv, dat a dalších informací nezbytných pro obnovu regulované služby po kybernetickém bezpečnostním incidentu;

   1.5. zajistit, že zálohy jsou:

      1.5.1 pravidelně testovány z hlediska jejich integrity, dostupnosti a obnovitelnosti;

      1.5.2 dokumentovány včetně výsledků testů provedených podle odstavce 1.5.1;

      1.5.3 chráněny před narušením jejich integrity a důvěrnosti, a to alespoň šifrováním těchto záloh v souladu s kapitolou X tohoto dokumentu;

      1.5.4 chráněny před narušením jejich dostupnosti

   1.6. zajistit bezpečnou správu konfigurací a nastavení technických aktiv s ohledem na jejich význam a související rizika;

   1.7. zajistit oddělení zálohovacího prostředí od produkčního a dalších prostředí tak, aby bylo omezeno šíření kybernetického bezpečnostního incidentu a minimalizován jeho dopad na regulovanou službu.

KAPITOLA XII – ZABEZPEČENÍ PRŮMYSLOVÝCH, ŘÍDICÍCH A OBDOBNÝCH SPECIFICKÝCH TECHNICKÝCH AKTIV

1. Dodavatel je v rozsahu předmětu plnění povinen:

    1.1. zajistit kybernetickou bezpečnost průmyslových, řídicích a obdobných specifických technických aktiv v souladu s obecnými požadavky ustanovenými ve všech kapitolách tohoto dokumentu a dále zajistit:

        1.1.1 omezení fyzického přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům;

        1.1.2 omezení oprávnění k přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům;

        1.1.3 segmentaci a oddělení komunikačních sítí průmyslových, řídicích a obdobných specifických technických aktiv od jiných prostředí a segmentaci a oddělení těchto komunikačních sítí;

        1.1.4 omezení vzdálených přístupů a vzdálené správy průmyslových, řídicích a obdobných specifických technických aktiv, včetně omezení komunikace mimo komunikační síť ČD;

        1.1.5 ochranu jednotlivých průmyslových, řídicích a obdobných specifických technických aktiv před využitím známých zranitelností a hrozeb;

        1.1.6 dostupnost a obnovu průmyslových, řídicích a obdobných specifických technických aktiv pro zajištění dostupnosti regulované služby.

KAPITOLA XIII – AKVIZICE, VÝVOJ A ÚDRŽBA

1. Dodavatel je v rozsahu předmětu plnění povinen:

    1.1. zajistit bezpečnou implementaci, inovaci, aktualizaci, testování technologií, které jsou předmětem plnění;

    1.2. předat ČD dokumentaci předmětu plnění v odpovídajícím rozsahu;

    1.3. v případě, že předmět plnění zahrnuje vývoj softwaru, je Dodavatel povinen:

        1.3.1. dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru definované na základě smluvního vztahu;

        1.3.2. pokud jsou softwarové auditní činnosti a předání zdrojového kódu k SW součástí plnění dle smlouvy, umožní Dodavatel audit prováděného nebo provedeného plnění a na písemnou žádost ČD předloží Dodavatel vyvíjený zdrojový kód k SW na provedení codereview (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), a to zejména za účelem ověření skutečnosti, zda Dodavatel postupuje či postupoval při poskytování plnění v souladu se smlouvou a těmito bezpečnostními pravidly;

1.3.3. poskytovat ČD v termínech stanovených ČD, resp. bez zbytečného odkladu požadovanou součinnost na provedení bezpečnostního testování v průběhu vývoje softwaru či kdykoli po jeho předání;

1.3.4. zajistit, že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování softwaru a/nebo které jsou specifikovány výslovně ve smlouvě (zejména, že software nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.).

1.3.5. pokud je součástí plnění i instalace operačního systému, případně softwaru třetích stran, zajistit v průběhu jeho instalace, že budou použity předepsané verze těchto produktů kompatibilní a funkční v prostředí ČD;

1.3.6. zajistit bezpečnost testovacího prostředí u Dodavatele a ochranu poskytnutých testovacích dat ČD;

1.3.7. zajistit, že v produkčním prostředí ČD bude dodán jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění;

1.3.8. zajistit, že v rámci poskytovaného plnění bude dodávaný software;

1.3.8.1. v souladu s bezpečnostními politikami a standardy ČD;

1.3.8.2. otestován na soulad s bezpečnostními politikami ČD (platí pro Dodavatele, pokud byl s takovými bezpečnostními politikami seznámen);

1.3.9. instalovat software pouze na základě ČD předem schválených migračních postupů;

1.3.10. předat zdrojový kód ČD bezpečnou formou zajišťující jeho integritu;

1.3.11. zajistit řízení verzí zdrojového kódu;

1.3.12. zajistit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí;

1.3.13. zajistit, aby distribuce zdrojových kódů obsahovala soubor z vývojového prostředí na řízenou kompilaci těchto zdrojových kódů;

