PRAVIDLA PRO DODAVATELE 1.0

KLASIFIKACE ČP	Interní
TLP	GREEN[1]

Obsah

[1] Viz https://nukib.gov.cz/cs/infoservis/doporuceni/1862-doporuceni-k-pouzivani-protokolu-tlp-ke-sdileni-chranenych-informaci-2/

1 Úvodní ustanovení

Česká pošta zastává pozici odpovědné osoby ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „**ZKB**“) a vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „**VKB**“), konkrétně je správcem kritické informační infrastruktury (dále jen „**KII**“). Z tohoto důvodu je ke všem informačním a komunikačním systémům státního podniku Česká pošta (dále jen „**ČP**“) přistupováno jako ke KII, kterou je potřeba náležitě chránit a zabezpečit před potenciálními hrozbami a riziky v rámci řízení kybernetické bezpečnosti.

Kybernetická bezpečnost představuje inherentní a neoddělitelnou součást činností ČP. V souladu s platnými právními předpisy, normami a osvědčenými postupy klade ČP důraz na efektivní implementaci opatření týkajících se kybernetické bezpečnosti a tato opatření jsou vyžadována také v rámci činnosti dodavatelů. Tímto ČP přispívá k dodržování nejnovějších standardů a osvědčených postupů v rámci celého dodavatelského řetězce, s cílem zajistit optimální ochranu informačních aktiv a udržení kybernetické odolnosti v digitálním prostředí.

1.1 Účel

Následující dokument stanovuje pravidla pro dodavatele ČP v souladu s ustanoveními ZKB, VKB a dalších příslušných vyhlášek, opatření a metodických pokynů za účelem zachování požadované úrovně kybernetické a informační bezpečnosti ČP a snížení bezpečnostních rizik spojených s přístupem dodavatelů k informačním aktivům ČP v rámci životního cyklu dodávky.

1.2 Zkratky a pojmy

POJMY	
Bezpečnost informací	Zachování důvěrnosti, integrity a dostupnosti informací.
Bezpečnostní událost	událost, která může způsobit nebo způsobila narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací
Bezpečnostní incident	narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku Bezpečnostní události
Dodavatel	Osoba, která má s ČP uzavřenou Smlouvu.
Dodavatelská smlouva	Smlouva mezi ČP a dodavatelem na dodávky zboží a/nebo poskytování služeb, ve kterých vystupuje dodavatel jako dodavatel zboží a/nebo poskytovatel služeb a ČP jako odběratel tohoto zboží a/nebo služeb a jejíž dodávka se týká aktiv ČP.
Dostupnost	Dostupnost informace v okamžiku její potřeby.
Důvěrnost	Dostupnost informace pouze oprávněným osobám.
Informační a komunikační technologie (ICT)	Veškerá technika, která se zabývá zpracováním a přenosem informací, a to je zejména výpočetní a komunikační technika (hardware i firmware) a programové vybavení (např. firemní aplikace, e-mail, cloudová a interní úložiště, Skype pro firmy, atd.)
Integrita	Zajištění správnosti a úplnosti informací.
Mobilní zařízení	Přenosný elektronický přístroj s různým programovým vybavením jako např. mobilní telefon, notebook, notebook, smartbook, PDA, tablet, USB zařízení apod.

