

Smlouva o poskytování podpory a rozvoje linuxové distribuce CentOS pro XAPOST a o zajištění přechodu na AlmaLinux vč. podpory a rozvoje této platformy

číslo 2025/03440

Česká pošta, s.p.

se sídlem: Politických vězňů 909/4, 225 99 Praha 1
IČO: 47114983
DIČ: CZ47114983
zastoupen: Ing. Martinem Götzem, ředitelem úseku ICT a eGovernment
zapsán v obchodním rejstříku u: Městského soudu v Praze, oddíl A, vložka 7565
bankovní spojení: [REDACTED]
[REDACTED]

dále jen „**Objednatel**“

a

LinuxBox.cz, s.r.o.

se sídlem: 28. října 1142/168, 709 00 Ostrava
IČO: 25862782
DIČ: CZ25862782
zastoupena: Ing. Dušanem Lampartem, jednatelem
zapsána v obchodním rejstříku u: Krajského soudu v Ostravě, oddíl C, vložka 22897
bankovní spojení: [REDACTED]
[REDACTED]

dále jen „**Dodavatel**“

dále jednotlivě jako „**Smluvní strana**“, nebo společně jako „**Smluvní strany**“ uzavírají v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“) a zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**Zákon o zadávání veřejných zakázek**“) tuto Smlouvu o poskytování podpory a rozvoje linuxové distribuce CentOS pro XAPOST a o zajištění přechodu na AlmaLinux vč. podpory a rozvoje této platformy (dále jen „**Smlouva**“).

Preambule

Objednatel provedl zadávací řízení k veřejné zakázce „Podpora a rozvoj linuxové distribuce CentOS pro XAPOST a přechod na AlmaLinux vč. podpory a rozvoje této platformy“ (dále jen „**Zadávací řízení**“) na uzavření této Smlouvy. Tato Smlouva je uzavřena s Dodavatelem na základě výsledku

Zadávacího řízení. Objednatel tímto ve smyslu ust. § 1740 odst. 3 Občanského zákoníku předem vylučuje přijetí nabídky na uzavření této Smlouvy s dodatkem nebo odchylkou.

1 Účel a předmět Smlouvy

- 1.1 Účelem této Smlouvy je vytvoření a zprovoznění distribuce AlmaLinux v prostředí XAPOST na pobočkách Objednatele, případně partnerů Objednatele, pro zajištění byznys-činností Objednatele, která po kompletní migraci plnohodnotně nahradí současnou distribuci CentOS pro XAPOST, kterou Objednatel využívá na stanicích na pobočkách. Účelem Smlouvy je dále komplexní zajištění přechodu, podpory provozu a rozvoje používaných linuxových distribucí na pobočkách Objednatele, případně partnerů Objednatele. Současná verze distribuce CentOS používaná Objednatelem je upravená verze distribuce (viz Příloha č.1 Smlouvy) pro potřeby prostředí XAPOST na pobočkách Objednatele.
- 1.2 Předmětem této Smlouvy je:
 - a) vytvoření návrhu přechodu linuxové distribuce CentOS pro XAPOST na distribuci AlmaLinux pro XAPOST, který bude obsahovat popis prostředí, návrh řešení, návrh postupu migrace, návrh testování a ladění, návrh pilotního provozu a návrh způsobu vyhodnocení realizace v rámci akceptace (dále jen „**Cílový koncept**“ nebo také „**CK**“);
 - b) zhotovení díla spočívajícího v úpravě distribuce AlmaLinux (včetně konfigurace a odladění) v prostředí XAPOST, na pobočkách Objednatele, případně partnerů Objednatele, včetně realizace prostředí (vývojového, testovacího, produkčního) pro nasazování patchů a SW-balíčků na jednotlivé stanice na dálku, bez zásahu obsluhy (dále jen „**AlmaLinux XAPOST**“ nebo také „**Systém**“). Součástí díla je rovněž realizace pilotního provozu na vybraných lokalitách a pobočkách Objednatele (dále jen „**Pilot**“);
 - c) provedení přechodu - plošné migrace na AlmaLinux XAPOST podle schváleného návrhu v CK na všech pobočkách Objednatele, případně partnerů Objednatele (dále jen „**Přechod**“);
 - d) poskytování podpory obou distribucí, tedy stávající distribuce CentOS pro XAPOST a po dokončení Přechodu rovněž odladěné distribuce AlmaLinux XAPOST na stanicích na pobočkách Objednatele, případně partnerů Objednatele (dále jen „**Podpora**“);
 - e) realizace rozvoje a řešení změnových požadavků obou Objednatelem používaných distribucí, příp. poskytnutí součinnosti při implementaci změnových požadavků používané linuxové distribuce v prostředí Objednatele (dále jen „**Rozvoj**“).(dále společně jen „**Plnění**“).
- 1.3 Dodavatel se podpisem této Smlouvy zavazuje poskytovat v souladu s ustanoveními Smlouvy Objednateli Plnění specifikované ve Smlouvě v co nejlepším provedení a jakosti odpovídající aktuálnímu stavu technologického vývoje a poznání na expertní úrovni.
- 1.4 Objednatel se tímto zavazuje za řádně poskytnuté Plnění zaplatit dohodnutou cenu způsobem ve Smlouvě definovaným.
- 1.5 Po uzavření Smlouvy sdělí Objednatel Dodavateli číslo evidenční objednávky pro účely fakturace Plnění dle odst. 1.2 písm. a) – d) Smlouvy (dále jen „**OBJ**“). Dodavateli je sděleno pouze číslo evidenční objednávky za účelem jeho uvedení na daňovém dokladu. Evidenční objednávka nemá vliv na plnění Smlouvy a povinnost Dodavatele dodat Plnění řádně a včas.

2 Podpora

- 2.1 Podpora podle odst. 1.2 písm. d) této Smlouvy zahrnuje následující plnění:
 - a) aktualizace Systému nasazením vyšší verze (upgrade) distribuce a SW, který je součástí instalace, včetně zajištění odpovídajících licencí a dodání instalačně servisního manuálu;

- b) automatické průběžné bezpečnostní aktualizace Systému, včetně integrace bezpečnostních prvků s ohledem na požadavky bezpečnosti;
 - c) poskytování a nasazení opravných patchů – verzí, service packů a hotfixů, včetně souvisejících licencí a dokumentace v českém jazyce a instalačních manuálů;
 - d) příjem, registraci a transparentní správu všech požadavků v rámci Podpory a hlášených incidentů;
 - e) řešení incidentů, včetně diagnostiky a odstraňování vad, chyb a vadných či nestandardních stavů (dále jen „vady“) Systému, včetně případných konzultací a jednání souvisejících s jejich řešením s Objednatelem; prioritu zásahu a kategorii vady definuje podle odst. 2.6 Smlouvy Objednatel;
 - f) řešení požadavků na integraci nových zařízení a SW do OS, včetně konzultací s vývojovými týmy SW, které jsou na daném OS provozovány;
 - g) zajištění podpory Systému poskytované výrobcem Systému;
 - h) související dokumentace v českém jazyce a poskytnutí bezplatného přístupu na internetové stránky výrobce Systému k informacím týkajícím se Systému, resp. obou distribucí;
 - i) provozování kontaktní hot-line v českém jazyce (veškerá komunikace bude probíhat v českém, případně slovenském jazyce);
 - j) průběžné upozorňování Objednatele formou doporučení na možnosti aktualizací a úprav a navrhování souvisejících úprav Systému, případně i HW;
 - k) podporu při testování, instalaci a implementaci;
 - l) podporu při případné integraci technologií třetích stran.
- 2.2 Dodavatel je povinen poskytovat Podporu v pracovních dnech (tj. mimo soboty, neděle a státní svátky) v čase 8:00 – 16:00 hodin po celou dobu účinnosti Smlouvy.
- 2.3 Hot-line je provozována na telefonním čísle a e-mailové adrese uvedených v Příloze č. 4 Smlouvy. Za dostupnou hot-line se považuje i případ, kdy bude možné zanechat vzkaz na záznamníku, nebo odeslat požadavek e-mailem, aniž by bylo Objednateli doručeno oznámení o nemožnosti doručit e-mailovou zprávu obsahující požadavek.
- 2.4 Podpora spočívající v odstraňování vad podle odst. 2.1 písm. e) Smlouvy bude poskytována na základě požadavků Objednatele zadaných prostřednictvím hot-line. Vadou Systému se rozumí rozpor mezi skutečnými vlastnostmi Systému a vlastnostmi specifikovanými v dokumentaci vztahující se k Systému. Požadavek zadává Objednatel telefonicky nebo písemně na uvedenou e-mailovou adresu. V případě zadání požadavku telefonicky je Objednatel povinen jej zaslat Dodavateli také písemně.
- 2.5 Požadavek dle předchozího odstavce Smlouvy musí obsahovat alespoň tyto údaje:
- a) jméno osoby, která vadu nahlásila;
 - b) jméno odpovědné osoby ze strany Objednatele dle Přílohy č. 4;
 - c) kategorii vady a očekávaný termín vyřešení;
 - d) popis vady včetně popisu simulace v testovacím prostředí.
- Každá vada bude hlášena samostatným požadavkem. Vzor požadavku je uveden v Příloze č. 3 Smlouvy.
- 2.6 Kategorie vad:

Kategorie	Definice
-----------	----------

A	Základní nefunkčnost Systému bránící v jeho užití/fungování nebo bránící v užití/fungování dalších částí IT systému Objednatele. Provoz nebo vývoj Systému je zastaven. Objednatel nemůže pokračovat v dalším provozu nebo vývoji.
B	Dílní nefunkčnost Systému vč. nefunkčnosti některé části/komponenty. Provoz nebo vývoj je pozastaven, ale s možností dočasného obejití problému (workaround) může pokračovat po určitou dobu.
C	Méně závažné vady nemající vliv na základní funkcionality Systému. Provoz nebo vývoj je problémem ovlivněn, ale Systém může pokračovat jiným způsobem.
D	Dílní drobné vady Systému. Provoz nebo vývoj může pokračovat.

- 2.7 Dodavatel garantuje, že doba odezvy ze strany Dodavatele je pro vady kategorie A a B do jedné (1) hodiny a pro vady kategorie C a D do dvou (2) hodin od nahlášení požadavku. Tato doba odezvy platí v časovém období dle odst. 2.2 této Smlouvy. Dobou odezvy se rozumí potvrzení Dodavatele o přijetí požadavku učiněné telefonicky a následně vždy písemně e-mailem na kontakt Objednatele uvedený v Příloze č. 4 Smlouvy, navržení způsobu řešení a zahájení prací na odstranění vady.
- 2.8 Maximální doba pro odstranění vady kategorie A je 24 hodin, pro kategorie B je 48 hodin a pro kategorie C a D do 5 pracovních dnů. Na termínu vyřešení problému, resp. odstranění vady se Smluvní strany dohodnou písemně prostřednictvím odpovědných osob ve věcech technických. O odstranění vady následně Smluvní strany vyhotoví oboustranně podepsaný zápis – akceptační protokol podle vzoru v Příloze č. 5 Smlouvy.
- 2.9 Bylo-li Objednatelem umožněno poskytování Podpory prostřednictvím vzdáleného přístupu, bude vada primárně odstraněna prostřednictvím vzdáleného přístupu. V ostatních případech nebo není-li Dodavatel schopen vadu prostřednictvím vzdáleného přístupu odstranit, garantuje Dodavatel příjezd experta-konzultanta Dodavatele na místo podle určení Objednatele za účelem poskytnutí Podpory spočívající v odstranění vady do osmi (8) hodin od nahlášení požadavku dle odst. 2.4 Smlouvy Objednatelem, nedohodnou-li se Smluvní strany na delší době.
- 2.10 Doba odezvy dle odst. 2.7 Smlouvy, doba pro vyřešení požadavku dle odst. 2.8 Smlouvy a doba pro příjezd experta-konzultanta Dodavatele dle odst. 2.9 Smlouvy se počítá od prvního (písemného nebo telefonického) nahlášení požadavku Objednatelem vždy v časovém období dle odst. 2.2 Smlouvy.

