BEZPEČNOSTNÍ POŽADAVKY

1. Definice
   1. Termíny uvedené dále v tomto čl. 1, jsou-li použity v tomto dokumentu a uvozeny velkým písmenem, mají význam uvedený dále v tomto čl. 1. Termíny definované v tomto dokumentu v množném čísle mají shodný význam i v jednotném čísle a naopak. Odkazy na články a přílohy v tomto dokumentu odkazují na články a přílohy tohoto Dokumentu, není-li uvedeno jinak.
   2. „**ČEPRO**“ je ČEPRO, a.s., se sídlem Dělnická 213/12, Holešovice, 170 00 Praha 7, IČO: 601 93 531, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. B 2341.
   3. „**Dodavatel**“ je osoba, která má s ČEPRO uzavřenu Dodavatelskou smlouvu.
   4. „**Dodavatelská smlouva**“ je smlouva mezi ČEPRO a Dodavatelem na dodávky zboží a/nebo poskytování služeb, ve kterých vystupuje Dodavatel jako dodavatel zboží a/nebo poskytovatel služeb a ČEPRO jako odběratel tohoto zboží a/nebo služeb.
   5. „**Dohoda**“ je Dohoda o bezpečnostních aspektech při poskytování plnění uzavřená mezi ČEPRO a Dodavatelem.
   6. „**Pracovníci Dodavatele**“ jsou zaměstnanci Dodavatele a fyzické osoby v obdobném postavení, kteří se podílí a/nebo mají podílet na plnění předmětu Dodavatelské smlouvy. Stanoví-li Pravidla povinnost Pracovníkům Dodavatele, Dodavatel odpovídá za veškerou újmu způsobenou porušením takové povinnosti.
   7. „**Pravidla**“ jsou tato Pravidla pro dodavatele/Bezpečnostní požadavky.
   8. Všechny výjimky z Pravidel, nad rámec výjimek uvedených v Dohodě a/nebo Dodavatelské smlouvě, musí být zdokumentovány a povoleny kontaktní osobou ČEPRO. Pokud není stanoveno jinak, kontaktní osobou pro schvalování výjimek je za ČEPRO Information Security Officer (ISO), manažer/ři kybernetické bezpečnosti a bezpečnostní architekt/i.
2. Personální bezpečnost
   1. Dodavatel je povinen informovat ČEPRO o ukončení pracovního nebo obdobného poměru Pracovníků Dodavatele, pro které byly u ČEPRO vytvořeny přístupové účty, minimálně v předstihu 5 pracovních dní před ukončením takového poměru. Dodavatel je také povinen zvážit, zdali takový Pracovník Dodavatele nepředstavuje po dobu výpovědní doby nebo obdobné doby bezpečnostní riziko (zejména s ohledem na důvod ukončení) a případně přijmout opatření k zabránění zneužití přístupového účtu takovým Pracovníkem Dodavatele.
   2. Dodavatel poskytne ČEPRO úplný jmenný seznam Pracovníků Dodavatele. Dodavatel se zavazuje informovat ČEPRO o změnách v personálním zabezpečení Dodavatelské smlouvy v předstihu minimálně 5 pracovních dní.
   3. Pracovníci Dodavatele:
      1. musí být seznámeni s těmito Pravidly, bezpečnostními požadavky Dodavatelské smlouvy a Dohody;
      2. mají dostatečné znalosti a praktické zkušenosti pro plnění přidělených úkolů;
      3. mají veškeré potřebné zkoušky a atestace, které vyplývají ze zákona nebo požadavků regulátora na druh práce, kterou mají v prostředí ČEPRO vykonávat;
      4. jsou Dodavatelem pravidelně školeni v oblastech (informační) bezpečnosti a právních a regulatorních požadavků relevantních pro naplnění předmětu Dodavatelské smlouvy a Dohody;
      5. kteří budou vstupovat nebo vjíždět do prostor ČEPRO, musí být před započetím výkonu práce podrobeni ve smyslu právních předpisů školení o požární ochraně a bezpečnosti práce a současně musí být seznámeni s povinnostmi Dodavatele jakožto osoby poskytující plnění z Dodavatelské smlouvy;

a Dodavatel se zavazuje dané provést a kontrolovat dodržování těchto povinností.

* 1. Pracovníci Dodavatele nejsou oprávněni vstupovat do prostor ČEPRO a/ nebo přistupovat k informačním aktivům ČEPRO pod vlivem návykových, omamných či psychotropních látek.

1. Fyzická bezpečnost
   1. Přístup Pracovníků Dodavatele do prostor ČEPRO je povolen, pouze pokud je jejich přítomnost nezbytná pro plnění pracovních povinností a na dobu nezbytně nutnou pro plnění pracovních povinností vyplývajících z Dodavatelské smlouvy.
   2. Pracovníci Dodavatele jsou povinni se v prostorách ČEPRO pohybovat pouze v doprovodu odpovědného zaměstnance ČEPRO, leda se uplatní odst. 3.3 těchto Pravidel.
   3. Volný pohyb Pracovníků Dodavatele v prostorách ČEPRO je povolen pouze v případě, že dané osobě byla vystavena osobní přístupová karta. Pracovník Dodavatele není oprávněn přístupovou kartu dále zapůjčit třetím osobám a/nebo umožnit přístup třetích osob do prostor ČEPRO.