Pracovník	Zaměstnanci dodavatele a fyzické osoby v obdobném postavení (například DPP, DPČ, fyzická osoba na IČO apod.), kteří se podílí a/nebo mají podílet na plnění předmětu Smlouvy. Stanoví-li Pravidla povinnost pracovníkům dodavatele, dodavatel odpovídá za její s/plnění pracovníkem, průběžnou kontrolu a audit takového plnění a odpovídá za veškerou újmu způsobenou porušením takové povinnosti.
Pravidla pro uživatele	Pravidla pro chování uživatelů v prostředí ČP.
Uživatel	Každá fyzická osoba (včetně Pracovníků, zaměstnanec ČP nebo smluvně pověřený zaměstnanec externí fyzické nebo právnické osoby), které byl přidělen přístup k ICT ČP a příslušná přístupová oprávnění. Pro účely tohoto dokumentu se jedná o uživatele ICT ČP.
ZKRATKY	
ČP	Státní podnik Česká pošta (Česká pošta, s.p.).
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
Politika ČP	Bezpečnostní politika ČP, jednotlivé dokumenty, které ji tvoří a část bezpečností dokumentace ČP, se kterými byl Dodavatel seznámen ze strany ČP pro účely plnění Smlouvy.
Pravidla	Tato Pravidla pro dodavatele.
Smlouva	Hlavní smlouva uzavřená mezi ČP a dodavatelem. Součástí Smlouvy může být také dohoda o bezpečnostních aspektech při poskytování plnění uzavřená mezi ČP a dodavatelem a/nebo vypracování dokumentů relevantních pro bezpečnost informací (bezpečnostní projekt, analýza rizik, softwarová analýza apod).
VKB	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), ve znění pozdějších předpisů.
ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

2 Organizace bezpečnosti informací

- Dodavatel se zavazuje respektovat Politiku ČP v rozsahu a míře, ve které je ze strany ČP aplikována na Smlouvu a vztahuje se na předmět dodávky dle Smlouvy „Technická podpora pro 2 balancery F5 Viprion“.
- Dodavatel je povinen užívat data, ke kterým získá přístup při plnění Smlouvy, jen k účelu, pro který byla poskytnuta a jen za podmínek, které byly pro jejich využití stanoveny Smlouvou a Politikou ČP, rovněž tak povinnost zachovávat důvěrnost dat, a to i po ukončení Smlouvy za podmínek dle Smlouvy.
- Dodavatel je povinen seznámit všechny uživatele, bez ohledu na úroveň oprávnění, s pravidly pro uživatele.
- Dodavatel je povinen poskytnout ČP veškerou součinnost nezbytnou k tomu, aby ČP řádně naplňovala právní povinnosti stanovené ZKB a VKB, opatřeními a metodikami NÚKIB (v rozsahu, v jakém jsou součástí Politiky ČP). Zejména se dodavatel zavazuje poskytnout ČP součinnost směřující k zavedení a provádění bezpečnostních opatření podle ZKB, VKB a Politiky ČP.

- Dodavatel se zavazuje přijmout, udržovat a dokumentovat systém řízení bezpečnosti informací spočívající v přijetí dostatečných organizačních a technických opatření pro zajištění kybernetické a informační bezpečnosti, mít jej připravený na audit a kdykoliv jej na žádost ČP bezodkladně (nejdéle do 5 pracovních dnů) předložit. Taková žádost nebude zasílána dříve jak 30 dnů po uzavření Smlouvy.