3 Cílový koncept, zhotovení AlmaLinux pro XAPOST, Pilot a Přechod

- 3.1 Dodavatel se zavazuje zajistit realizaci Plnění dle odst. 1.2 písm. a) – c) Smlouvy dle dále uvedených podmínek.
- 3.2 Dodavatel provede rekognoskaci a analýzu prostředí Objednatele tak, aby měl aktuální informace o prostředí a aktuální verzi a konfiguraci distribuce CentOS pro XAPOST v prostředí Objednatele. Výsledky analýzy a popis prostředí budou součástí Cílového konceptu.
- 3.3 Dodavatel vypracuje v českém jazyce Cílový koncept, kde popíše postup dalšího průběhu Plnění, včetně harmonogramu, který bude respektovat termíny dle této Smlouvy, zejm. pak dle odst. 5.2 Smlouvy. Součástí CK bude zejména:
- a) podrobný harmonogram Plnění;

- b) popis průběhu pilotního ověření funkčnosti AlmaLinux XAPOST v prostředí Objednatele, tj. návrh postupu pilotního nasazení, lokality pilotního nasazení, instalační postupy, testovací scénáře a akceptační postupy;
 - c) popis postupu při Přechodu a testovací scénáře pro testování verzí distribuce AlmaLinux XAPOST.
- 3.4 Cílový koncept projde u Objednatele schvalovacím procesem, v němž Objednatel ověří, že Cílový koncept respektuje požadavky a termíny uvedené v této Smlouvě. Řádné dokončení a předání Cílového konceptu Objednatel potvrdí podpisem Akceptačního protokolu, jehož vzor tvoří Přílohu č. 5 této Smlouvy.
- 3.5 Na základě Objednatelem schváleného Cílového konceptu Dodavatel zhotoví AlmaLinux XAPOST a následně provede Pilot, tj. migraci současné distribuce CentOS pro XAPOST na distribuci AlmaLinux XAPOST v pilotních lokalitách Objednatele schválených v rámci CK.
- 3.6 Po dokončení Pilotu proběhne vyhodnocení ověření funkčnosti a spolehlivosti nového Systému na pilotních pobočkách postupem dle schváleného Cílového konceptu. Dodavatel je povinen před akceptací Systému odstranit veškeré vady, chyby, nefunkčnosti či jiné nálezy zjištěné v rámci Pilotu.
- 3.7 Úspěšné dokončení Pilotu, zahrnující odstranění veškerých vad, chyb, nefunkčností, nesouladů s CK či jiných nálezů Systému a úspěšné provedení všech akceptačních testů ověřujících funkcionalitu, potvrdí Objednatel podpisem akceptačního protokolu, jehož vzor tvoří Přílohu č. 5 Smlouvy.
- 3.8 Pokud Pilot neproběhne úspěšně, plošný Přechod se nesmí zahájit, Dodavatel je povinen přehodnotit a upravit Cílový koncept, který musí být opětovně postoupen Objednateli ke schválení, musí dojít znovu k vývoji a ladění Systému a následně bude opět provedeno pilotní nasazení. Odpovědnost Dodavatele za prodlení tím není dotčena.
- 3.9 Objednatel si vyhrazuje právo posoudit úspěšnost Pilotu a rozhodnout o realizaci či nerealizaci plošného nasazení - Přechodu distribuce AlmaLinux pro XAPOST v prostředí Objednatele, případně partnerů Objednatele.
- 3.10 V případě rozhodnutí Objednatele o nerealizaci plošného Přechodu je Dodavatel povinen pilotní lokality uvést na vlastní náklady do původního stavu.
- 3.11 Pokud Pilot proběhl úspěšně a Objednatel rozhodl o plošném nasazení, Dodavatel provede podle Cílového konceptu plošný Přechod na novou distribuci AlmaLinux XAPOST na všech pobočkách Objednatele, případně partnerů Objednatele dle seznamu, který bude součástí Cílového konceptu. Přechod bude ukončen akceptačním řízením a podpisem Akceptačního protokolu, jehož vzor tvoří Přílohu č. 5 Smlouvy. Podmínkou akceptace je plně funkční veškerý SW a HW v novém Systému a plně funkční systém dálkového řízení updatu a upgradu Systému na pobočkách Objednatele, případně partnerů Objednatele, a odstranění veškerých incidentů, chyb či jiných nálezů po provedení Přechodu.

4 Rozvoj

- 4.1 Rozvojem dle odst. 1.1 písm. e) Smlouvy, který se Dodavatel Objednateli zavazuje zajistit, se rozumí realizace dílčích změnových požadavků (dále též jen „**Dílčí požadavek**“) Objednatele nad rámec poskytované Podpory Dodavatelem dle této Smlouvy, příp. zajištění součinnosti související se Systémem či Dílčím požadavkem. Rozvoj bude realizován na základě dílčí objednávky od Objednatele.
- 4.2 Dodavatel se zavazuje zajistit Rozvoj na základě objednávky doručené Objednatelem Dodavateli (dále jen „Objednávka“) a následně uzavřené dílčí smlouvy na Rozvoj o realizaci konkrétního

Dílčího požadavku / poskytnutí školení či expertízy (dále jen „**Dílčí smlouva**“). Objednatel je oprávněn, avšak nikoli povinen, vystavovat dle svého uvážení Objednávky ode dne účinnosti Smlouvy bez omezení jejich počtu. Objednávka se považuje za návrh na uzavření Dílčí smlouvy.

- 4.3 Objednávka Rozvoje musí obsahovat minimálně tyto náležitosti:
- a) identifikační údaje Dodavatele a Objednatele;
 - b) číslo Objednávky a datum vystavení;
 - c) číslo Smlouvy;
 - d) název a popis Rozvoje a jeho rozsah;
 - e) pracnost realizace (v MD) a cenu;
 - f) podmínky akceptace;
 - g) termín a místo realizace;
 - h) podpis/zaručený elektronický podpis oprávněné osoby Objednatele.
- 4.4 Neobsahuje-li Objednávka shora uvedené náležitosti, je Dodavatel povinen na tuto skutečnost Objednatele neprodleně upozornit. Objednatel poté neprodleně vystaví novou Objednávku. Veškeré doby a lhůty vázané na okamžik doručení Objednávky Dodavateli běží od okamžiku doručení této nové Objednávky.
- 4.5 Dodavatel je povinen přijmout Objednávku do dvou (2) pracovních dnů od jejího doručení. Dodavatel je oprávněn Objednávku odmítnout pouze v případě, že je učiněna v rozporu s touto Smlouvou nebo došlo již k překročení celkové hodnoty Plnění dle odst. 6.6 Smlouvy. Doručením přijetí Objednávky Objednateli dojde i k uzavření Dílčí smlouvy, přičemž práva a povinnosti Smluvních stran dle Dílčí smlouvy odpovídají v celém rozsahu právům a povinnostem Objednatele a Dodavatele stanovených touto Smlouvou. Není-li dále v této Smlouvě sjednáno jinak, Objednávka i její přijetí musí mít písemnou formu.
- 4.6 Přijetí Objednávky musí obsahovat minimálně tyto náležitosti:
- a) identifikační údaje Objednatele a Dodavatele;
 - b) číslo přijaté Objednávky a datum vystavení přijetí;
 - c) podmínky akceptace;
 - d) podpis/zaručený elektronický podpis oprávněné osoby Dodavatele.
- 4.7 Přijetí Objednávky, které obsahuje dodatky, výhrady, omezení nebo jiné změny a odchylky se považuje za odmítnutí Objednávky a za nový návrh Dodavatele na uzavření Dílčí smlouvy, a to i v případě dodatku, výhrady, odchylky, omezení nebo jiné změny, která podstatně nemění obsah a podmínky Objednávky. Dílčí smlouva je v takovém případě uzavřena pouze tehdy, pokud Objednatel tento návrh Dodavateli písemně potvrdí. Okamžikem uzavření Dílčí smlouvy je v tomto případě doručení potvrzení Objednatele Dodavateli.
- 4.8 Realizovaný Dílčí požadavek musí představovat řešení, které je navrženo jako robustní a spolehlivé, bez „Single point of failure“, tedy tak, aby výpadek jediné komponenty nezpůsobil výpadek celého systému. Při návrhu architektury řešení budou využity postupy a technologie umožňující budoucí škálovatelnost aplikace. Realizovaný Dílčí požadavek musí být připraven na dodatečná rozšíření a úpravy funkcionality, datových struktur a dalších prvků dle požadavků Objednatele. Realizovaný Dílčí požadavek bude co nejvíce využívat ověřené technologie a otevřené standardy. Dodavatel odpovídá za to, že Realizovaný Dílčí požadavek bude splňovat požadavky uvedené v tomto odstavci.

- 4.9 Součástí realizovaného Dílčího požadavku je i jeho instalace a implementace v informačním systému a prostředí Objednatele a uvedení do rutinního (produkčního) provozu, včetně předání související dokumentace s popisem realizovaného Dílčího požadavku, jeho implementace a instalace do systému, případně dokumentace související s provozem realizovaného Dílčího požadavku a uživatelská dokumentace. Konkrétní specifikace požadované dokumentace bude součástí každé Objednávky.
- 4.10 Dodavatel se zavazuje, že popis realizace Dílčího požadavku bude vyhotoven v české jazykové verzi.
- 4.11 Dodavatel se zavazuje vytvořit a předat realizovaný Dílčí požadavek v nejvyšší kvalitě a jakosti bez faktických a právních vad.
- 4.12 Výstup realizace dle příslušné Dílčí smlouvy (Dílčí požadavek) bude předán Objednateli v termínu sjednaném v Dílčí smlouvě. Odpovídá-li to povaze Dílčího požadavku, budou Objednatelem provedeny akceptační testy ověřující funkcionálníitu Dílčího požadavku podle Smluvními stranami odsouhlaseného akceptačního scénáře. V takovém případě musí být Dílčí požadavek před předáním a převzetím poskytnut k akceptaci v termínu předem sjednaném v Dílčí smlouvě, jinak v termínu přiměřeném s ohledem na předpokládanou dobu trvání akceptačních testů a sjednaný termín poskytnutí Rozvoje. Akceptační scénář může v rámci Objednávky stanovit Objednatel, pokud tak neučiní akceptační scénář navrhuje v rámci přijetí Objednávky Dodavatel a schvaluje Objednatel v podobě upravené Objednávky. V případě neshody Smluvních stran o obsahu akceptačního scénáře a akceptačních testů je rozhodující stanovisko Objednatele. Akceptační testy provádí Objednatel za součinnosti Dodavatele. K převzetí Dílčího požadavku dojde až podpisem akceptačního protokolu Objednatelem po úspěšném provedení akceptačních testů s výsledkem „Dílčí požadavek vyhovuje“. Dílčí požadavek je však dokončen až odstraněním všech vad zjištěných při akceptačních testech uvedených v akceptačním protokolu. Pokud se bude jednat o Rozvoj bez konkrétního zachytitelného výstupu (např. ústní konzultace, školení apod.), potvrdí Smluvní strany jejich předání a převzetí písemným zápisem – akceptačním protokolem, včetně uvedení odpracovaného počtu MD.
- 4.13 Kategorizace vad zjištěných v průběhu akceptačních testů:
- a) **vadou kategorie A** se rozumí taková vada, která způsobuje tak závažné problémy, že nemůže být zaručeno fungování Dílčího požadavku v rámci Systému a jeho použití Objednatelem. Vadou kategorie A jsou i právní vady Dílčího požadavku;
 - b) **vadou kategorie B** se rozumí taková vada, která ohrozí další pokračování akceptačních testů, jestliže nebude odstraněna, anebo provoz dalších částí Dílčího požadavku. Za vadu kategorie B se považuje také taková vada, která zapříčiní, že by nebyly podporovány některé části Dílčího požadavku nebo některé části Systému bez přiměřené náhrady;
 - c) **vadou kategorie C** se rozumí taková vada, která způsobí částečný neúspěch akceptačních testů. V případě existence vady kategorie C nesmí dojít za provozních podmínek ke ztrátě žádné závažné funkce Dílčího požadavku, anebo je možné pro její překonání nalézt odpovídající alternativu.
- 4.14 Kategorizaci vad provádí Objednatel. Vadami nemohou být označovány vady software/hardware jehož není Dodavatel dodavatelem, pro odstranění takovýchto vad poskytne Dodavatel součinnost. Za vady se však považují nefunkčnost, omezená funkčnost a jiné vady ve fungování software/hardware, jehož dodavatelem není Dodavatel, vzniklé v důsledku nebo v souvislosti s jakýmkoli jednáním Dodavatele, zejména vlivem jakéhokoli zásahu Dodavatele. O vadách a jejich zařazení Objednatel písemně informuje neprodleně Dodavatele.
- 4.15 Termíny odstranění vad:
- a) vadu kategorie A je Dodavatel povinen odstranit nejpozději do dvou (2) pracovních dnů následujících od jejího písemného nahlášení Objednatelem, pokud se Smluvní strany

nedohodnou jinak. Neodstranění vady kategorie A ve stanovené lhůtě má za následek zastavení akceptačních testů, pokud se Smluvní strany nedohodnou jinak. Po odstranění vady kategorie A je Dodavatel povinen Objednateli na jeho žádost předvést, že vada byla úspěšně odstraněna;

- b) vadu kategorie B je Dodavatel povinen odstranit do dvou (2) pracovních dnů následujících od jejího písemného nahlášení Objednatelem, pokud se Smluvní strany nedohodnou jinak. Neodstranění vad kategorie B tak, aby jejich počet byl menší než tři (3), má za následek zastavení akceptačních testů, pokud se Smluvní strany nedohodnou jinak;
- c) vadu kategorie C je Dodavatel povinen odstranit nejpozději do pěti (5) pracovních dnů následujících od jejího písemného nahlášení Objednatelem, pokud se Smluvní strany nedohodnou jinak. Neodstranění vad kategorie C tak, aby jejich počet byl menší než deset (10), má za následek zastavení akceptačních testů, pokud se Smluvní strany nedohodnou jinak.

4.16 Dodavatel může písemně požádat Objednatele o prodloužení lhůty pro odstranění vad, a to nejméně jeden (1) pracovní den před uplynutím běžné lhůty pro odstranění vad. Objednatel je povinen na tuto žádost odpovědět do konce prvního pracovního dne následujícího po obdržení žádosti. Neučiní-li tak, má se za to, že žádosti Dodavatele nevyhovuje.

4.17 Zastavení akceptačních testů:

Pokud počet zjištěných, nahlášených a v jednom okamžiku neopravených vad dosáhne jakéhokoli z těchto limitů:

- a) jedna (1) vada kategorie A;
- b) tři (3) vady kategorie B;
- c) deset (10) vad kategorie C (prostý součet);

má Objednatel právo zastavit akceptační testy, a to až do doby, než počet neopravených vad bude nižší než tyto limity, a o této skutečnosti neprodleně písemně uvědomí Dodavatele.

4.18 Obnovení akceptačních testů po jejich zastavení:

Objednatel je povinen neprodleně zahájit zastavené akceptační testy na základě písemného sdělení Dodavatele o snížení počtu vad pod shora uvedené limity. Lhůta pro předání a dokončení Dílčího požadavku zůstává v případě zastavení akceptačních testů nezměněna.