   4. Pracovníci Dodavatele nejsou oprávněni do prostředí ČEPRO přinést zbraně, výbušniny, hořlaviny, bojové prostředky, jedy, radioaktivní a toxické látky, popř. jakékoli jiné látky ohrožující lidský život a/nebo zdraví.
   5. Bez písemného povolení ČEPRO je zakázáno vynášení jakýchkoliv předmětů nepatřících Pracovníkům Dodavatele a/nebo nesloužících k plnění Dodavatelské smlouvy, zejména jakékoliv dokumentace a/nebo paměťové médium (CD/DVD/Blu-ray disk, flash disk / paměťové karty, hard disk, zálohovací pásky apod.) z prostor ČEPRO, popř. jiného místa plnění příslušné Dodavatelské smlouvy určeného Dodavatelskou smlouvou, a jejich kopírování, fotografování, pořizování videozáznamů, připojování k jiným zařízením (než zařízení ČEPRO) apod., pokud není v Dodavatelské smlouvě anebo jinde písemně dohodnuto jinak.
   6. Přístup Pracovníků Dodavatele do prostor ČEPRO se zvýšeným stupněm bezpečnosti – chráněných zón (jako jsou serverové místnosti, datové místnosti, technické místnosti, trezor, pokladna apod.) je povolen pouze v doprovodu oprávněného zaměstnance ČEPRO. Doprovod je nezbytný po celou dobu fyzické přítomnosti zaměstnanců Dodavatele v těchto prostorách.
   7. V případě ztráty přístupové karty nebo v případě podezření ze ztráty přístupové karty je Dodavatel povinen bezodkladně zajistit blokaci přístupové karty.
   8. Před vrácením zapůjčených paměťových médií Dodavateli musí být veškerá data ČEPRO vymazána způsobem, který znemožňuje jejich opětovné obnovení; pokud toto nebylo provedeno ze strany ČEPRO, je Dodavatel povinen dané provést. O tomto je sepsán protokol.
   9. Za prostory ČEPRO se považují také prostory využívané ČEPRO na základě smluvního vztahu s jejich vlastníkem a/nebo oprávněným uživatelem.
2. Přístupová oprávnění
   1. Každý, kdo přistupuje k informacím a datům uloženým nebo přenášeným informačními a komunikačními systémy ČEPRO nebo využívá některé technické nebo netechnické prostředky ČEPRO, musí disponovat platnými přístupovými oprávněními. O přístupová oprávnění pro Pracovníky Dodavatele může požádat pouze zaměstnanec ČEPRO. Požadavek na zřízení přístupového oprávnění předkládá zaměstnanec ČEPRO odpovědný za komunikaci mezi Dodavatelem a ČEPRO. Zaměstnanec ČEPRO může požádat o přístupová oprávnění pouze pro Pracovníky Dodavatele, je-li to zároveň nezbytné pro řádné plnění Dodavatelské smlouvy. Doba platnosti přístupového oprávnění nesmí být na dobu delší, než je doba trvání Dodavatelské smlouvy nebo předpokládaná doba plnění Dodavatele. Při ukončení Dodavatelské smlouvy a/nebo plnění poskytovaného Dodavatelem zaměstnanec ČEPRO vždy požádá o ukončení přístupového oprávnění.
   2. K žádosti zřízení účtu je nutné předložit ČEPRO tyto informace:
      1. jméno a příjmení osoby, pro kterou je požadováno přístupové oprávnění;
      2. vztah této osoby k Dodavateli a ČEPRO;
      3. doba platnosti přístupového oprávnění;
      4. důvody zřízení přístupového oprávnění.
   3. Požadavek na zřízení nebo zrušení přístupového oprávnění se provádí prostřednictvím HelpDesk IT (oddělení provozu IT a podpory uživatelů).
   4. Dodavatel odpovídá v plném rozsahu za využití, resp. zneužití, přístupového oprávnění (včetně loginu, hesla, popř. i dalších přidělených přihlašovacích údajů, jako je PIN, certifikát, token).
   5. Dodavatel není oprávněn po ukončení příslušné Dodavatelské smlouvy, při jejímž plnění měl zřízeno a užíval přístupové oprávnění, nadále takové přístupové oprávnění užívat, a to bez ohledu na skutečnost, že takové přístupové oprávnění nebylo při ukončení příslušné Dodavatelské smlouvy ze strany ČEPRO zrušeno.
3. Identifikace a autentizace
   1. Pracovníkům Dodavatele jsou přiděleny pouze účty, které nezbytně potřebují pro plnění pracovních povinností vyplývajících z Dodavatelské smlouvy.
   2. Účtům Dodavatele jsou přidělena pouze oprávnění nezbytná k plnění pracovních povinností dle Dodavatelské smlouvy.
   3. Dodavatel pracuje v prostředí ČEPRO pouze s účty umožňujícími jednoznačnou identifikaci uživatele – konkrétní fyzické osoby. ČEPRO se zavazuje vytvořit účty v produkčních i testovacích systémech pro všechny Pracovníky Dodavatele uvedené v Dodavatelské smlouvě nebo později odsouhlasené v rámci a procesem daným v Dodavatelské smlouvě.