1.3.14. nevyvíjet, nekompilovat a nešířit v prostředí ČD programový kód, jehož účelem je neautorizované získání přístupu k aktivům, překonání systémových či aplikačních kontrol, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

KAPITOLA XIV – FYZICKÁ BEZPEČNOST

1. Dodavatel je v rozsahu předmětu plnění povinen:

1.1. dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny komponenty systémů ICT, anebo datové nosiče;

1.2. v rozsahu předmětu plnění zajistit fyzické zabezpečení instalačních, záložních nebo archivních médií a dokumentace minimálně v souladu s vyhláškou či jiným interním řídícím aktem ČD (pokud byl poskytnut). Přičemž, pokud není určena klasifikace aktiva, bude použit způsob pro úroveň – kritická.

KAPITOLA XV – ZVLÁDÁNÍ KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ A INCIDENTŮ

1. Dodavatel je povinen informovat oprávněné zástupce ČD o vzniku kybernetické bezpečnostní události související s předmětem plnění bez zbytečného odkladu. V případě odůvodněného podezření či potvrzení kybernetického bezpečnostního incidentu Dodavatelem je Dodavatel povinen informovat ČD nejpozději do 12 hodin od okamžiku, kdy se Dodavatel měl a mohl o kybernetickém bezpečnostním incidentu dozvědět tak, by ČD mohla splnit svou zákonnou povinnost (24 h) vůči NÚKIB.

2. Dodavatel je dále povinen realizovat a sdělit ČD reaktivní opatření, která provedl ve vztahu k tomuto kybernetickému bezpečnostnímu incidentu. Současně je Dodavatel povinen sdělit ČD i nápravná opatření, která navrhuje realizovat ve vztahu ke kybernetickému bezpečnostnímu incidentu a po konzultaci s ČD tato opatření dle dohody realizovat v dohodnutých termínech.

3. Pokud dojde ke kybernetické bezpečnostní události nebo kybernetickému bezpečnostnímu incidentu a následnému zvládání a vyhodnocování kybernetického bezpečnostního incidentu na straně ČD, poskytne Dodavatel požadovanou součinnost (například poskytne logy a identifikační údaje) dotyčného koncového zařízení k analýze obsahu, případně bez zbytečného odkladu zrealizuje opatření požadovaná ČD.

KAPITOLA XVI – ŘÍZENÍ KONTINUITY ČINNOSTÍ

1. Dodavatel je v rozsahu předmětu plnění povinen:

   1.1. zajistit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování předmětu plnění.

   1.2. pravidelně kontrolovat a testovat, že je schopen kontinuity aktiv souvisejících s předmětem plnění zajistit dle sjednané úrovně služeb.

2. ČD má oprávnění zapojit Dodavatele do řízení kontinuity činností, které souvisí s předmětem plnění. Dodavatel je v takovém případě povinen se řízení kontinuity činností účastnit.

KAPITOLA XVII – ZÁVĚREČNÁ USTANOVENÍ

1. Tato bezpečnostní pravidla jsou součástí smluv v oblasti jakýchkoli informačních a provozních technologií (IT a OT) včetně smluv v oblasti železničních kolejových vozidel uzavíraných mezi ČD a jejími obchodními partnery jakožto Dodavateli. ČD si vyhrazuje právo v odůvodněných případech změnit pravidla a zásady obsažené v těchto bezpečnostních pravidlech, v takovém případě očekává od svých Dodavatelů, že budou takové změny akceptovat.

2. Dodavatelé musí učinit všechna nezbytná opatření s cílem zajistit, aby základní požadavky těchto pravidel v souladu s kapitolou V byly sděleny jejich zaměstnancům, a jsou rovněž povinni učinit všechna přiměřená opatření s cílem zajistit dodržování těchto bezpečnostních pravidel u všech osob a subjektů, které použijí v rámci spolupráce s ČD.

3. Bude-li zjištěno porušení těchto pravidel, ČD definuje nápravná opatření, která je Dodavatel povinen provést a napravit tak vzniklé porušení během stanovené přiměřené doby. V případě neprovedení

dostatečných nápravných opatření ze strany Dodavatele může ČD obchodní vztahy s daným Dodavatelem ukončit a přistoupit k vypovězení příslušných smluv s výpovědní dobou 3 měsíce plynoucí od prvního dne následujícího po měsíci doručení výpovědi, pokud nebude stanoveno v konkrétní smlouvě jinak.

4. V případě důvodného podezření na porušení těchto bezpečnostních pravidel jsou ČD oprávněny požadovat, aby jim Dodavatel poskytl vysvětlení nebo bližší informace týkající se prověřovaného podezření, včetně informací o tom, zda a jaká opatření přijal.

5. Toto úplné znění bezpečnostních pravidel nabývá účinnosti dne 18.9.2026.

Toto úplné znění bezpečnostních pravidel je dostupné na webových stránkách společnosti www.ceskedrahy.cz.