4.19 Neúspěšné ukončení akceptačních testů z důvodů vad:

- a) Pokud nedojde k obnovení zastavených akceptačních testů z důvodů ležících na straně Dodavatele do pěti (5) pracovních dnů následujících po oznámení Objednatele o zastavení akceptačních testů, jsou akceptační testy považovány za ukončené s výsledkem „Dílčí požadavek nevyhovuje“ (viz níže), pokud se Smluvní strany nedohodnou jinak.
- b) Pokud nedojde k obnovení akceptačních testů z důvodů na straně Objednatele, bude vzniklá situace řešena dohodou Smluvních stran. O dobu trvání řešení takové situace se prodlužuje doba k předání a převzetí Dílčího požadavku.

4.20 Jestliže akceptační testy byly ukončeny úspěšně, nebyla zjištěna žádná vada kategorie A, více než dvě (2) vady kategorie B a/nebo více než devět (9) vad kategorie C, anebo byly všechny vady, jejichž počet překračuje tyto stanovené limity, odstraněny a jejich odstranění bylo prokazatelně ověřeno před ukončením akceptačních testů, pak „**Dílčí požadavek vyhovuje**“ a Objednatel je povinen ho převzít. Objednatel s Dodavatelem se v akceptačním protokolu písemně dohodnou na termínu odstranění všech zbývajících vad.

4.21 Jestliže akceptační testy nebyly ukončeny úspěšně, byla zjištěna vada či vady kategorie A, více než dvě (2) vady kategorie B a/nebo více než devět (9) vad kategorie C s tím, že vady, jejichž

počet překračuje tyto limity, nebyly odstraněny nebo jejich odstranění nebylo prokazatelně ověřeno do konce akceptačních testů z důvodů neležících na straně Objednatele, není Objednatel povinen Dílčí požadavek převzít. Ukončení akceptačních testů s odůvodněným výrokem „**Dílčí požadavek nevyhovuje**“ je považováno za podstatné porušení Smlouvy ze strany Dodavatele.

- 4.22 V případě výroku „Dílčí požadavek nevyhovuje“ je Dodavatel nadále povinen pracovat na řádném odstranění zjištěných vad, přičemž je povinen po jejich odstranění bez zbytečného odkladu vyzvat Objednatele k opakování akceptačních testů.
- 4.23 Dojde-li v průběhu akceptačních testů k zjištění neodstranitelné vady jakékoli kategorie, bude to považováno za podstatné porušení této Smlouvy nebo Dílčí smlouvy Dodavatelem, jestliže taková vada vážným způsobem narušuje užívání Dílčího požadavku nebo Systému.
- 4.24 Pro každé z podstatných porušení Smlouvy Dodavatelem popsanych v čl. 4 Smlouvy je Objednatel oprávněn od této Smlouvy nebo jen od předmětné Dílčí smlouvy odstoupit.
- 4.25 Dodavatel není oprávněn ve smyslu ust. § 2609 Občanského zákoníku Dílčí požadavek na účet Objednatele vhodným způsobem prodat, nepřevzme-li Objednatel Dílčí požadavek bez zbytečného odkladu poté, co mělo být dokončeno, a bylo-li dokončeno později, tak bez zbytečného odkladu po vyrozumění o dokončení Dílčího požadavku.

5 Termín, místo a podmínky plnění

- 5.1 Místem plnění je Česká pošta, s.p., Olšanská 38/9, 130 00 Praha 3, není-li v Dílčí smlouvě ujednáno jinak nebo nestanoví-li jinak Objednatel v požadavku na Podporu dle odst. 2.4 Smlouvy. Podpora může být poskytována i prostřednictvím vzdáleného přístupu.
- 5.2 Dodavatel se zavazuje realizovat Plnění v následujících termínech:
 - a) Cílový koncept musí být dokončen nejpozději do 3 měsíců ode dne nabytí účinnosti Smlouvy,
 - b) Zhotovení AlmaLinux XAPOST musí být dokončeno před zahájením Pilotního provozu. Pilotní provoz musí být zahájen do 6 měsíců a dokončen nejpozději do 12 měsíců ode dne nabytí účinnosti Smlouvy.
 - c) Přechod musí být dokončen nejpozději do 18 měsíců ode dne nabytí účinnosti Smlouvy.Dokončením se rozumí akceptace příslušné části Plnění Objednatelem. Podrobnější termíny Plnění budou stanoveny v Cílovém konceptu.
- 5.3 Poskytování Podpory je Dodavatel povinen zahájit od nabytí účinnosti Smlouvy, nejdříve však od 1. 6. 2025. Podpora bude poskytována po dobu 4 let.
- 5.4 Rozvoj je Dodavatel povinen zajišťovat dle aktuálních potřeb Objednatele po celou dobu účinnosti Smlouvy, v termínech sjednaných konkrétní Dílčí smlouvou.
- 5.5 Nedílnou součástí Plnění je v případech, kdy to vyplývá z charakteru příslušného předmětu Plnění, také licenční dokumentace (licenční certifikáty, licenční podmínky a ostatní dokumentace k licencím) vztahující se k užívání software nebo jeho části nebo jiného autorského díla či databáze a ostatní dokumentace potřebná pro řádné užívání Plnění.

6 Cena

- 6.1 Cena za **Podporu** dle odst. 1.1 písm. d) Smlouvy činí 2 400 000,- Kč bez DPH za 1 rok, přičemž tato cena je platná po celou dobu trvání této Smlouvy.
- 6.2 Cena za vytvoření **Cílového konceptu** dle odst. 1.1 písm. a) Smlouvy činí 600 000,- Kč bez DPH.

- 6.3 Cena za zhotovení **AlmaLinux XAPOST** dle odst. 1.1 písm. b) Smlouvy (realizaci, konfiguraci a ladění distribuce AlmaLinux pro XAPOST v prostředí České pošty, včetně realizace **Pilotu**, činí 1 600 000,- Kč bez DPH.
- 6.4 Cena za **Přechod** dle odst. 1.1. odst. c) Smlouvy činí 1 600 000,- Kč bez DPH.
- 6.5 Cena za jeden (1) MD (resp. minimálně 8 hodin práce jedné osoby Dodavatele) poskytování **služeb Rozvoje** dle odst. 1.1 písm. e) Smlouvy činí 19 300,- Kč bez DPH po celou dobu trvání této Smlouvy.
- 6.6 Maximální cena za Plnění poskytnuté na základě této Smlouvy nesmí převýšit částku 14 000 000,- Kč bez DPH.
- 6.7 Ke smluvní ceně dle této Smlouvy bude připočtena DPH v zákonné výši.
- 6.8 Ceny uvedené v tomto článku Smlouvy jsou konečné a obsahují již veškeré náklady související s poskytnutím Plnění dle Smlouvy v místě plnění, včetně cestovních a jiných nákladů Dodavatele souvisejících s Plněním. Sjednané ceny jsou konečné, nejvýše přípustné a nemohou být změněny.
- 6.9 Smluvní strany si ve smyslu ustanovení § 2620 odst. 2 Občanského zákoníku ujednaly, že Dodavatel na sebe přebírá nebezpečí změny okolností.

7 Platební podmínky

- 7.1 Cena včetně DPH za Podporu na rok bude hrazena na základě daňového dokladu – faktury Dodavatele ročně předem. Dodavatel vystaví první daňový doklad k prvnímu dni zahájení poskytování Podpory podle odst. 5.2 Smlouvy. Následně na každý další rok poskytování Podpory vystaví Dodavatel daňový doklad v den výročí poskytování Podpory, tj. k prvnímu dni příslušného ročního období, ve kterém bude Podpora Objednateli poskytována. Den vystavení daňového dokladu bude dnem uskutečnění zdanitelného plnění.
- 7.2 Cena za vytvoření Cílového konceptu dle odst. 6.2 této Smlouvy bude uhrazena na základě daňového dokladu – faktury Dodavatele vystavené po akceptaci Cílového konceptu Objednatelem. Nedílnou součástí daňového dokladu je Objednatelem potvrzený akceptační protokol stvrzující řádné předání plnění Objednateli a jeho schválení.
- 7.3 Cena za zhotovení díla AlmaLinux XAPOST dle odst. 6.3 této Smlouvy bude uhrazena na základě daňového dokladu – faktury Dodavatele vystavené po úspěšném dokončení Pilotu a akceptaci Systému Objednatelem ve smyslu odst. 3.7 Smlouvy. Nedílnou součástí daňového dokladu je Objednatelem potvrzený Akceptační protokol stvrzující řádné poskytnutí plnění Objednateli a jeho schválení.
- 7.4 Cena za provedení Přechodu dle odst. 6.4 této Smlouvy bude uhrazena na základě daňového dokladu – faktury Dodavatele vystavené po úspěšném dokončení Přechodu, tj. plošného nasazení AlmaLinux APOST na všech pobočkách Objednatele v souladu s touto Smlouvou a Cílovým konceptem. Nedílnou součástí daňového dokladu je Objednatelem potvrzený Akceptační protokol stvrzující řádné poskytnutí plnění Objednateli a jeho schválení.
- 7.5 Cena včetně DPH za Rozvoj bude hrazena na základě daňového dokladu – faktury Dodavatele vždy po akceptaci příslušného plnění na základě Dílčí smlouvy odpovědným pracovníkem za Objednatele dle čl. 16 Smlouvy. Nedílnou součástí daňového dokladu je Objednatelem potvrzený akceptační protokol stvrzující řádné poskytnutí plnění Objednateli a jeho schválení. Dodavatel je povinen vystavit daňový doklad nejdéle do deseti (10) kalendářních dnů od data akceptace příslušného plnění. Dnem uskutečnění zdanitelného plnění je den akceptace příslušného plnění Objednatelem.
- 7.6 Dodavatel zašle každý daňový doklad spolu s veškerými požadovanými dokumenty Objednateli:

- a) doporučeným dopisem na adresu: Česká pošta, s.p., skenovací centrum, Poštovní 1368/20, 701 06 Ostrava 1; nebo
 - b) elektronicky, je-li elektronický způsob zasílání výslovně odsouhlasen Objednatelem na základě žádosti Dodavatele zaslané do technologické schránky [REDACTED] nebo
 - c) na výzvu Objednatele způsobem uvedeným v odst. 7.11 Smlouvy.
- 7.7 Doba splatnosti daňového dokladu vystaveného na základě této Smlouvy je šedesát (60) kalendářních dnů ode dne jeho vystavení Dodavatelem. Dodavatel zašle daňový doklad spolu s veškerými požadovanými dokumenty Objednateli nejpozději do pěti (5) kalendářních dnů od jeho vystavení. Dodavatel je povinen vystavit daňový doklad do deseti (10) kalendářních dnů ode dne uskutečnění zdanitelného plnění. Cena Plnění bude hrazena na bankovní účet Dodavatele uvedený v jeho identifikačních údajích ve Smlouvě. Změna bankovních údajů je možná pouze formou dodatku ke Smlouvě.
- 7.8 Daňový doklad musí obsahovat náležitosti řádného daňového dokladu podle příslušných právních předpisů, zejména pak zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „**Zákon o DPH**“), a níže uvedené údaje:
- a) číslo Smlouvy;
 - b) číslo OBJ nebo Objednávky;
 - c) platební podmínky v souladu se Smlouvou;
 - d) popis fakturovaného Plnění, rozsah poskytovaného Plnění;
 - e) cenu;
 - f) přílohou daňového dokladu bude Akceptační protokol potvrzený Objednatelem.
- 7.9 V případě, že daňový doklad nebude mít odpovídající náležitosti nebo nebude vystaven v souladu s touto Smlouvou, je Objednatel oprávněn zaslat jej v době splatnosti zpět k doplnění Dodavateli, aniž se dostane do prodlení se splatností. Doba splatnosti šedesát (60) kalendářních dnů počíná běžet znovu od vystavení doplněného/opraveného daňového dokladu Dodavatelem.
- 7.10 Objednatel neposkytuje Dodavateli jakékoliv zálohy na cenu Plnění.
- 7.11 Dodavatel se zavazuje, že na výzvu Objednatele bude akceptovat oboustranné elektronické zasílání dokladů spojených s realizací Plnění dle Smlouvy (zejména Objednávek a jejich potvrzení, daňových dokladů) prostřednictvím portálu SAP Ariba Network. Dodavatel se zavazuje v takovém případě zaregistrovat na portálu SAP Ariba Network. Objednatele iniciuje registraci Dodavatele k portálu SAP Ariba Network zasláním elektronické výzvy na kontaktní e-mail Dodavatele dle čl. 16 Smlouvy. Objednatel prohlašuje, že pro požadované aktivity Dodavatele v rámci plnění dle Smlouvy je postačující registrace Dodavatele se standardním účtem Ariba Network. Je-li Dodavatel již v SAP Ariba Network registrován, pak lze pro elektronickou komunikaci využít existující AN-ID.
- 7.12 Smluvní strany se dohodly, že pokud bude v okamžiku uskutečnění zdanitelného plnění správcem daně zveřejněna způsobem umožňujícím dálkový přístup skutečnost, že Dodavatel je nespolehlivým plátcem ve smyslu § 106a zákona o DPH, nebo nastane některá z dalších skutečností uvedených v § 109 zákona o DPH, je příjemce zdanitelného plnění (tj. Objednatel) oprávněn část ceny odpovídající dani z přidané hodnoty zaplatit přímo na bankovní účet správce daně ve smyslu § 109a zákona o DPH. Na bankovní účet Dodavatele bude v tomto případě uhrazena část ceny odpovídající výši základu daně z přidané hodnoty. Úhrada ceny plnění (základu daně) provedená Objednatelem v souladu s ustanovením tohoto odstavce Smlouvy bude považována za řádnou úhradu ceny plnění poskytnutého dle této Smlouvy.