   4. Dodavatel je povinen neaktivní účty Dodavatele v prostředí ČEPRO proaktivně oznamovat ČEPRO bezodkladně poté, co se stanou anebo mají stát neaktivními. Postup při ukončení spolupráce s Pracovníkem Dodavatele je popsán v odst. 2.1.
4. Nakládání s certifikáty
   1. Přístup k certifikátům (logický i fyzický) bude umožněn pouze Pracovníkům Dodavatele, u kterých je tento přístup nezbytný pro plnění jejich pracovních povinností vyplývajících z Dodavatelské smlouvy.
   2. Dodavatel a Pracovníci Dodavatele nejsou oprávněni certifikáty poskytnout či zpřístupnit třetím stranám bez písemného souhlasu ČEPRO.
   3. Dodavatel odpovídá za to, že certifikáty budou po instalaci uloženy pouze v bezpečném úložišti na serverech (zpravidla produkčních serverech), na kterých je jejich uložení nezbytné pro zajištění plnění dle Dodavatelské smlouvy, a veškeré další kopie budou odstraněny či zničeny způsobem, který znemožňuje jejich opětovnou obnovu.
   4. Pakliže je to možné, Dodavatel nastaví privátní klíč jako neexportovatelný z bezpečného úložiště certifikátů.
   5. Certifikát musí být vždy chráněn silným heslem odpovídajícím nejméně požadavkům na kvalitu hesel dle čl. 7 a nesmí být uložen v nešifrované podobě.
   6. Dodavatel se zavazuje neprodleně informovat ČEPRO o ztrátě a/nebo podezření ze ztráty důvěrnosti privátního klíče.
   7. Dodavatel se zavazuje minimalizovat množství záložních kopií, ve kterých je certifikát uložen a zavazuje se zničit veškeré záložní kopie předaných certifikátů způsobem, který znemožňuje jejich opětovnou obnovu, a to vždy po zániku potřeby existence dané záložní kopie a/nebo zániku Dodavatelské smlouvy. Dodavatel odpovídá za to, že přístup k záložním kopiím (logický i fyzický), na kterých je kopie certifikátu uložena, bude umožněn pouze těm Pracovníkům Dodavatele, u kterých je tento přístup nezbytný pro plnění pracovních povinností vyplývajících z Dodavatelské smlouvy.
   8. Dodavatel odpovídá za to, že šifrovací hesla k předaným certifikátům budou bezpečně uložena a přístup k nim bude poskytnut pouze těm Pracovníkům Dodavatele, u kterých je tento přístup nezbytný pro plnění pracovních povinností vyplývajících z Dodavatelské smlouvy.
5. Požadavky na kvalitu hesel a nakládání s nimi
   1. Pracovníci Dodavatele jsou povinni vytvářet hesla k osobním účtům v souladu s následujícími pravidly za předpokladu, že ČEPRO zajistí technickou způsobilost podporovaných aplikací k uplatnění požadovaných pravidel:
      1. minimální délka hesla je 12 znaků;
      2. minimální doba platnosti hesla je 5 dnů;
      3. pokud ČEPRO nestanoví jinak, heslo musí být pravidelně měněno každých 90 dnů; a
      4. heslo musí splňovat požadavky na komplexitu obvyklé v daném oboru s přihlédnutím k aktivům ČEPRO, nejméně však dle odst. 7.4.
   2. Hesla k účtům, kterým jsou v prostředí ČEPRO přidělena administrátorská oprávnění, musí být vytvořena v souladu s následujícími pravidly:
      1. minimální délka hesla je 17 znaků;
      2. minimální doba platnosti hesla je 5 dnů;
      3. pokud ČEPRO nestanoví jinak, heslo musí být pravidelně měněno každých 90 dnů; a
      4. heslo musí splňovat požadavky na komplexitu, obvyklé v daném oboru s přihlédnutím k aktivům ČEPRO, nejméně však dle odst. 7.4.
   3. Hesla k technickým nebo servisním účtům musí být vytvořena v souladu s následujícími pravidly:
      1. minimální délka hesla je 30 znaků;
      2. minimální doba platnosti hesla je 5 dnů;
      3. k vytvoření hesla musí být použit pseudo-náhodný generátor hesel; a
      4. pokud ČEPRO nestanoví jinak, heslo musí být pravidelně měněno každých 365 dnů.
   4. Veškerá hesla vytvořená Dodavatelem v prostředí ČEPRO musí dále splňovat následující požadavky:
      1. heslo musí obsahovat kombinaci velkých a malých písmen, číslic a speciálních znaků;
      2. heslo nesmí být jednoduše uhodnutelné, nesmí obsahovat žádnou část jména, přihlašovacího jména, jména společností Dodavatele a ČEPRO apod. a musí být tvořeno tak, aby znemožňovalo úspěšné uhodnutí pomocí slovníkového útoku;
      3. heslo nesmí obsahovat datum v některém z běžně užívaných formátů nebo ve slovním vyjádření;
      4. každé nově zadané heslo musí být vždy odlišné od všech dříve použitých hesel, o nichž daný Pracovník Dodavatele ví;
      5. heslo nesmí být uloženo s možností nešifrovaného přístupu;
      6. heslo nesmí být uloženo v místě, kde by mohlo být úmyslně či neúmyslně zjištěno jinou osobou; a
      7. heslo nesmí být sdíleno s další osobou, pokud k tomuto nebyl v předstihu vydán písemný souhlas ČEPRO.