3 Personální bezpečnost

- Dodavatel se zavazuje poskytnout ČP úplný jmenný seznam pracovníků dodavatele, kteří se podílejí na předmětu plnění Smlouvy. Dodavatel se zavazuje informovat ČP o změnách v pracovnících a personálním zabezpečení Smlouvy v předstihu minimálně 5 pracovních dní.
- Dodavatel se zavazuje informovat ČP o ukončení pracovního nebo obdobného poměru pracovníků dodavatele, pro které byly u ČP 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 (pokud je nutné zamezit přístup pracovníkovi ihned, oznámí to ČP).
- Dodavatel se zavazuje zavést systém prověřování uchazečů o zaměstnání a pracovníků, kteří se budou podílet na plnění pro ČP, aby zamezil vzniku potenciálního rizika v rámci přístupu k informačním a komunikačním systémům ČP.
- Dodavatel se zavazuje přijmout ve smlouvách se svými pracovníky odpovídající pravidla pro nakládání s informacemi, zachovávání kybernetické a informační bezpečnosti, zachování mlčenlivosti a zpracování osobních údajů v souladu s účinnými právními předpisy a poskytnout pracovníkům pravidla pro uživatele a smluvně či jiným podobným závazným způsobem (např. vnitřním předpisem) je zavázat k jejich dodržování.
- Pracovníci dodavatele:
    - musí být seznámeni s těmito Pravidly s bezpečnostními požadavky Smlouvy;
    - mají dostatečné znalosti a praktické zkušenosti pro plnění přidělených úkolů;
    - mají veškeré potřebné zkoušky a atestace, které vyplývají ze zákona nebo požadavků regulátora a/nebo Smlouvy na druh práce, kterou mají v prostředí ČP vykonávat;
    - jsou dodavatelem pravidelně školeni v oblastech bezpečnosti informací, kybernetické a informační bezpečnosti a právních a regulatorních požadavků relevantních pro naplnění předmětu Smlouvy;
    - kteří budou vstupovat nebo vjíždět do prostor ČP, 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 při pohybu v prostorách ČP.
- Dodavatel se zavazuje k vytvoření odpovídajícího disciplinárního procesu k přijetí opatření proti pracovníkům, kteří se dopustí porušení pravidel kybernetické a informační bezpečnosti v rámci nastaveného systému řízení kybernetické a informační bezpečnosti u dodavatele a komunikovaných pravidel pro zajištění kybernetické a informační bezpečnosti ČP.

4 Fyzická bezpečnost

- Přístup pracovníků dodavatele do prostor ČP je povolen, pouze pokud je jejich přítomnost nezbytná pro plnění pracovních povinností a na dobu nezbytně nutnou pro plnění pracovních povinností ze Smlouvy.
- Pracovníci dodavatele jsou povinni se v prostorách ČP pohybovat pouze v doprovodu odpovědného zaměstnance ČP.

- Pracovníci dodavatele nejsou oprávněni do prostředí ČP přinést zbraně, výbušniny, hořlaviny, bojové prostředky, jedy, radioaktivní a toxické látky, popř. jakékoli jiné látky ohrožující lidský život a/nebo zdraví.
- Bez písemného povolení ČP je zakázáno vynášení jakýchkoliv předmětů nepatřících pracovníkům dodavatele a/nebo nesloužících k plnění Smlouvy, zejména jakékoliv dokumentace a/nebo paměťové médium (CD/DVD/Blu-ray disk, flash disk / paměťové karty, hard disk, zálohovací pásky apod.) z prostor ČP, popř. jiného místa plnění příslušné Smlouvy určeného Smlouvou, a jejich kopírování, fotografování, pořizování videozáznamů, připojování k jiným zařízením (než zařízení ČP) apod., pokud není ve Smlouvě anebo jinde písemně dohodnuto jinak.
- Přístup pracovníků dodavatele do prostor ČP se zvýšeným stupněm bezpečnosti – chráněných zón se řídí Provozním řádem daného pracoviště, odpovědný zaměstnanec daného pracoviště seznámí pracovníka objednatele s pravidly daného pracoviště.
- Před vrácením paměťových médií dodavateli budou veškerá data ČP vymazána způsobem, který znemožňuje jejich opětovné obnovení.
- Za prostory ČP se považují také prostory využívané ČP na základě smluvního vztahu s jejich vlastníkem a/nebo oprávněným uživatelem.

5 Řízení aktiv

- Dodavatel je povinen zpracovávat a uchovávat důvěrná data a informace související s předmětem plnění Smlouvy pouze na IT prostředcích, které jsou umístěny v bezpečném perimetru definovaném Dodavatelem, pokud ČP nestanoví jinak v rámci Smlouvy či jiného právně závazného dokumentu.
- Dodavatel je povinen přistupovat k aktivům ČP pouze z prostředí a za použití prostředků dohodnutých ve Smlouvě; pokud nebyly dohodnuty ve Smlouvě, pak ze zabezpečeného prostředí a za použití důvěryhodných prostředků zabezpečených v souladu s best practice a nejméně zabezpečených v souladu s minimálními doporučenými požadavky NÚKIB. Za důvěryhodné se považují prostředí a prostředky, které jsou určené pro použití v podnikovém prostředí a jsou odpovídající pro plnění dle Smlouvy.