- 7.13 Bankovní účet uvedený na daňovém dokladu, na který bude ze strany Dodavatele požadována úhrada ceny za poskytnuté zdanitelné plnění, musí být Dodavatelem zveřejněn způsobem umožňujícím dálkový přístup ve smyslu § 96 zákona o DPH. Smluvní strany se výslovně dohodly, že pokud číslo bankovního účtu Dodavatele, na který bude ze strany Dodavatele požadována úhrada ceny za poskytnuté zdanitelné plnění dle příslušného daňového dokladu, nebude zveřejněno způsobem umožňujícím dálkový přístup ve smyslu § 96 zákona o DPH, je Objednatel oprávněn zaslat daňový doklad zpět Dodavateli k opravě. V takovém případě se doba splatnosti zastavuje a nová doba splatnosti počíná běžet dnem vystavení opraveného daňového dokladu s uvedením správného bankovního účtu Dodavatele, tj. bankovního účtu zveřejněného správcem daně.
- 7.14 Cena za Plnění bude hrazena na bankovní účet Dodavatele uvedený v jeho identifikačních údajích ve Smlouvě. Změna bankovních údajů je možná pouze formou dodatku ke Smlouvě.
- 7.15 Dodavatel se zavazuje, že na výzvu Objednatele zajistí zasílání daňových dokladů v elektronickém formátu ISDOC (Information System Document), který je standardem pro elektronickou fakturaci v ČR, a to do 6 měsíců od obdržení takové výzvy. Takto zaslané daňové doklady musí být opatřeny elektronickým podpisem, včetně časového razítka, dle příslušných právních předpisů.

8 Práva duševního vlastnictví

- 8.1 Software – Systém je autorským dílem ve smyslu podle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „**Autorský zákon**“). Podmínky užití Systému se řídí licenčními podmínkami výrobce Systému uvedenými v Příloze č. 2 Smlouvy (dále jen „**Licenční ujednání**“). Dodavatel je povinen zajistit Objednateli oprávnění k výkonu práva užití Systém a jakékoli aktualizace (update), nové verze (upgrade), opravy či úpravy Systému dodané v rámci poskytování Plnění, nejméně v rozsahu a za podmínek vymezených v Licenčním ujednání.
- 8.2 Vznikne-li v souvislosti s poskytováním Plnění Dodavatelem Objednateli autorské dílo, které se neřídí Licenčním ujednáním ve smyslu předchozího odstavce Smlouvy, a které bylo vytvořeno na základě této Smlouvy či Dílčí smlouvy, poskytuje Dodavatel Objednateli k takovému autorskému dílu výhradní, množstevně a územně neomezenou volně převoditelnou licenci na celou dobu trvání majetkových autorských práv k takovému dílu a ke všem způsobům a formám užití za jakýmkoli účelem, nebude-li v daném případě dohodnuto jinak (např. z důvodu dodání standardního software třetí strany, který neumožňuje udělení takovýchto licenčních práv). Dodavatel prohlašuje, že je oprávněn licenci v uvedeném rozsahu Objednateli udělit a poskytnout výše uvedená oprávnění a souhlasí Objednateli v celém rozsahu. V případě, že se uvedené prohlášení Dodavatele nezakládá na pravdě, odpovídá Dodavatel Objednateli za vyplývající důsledky v plném rozsahu včetně odpovědnosti za majetkovou i nemajetkovou újmu.
- 8.3 Současně s licencí uděluje Dodavatel Objednateli souhlas k provádění jakýchkoliv modifikací, úprav, změn díla ve smyslu předchozího odstavce včetně práva do něj dle svého uvážení zasahovat, zapracovávat do dalších autorských děl a spojovat jej s jinými autorskými díly, případně zařazovat do databází, a to včetně oprávnění Objednatele takovými zásahy do díla pověřit třetí osoby. Objednatel je oprávněn provádět servis, údržbu či podporu díla sám nebo prostřednictvím třetích osob, k čemuž Dodavatel poskytuje výslovný souhlas.
- 8.4 Objednatel je oprávněn poskytovat neomezený počet podlicencí pro autorské dílo ve smyslu odst. 8.2 Smlouvy, které se neřídí Licenčním ujednáním, ve stejném nebo omezeném rozsahu, ve kterém je dílo oprávněn užívat dle této Smlouvy. Objednatel je oprávněn převést, respektive postoupit právo užívat dílo na třetí osobu ve stejném nebo omezeném rozsahu, ve kterém je dílo oprávněn užívat dle této Smlouvy.

- 8.5 Dodavatel prohlašuje, že Plnění ani jeho části, které jsou autorským dílem, nemá žádné právní vady, že není zatíženo právy třetích osob a že Dodavatel je zcela oprávněn vykonávat veškerá majetková autorská práva a poskytnout výše uvedená oprávnění a souhlasy Objednateli v celém rozsahu, s dílem disponovat a uzavřít s Objednatелеm Smlouvu na celý rozsah předmětu plnění. V případě, že se uvedené prohlášení Dodavatele nezakládá na pravdě, Dodavatel odpovídá Objednateli za vyplývající důsledky v plném rozsahu včetně odpovědnosti za majetkovou i nemajetkovou újmu. Sankční ujednání dle této Smlouvy tímto nejsou dotčena. Uplatní-li třetí osoba své právo k dílu nebo jeho části, zavazuje se Dodavatel bez zbytečného odkladu a na vlastní náklady učinit potřebná opatření k ochraně výkonu práv Objednatele, pokud jej k tomu Objednatel zmocní, a nahradit veškerou majetkovou i nemajetkovou újmu vzniklou tím Objednateli.
- 8.6 Veškeré odměny za poskytnutí či zajištění všech licencí dle tohoto článku Smlouvy jsou již zahrnuty v ceně Plnění. Objednatel není povinen žádnou z licencí nabytých na základě této Smlouvy využít.
- 8.7 Licence dle tohoto článku Smlouvy je udělena Dodavatelem Objednateli v souvislosti s realizací Plnění a Dodavatel není oprávněn tuto licenci vypovědět ani ukončit jiným způsobem, než jak předpokládá tato Smlouva. Smluvní strany výslovně uvádějí, že bez ohledu na důvod a způsob ukončení této Smlouvy nejsou dotčena ustanovení tohoto článku Smlouvy.
- 8.8 V souvislosti s těmito ujednáními o licenční smlouvě ve smyslu tohoto článku Smlouvy Smluvní strany výslovně vylučují ustanovení občanského zákoníku § 2378, § 2379, § 2380, § 2381 a § 2382.
- 8.9 V případě, že jsou součástí Plnění realizovaného Dodavatelem dle této Smlouvy databáze (ve smyslu ustanovení § 88 Autorského zákona), jejichž pořizovatelem je Dodavatel, převádí tímto Dodavatel právo pořizovatele databáze ve smyslu § 90 Autorského zákona na Objednatele. Objednatel je oprávněn databáze zužitkovat a vytěžovat libovolně dle svého uvážení, k čemuž Dodavatel poskytuje výslovný souhlas.
- 8.10 Bude-li autorské dílo vytvořeno činností Dodavatele pro Objednatele dle této Smlouvy, Smluvní strany činí nesporným, že jakékoliv takovéto autorské dílo vzniklo z podnětu a pod vedením Objednatele.

9 Záruka

- 9.1 Dodavatel poskytuje záruku na dílo, Systém AlmaLinux XAPOST i na každý Dílčí požadavek realizovaný v rámci Rozvoje (dále pro účely tohoto článku Smlouvy společně jen „dílo“) v trvání dvanácti (12) měsíců ode dne podpisu příslušného akceptačního protokolu k dílu Objednatелеm. Záruka se uplatní pro všechny části díla, a to i v případě, že licenční podmínky příslušného systému obsahují vyloučení záruky výrobce / držitele autorských práv k takovému systému / dílu. Vady, které se vyskytnou či vzniknou v záruční době, je Dodavatel povinen bezplatně odstranit.
- 9.2 Na vady realizovaného díla v záruční době se vztahuje kategorizace vad dle odst. 4.13 a 4.14 Smlouvy.
- 9.3 Vady realizovaného díla vzniklé nebo odhalené v záruční době bude Objednatel oznamovat Dodavateli bez zbytečného odkladu e-mailem na adresu: [REDACTED] a na tel. č. [REDACTED]. Jestliže bude vada oznámena telefonicky, musí být následně oznámení potvrzeno písemně.
- 9.4 Dodavatel garantuje dobu odezvy pro vady kategorie A do dvou (2) hodin, pro vady kategorie B do jednoho (1) pracovního dne a pro vady kategorie C do tří (3) pracovních dnů od nahlášení vady Objednatелеm.

- 9.5 Dodavatel garantuje, že odstraní vady kategorie A do jednoho (1) pracovního dne, vady kategorie B do tří (3) pracovních dnů a vady kategorie C do deseti (10) pracovních dnů od nahlášení vady Objednatelem.
- 9.6 Dodavatel garantuje nepřetržitou práci na odstranění vady až do jejího úplného odstranění, pokud se Smluvní strany nedohodnou jinak. Dodavatel se zavazuje průběžně informovat Objednatele o stavu řešení vad až do jejich odstranění.
- 9.7 Záruka Dodavatele se nevztahuje na vady té části díla, která byla užívána v rozporu s jejím funkčním určením a písemnými doporučeními Dodavatele a/nebo způsobené neoprávněným nebo neodborným zásahem Objednatele nebo třetí osobou, která není ve smluvním vztahu k Dodavateli. Funkční určení je specifikováno v dokumentaci, která je součástí předání a převzetí díla.
- 9.8 Pokud bude vada kategorie A Objednatelem přerazena do kategorie B nebo C, popřípadě vada kategorie B přerazena do kategorie C, mění se příslušná lhůta k odstranění vady na tu, jež se vztahuje k nové kategorii vady. To neplatí, byl-li Dodavatel v okamžiku převedení vady do nižší kategorie již v prodlení s odstraňováním vady.
- 9.9 Zjistí-li Dodavatel v průběhu záruční doby, že vada je neodstranitelná, je povinen nepřetržitě pracovat na náhradním řešení problému a informovat o tomto stavu Objednatele. Výskyt neodstranitelné vady, pokud je zapříčiněna Dodavatelem bude ze strany Objednatele považován za podstatné porušení této Smlouvy.
- 9.10 Pokud považuje Dodavatel vadu za odstraněnou, předá předmětnou část díla Objednateli, který je oprávněn ověřovat všechny funkce díla ve smyslu jeho specifikace. Odstranění vady potvrdí Objednatel svým podpisem na Akceptačním protokolu.

10 Obchodní tajemství a důvěrné informace

- 10.1 Veškeré konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti související se Smluvními stranami, a se kterými se Smluvní strany seznámí při realizaci předmětu Smlouvy nebo v souvislosti s touto Smlouvou přijdou do styku, a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení, jsou obchodním tajemstvím. Smluvní strany se zavazují zachovat mlčenlivost o obchodním tajemství druhé Smluvní strany, a dále o skutečnostech a informacích, které označí jako důvěrné dle § 1730 Občanského zákoníku. Povinnost mlčenlivosti trvá až do doby, kdy se informace této povahy stanou obecně známými za předpokladu, že se tak nestane porušením povinnosti mlčenlivosti. Na povinnost mlčenlivosti nemá vliv forma sdělení informací (písemně nebo ústně) a jejich podoba (materializované nebo dematerializované).
- 10.2 Smluvní strany se zavazují, že důvěrné informace a obchodní tajemství druhé Smluvní strany jiným subjektům nesdělí, nezpřístupní, ani nevyužijí pro sebe nebo pro jinou osobu. Zavazují se zachovat je v přísné tajnosti a sdělit je výlučně těm svým zaměstnancům nebo subdodavatelům, kteří jsou pověřeni plněním Smlouvy a za tímto účelem jsou oprávněni se s těmito informacemi v nezbytném rozsahu seznámit. Smluvní strany se zavazují zabezpečit, aby i tyto osoby považovaly uvedené informace za důvěrné a zachovávaly o nich mlčenlivost.
- 10.3 V případě porušení obchodního tajemství ve smyslu § 2985 Občanského zákoníku, použijí Smluvní strany prostředky právní ochrany proti nekalé soutěži.
- 10.4 Poškozená Smluvní strana má právo na náhradu újmy, která jí takovýmto jednáním druhé Smluvní strany vznikne.
- 10.5 Povinnost plnit ustanovení dle tohoto článku Smlouvy se nevztahuje na informace, které:
 - a) mohou být zveřejněny bez porušení této Smlouvy;

- b) byly písemným souhlasem obou Smluvních stran zproštěny těchto omezení;
- c) jsou známé nebo byly zveřejněny jinak, než následkem zanedbání povinnosti jedné ze Smluvních stran;
- d) příjemce je zná dříve, než mu je sdělí Smluvní strana;
- e) jsou vyžádány soudem, státním zastupitelstvím nebo příslušným správním orgánem v souladu a na základě zákona;
- f) Smluvní strana je sdělí osobě vázané zákonnou povinností mlčenlivosti (např. advokátovi nebo daňovému poradci) za účelem uplatňování svých práv nebo při plnění povinností stanovených právními předpisy;
- g) jsou zveřejněny v souladu a na základě právního předpisu (např. o svobodném přístupu k informacím, o registru smluv);
- h) je Objednatel povinen sdělit svému zakladateli.