   5. Pokud tato Pravidla nestanoví podmínky pro heslo k určitým specifickým typům účtů, které nejsou uvedeny v odst. 7.1 až 7.3, uplatní se na takové účty pravidlo dle odst. 7.1.
   6. Pokud je prvotní heslo k účtu vytvořeno zaměstnanci ČEPRO, je Dodavatel po získání prvotního hesla povinen heslo neprodleně změnit.
   7. Předávání prvotního hesla musí probíhat vždy způsobem, který vylučuje vyzrazení hesla dalším osobám.
   8. Heslo nesmí být zadáváno, pokud existuje riziko odpozorování hesla při zadávání jinou osobou. V případě vyzrazení hesla nebo v případě podezření z vyzrazení hesla musí Dodavatel bezodkladně zajistit změnu/blokaci hesla vhodným způsobem (pokud je to nezbytné za součinnosti ČEPRO).
   9. Hesla ČEPRO uložená v prostředí Dodavatele musí být uložena na úložišti, ke kterému je přístup šifrován. Hesla musí být dále chráněna před neautorizovaným přístupem osob, které tento přístup bezpodmínečně nepotřebují k plnění pracovních povinností vyplývajících z Dodavatelské smlouvy.
6. Nakládání s informacemi ČEPRO
   1. Přístup k informacím ČEPRO (ať už primárním aktivům nebo jiným) je přidělen pouze Pracovníkům Dodavatele, kteří tento přístup potřebují pro plnění pracovních povinností vyplývajících z Dodavatelské smlouvy.
   2. Dodavatel nesmí zpracovávat nebo ukládat následující typy informací mimo prostředí ČEPRO a/ nebo informační systémy ČEPRO:
      1. osobní údaje ve smyslu nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů);
      2. současné i historické informace o klientech ČEPRO, jejich majetku, finančních transakcích, využívaných produktech a/ nebo jejich smluvních vztazích; a
      3. současné i historické účetní záznamy ČEPRO a smluvní dokumentaci ČEPRO.
   3. Po ukončení prací vyplývajících z Dodavatelské smlouvy a/nebo v případě ukončení účinnosti Dodavatelské smlouvy se Dodavatel bez zbytečného prodlení zavazuje vrátit a/nebo odstranit (podle volby ČEPRO) informace ČEPRO uložené v prostředí Dodavatele související s plněním předmětu takové Dodavatelské smlouvy, pakliže držení těchto informací není vyžadováno zákony České republiky. Toto se týká také elektronické i papírové dokumentace. Odstranění informací musí být provedeno způsobem, který znemožňuje jejich opětovné obnovení.
7. Bezpečnostní požadavky na Dodavatele
   1. Přístup k aktivům ČEPRO nesmí Dodavatel poskytnout bez předchozího písemného souhlasu ČEPRO žádným třetím stranám, včetně externích zaměstnanců Dodavatele, dodavatelů Dodavatele, mateřských či sesterských společností Dodavatele, dodavatelů outsourcingu Dodavatele a dodavatelů cloudových služeb a/nebo cloudových úložišť; souhlas ČEPRO může být udělen v Dodavatelské smlouvě.
   2. Dodavatel je povinen zajistit adekvátní zabezpečení výpočetní techniky, na které jsou uloženy či zpracovávány informace ČEPRO nebo přes které jsou tato přenášeny. Vzhledem k informacím ČEPRO je Dodavatel povinen zajistit splnění minimálně následujících požadavků:
      1. v prostředí Dodavatele jsou používány nástroje pro detekci a odstranění škodlivého kódu s nastavením pravidelné aktualizace databáze signatur škodlivého kódu s frekvencí nepřesahující jeden týden. Tento software je centrálně spravován a jsou nastaveny odpovídající procesy dohledu, logování a reakce na pozitivní nález škodlivého kódu v prostředí Dodavatele;
      2. v prostředí Dodavatele jsou definovány, nastaveny, vykonávány a centrálně monitorovány procesy aktualizace bezpečnostních záplat softwarových komponent (minimálně však operačního systému, nástrojů kancelářského softwaru, webových prohlížečů a jejich doplňků – např. JAVA, Adobe Reader a doplňky sady Microsoft Office) v intervalu nepřesahující jeden měsíc od vydání záplat;
      3. vnitřní prostředí Dodavatele je od internetu odděleno firewallem, který je připojen k centrálnímu dohledu. Zaměstnanci Dodavatele při vzdáleném přístupu do vnitřního prostředí Dodavatele využívají šifrované připojení zamezující neautorizovaný odposlech a změnu přenášené komunikace;
      4. v prostředí Dodavatele není instalován, provozován nebo jinak spouštěn nepodporovaný software a/nebo software, u kterého byly zveřejněny a jsou odborné veřejnosti známy zásadní bezpečnostní chyby, u kterých nelze rozumně předpokládat, že budou v přijatelné době odstraněny, například Adobe Flash Player apod., ledaže je to nezbytné pro plnění Dodavatelské smlouvy.