6 Řízení přístupových oprávnění

- Dodavatel se zavazuje řídit všechna přístupová oprávnění v souladu s principem minimálního oprávnění („need to know“).
- Dodavatel se zavazuje zajistit jedinečnou identifikaci osob, popřípadě i aplikací s právem přístupu. Jedinečná identifikace osob musí být spravována v rámci centrálního IDM v souladu s požadavky Smlouvy a nejsou-li takové, pak s požadavky VKB minimálními doporučenými požadavky NÚKIB.
- Dodavatel se zavazuje na své straně evidovat přístup svých pracovníků k rozhraním, službám a prostředkům ČP, které jim byly pro plnění Smlouvy poskytnuty.
- Dodavatel se zavazuje neprodleně oznamovat veškeré personální a jiné změny u svých pracovníků podílejících se na plnění pro ČP, které jsou relevantní pro přidělování, změnu nebo odejmutí přístupového oprávnění.
- Dodavatel se zavazuje monitorovat a dokumentovat činnost svých pracovníků při užívání vlastních rozhraní, služeb a prostředků, pokud jsou tyto technické prostředky využívány k plnění Smlouvy.
- Dodavatel odpovídá v plném rozsahu za neoprávněné využití, resp. zneužití, přístupového oprávnění (včetně loginu, hesla, popř. i dalších přidělených přihlašovacích údajů, jako je PIN, certifikát, token).
- Dodavatel není oprávněn po ukončení příslušné 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 Smlouvy ze strany ČP zrušeno.

- Dodavatel si je vědom toho, že ČP může jednostranně odebrat přístup do prostředí ČP v případě porušení Politiky ČP, Smlouvy a/nebo Pravidel, v případě bezpečnostního incidentu nebo jiného chování ohrožujícího (včetně navýšení rizika) bezpečnost informací a/nebo aktiv ČP.
- Individuální účty musí být dodavatelem vždy chráněny PIN nebo heslem (pokud jsou vydávány ze strany ČP, zajišťuje dané ČP). Heslo musí odpovídat minimálním požadavkům na hesla ČP a nejsou-li takové, pak minimálním požadavkům ZKB, VKB a metodických pokynů NÚKIB.

7 Bezpečnost provozu

- Dodavatel je povinen provádět pravidelný bezpečnostní monitoring IT prostředí dodavatele, logovat události na prostředí dodavatele a na rozhraní komunikace směrem k systémům ČP a periodické ověřování zranitelností u aplikací a nástrojů komunikujících se systémy ČP a u souvisejících podpůrných aktiv.
- Dodavatel je povinen na svém prostředí implementovat tzv. bezpečnostní záplaty do aplikací, operačních systému, nástrojů pro ošetření zranitelností, a to bez zbytečného prodlení v případě zjištění jakékoliv zranitelnosti.
- V případech, kdy to bude žádoucí a vhodné, je dodavatel povinen provádět i penetrační testování vlastního prostředí.

8 Bezpečnost komunikací

- Dodavatel se zavazuje k zavedení bezpečnostních mechanismů k zajištění bezpečnosti sítě na svém prostředí.
- V případě, že je Smlouvou a/nebo v rámci opatření pro snížení rizik navrženo zavedení šifrování, musí parametry kryptografických prostředků a povolené algoritmy naplňovat požadavky na šifrování dle Politiky ČP a nejsou-li takové, pak požadavky dle VKB § 26 Kryptografické prostředky a aktuální doporučení NÚKIB v oblasti kryptografických prostředků.
- Komunikace mezi prostředím dodavatele a prostředím ČP musí probíhat pouze na zabezpečeném rozraní, které je monitorováno, není-li ve Smlouvě uvedeno jinak.