10.6 Povinnost mlčenlivosti trvá bez ohledu na ukončení účinnosti této Smlouvy.

10.7 Smluvní strany berou na vědomí, že tato Smlouva bude uveřejněna v registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů (dále jen „**zákon o registru smluv**“). Dle dohody Smluvních stran zajistí odeslání této Smlouvy správci registru smluv Objednatel. Objednatel je oprávněn před odesláním Smlouvy správci registru smluv ve Smlouvě znečitelnit informace, na něž se nevztahuje uveřejňovací povinnost podle zákona o registru smluv.

11 Zpracování osobních údajů

- 11.1 Pro případ, že Dodavatel v rámci plnění Smlouvy získá nahodilý přístup k informacím, které budou obsahovat osobní údaje podléhající ochraně dle právních předpisů, je Dodavatel oprávněn přistupovat k takovým osobním údajům pouze v nezbytném rozsahu pro plnění předmětu Smlouvy (např. kontaktní informace a údaje, k nimž má Dodavatel v průběhu plnění Smlouvy přístup). Dodavatel se zavazuje nakládat se zpřístupněnými osobními údaji pouze na základě pokynů Objednatele jako správce osobních údajů, pouze pro účely plnění Smlouvy, zachovat o nich mlčenlivost a zajistit jejich bezpečnost proti úniku, náhodnému nebo neoprávněnému zničení, ztrátě, pozměňování nebo neoprávněnému zpřístupnění třetím osobám.
- 11.2 Objednatel jako správce zpracovává osobní údaje Dodavatele, je-li Dodavatelem fyzická osoba, a obě Smluvní strany jako správci osobní údaje kontaktních osob poskytnuté v této Smlouvě, popřípadě osobní údaje dalších osob poskytnuté v rámci Smlouvy výhradně pro účely související s plněním této Smlouvy, a to po dobu trvání Smlouvy, resp. pro účely vyplývající z právních předpisů, a to po dobu delší těmito právními předpisy odůvodněnou. Dodavatel je povinen informovat obdobně fyzické osoby, jejichž osobní údaje pro účely související s plněním této Smlouvy Objednateli předává.
- 11.3 Další informace související se zpracováním osobních údajů Objednatelem včetně práv s tímto zpracováním souvisejících jsou k dispozici na webových stránkách Objednatele na adrese www.ceskaposta.cz v záložce „Ochrana osobních údajů – GDPR“.
- 11.4 Vyjde-li najevo, že v souvislosti s touto Smlouvou bude docházet k předávání osobních údajů mezi Smluvními stranami nad rámec uvedený v tomto článku Smlouvy, jsou Smluvní strany povinny v dostatečném předstihu uzavřít smlouvu o zpracování osobních údajů v souladu s právními předpisy na ochranu osobních údajů.

12 Pravidla bezpečnosti ICT systémů Objednatele

- 12.1 Objednatel zastává pozici pověřené 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“) a je správcem kritické informační infrastruktury (dále jen „KII“). Předmět plnění je nedílnou součástí KII Objednatele, a proto je **Dodavatel jmenován významným dodavatelem**.
- 12.2 Dodavatel se zavazuje dodržovat požadavky na bezpečnost ICT, které vyplývají z ZKB, VKB, GDPR a požadavky vyplývající z bezpečnostního standardu PCI DSS, a které jsou podrobně vymezeny v Příloze č. 7 Smlouvy a matice odpovědnosti definované v Příloze č. 8 Smlouvy.

13 Pravidla compliance

- 13.1 Smluvní strany se zavazují dodržovat právní předpisy a chovat se tak, aby jejich jednání nemohlo vzbudit důvodné podezření ze spáchání nebo páchaní trestného činu přičitatelného jedné nebo oběma smluvním stranám podle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů.
- 13.2 Smluvní strany se zavazují, že učiní všechna opatření k tomu, aby se nedopustily ony a ani nikdo z jejich zaměstnanců či zástupců jakékoliv formy korupčního jednání, zejména jednání, které by mohlo být vnímáno jako přijetí úplatku, podplácení nebo nepřímé úplatkářství či jiný trestný čin spojený s korupcí dle zákona č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů.
- 13.3 Smluvní strany se zavazují, že neposkytnou, nenabídnou ani neslíbí úplatek jinému nebo pro jiného v souvislosti s obstaráváním věcí obecného zájmu anebo v souvislosti s podnikáním svým nebo jiného. Smluvní strany se rovněž zavazují, že úplatek nepřijmou, ani si jej nedají slíbit, ať už pro sebe nebo pro jiného v souvislosti s obstaráním věcí obecného zájmu nebo v souvislosti s podnikáním svým nebo jiného. Úplatkem se přitom rozumí neoprávněná výhoda spočívající v přímém majetkovém obohacení nebo jiném zvýhodnění, které se dostává nebo má dostat uplácené osobě nebo s jejím souhlasem jiné osobě, a na kterou není nárok.
- 13.4 Smluvní strany nebudou ani u svých obchodních partnerů tolerovat jakoukoliv formu korupce či uplácení.
- 13.5 V případě, že je zahájeno trestní stíhání Dodavatele, zavazuje se Dodavatel o tomto bez zbytečného odkladu Objednatele písemně informovat.
- 13.6 Objednatel očekává, že se Dodavatel seznámí s „Kodexem dodavatele České pošty“, ve znění k datu účinnosti této Smlouvy, který je dostupný na webu Objednatele na adrese, <https://www.ceskaposta.cz/documents/10180/5513790/KODEX-DODAVATELE-CP.pdf/bc2586e7-6211-3309-afb3-f9671da3af06> a bude jej dodržovat.

14 Nemožnost plnění

- 14.1 Jestliže vznikne na straně Dodavatele nemožnost plnění ve smyslu § 2006 nebo § 2007 Občanského zákoníku, Dodavatel písemně uvědomí bez zbytečného odkladu o této skutečnosti a její příčině Objednatele. Pokud není jinak stanoveno písemně Objednatelem, bude Dodavatel pokračovat v realizaci svých povinností vyplývajících ze Smlouvy v rozsahu svých nejlepších možností a schopností a bude hledat alternativní prostředky pro realizaci té části plnění, kde není možné plnit. Pokud by podmínky nemožnosti plnění trvaly déle než devadesát (90) kalendářních dní, je Objednatel oprávněn od Smlouvy odstoupit.

- 14.2 Ustanovení tohoto článku Smlouvy nezbavuje žádnou ze Smluvních stran její povinnosti k úhradě plateb v té době již splatných.

15 Další práva a povinnosti Smluvních stran

- 15.1 Dodavatel se zavazuje při poskytování Plnění poskytnout Objednateli všechny případné nezbytné dokumenty pro jejich řádné poskytování a využití.
- 15.2 Objednatel se zavazuje zajistit pracovníkům Dodavatele během plnění této Smlouvy, je-li to nezbytné, přístup na příslušná pracoviště Objednatele a součinnost nezbytnou k provedení Plnění. Dodavatel se zavazuje dodržovat v objektech Objednatele příslušné vnitřní pokyny a směrnice stanovující provozně technické a bezpečnostní podmínky pohybu osob v objektech Objednatele. Při plnění této Smlouvy v objektech Objednatele musí Dodavatel v maximální míře respektovat nutnost zajištění nerušeného užívání objektů jejich uživateli.
- 15.3 Dodavatel se zavazuje:
- a) informovat neprodleně Objednatele o všech skutečnostech majících vliv na plnění dle této Smlouvy;
 - b) plnit řádně a ve stanoveném termínu své povinnosti vyplývající z této Smlouvy;
 - c) požádat včas Objednatele o potřebnou součinnost za účelem řádného plnění této Smlouvy;
 - d) na vyžádání Objednatele se zúčastnit osobní schůzky, pokud Objednatel požádá o schůzku nejpozději pět (5) pracovních dnů předem. V mimořádně naléhavých případech je možno tento termín po dohodě obou Smluvních stran zkrátit.
- 15.4 Dodavatel je povinen postupovat při plnění této Smlouvy svědomitě a s řádnou a odbornou péčí. Dodavatel je povinen pověřit plněním povinností z této Smlouvy pouze ty své pracovníky, kteří jsou k tomu odborně způsobilí. Při poskytování Plnění je Dodavatel vázán touto Smlouvou, zákony, obecně závaznými právními předpisy a pokyny Objednatele, pokud tyto nejsou v rozporu s těmito normami nebo zájmy Objednatele. Dodavatel je povinen při výkonu své činnosti včas písemně upozornit Objednatele na zřejmou nevhodnost jeho pokynů, jejichž následkem může vzniknout škoda nebo nesoulad se zákony nebo obecně závaznými právními předpisy. Pokud Objednatel navzdory tomuto upozornění trvá na svých pokynech, Dodavatel neodpovídá za jakoukoli škodu vzniklou v této příčinné souvislosti.
- 15.5 Dodavatel se zavazuje, že při své činnosti bude dbát, aby nebyla poškozena dobrá obchodní pověst a obchodní firma Objednatele. Při poskytování Plnění musí Dodavatel vždy sledovat zájmy Objednatele. Dodavatel se zavazuje nevyvíjet jakékoliv aktivity, a to jak přímo, tak zprostředkovaně, které jsou v rozporu se zájmy Objednatele ve všech oblastech jeho činnosti.
- 15.6 Dodavatel není oprávněn použít ve svých dokumentech, prezentacích či reklamě odkazy na obchodní firmu Objednatele nebo jakýkoliv jiný odkaz, který by mohl, byť i nepřímou, vést k identifikaci Objednatele, bez předchozího písemného souhlasu Objednatele.
- 15.7 Veškerá komunikace mezi Smluvními stranami je činěna písemně, není-li touto Smlouvou stanoveno jinak. Písemná komunikace se činí v listinné nebo elektronické podobě prostřednictvím doporučené pošty či e-mailu na adresy Smluvních stran uvedené v záhlaví nebo v čl. 16 Smlouvy.
- 15.8 Dodavatel není oprávněn postoupit ani převést jakákoliv svá práva či povinnosti vyplývající z této Smlouvy ani Smlouvu jako celek bez předchozího písemného souhlasu Objednatele.
- 15.9 V případě, že činností, nečinností anebo opomenutím Dodavatele anebo jeho pracovníků vznikne Objednateli nemajetková újma, je Dodavatel povinen ji odčinit.
- 15.10 Dodavatel odpovídá Objednateli za své případné poddodavatele jako za plnění vlastní, včetně odpovědnosti za způsobenou újmu.

- 15.11 Pokud v průběhu plnění povinností vznikne na straně Dodavatele potřeba využít služeb třetí strany – poddodavatele, je oprávněn tak učinit jen po předchozím souhlasu Objednatele a jen tehdy, pokud bude nový poddodavatel splňovat potřebnou kvalifikaci. V případě, že Objednatel souhlas k využití poddodavatele neudělí, není Dodavatel oprávněn takovou poddodávku udělit. V případě souhlasu Objednatele a následného využití služeb třetí strany bude Dodavatel odpovídat za třetí stranu, jako by plnil sám, včetně odpovědnosti za způsobenou újmu. Dodavatel je povinen zajistit, aby jeho poddodavatel poskytoval Plnění v souladu s touto Smlouvou a dodržoval veškerá ujednání mezi Smluvními stranami.
- 15.12 Dodavatel je povinen po celou dobu trvání Smlouvy mít sjednáno pojištění odpovědnosti za majetkové i nemajetkové újmy způsobené v souvislosti se Smlouvou Dodavatelem nebo osobou, za niž odpovídá, s pojistnou částkou nejméně ve výši 10 000 000,- Kč. Dodavatel je povinen kdykoli v průběhu trvání této Smlouvy předložit na výzvu Objednatele doklad o pojištění v rozsahu dle tohoto odstavce Smlouvy a to do 5 pracovních dní od písemné výzvy Objednatele. Při vzniku pojistné události zabezpečuje ihned po jejím vzniku veškeré úkony vůči pojistiteli Dodavatel. Objednatel je povinen poskytnout v souvislosti s pojistnou událostí Dodavatele veškerou součinnost, která je v jeho možnostech.
- 15.13 Objednatel je oprávněn započíst jakoukoliv svoji pohledávku, byť i nesplatnou, vůči Dodavateli proti jakékoliv pohledávce, byť i nesplatné, kterou má Dodavatel vůči Objednateli. Dodavatel je oprávněn jednostranně započíst své splatné či nesplatné pohledávky vůči Objednateli pouze s předchozím písemným souhlasem Objednatele.