   3. Jsou-li informace ČEPRO přenášeny Dodavatelem mimo prostory ČEPRO, je Dodavatel povinen důsledně dbát na fyzickou bezpečnost těchto aktiv a mít je stále pod dohledem. Dodavatel zejm. nesmí:
      1. ponechat informace ČEPRO na veřejných místech bez dozoru;
      2. ponechat informace ČEPRO bez dozoru v zaparkovaném vozidle;
      3. ponechat informace ČEPRO bez dozoru v hotelovém pokoji. Informace musí být uloženy v hotelovém trezoru a/ nebo jinak uzamčeny a adekvátně chráněny proti odcizení;
      4. při přepravě letadlem ponechat informace ČEPRO v odbavovaných zavazadlech uskladněných v přepravním prostoru letadel. Pokud to bezpečnostní pravidla leteckých přepravců nevylučují, musí být informace ČEPRO přepravovány na palubě letadel.
   4. Dodavatel je povinen dodržovat bezpečnostní a provozní pokyny výrobce hardwaru, na kterém jsou informace ČEPRO uloženy/zpracovávány.
   5. Dodavatel používá pouze řádně licencovaný software a pouze v souladu s licenčními ujednáními jednotlivých dodavatelů licence.
   6. Pokud nelze zajistit bezpečnost dat nebo komunikace jiným způsobem (např. při přenosu citlivých dat přes nedůvěryhodné sítě nebo při přístupu externích stran k citlivým zdrojům atd.), musí být ze strany Dodavatele používány šifrovací prostředky. Pokud je to možné, mělo by být používáno end-to-end šifrování.
   7. Tam, kde je vyžadováno šifrování, je Dodavatel povinen zajistit používání pouze takových šifrovacích algoritmů a protokolů, které jsou obecně považovány za bezpečné podle současných standardů. Algoritmy a délky klíčů musí odpovídat nejméně požadavkům NÚKIB[[1]](#footnote-2), pokud takové jsou. Proprietární algoritmy a takové algoritmy, které nejsou obecně standardizované, nesmí být používány. Šifrovací klíče musí být dostupné v rámci úschovné služby, aby zašifrované informace ČEPRO mohly být v případě nutnosti rozšifrovány. Úschova klíčů musí být zabezpečená tak, aby v největší možné míře zajistila, že třetí strany nemohou získat přístup ke klíčům.
8. Práce v prostředí ČEPRO
   1. Dodavatele je oprávněn (vzdáleně) přistupovat pouze k aktivům ČEPRO, které nezbytně potřebuje k plnění pracovních povinností vyplývajících z této Smlouvy, a to v souladu s těmito Pravidly, Dodavatelskou smlouvou, Dohodou a pokyny zaměstnanců ČEPRO.
   2. Dodavatele je oprávněn (vzdáleně) přistupovat pouze prostřednictvím VPN a nástrojů schválených ČEPRO, a to jak na servery, tak na klientské stanice, a to hlavně s ohledem na bezpečnost aktiv ČEPRO a ochranu osobních údajů.
   3. Do prostředí ČEPRO jsou oprávněni (vzdáleně) přistupovat pouze k tomu autorizováni Pracovníci Dodavatele.
   4. Bez předchozího písemného souhlasu ČEPRO není Dodavatel v prostředí ČEPRO oprávněn instalovat a/nebo spouštět žádný, předem ze strany ČEPRO neschválený, software.
   5. Bez písemného souhlasu ČEPRO není Dodavatel oprávněn v prostředí ČEPRO provádět jakékoliv testování fyzické nebo logické bezpečnosti a/nebo kontrolních mechanismů jakéhokoliv typu.
   6. ČEPRO je vlastníkem (a pořizovatelem) veškerých auditních stop nebo protokolů generovaných jakýmkoli systémem v rámci aktiv ČEPRO a/nebo v rámci plnění Dodavatelské smlouvy (vč. HelpDesk apod). Dodavatel je povinen na požádání poskytnout k nim přístup (pokud nejsou v prostředí ČEPRO) nebo je extrahovat pro ČEPRO. Veškerá generovaná data v rámci plnění Dodavatelské smlouvy jsou považována za majetek ČEPRO.
   7. Dodavatel v prostředí ČEPRO není oprávněn zejm.:
      1. mazat auditní záznamy;
      2. přistupovat k auditním záznamům nebo je měnit či s nimi jinak neoprávněně manipulovat;
      3. generovat auditní záznamy s cílem ztížit orientaci v auditní stopě; a
      4. generovat auditní záznamy s cílem zajistit vymazání jiného auditního záznamu (např. rotace auditních záznamů z důvodu omezení velikosti úložiště auditní stopy).
   8. Pracovníci Dodavatele v prostředí ČEPRO nemají oprávnění stahovat nelegální obsah (obsah, pro jehož použití nemají souhlas majitele licence) a nesmí navštěvovat stránky, jejichž obsah přímo nesouvisí s plněním pracovních povinností vyplývajících z Dodavatelské smlouvy.
   9. V prostředí ČEPRO pak zaměstnanci Dodavatele výslovně nesmí stahovat obsah nebo navštěvovat zejm. stránky:
      1. se sexuální tématikou / porno stránky;
      2. narušující výchovu mládeže či nabádající k chování, které je v rozporu se společensky přijatelnými normami chování;
      3. propagující diskriminaci jednotlivce či skupiny;
      4. propagující či zobrazující násilí, ať už vůči jednotlivci, skupině, celému národu, či demokratickému společenskému zřízení;
      5. propagující terorismus a teroristické organizace a/nebo genocidu národa;
      6. propagující či zobrazující násilí na zvířatech;
      7. navádějící ke spáchání trestného činu;
      8. jež hrubě zasahují do práv jednotlivce a zobrazují jej dehonestujícím způsobem.