9 Řízení poddodavatelů

- Dodavatel se zavazuje zavést pravidla výběru a postupy pro řízení a evidenci svých poddodavatelů, podílejících se na plnění této zakázky v souladu s pravidly a postupy ČP.
- Dodavatel se zavazuje využít pro plnění zakázky pouze bezúhonné subjekty a osoby, na jejichž straně nestojí žádné bezpečnostní překážky (ve smyslu kybernetické bezpečnosti).
- Dodavatel se zavazuje přenést na tyto subjekty povinnost poskytnout veškerou potřebnou součinnost pro provedení hodnocení rizik.
- Dodavatel se zavazuje své poddodavatele smluvně či podobným způsobem zavázat k dodržování těchto Pravidel, Politiky ČP a dalších povinností v oblasti bezpečnosti informací vyplývajících ze Smlouvy v rozsahu, v jakém je k nim zavázán sám.

10 Řízení bezpečnostních incidentů

- Dodavatel je povinen vyhodnocovat bezpečnostní události svých aplikací a nástrojů a souvisejících podpůrných aktiv, které se podílejí na této zakázce a mohou ovlivnit bezpečnost ČP.

- Dodavatel je povinen nahlásit ČP podezření na bezpečnostní zranitelnosti, bezpečnostní události nebo bezpečnostní incidenty vzniklé v jakékoliv souvislosti s plněním povinností dodavatele, ať už by k tomu došlo při užívání rozhraní, služeb a prostředků ČP anebo na straně dodavatele či jeho poddodavatele (či kterékoliv jiné osoby, např. pracovníků), které jsou relevantní pro zachování bezpečnosti informací aktiv ČP (včetně schopnosti způsobit změnu v hodnocení rizik) a/nebo by mohly mít negativní vliv na předmět plnění nebo ohrozit chod IS ČP. Pokud je v takovém případě možné přijmout opatření k zabránění vzniku bezpečnostního incidentu, je dodavatel povinen je přijmout a doporučit ČP kroky k přijetí takových opatření (na ostatním prostředí ČP).
- Dodavatel je povinen oznámit ČP a evidovat každý bezpečností incident vzniklý v jakékoliv souvislosti s plněním povinností dodavatele, ať už by k tomu došlo při užívání rozhraní, služeb a prostředků ČP anebo na straně dodavatele či jeho poddodavatele (či kterékoliv jiné osoby, např. pracovníků), které jsou relevantní pro zachování bezpečnosti informací aktiv ČP (včetně schopnosti způsobit změnu v hodnocení rizik) a/nebo by mohly mít negativní vliv na předmět plnění nebo ohrozit chod IS ČP. Dodavatel je povinen oznámit takový bezpečností incident nejpozději do čtyř (4) hodin po jeho zjištění. Dodavatel zároveň sdělí ČP opatření, která již provedl ve vztahu k tomuto bezpečnostnímu incidentu, aby ČP mohla případně splnit svou ohlašovací povinnost dle ZKB.
- Dodavatel je povinen ohlásit jednotlivý bezpečnostní incident nebo událost [redacted]