16 Odpovědní pracovníci

- 16.1 Odpovědnými pracovníky Objednatele a Dodavatele ve věcech obchodních pro účely této Smlouvy jsou:

a) Za Objednatele:

██████████
██████████
██████████
██████████

b) Za Dodavatele:

██████████
██████████
██████████
██████████

- 16.2 Odpovědnými pracovníky Objednatele a Dodavatele ve věcech technických pro účely této Smlouvy jsou:

a) Za Objednatele:

██████████
██████████
██████████
██████████

b) Za Dodavatele:

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

17 Sankce

- 17.1 V případě prodlení Dodavatele se zahájením poskytování Podpory v termínu dle odst. 3 této Smlouvy, je Dodavatel povinen uhradit Objednateli smluvní pokutu ve výši 2% z roční ceny Podpory sjednané v odst. 6.1 Smlouvy za každý započatý den prodlení.
- 17.2 V případě prodlení Dodavatele s dokončením jednotlivých fází Plnění dle odst. 5.2 Smlouvy (Cílový koncept, AlmaLinux XAPOST, Pilot, Přechod) je Dodavatel povinen uhradit Objednateli smluvní pokutu ve výši 2% z ceny příslušné složky Plnění dle čl. 6.2 – 6.4 Smlouvy, se kterou je v prodlení, za každý započatý den prodlení.
- 17.3 V případě prodlení Dodavatele s poskytováním služeb Rozvoje v termínu dle příslušné Dílčí smlouvy, je Dodavatel povinen uhradit Objednateli smluvní pokutu ve výši 2 % z ceny Rozvoje sjednané v příslušné Dílčí smlouvě za každý započatý den prodlení. Převzetí Plnění nebo jeho části ze strany Objednatele nemá na vliv na odpovědnost Dodavatele za prodlení.
- 17.4 Bude-li Objednatel v prodlení s úhradou ceny předmětu plnění, má Dodavatel právo žádat na Objednateli úrok z prodlení v souladu s nařízením vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměnu likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku a veřejných rejstříků právnických a fyzických osob, ve znění pozdějších předpisů.
- 17.5 Je-li Dodavatel v prodlení s dodržáním kterékoli lhůty či termínu plnění uvedených v odst. 2.7, 2.8. nebo 2.9 Smlouvy, je Dodavatel povinen zaplatit Objednateli smluvní pokutu ve výši 1 000,- Kč za každý jednotlivý případ a každou započatou hodinu prodlení, byla-li lhůta (termín) sjednána v hodinách, a 10 000,- Kč za každý jednotlivý případ a každý započatý den prodlení, byla-li lhůta (termín) sjednána ve dnech.
- 17.6 V každém jednotlivém případě porušení povinností dle čl. 8 nebo čl. 10 nebo čl. 11 Smlouvy ze strany Dodavatele, je Dodavatel povinen uhradit Objednateli smluvní pokutu ve výši 500 000,- Kč.
- 17.7 V každém jednotlivém případě porušení povinnosti uvedené v Příloze č. 7 Smlouvy (Požadavky na bezpečnost ICT - Pravidla pro dodavatele), je Dodavatel povinen uhradit Objednateli smluvní pokutu ve výši 500 000,- Kč.
- 17.8 Je-li Dodavatel v prodlení s plněním povinnosti odstranit vady dle čl. 4 Smlouvy nebo s plněním povinnosti odstranit záruční vady dle čl. 9 Smlouvy, je Dodavatel povinen zaplatit Objednateli smluvní pokutu ve výši 100 000,- Kč za každý započatý den prodlení s odstraněním každé vady kategorie A; ve výši 10 000,- Kč za každý započatý den prodlení s odstraněním každé vady kategorie B; a ve výši 1 000,- Kč za každý započatý den prodlení s odstraněním každé vady kategorie C.
- 17.9 V případě porušení povinnosti předložit na výzvu Objednatele doklad o pojištění dle odst. 15.12 Smlouvy je Dodavatel povinen uhradit Objednateli smluvní pokutu ve výši 100 000,- Kč, a to i opakovaně.

- 17.10 V případě, že dojde k porušení povinnosti Dodavatele, která zakládá nárok Objednatele k okamžitému odstoupení od Smlouvy, je Objednatel bez ohledu na skutečnost, zda využije svého práva na odstoupení od Smlouvy, oprávněn účtovat Dodavateli smluvní pokutu ve výši 750 000,- Kč za každý jednotlivý případ porušení takové povinnosti.
- 17.11 Uplatněním jakékoliv smluvní pokuty není dotčeno právo na náhradu vzniklé újmy v celém rozsahu.
- 17.12 V případě prokazatelného prodlení povinné Smluvní strany s poskytnutím součinnosti není druhá Smluvní strana v prodlení s plněním svých závazků závislých na poskytnutí součinnosti povinné Smluvní strany a veškeré lhůty se o prokazatelné prodlení povinné Smluvní strany prodlužují, nedohodnou-li se Smluvní strany jinak.
- 17.13 Vyúčtování smluvní pokuty musí být zasláno doporučeně s dodejkou. V případě zaslání v elektronické podobě musí být vyúčtování smluvní pokuty zasláno do datové schránky. Smluvní pokuta je splatná v době třiceti (30) kalendářních dnů ode dne doručení vyúčtování o smluvní pokutě druhé Smluvní straně.
- 17.14 Objednatel je v případě uplatnění smluvní pokuty vůči Dodavateli dle této Smlouvy a neuhrazení smluvní pokuty ze strany Dodavatele oprávněn využít jednostranné započtení vzájemných pohledávek, a to i v případě, že kterákoli ze započítávaných pohledávek ještě není splatnou. Dodavatel není oprávněn své pohledávky jednostranně započítat oproti pohledávkám Objednatele bez předchozího písemného souhlasu Objednatele.

18 Doba trvání Smlouvy

- 18.1 Tato Smlouva nabývá platnosti dnem jejího podpisu Smluvními stranami a účinnosti zveřejněním Smlouvy v registru smluv. Plnění předmětu této Smlouvy v době od platnosti Smlouvy do její účinnosti se považuje za plnění podle této Smlouvy a práva a povinnosti z něj vzniklé se řídí touto Smlouvou.
- 18.2 Tato Smlouva se uzavírá na dobu určitou, a to na 4 roky ode dne zahájení poskytování Podpory.
- 18.3 Předčasně ukončit účinnost této Smlouvy lze písemnou dohodou Smluvních stran, výpovědí Objednatele nebo jednostranným odstoupením v případě podstatného porušení Smlouvy a v dalších případech stanovených právními předpisy.
- 18.4 Za podstatné porušení této Smlouvy se, ve smyslu § 2002 Občanského zákoníku, považují situace výslovně zmíněné v této Smlouvě a dále zejména případy kdy:
- a) je Objednatel přes písemné upozornění Dodavatele v prodlení s úhradou daňového dokladu vystaveného na základě a v souladu s podmínkami této Smlouvy déle než dvacet (20) kalendářních dnů od písemného upozornění;
 - b) je Dodavatel v prodlení s plněním jakékoli povinnosti dle této Smlouvy déle než čtrnáct (14) kalendářních dnů;
 - c) je Dodavatel pravomocně odsouzen pro trestný čin;
 - d) je Dodavatel v likvidaci nebo vůči jeho majetku probíhá insolvenční řízení, v němž bylo vydáno rozhodnutí o úpadku nebo insolvenční návrh byl zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení, nebo byl konkurs zrušen proto, že majetek byl zcela nepostačující nebo byla zavedena nucená správa podle zvláštních právních předpisů;
 - e) se Smluvní strana dopustila vůči druhé Smluvní straně jednání vykazujícího znaky nekalé soutěže.
- 18.5 Odstoupení je účinné od okamžiku, kdy je doručeno písemné prohlášení jedné Smluvní strany o odstoupení od Smlouvy druhé Smluvní straně. Odstoupit lze i pouze od příslušné Dílčí smlouvy.

- 18.6 Odstoupením od Smlouvy nebo její části nejsou dotčena ustanovení týkající se smluvní pokuty, záruky, náhrady újmy, licencí a jiných ze své povahy přetrvávajících nároků či závazků.
- 18.7 V případě odstoupení od Smlouvy jsou Smluvní strany povinny vzájemnou dohodou písemně vypořádat dosavadní přijaté smluvní plnění nejpozději do jednoho (1) měsíce od účinnosti odstoupení od Smlouvy, přičemž platí, že Plnění řádně (bez vad) poskytnutá do okamžiku ukončení účinnosti této Smlouvy si nebudou vracet.
- 18.8 Objednatel má právo tuto Smlouvu vypovědět bez udání důvodů s výpovědní dobou tři (3) měsíce, jež začne plynout prvním dnem kalendářního měsíce následujícího po doručení písemné výpovědi druhé Smluvní straně.

19 Závěrečná ujednání

- 19.1 Tato Smlouva a vztahy z ní vyplývající se řídí právním řádem České republiky, zejména příslušnými ustanoveními Občanského zákoníku, Zákona o zadávání veřejných zakázek a Autorského zákona. V případě rozporu mezi vlastním textem Smlouvy a přílohami má přednost vlastní text Smlouvy.
- 19.2 Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů, vzniklých na základě této Smlouvy nebo v souvislosti s touto Smlouvou, a k jejich vyřešení zejména prostřednictvím jednání odpovědných pracovníků nebo jiných pověřených subjektů. Nedohodnou-li se Smluvní strany na způsobu řešení vzájemného sporu, má každá ze Smluvních stran právo uplatnit svůj nárok u soudu České republiky příslušného dle platných právních předpisů. Smluvní strany se dohodly, že místně příslušným soudem pro řešení případných sporů bude soud příslušný dle místa sídla Objednatele.
- 19.3 Tato Smlouva může být měněna pouze výslovným písemným ujednáním Smluvních stran, podepsaným oprávněnými zástupci Smluvních stran. Tato ujednání budou nazývána „Dodatek“ a budou číslována vzestupnou číselnou řadou. Jakákoliv Smluvní strana je oprávněna vyvolat jednání k doplnění či změně této Smlouvy. Změnu kontaktních osob a spojení uvedených v čl. 16 nebo v Příloze č. 4 Smlouvy je účinná v okamžiku doručení oznámení o této změně druhé Smluvní straně, aniž by bylo nutno vyhotovovat dodatek k této Smlouvě.
- 19.4 Objednatel je oprávněn převést práva a povinnosti ze Smlouvy nebo její části na třetí osobu. K takovému převodu uděluje Dodavatel Objednateli výslovný souhlas. Postoupení Smlouvy či její části je vůči Dodavateli účinné okamžikem doručení oznámení o postoupení Smlouvy Objednatelům Dodavateli nebo okamžikem, kdy třetí osoba Dodavateli postoupení Smlouvy či její části prokáže. Objednatel a Dodavatel se dohodli, že ustanovení § 1899 Občanského zákoníku o tom, že v případě neplnění převzaté povinnosti postupníkem může Dodavatel po Objednateli požadovat, aby tuto povinnost splnil místo postupníka, se nepoužije.
- 19.5 Smluvní strany si ve smyslu ustanovení § 1765 odst. 2 Občanského zákoníku ujednaly, že Dodavatel na sebe přebírá nebezpečí změny okolností.
- 19.6 Smluvní strany se dohodly, že ustanovení § 1799 a 1800 Občanského zákoníku se nepoužijí.
- 19.7 Je-li Smlouva vyhotovena v listinné podobě, je vyhotovena ve dvou (2) stejnopisech s platností originálu, z nichž každá ze smluvních stran obdrží po jednom (1) stejnopisu. Pokud je Smlouva vyhotovena v elektronické podobě, obě smluvní strany obdrží elektronický originál opatřený elektronickými podpisy obou smluvních stran, včetně časového razítka dle příslušných právních předpisů.
- 19.8 Pokud jakákoliv ustanovení nebo jakékoliv části ustanovení Smlouvy budou považovány za neplatné nebo nevymahatelné, nebude mít taková neplatnost nebo nevymahatelnost za následek neplatnost nebo nevymahatelnost celé Smlouvy, ale celá Smlouva se bude vykládat tak, jako kdyby neobsahovala příslušná neplatná nebo nevymahatelná ustanovení nebo části ustanovení a

práva a povinnosti Smluvních stran se budou vykládat přiměřeně. Smluvní strany se dále zavazují, že budou navzájem spolupracovat s cílem nahradit takové neplatné nebo nevymahatelné ustanovení platným a vymahatelným ustanovením, jímž bude dosaženo stejného ekonomického výsledku (v maximálním možném rozsahu v souladu s právními předpisy), jako bylo zamýšleno ustanovením, jež bylo shledáno neplatným či nevymahatelným.

- 19.9 Dnem doručení písemností odeslaných na základě této Smlouvy nebo v souvislosti s touto Smlouvou, pokud není prokázán jiný den doručení, se rozumí poslední den lhůty, ve které byla písemnost pro adresáta uložena u provozovatele poštovních služeb, a to i tehdy, jestliže se adresát o jejím uložení nedověděl. Smluvní strany tímto výslovně vylučují ust. § 573 Občanského zákoníku.
- 19.10 Dodavatel tímto prohlašuje, že mu byly ze strany Objednatele sděleny veškeré skutkové a právní okolnosti související s uzavřením této Smlouvy a že Dodavatel je v tomto ohledu přesvědčen o jeho schopnosti uzavřít tuto Smlouvu, má zájem tuto Smlouvu uzavřít a jeho schopen plnit veškeré povinnosti z této Smlouvy plynoucí.
- 19.11 Smluvní strany tímto prohlašují, že neexistuje žádné ústní ujednání, Smlouva či řízení některé Smluvní strany, které by nepříznivě ovlivnilo výkon jakýchkoliv práv a povinností dle této Smlouvy. Zároveň potvrzují svým podpisem, že veškerá ujištění a dokumenty dle této Smlouvy jsou pravdivé, platné a právně vymahatelné.
- 19.12 Pro případ, že tato Smlouva není uzavírána za přítomnosti obou Smluvních stran, platí, že Smlouva nebude uzavřena, pokud ji Dodavatel podepíše s jakoukoliv změnou či odchylkou, byť nepodstatnou, nebo dodatkem. To platí i v případě připojení obchodních podmínek Dodavatele, které budou odporovat svým obsahem jakýmkoliv způsobem textu této Smlouvy.
- 19.13 Nedílnou součástí Smlouvy jsou přílohy:
- Příloha č. 1 – Popis prostředí ČP (OS, SW a přehled typů HW)
 - Příloha č. 2 – Licenční ujednání
 - Příloha č. 3 – Vzor formuláře požadavku na poskytnutí Podpory
 - Příloha č. 4 – Kontaktní informace (hot-line Dodavatele a osoby Objednatele oprávněné k zadávání/přijímání požadavků a odezvy ve věci Podpory)
 - Příloha č. 5 – Vzor akceptačního protokolu
 - Příloha č. 6 – Seznam poddodavatelů
 - Příloha č. 7 - Požadavky na bezpečnost ICT – Pravidla pro dodavatele

NA DŮKAZ TOHO, že Smluvní strany s obsahem Smlouvy souhlasí, rozumí ji a zavazují se k jejímu plnění, připojují své podpisy a prohlašují, že tato Smlouva byla uzavřena podle jejich svobodné a vážné vůle prosté tísně, zejména tísně finanční.