   10. Pracovníci Dodavatele v prostředí ČEPRO nesmí provádět jakékoliv aktivity poškozující jiné fyzické nebo právnické osoby, včetně rozesílání nevyžádaných e-mailů (spamu), rozesílání podvodných e-mailů (phishing), distribuce škodlivého kódu nebo podílení se na útocích s cílem vyřadit dostupnost služeb (DoS, resp. DDoS).
   11. Na poskytnutém pracovním místě v prostorách ČEPRO je Dodavatel povinen zajistit:
       1. čistotu a pořádek tak, aby pracovní místo mohlo být bezpečně využito po čas fyzické nepřítomnosti Pracovníků Dodavatele;
       2. adekvátní fyzickou bezpečnost veškerých paměťových médií a tištěných dokumentů po čas fyzické nepřítomnosti Pracovníků Dodavatele; a
       3. logické uzamčení přístupu k informacím (datům, informačním službám, aplikacím) ČEPRO po čas fyzické nepřítomnosti Pracovníků Dodavatele tak, aby nemohlo dojít k neautorizovanému přístupu k těmto aktivům – např. uzamčení obrazovky počítače, odhlášení uživatele operačního systému, ukončení vzdálených relací a připojení apod.
   12. Pracovníci Dodavatele nejsou bez předchozího písemného souhlasu ČEPRO oprávněni v prostředí ČEPRO instalovat zařízení umožňující vzdálený odposlech a/nebo pořizovat jakýkoliv audiozáznam a/nebo videozáznam.
9. Vývoj a testování programového kódu
   1. Před započetím vývojových prací je Dodavatel povinen seznámit se se softwarovými a hardwarovými technologiemi, které jsou v prostředí ČEPRO podporované a používané. Dále je Dodavatel povinen si nechat odsouhlasit požadované zdroje (hardware, software atd.) a design/architekturu a z toho vyplívající případné další požadavky.
   2. Před započetím vývojových prací je Dodavatel povinen seznámit se s bezpečnostními a auditními požadavky ČEPRO na vyvíjený software.
   3. Dodavatel je povinen přistupovat k bezpečnosti informací jako k integrální součásti celého vývojového cyklu vývoje softwaru. Požadavky na informační bezpečnost musí být součástí analýzy požadavků na vyvíjený software, fáze plánování a návrhu vyvíjeného softwaru, a to ve vztahu k zamýšlenému nasazení a integraci do existujících procesů ČEPRO.
   4. Pro veškeré změny provedené Dodavatelem v produkčním prostředí ČEPRO musí existovat schválený helpdeskový požadavek ČEPRO.
   5. Pokud není v Dodavatelské smlouvě uvedeno jinak, součástí vývojových prací je i dodání úplné dokumentace, včetně:
      1. dokumentace architektury/designu – zahrnuje vztahy k prostředí a stavebním základům, které budou použity v návrhu softwarových komponent;
      2. technická dokumentace – dokumentace kódu, popis rozhraní a API;
      3. uživatelská dokumentace – manuály pro koncového uživatele, systémové administrátory a osazenstvo podpory;
      4. příručka pro administraci, instalaci a údržbu.
   6. Dodavatel musí ČEPRO proaktivně upozornit na všechny jemu známé skutečnosti spojené s vývojem a chováním dodaného kódu, které by po nasazení mohly negativně ovlivnit běh v produkčním prostředí a/nebo návazné systémy.
   7. Dodavatel odpovídá za životní cyklus programového kódu a souvisejících aktiv v tom smyslu, že ČEPRO bude včas podrobně informováno o jejich stavu, využití, potřebnosti apod.
10. Audit
    1. ČEPRO si vyhrazuje právo auditu, jehož cílem je ověřit soulad plnění bezpečnostních požadavků ČEPRO.
11. Krizové řízení
    1. Pracovníci Dodavatele jsou povinni maximálně předcházet vzniku krizových situací (např. požáru) a situacím, při kterých by mohlo dojít ke zranění osob nebo poškození majetku ČEPRO.
    2. V případě vzniku krizové nebo mimořádné situace (např. požár, výbuch, povodeň apod.) jsou Pracovníci Dodavatele, kteří jsou fyzicky přítomni v místě události, povinni bez výjimky a odkladu dodržovat předpisy a direktivy platné v dané lokalitě a uposlechnout pokynů k evakuaci a ochraně osob. Toto platí i pro případ cvičení.
    3. V případě krizového řízení jsou Pracovníci Dodavatele povinni bezodkladně uposlechnout pokynů krizového manažera ČEPRO, vedoucích k ochraně aktiv ČEPRO.
12. Hlášení požadavků a bezpečnostních incidentů
    1. Veškeré požadavky Dodavatele na součinnost ČEPRO související s přístupem, nákupem, provozem, bezpečnostním nastavením, konfiguračními změnami či jinými změnami informačních systémů a/nebo IT infrastruktury ČEPRO jsou evidovány v nástroji (Help Desk) ČEPRO nebo Dodavatele (podle Dodavatelské smlouvy).