11 Zabezpečení mobilních zařízení

- Mobilní zařízení, skrz které mají pracovníci a/nebo dodavatel přístup k aktivům ČP a/nebo na nich mají uložena aktiva ČP, musí nad rámec dalších požadavků uvedených v těchto Pravidlech, splňovat v tomto článku níže uvedené požadavky.
- Mobilní zařízení musí být vždy chráněno PIN nebo heslem. Heslo musí odpovídat minimálním požadavkům na hesla ČP a nejsou-li takové, pak minimálním požadavkům ZKB, VKB a metodických pokynů NÚKIB.
- Mobilní zařízení musí být adekvátním způsobem chráněna proti:
  - narušení bezpečnosti dat a informací ČP;
  - zneužití třetími osobami (průnik do systému, aplikací atp.);
  - ztrátě nebo poškození (zničení, odcizení nebo poškození dat nebo výpočetní techniky atp.);
  - neoprávněnému použití (přístup k důvěrným informacím, službám, technických prostředků atp.);
  - použití, které není v souladu s účelem jejich pořízení a/nebo účelem, pro které jim byl umožněn přístup k aktivům ČP; a
  - útokům třetích stran (škodlivé programové vybavení, hackerské útoky, nezáplatované zranitelnosti atp.).
- Pokud dodavatel používá zařízení dodané ČP je Dodavatel povinen vrátit užívané mobilní zařízení ČP ve stavu, ve kterém je převzal, s přihlédnutím k běžnému opotřebení, při ukončení Smlouvy, popř. dříve, byl-li o to ze strany ČP výslovně požádán, a to vždy bez prodlení.

12 Soulad s pravidly pro dodavatele

- Dodavatel se zavazuje k součinnosti v rámci pravidelných kontrol ze strany ČP, které mají za cíl ověřit soulad procesů a postupů s těmito Pravidly, a to za podmínek dle Politiky ČP a/nebo Smlouvy.

13

ČÍSLO PŘÍLOHY	NÁZEV
1.	Pravidla pro externí uživatele

Příloha č.1.

Pravidla pro Externí Uživatele Přistupující k Informačním Systémům ČP

Úvod

Tento dokument stanovuje pravidla a směrnice pro externí uživatele, kteří budou v rámci podpory **balancerů F5 Viprion** přistupovat k informačním systémům objednatele. Cílem je zajistit bezpečnost, spolehlivost a soulad s předpisy při manipulaci s těmito systémy.

1. Oprávnění:

a. Přístup k informačním systémům objednatele v rámci podpory balancerů F5 Viprion je povolen pouze osobám, které obdržely příslušná oprávnění od odpovědného řídícího pracovníka objednatele.
b. Externí uživatelé jsou povinni respektovat platné zákony, předpisy a interní politiky objednatele týkající se bezpečnosti informací.

2. Zabezpečení:

a. Externí uživatelé jsou povinni dodržovat veškerá bezpečnostní opatření a postupy, včetně autentizace, šifrování a monitorování přístupů.
b. Přístup k informačním systémům musí být zabezpečen použitím bezpečných metod, jako je dvoufaktorová autentizace VPN připojení.

3. Dostupnost a výkon:

a. Externí uživatelé jsou povinni minimalizovat jakékoli zásahy do provozu informačních systémů objednatele a dbát na to, aby jejich činnost nepoškozovala dostupnost nebo výkon systémů.
b. Při provádění údržby nebo konfigurace balanceru F5 Viprion je nutné zajistit minimální vliv na provoz systémů objednatele a předem koordinovat veškeré plánované změny s odpovědnými pracovníky objednatele.

4. Odpovědnost:

a. Externí uživatelé jsou plně odpovědní za své jednání a za důsledky svých akcí spojených s přístupem k informačním systémům objednatele.
b. Každý incident, který může ohrozit bezpečnost nebo integrity dat, musí být okamžitě nahlášen odpovědnému řídícímu pracovníkovi objednatele.

5. Dodržování pravidel:

a. Porušení těchto pravidel může vést k okamžitému odebrání přístupových práv a může mít právní následky.
b. Externí uživatelé jsou povinni pravidelně revidovat tato pravidla a zajistit jejich dodržování.

Tento dokument je platný od 1.3.2024 a jeho dodržování je povinné pro všechny externí uživatele přistupující k informačním systémům objednatele v rámci smlouvy o poskytování technické podpory pro balancery F5 viprion.