V Praze

V Ostravě

Ing. Martin Götz
ředitel úseku ICT a eGovernment
Česká pošta, s.p.

Ing. Dušan Lampart
jednatel
LinuxBox.cz, s.r.o.

Příloha č. 1 – Technická specifikace Podpory a Rozvoje, popis OS, SW a přehled typů HW

1 Popis OS, SW:

Instalace OS vychází z linuxové distribuce CentOS řady 7 ve variantě jak pro servery, tak klientské stanice na poštách.

OS využívá vlastní custom-built kernel s několika modifikacemi (podpora více paralelních portů, podpora víceportových karet, převodníků usb > RS232. Úpravy MPT-Fusion SCSI řadiče).

Instalace klientů a serverů je plně automatická včetně automatické konfigurace hardware.

Instalace klientů je redukována na nejnutnější služby a SW, probíhá formou instalačního image rovněž pomocí síťové instalace (PXE).

Uživatelské profily jsou připojovány na klienty pomocí NFS síťově ze serveru s patřičnou rolí.

Serverová instalace OS lze použít jako instalační server pro další instalace serverů a klientů síťově pomocí PXE

Součástí OS je také funkcionality centrální správy aktualizací jak serverů, tak klientů.

Dodavatel OS nemá (plošný) přístup na servery ani na klienty.

Instalovaný OS obsahuje tyto možnosti aktualizace OS/SW komponent a dat:

- Automatické stahování a instalace patchů OS z centra
- Automatické stahování a instalace aplikací (mimo aplikace APOST) z centra
- Automatické aktualizace kancelářských dokumentů z centra
- Automatická synchronizace času

Instalace pro typ Server obsahuje tyto aplikace (klíčová pro plynulý přechod na novou distribuci či verzi podporovaného OS):

- APOST – interní aplikace pošty – interpretační vrstva s daty
- Všechny aplikace, které obsahuje instalace klient
- Nástroje pro připojení a konfigurace UPS
- Nástroje pro připojení a konfigurace tiskáren
- Nástroje komunikace s centrem APOST
- Nástroje pro zálohování a archivaci dat na poště
- Nástroje monitoringu OS a HW

Uživatelské prostředí obsahuje tyto možnosti konfigurace:

- Vlastní grafické uživatelské prostředí se základním rozlišením 800x600 a s možností jeho další konfigurace, použití klávesnice a myši
- Aplikace jsou spouštěny z předdefinovaných ikon na ploše i z lišty
- Barva plochy se liší podle role přihlášeného
- Správa uživatelů je napojena na správu uživatelů v aplikaci APOST interpretační server nebo na centrální správu uživatelů
- Možnost předdefinovaných uživatelských profilů dle role uživatele a jeho práv
- Možnost výběru a konfigurace periférií

Desktopové prostředí zahrnuje instalované aplikace a další SW komponenty:

- SW APOST včetně custom made PAM modulu (APOST – interní, přepážková aplikace pošty)
- Webový prohlížeč s automatickou konfigurací profilů – Mozilla Firefox – klient zajišťuje připojení přepážek dané pošty na intranetové servery k poskytování služeb externích subjektů na poštách prostřednictvím jednotné domovské stránky na portálu ČP

- E-mailový klient – Mozilla Thunderbird – klient zajišťuje připojení dané pošty do centrálního systému elektronické pošty, s možností centrálně upravovat konfiguraci profilů
- SW 602 FormFiller – klient CzechPoint – klient zajišťuje připojení k univerzálnímu rozhraní CzechPoint
- VMWare Horizont client včetně automatické konfigurace passthrough tiskáren
- Rezidentní antivirový štít – Eset antivirus, včetně centrální aktualizace, případně jiný antivirus, který využívá centrálně Česká pošta
- Kancelářský balík SW – Libre Office – klient zajišťuje používání standardních kancelářských aplikací (textový editor kompatibilní s MS Word a tabulkový kalkulátor kompatibilní s MS Excel)
- Grafický souborový manažer
- Prohlížeč PDF dokumentů s podporou certifikátů a elektronických značek
- Ovladače pro tokeny (v současné době využíván eToken5110)
- Ovladače pro laserové tiskárny
- Java Runtime Environment
- Citrix Receiver
- Souborový manažer
- Modul postOffice pro podporu služeb Atlas, Calypso a Dálniční známky z aplikace APOST
- Servisní ikona pro hrubou uživatelskou diagnostiku
- Security modul pro tlačítko tísňe
- (Volitelně) Modul pro vyvolávací systémy v lokalitách, kde jsou tyto instalovány, včetně ikon na ovládání nVS ze spodní lišty
- Nástroj pro možnost vytvoření PrintScreenu obrazovky
- Podpora UEFI pro nové typy počítačových stanic
- Zabbix klient - vzdálený monitoring HW a stavu některých systémových služeb
- A další drobné funkcionality ve stávajícím systému k 10/2022

Podpora hardware:

- RAID řadiče v Lenovo serverech včetně management utilit, síťové karty, grafické karty (dle přehledu HW dále)
- V Lenovo serverech grafické karty, řadiče, síťové karty
- Snímače čárových kódů, multiportové karty, GPS trackery, tiskárny včetně možnosti centrální rekonfigurace (dle přehledu HW dále)
- UPS (dle přehledu HW dále)
- Podpora security tokenů eToken5110 – 64bitů
- Podpora monitorů 4:3 i širokoúhlých 16:10

2 Přehled typů HW:

Přehled typů PC pro instalaci Linux APOST serverová část *
Typ PC
IBM xSeries 3200Serv. 4368PCD
IBM xSeries 3200Serv. 4368PDR
IBM xSeries 3200Serv. 4368PDQ
IBM xSeries 3200Serv. 4368Z9G
IBM xSeries 3200Serv. 7328PDJ

IBM xSeries 3200Serv. 7328PEJ
IBM xSeries 3200Serv. 7328Z5B
Lenovo M58 typ 7298
Lenovo M58 typ 7306
Lenovo System x3100 M5
Lenovo System x3250 M6
Lenovo ThinkCentre M57e
Lenovo ThinkCentre M700 SFF
Lenovo ThinkCentre M700 TWR
Lenovo ThinkCentre M70e Server
Lenovo ThinkCentre M710s SFF
Lenovo ThinkCentre M720s SFF
Lenovo ThinkCentre M73
Lenovo ThinkServer SR 250
Lenovo ThinkServer RS160
Lenovo ThinkServer TS440
Lenovo ThinkServer SR 250 - V2

*) Po ukončení výroby jednotlivých uvedených typů mohou být tyto typy nahrazeny následující typovou řadou

Přehled typů PC pro instalaci LINUX APOST část klientská stanice *
Typ PC
Lenovo M58 typ 7298
Lenovo M58 typ 7306
Lenovo ThinkCentre M57e
Lenovo ThinkCentre M700 SFF
Lenovo ThinkCentre M700 TWR
Lenovo ThinkCentre M70e Server
Lenovo ThinkCentre M710s SFF
Lenovo ThinkCentre M720s SFF
Lenovo ThinkCentre M73
ASUS PN41
ASUS PN51

*) Po ukončení výroby jednotlivých uvedených typů mohou být tyto typy nahrazeny následující typovou řadou

Přehled záložních zdrojů (UPS) pro instalaci LINUX *
Typ HW
EATON 5SC
NetUPS 450
NetUPS 700
NetUPS 1500
POWERWARE 3110
POWERWARE 5105
POWERWARE 5115
POWERWARE 5119
POWERWARE 9120
POWERWARE 9130
POWERWARE 9305
POWERWARE 9355
POWERWARE 9390
POWERWARE PRIME
PRESTIGE 600
PRESTIGE 1500
Riello NPW 800
Riello SDH 1000
Riello SDH 2200

*) Po ukončení výroby jednotlivých uvedených typů mohou být tyto typy nahrazeny následující typovou řadou

Přehled laserových tiskáren pro instalaci LINUX *
Typ HW
HP M607dn
OKI B411dn
OKI B4300
OKI B430dn
OKI B431dn
OKI B432dn
OKI B4350
OKI B4350n
OKI B4600n
OKI B512dn
OKI B731dn

*) Po ukončení výroby jednotlivých uvedených typů mohou být tyto typy nahrazeny následující typovou řadou

Přehled laserových multifunkčních tiskáren pro instalaci LINUX *
Typ HW
Brother MFC-8860DN
CANON MF 4570dn
CANON MF 5770
HP LJ 2420
HP LJ 3055
HP M527f
HP M528f
HP M553dn
HP M577f
OKI B4545MFP
OKI C5550MFP+DUP
OKI ES5162dnw
OKI MB562 dn
OKI MC560dn
OKI MC573dn
OKI MC760dn
RICOH Aficio MP 201SPF
RICOH Aficio MP 301SPF
RICOH Aficio MP 4002SP
RICOH Aficio SP 4510SF
SHARP AR-122E
XEROX Phaser 3100MFPV S
XEROX WorkCentre 3100MFP

*) Po ukončení výroby jednotlivých uvedených typů mohou být tyto typy nahrazeny následující typovou řadou

Přehled jehličkových tiskáren pro instalaci LINUX *
Typ HW
HighPrint 4915xe
HighPrint 4920
EPSON LQ 690
OKI ML 320
OKI ML 320FB
OKI ML 321
OKI ML 3320
OKI ML 3321
OKI ML 3410
OKI ML 521
OKI ML 5520
OKI ML 5590
OKI ML 5720
OKI ML 6300FB
OLIVETTI PR2
OLIVETTI PR2E

*) Po ukončení výroby jednotlivých uvedených typů mohou být tyto typy nahrazeny následující typovou řadou

Přehled termotransferových tiskáren pro instalaci LINUX *
Typ HW
Zebra 140Xi
Zebra ZT230
Zebra 110Xi
Ithaca 9000

*) Po ukončení výroby jednotlivých uvedených typů mohou být tyto typy nahrazeny následující typovou řadou

Přehled snímačů platebních karet pro instalaci LINUX *
Typ HW
Ingenico IPP 320
Ingenico Move 3500

*) Po ukončení výroby jednotlivých uvedených typů mohou být tyto typy nahrazeny následující typovou řadou

Přehled snímačů čárových kódů pro instalaci LINUX *
Typ HW
CCD snímač
CL3800LRB2
CPT 8001
CPT 8001-L
CPT-711 terminál
DL8600 terminál
DS4208
DS4308-SR kit
DS6708
IT 3800
LS 2080
LS 2208
LS 3578
LS 3603
LS 4208
MC 3000
MC 3100
MC 3190
MC3090
MT9060
PDT 3100
SYMBOL P370
MC32N0
Zebra DS4608
Zebra LI2208
Zebra LI3678
Zebra TC55
Zebra TC56
Zebra TC57

*) Po ukončení výroby jednotlivých uvedených typů mohou být tyto typy nahrazeny následující typovou řadou

Přehled elektronických vah pro instalaci LINUX *
Typ HW
Tonava TC5
Tonava TL5
Tonava TLA5
Tonava TC33
Tonava TL33
Tonava TLA30
Tonava TLA33
Tonava TLA60
Lesák TLB4

*) Po ukončení výroby jednotlivých uvedených typů mohou být tyto typy nahrazeny následující typovou řadou

Přehled zákaznických displejů pro instalaci LINUX *
Typ HW
Zákaz. displej – seriové rozhraní
Zákaz. displej – paralelní rozhraní

*) Po ukončení výroby jednotlivých uvedených typů mohou být tyto typy nahrazeny následující typovou řadou

Příloha č. 2 – Licenční ujednání

Licence k Systému, jakékoli aktualizace (update), nové verze (upgrade), opravy či úpravy Systému dodané v rámci poskytování Plnění, vyjma Rozvoje, jsou touto Smlouvou poskytovány jako nevýhradní, na území České republiky. Dodavatel poskytne na dobu trvání majetkových práv autora k Systému nevýhradní, převoditelnou licenci k výkonu práva Systém užít, a to neomezeně co do místa a množství, způsobu a formy s tím, že toto oprávnění začne platit ode dne podpisu akceptačního protokolu.

Obecná veřejná licence GNU v.2 (GNU GPL v.2)

2. verze, Červen 1991

Copyright © 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Kopírování a distribuce doslovných kopií tohoto licenčního dokumentu jsou povoleny, ale jeho úpravy jsou zakázány.

Obsah

- [Preamble](#)
- [USTANOVENÍ a PODMÍNKY](#)
 - [Bez záruky](#)
- [Jak uplatnit tato ustanovení na vaše nové programy](#)

Preamble

Většina softwarových licencí je navržena tak, aby omezovaly svobodu jeho sdílení a úprav. Naproti tomu, smyslem Obecné veřejné licence GNU je zaručit svobodu sdílení a úprav svobodného softwaru – pro zajištění svobodného přístupu k tomuto softwaru pro všechny jeho uživatele. Tato Obecná veřejná licence GNU se vztahuje na většinu softwaru nadace Free Software Foundation a na jakýkoli jiný program, jehož autor jí přijme. (Některý jiný software od Free Software Foundation je namísto toho licencován pod GNU Lesser General Public Licence.) Můžete ji rovněž použít pro své programy.