    2. Dodavatel je povinen informovat ČEPRO i v případě (podezření ze) ztráty svěřeného informačního aktiva (např. přístupové karty, hesla, certifikátu apod.) a/nebo (podezření z) narušení bezpečnosti prostředí ČEPRO.
13. Utajení podkladů a informací
    1. Dodavatel bere na vědomí, že veškeré informace o skutečnostech týkající se ČEPRO, jeho podnikatelské činnosti s výjimkou informací všeobecně známých a dalších skutečností, jejichž zveřejnění by se mohlo jakýmkoliv způsobem dotknout obchodních zájmů nebo dobré pověsti ČEPRO, získané v jakékoliv formě v souvislosti s plněním Dodavatelských smluv nebo této Dohody, jakož i veškeré obchodní a technické informace, které byly sděleny (dále jen „**Důvěrné informace**“) se považují za důvěrné. Pro vyloučení jakýchkoliv pochybností se za Důvěrné informace považují také veškerá data a informace přímo a/nebo nepřímo se dotýkající IS KII.
    2. Dodavatel je povinen uchovávat získané Důvěrné informace tak, aby k nim neměly přístup třetí osoby, nepořizovat z nich kopie ani opisy, ani je jinak využívat, pokud k tomu nedá výslovný souhlas ČEPRO. Dodavatel je povinen neprodleně důvěrné informace podle dohody s ČEPRO buď vrátit, nebo je prokazatelně zničit, nejpozději však do 14 dnů po ukončení účinnosti příslušné Dodavatelské smlouvy. O vrácení nebo zničení musí být sepsán protokol, který musí podepsat odpovědná osoba ČEPRO. Za třetí osoby se pro účely tohoto článku nepovažují právní zástupci a auditoři Dodavatele.
    3. Povinnosti Dodavatele podle tohoto čl. 15 platí i po ukončení účinnosti příslušné Dodavatelské smlouvy, po dobu, dokud se Důvěrné informace nestanou všeobecně známými nebo neaktuálními (vyjma informací jakkoliv se dotýkajících IS KII), maximálně však po dobu 3 let po ukončení účinnosti příslušné Dodavatelské smlouvy (vyjma informací jakkoliv se dotýkajících IS KII a osobních údajů, na které to platí bez omezení).
    4. Dodavatel je povinen zajistit, že všechny osoby, které přijdou do styku s Důvěrnými informacemi budou vázány povinností mlčenlivosti a povinností utajovat tyto Důvěrné informace ve stejném nebo větším rozsahu, než jak je stanoveno tímto čl. 15.
14. Ochrana informačních a komunikačních systémů
    1. Dodavatel není oprávněn bez výslovného předchozího písemného souhlasu ČEPRO užívat informační a komunikační systémy ČEPRO, resp. k nim přistupovat.
    2. Dodavatel se zavazuje, že nezpůsobí, resp. učiní vše nezbytné a vynaloží veškerou možnou péči, kterou lze po něm objektivně požadovat, aby nedošlo k narušení, poškození nebo zničení informačních a komunikačních systémů ČEPRO, narušení důvěrnosti dostupnosti a integrity dat ČEPRO, a to včetně napadení informačních a komunikačních systémů a/nebo dat ČEPRO škodlivým softwarem, neoprávněným přístupem apod. Pokud Dodavatel způsobí uvedené v předchozí větě, je povinen učinit vše nezbytné a vynaložit veškerou možnou péči, kterou lze po něm spravedlivě požadovat, aby takové porušení odstranil. To Dodavatele nezbavuje povinnosti uhradit ČEPRO škodu vzniklou tímto porušením povinnosti ze strany Dodavatele.
15. Používání přístupové karty
    1. Přístup do prostor sídla ČEPRO a jeho dalších objektů je zabezpečen vstupním karetním systémem. Přístupová karta nahrazuje funkci bezpečnostního zámku. Každá z přístupových karet má přednastavena určitá oprávnění přístupu, která jsou centrálně spravována a řízena. Před přístupem do některých prostor ČEPRO je také kontrolována totožnost osob pomocí osobního dokladu. Je proto nutné, aby všichni, kdo potřebují vstoupit do prostor ČEPRO z důvodu plnění Dodavatelské smlouvy a/nebo v souvislosti s ní, byli schopni prokázat svou totožnost pomocí průkazu totožnosti (občanský průkaz, případně cestovní pas).
    2. ČEPRO zajistí pro Pracovníky Dodavatele přístupovou kartu, pouze je-li to nezbytné pro řádné plnění Dodavatelské smlouvy a na základě písemně žádosti, kterou může předložit pouze zaměstnanec ČEPRO. Požadavek na poskytnutí přístupové karty předkládá zaměstnanec ČEPRO odpovědný za komunikaci mezi Dodavatelem a ČEPRO. Zaměstnanec ČEPRO může požádat o poskytnutí přístupové karty pouze pro Pracovníka Dodavatele, je-li to zároveň nezbytné pro řádné plnění Dodavatelské smlouvy.
    3. Dodavatel, jehož Pracovníkovi Dodavatele byla přidělena přístupová karta, je povinen dodržovat následující pravidla:
       1. používat přístupovou kartu výhradně k účelům plnění Dodavatelské smlouvy;
       2. neposkytnout přístupovou kartu třetí osobě, resp. neumožnit třetí osobě vstup do prostor ČEPRO;
       3. ztrátu, odcizení nebo poškození přístupové karty hlásit okamžitě příslušnému útvaru, který kartu vydal;
       4. nepokoušet se o neoprávněný přístup do prostor, ke kterým nemá oprávnění; a
       5. na režimových pracovištích dodržovat pravidla stanovená pro tyto prostory.
    4. Dodavatel odpovídá v plném rozsahu za využití, resp. zneužití, přístupové karty.
    5. Dodavatel je povinen vrátit přístupovou kartu ČEPRO při ukončení Dodavatelské smlouvy, popř. dříve, byl-li o to ČEPRO výslovně požádán, a to vždy bez prodlení.
16. Používání technických a netechnických prostředků ČEPRO
    1. Dodavatel není oprávněn bez výslovného předchozího písemného souhlasu ČEPRO užívat technických nebo netechnických prostředků ČEPRO.
    2. Pro veškeré technické i netechnické prostředky instalované nebo provozované v ČEPRO platí následující pravidla:
       1. provozování a využívání veškerých technických i netechnických prostředků vyplývá z rozsahu plnění dle Dodavatelské smlouvy a konkrétně je schvalují odpovědní zástupci ČEPRO (vedoucí odboru IT a OBIA);
       2. ČEPRO si vyhrazuje právo rozhodnout, které z těchto prostředků je možné využívat a které nikoliv; příslušné rozhodnutí provádí úsek provozu příslušného IS KII / odbor IT;
       3. instalace, konfigurace nebo jiné nastavení technických i netechnických prostředků v prostředích ČEPRO provádí výhradně zástupci ČEPRO (úsek provozu příslušného IS KII / odbor IT) nebo jím jednoznačně určené osoby;
       4. nekompatibilní, nepodporované nebo nezpůsobilé prostředky nesmí být instalovány, konfigurovány nebo provozovány;
       5. veškeré prostředky využívané Dodavatelem musí být Dodavatelem adekvátním způsobem chráněny proti:
          1. narušení bezpečnosti dat a informací ČEPRO ve smyslu důvěrnosti, dostupnosti a integrity;
          2. zneužití třetími osobami (průnik do systému, aplikací atp.);
          3. ztrátě nebo poškození (zničení, odcizení nebo poškození dat nebo výpočetní techniky atp.);
          4. neoprávněnému použití (přístup k důvěrným informacím, službám, technických prostředků atp.);
          5. použití, které není v souladu s účelem jejich pořízení; a
          6. útokům třetích stran (škodlivé programové vybavení, hackerské útoky, nezáplatované zranitelnosti atp.).
    3. Ke kontrole využívání prostředků v souladu s výše uvedenými pravidly si vyhrazuje ČEPRO provádět jejich aktivní dohled včetně záznamu prováděných činností.
    4. Veškeré informace a data přenášené nebo uložené na technických prostředcích ČEPRO jsou vlastnictvím ČEPRO. Pro řádné spravování těchto firemních aktiv si ČEPRO vyhrazuje právo je prověřovat a analyzovat. Vzhledem k tomu, že jsou veškeré technické a komunikační systémy ČEPRO určeny především pro podporu jejích obchodních a dalších firemních aktivit, osoby, které je využívají, berou na vědomí, že na informace a data, které si v těchto systémech uloží, nebo pro jejichž přenos tyto prostředky použijí, se nepohlíží jako na informace privátní.
    5. Dodavatel je povinen vrátit užívané technické nebo netechnické prostředky ČEPRO ve stavu, ve kterém je převzal, s přihlédnutím k běžnému opotřebení, při ukončení Dodavatelské smlouvy, popř. dříve, byl-li o to ČEPRO výslovně požádán, a to vždy bez prodlení.
17. Zálohování
    1. Pro relevantní aktiva Dodavatele, která jsou používána pro anebo v souvislosti s plněním Dodavatelské smlouvy, je Dodavatel povinen zajistit vhodný cyklus zálohy dat, který splňuje smluvně ujednané požadavky dle Dodavatelské smlouvy. Přitom musí Dodavatel posoudit minimálně následující:
       1. plán zálohy ČEPRO a Dodavatele;
       2. umístění záloh (zálohy by měly být ukládány v jiné oblasti, než zálohována data);
       3. metody zálohování, formáty dat a médií;
       4. retenční období pro zálohování;
       5. ověřování integrity záloh;
       6. postupy obnovení a testování, včetně harmonogramů obnovy v případě narušení;
       7. použití šifrování;
       8. oddělení záloh v cloudovém prostředí s více zákazníky;
       9. frekvence a metody revize procesů pro zálohování a obnovu;
       10. dokumentace záloh a jejich obsahu, včetně označování médií.
    2. Zálohovaná data musí být chráněna před neoprávněným přístupem. Tato data musí být chráněna dalšími bezpečnostními opatřeními, které vyžaduje jejich klasifikace.
18. Účinnost Pravidel
    1. Tato Pravidla jsou účinná ode dne 17.9.2025.

1. Např. <https://www.nukib.cz/cs/infoservis/doporuceni/1843-doporuceni-v-oblasti-kryptografickych-prostredku-verze-2-0/> [↑](#footnote-ref-2)