Pokud mluvíme o svobodném softwaru, myslíme tím svobodu používání, nikoliv cenu. Naše Obecné veřejné licence jsou navrženy tak, abyste mohli volně šířit kopie svobodného softwaru (a pokud chcete, nechat si za to i zaplatit), abyste obdrželi zdrojový kód, nebo jej měli možnost získat, abyste mohli tento software měnit nebo jeho části použít v nových programech a abyste věděli, že tyto věci smíte dělat.

Abychom mohli vaše práva chránit, musíme zabránit tomu, aby vám kdokoliv tato práva odepíral, nebo vás žádal, abyste se těchto práv vzdali. Tato omezení se promítají do jistých povinností, které musíte dodržet, pokud šíříte nebo upravujete takový software.

Například, šíříte-li kopie takového programu, ať již zdarma nebo za poplatek, musíte poskytnout příjemcům všechna práva, která máte sám. Musíte zaručit, že příjemci rovněž dostanou, anebo mohou získat zdrojový kód. A musíte je upozornit na tyto podmínky, aby i oni znali svá práva.

Vaše práva chráníme ve dvou krocích: (1) zabezpečením autorských práv k softwaru, a (2) nabídkou této licence, která vám dává právoplatné svolení k jeho kopírování, šíření a/nebo jeho úpravě.

Kvůli ochraně každého autora i nás samotných chceme zajistit, aby každý chápal skutečnost, že pro tento svobodný software neexistuje žádná záruka. Je-li software někým jiným upraven a šířen dále, chceme, aby příjemci věděli, že to, co mají, není originál, takže jakékoliv problémy vnesené jinými se neodrazí na reputaci původních autorů.

Závěrem, každý svobodný program je neustále ohrožen softwarovými patenty. Přejeme si zamezit nebezpečí, že distributoři svobodného programu obdrží samostatná patentová osvědčení a tím učiní program vázaným. Abychom tomu zamezili,

deklarujeme, že každý patent vztahující se na svobodný program musí umožňovat svobodné užití, anebo nesmí být vydán vůbec.

Přesná ustanovení a podmínky pro kopírování, šíření a úpravu jsou uvedeny níže.

USTANOVENÍ a PODMÍNKY pro KOPÍROVÁNÍ, ŠÍŘENÍ a ÚPRAVU

0. Tato Licence se vztahuje na kterýkoliv program či jiné dílo, které obsahuje autorem umístěnou zmínku o tom, že může být šířeno podle ustanovení Obecné veřejné licence GNU. V dalším textu znamená "Program" každý takový program nebo dílo a "dílo založené na Programu" znamená buď program samotný anebo každé jiné dílo z něj odvozené dle autorského zákona: tím se míní dílo obsahující Program nebo jeho část, buď doslovně anebo s úpravami, popřípadě v překladu do jiného jazyka. (Dále je překlad zahrnován bez omezení pod pojem "úprava".) Uživatel Licence je označován jako "Vy".

Jiné činnosti než kopírování, šíření a úpravy Programu nejsou pokryty Licencí, sahají mimo její rámec. Akt spuštění Programu není omezen a výstup z Programu je pokryt Licencí pouze tehdy, jestliže obsah výstupu vytvoří dílo založené na Programu (nezávisle na tom, zda bylo vytvořeno činností Programu). Posouzení platnosti předchozí věty závisí na tom, co Program dělá.

1. Můžete kopírovat a šířit doslovné kopie zdrojového kódu Programu tak, jak jste jej obdrželi, a na libovolném médiu, za předpokladu, že na každé kopii viditelně a náležitě zveřejníte zmínku o autorských právech a absenci záruky; ponecháte nedotčené všechny zmínky vztahující se k této Licenci a k absenci záruky; a dáte každému příjemci spolu s Programem kopii této licence.

Za fyzický akt přenesení kopie můžete žádat poplatek a podle vlastního uvážení můžete nabídnout za poplatek i záruční ochranu.

2. Můžete upravovat vaši kopii, či kopie Programu, anebo kterékoliv jeho části a tak vytvořit dílo založené na Programu, a kopírovat a šířit takové úpravy, či dílo, podle podmínek odstavce 1 výše, za předpokladu, že splníte všechny tyto podmínky:

- a) Upravené soubory musíte opatřit zřetelnou zmínkou uvádějící, že jste soubory změnily s datem každé změny.
- b) Musíte umožnit, aby jakékoliv vámi zveřejněné či šířené dílo, které jako celek nebo zčásti obsahuje Program nebo jakoukoli jeho část, popřípadě je z Programu nebo jeho části odvozeno, mohlo být jako celek bezplatně poskytnuto každé třetí osobě v souladu s ustanoveními této Licence.
- c) Pokud upravený Program interaktivně čte povely, musíte zajistit, že při nejběžnějším způsobu jeho spuštění vytiskne nebo zobrazí hlášení příslušnou zmínku o autorském právu a zmínku o tom, že neexistuje žádná záruka (nebo případně, že záruku poskytnete vy), a že uživatelé mohou za těchto podmínek Program šířit dále, a musí uživateli sdělit, jakým způsobem může nahlédnout do textu této Licence. (Výjimka: v případě, že sám Program je interaktivní, avšak žádné takové hlášení nevypisuje, nepožaduje se, aby vaše dílo založené na Programu takové hlášení vypisovalo.)

Tyto požadavky se vztahují k upravenému dílu jako celku. Pokud identifikovatelné části díla nejsou odvozeny z Programu a mohou být samy o sobě považovány za nezávislá a samostatná díla, pak se tato Licence a její ustanovení nevztahují na tyto části, jsou-li šířeny jako nezávislá díla. Avšak jakmile tytéž části šíříte jako části celku, jímž je dílo založené na Programu, musí být rozšiřování tohoto celku podřízeno ustanovením této Licence tak, že povolení poskytnutá dalším uživatelům se rozšíří na celé dílo, tedy na všechny jeho části bez ohledu na to, kdo kterou část napsal.

Smyslem tohoto odstavce tedy není získání práv na dílo zcela napsané vámi ani popírání vašich práv vůči němu; skutečným smyslem je výkon práva na řízení distribuce odvozených nebo kolektivních děl založených na Programu.

Pouhé spojení jiného díla, jež není na Programu založeno, s Programem (anebo dílem založeným na Programu) na paměťovém nebo distribučním médiu neuvazuje toto jiné dílo do působnosti této licence.

3. Můžete kopírovat a šířit Program (nebo dílo na něm založené, viz odstavec 2) pomocí strojového kódu anebo ve spustitelné podobě podle ustanovení odstavců 1 a 2 výše, pokud splníte některou z následujících náležitostí:

- a) Doprovodíte jej strojově čitelným zdrojovým kódem, který musí být šířen podle ustanovení odstavců 1 a 2 výše, a to na médiu běžně používaném pro výměnu softwaru.
- b) Doprovodíte jej písemnou nabídkou s platností nejméně tři roky, podle níž poskytnete jakékoli třetí straně kompletní strojově čitelnou kopii odpovídajícího zdrojového kódu, jenž musí být šířen podle ustanovení odstavců 1

a 2 výše, na médiu běžně používaném pro výměnu softwaru a za poplatek nepřevyšující vaše výdaje vynaložené na fyzickou výrobu kopie zdroje.

- c) Doprovodíte jej informacemi, které jste dostal ohledně nabídky na poskytnutí příslušného zdrojového kódu. (Tato alternativa je povolena jen pro nekomerční šíření a jenom tehdy, pokud jste obdržel Program za pomoci strojového kódu nebo ve spustitelné podobě spolu s takovou nabídkou, v souladu s podmínkou b) výše.)

Zdrojový kód k dílu je nejvhodnější formou díla pro jeho případné úpravy. Pro spustitelné dílo úplný zdrojový kód znamená veškerý zdrojový kód pro všechny moduly, které obsahuje, včetně jakýchkoli dalších souborů pro definici rozhraní a dávkových souborů potřebných pro kompilaci a instalaci spustitelného díla. Zvláštní výjimkou jsou části, které jsou běžně šířeny (ve zdrojové nebo binární formě) s hlavními součástmi (kompilátor, jádro, apod.) operačního systému, na němž spustitelné dílo běží, pokud ovšem taková část sama nedoprovází spustitelné dílo.

Je-li šíření strojového kódu nebo spustitelného díla činěno nabídkou přístupu ke kopírování z určitého místa, potom se za šíření zdrojového kódu počítá i nabídnutí ekvivalentního přístupu ke kopírování zdrojového kódu ze stejného místa, byť přitom nejsou třetí strany nuceny ke zkopírování zdrojového kódu spolu se strojovým.

4. Nesmíte kopírovat, upravovat, poskytovat sublicence anebo šířit program jiným způsobem než výslovně uvedeným v této Licenci. Jakýkoli jiný pokus o kopírování, upravování, poskytnutí sublicence anebo šíření Programu je neplatný a automaticky ukončí vaše práva daná touto Licencí. Strany, které od vás obdržely kopie anebo práva v souladu s touto Licencí, však nemají své práva dané touto Licencí ukončeny, dokud se jim plně podřizují.

5. Jelikož jste tuto Licenci nepodepsali, není vaší povinností ji přijmout. Nic jiného vám však nedává možnost kopírovat nebo šířit Program nebo odvozená díla. V případě, že tuto Licenci nepřijmete, jsou tyto činnosti zákonem zakázány. Tím pádem úpravou anebo šířením programu (anebo každého díla založeného na Programu) vyjadřujete souhlas s Licencí a všem jejím ustanovením a podmínkám pro kopírování, upravování a šíření Programu a děl na něm založených.

6. Pokaždé, když dále šíříte Program (nebo dílo založené na Programu), získává příjemce od původního držitele Licence právo kopírovat, upravovat a šířit Program v souladu s těmito ustanoveními a podmínkami. Nesmíte klást žádné další překážky výkonu zde zaručených příjemcových práv. Nejste odpovědný za vymáhání dodržování této Licence třetími stranami.

7. Jsou-li vám z rozhodnutí soudu, obviněním z porušení patentu, nebo z jakéhokoli jiného důvodu (nejen v souvislosti s patenty) uloženy takové podmínky (ať již příkazem soudu, smlouvou nebo jinak), které se vylučují s podmínkami této Licence, nejste tím osvobozeni od podmínek této Licence. Pokud nemůžete Program šířit tak, abyste vyhověl zároveň svým závazkům vyplývajícím z této Licence a jiným platným závazkům, nesmíte jej v důsledku toho šířit vůbec. Pokud by například patentové osvědčení nepovolovalo bezplatné šíření Programu všemi, kdo vašim přičiněním získají přímo nebo nepřímo jeho kopie, pak by jediný možný způsob, jak vyhovět zároveň patentovému osvědčení i této Licenci, spočíval v úplném ukončení šíření Programu.

Pokud by se za jistých okolností jevila některá část tohoto odstavce jako neplatná nebo nevynutitelná, ostává krom této části v platnosti celý zbytek tohoto odstavce a za všech jiných jako těchto okolností ostává platný odstavec jako celek.

Smyslem tohoto odstavce není navádět vás k porušování patentů či jiných vlastnických práv, anebo tato ustanovení zpochybňovat. Jediným jeho smyslem je ochrana integrity systému šíření svobodného softwaru, který je používán veřejnými licencemi. Mnozí lidé přispěli do velkého množství softwaru šířeného tímto systémem, spolehnuvše se na jeho důsledné uplatňování. Záleží na autorovi/dárci, aby rozhodl, zda si přeje šířit software pomocí nějakého jiného systému a žádný uživatel Licence nemůže takové rozhodnutí zpochybňovat.

Smyslem tohoto odstavce je zevrubně osvětlit to, co je považováno za důsledek plynoucí ze zbytku této Licence.

8. Pokud je šíření či použití Programu v některých zemích omezeno, buď patenty, anebo autorským zákonem, může držitel původních autorských práv, který světuje Program do působnosti této Licence, přidat výslovné omezení pro geografické šíření vylučující takové země, takže šíření je povoleno jen v těch zemích nebo mezi těmi zeměmi, které nejsou tímto způsobem vyloučeny. Potom se takové geografické omezení stávají součástí této Licence.

9. Free Software Foundation může čas od času vydávat upravené nebo nové verze Obecné veřejné licence. Takové nové verze se budou svým duchem podobat současným verzím, mohou se však v řešení nových problémů či zájmů lišit v některých detailech.

Každé verzi je přiděleno rozlišující číslo verze. Pokud Program určí číslo verze, vztahuje se na něj daná verze nebo "všechny následující verze", a můžete se podle uvážení řídit ustanoveními a podmínkami buďto oné konkrétní verze anebo kterékoliv

následující verze, kterou vydala Free Software Foundation. Jestliže Program nespecifikuje číslo verze této Licence, můžete si vybrat libovolnou verzi, kterou kdy Free Software Foundation vydala.

10. Pokud si přejete zahrnout části Programu do jiných svobodných programů, jejichž distribuční podmínky jsou odlišné, zašlete autorovi žádost o povolení. V případě softwaru, k němuž vlastní autorská práva Free Software Foundation, napište Free Software Foundation; někdy činíme výjimky ze zde uvedených ustanovení. Naše rozhodnutí bude vedeno dvěma cíli – zachováním volného šíření všech odvozenin našeho svobodného softwaru a podporou sdílení a opětovného využití softwaru obecně.

Bez záruky

11. VZHLÉDEM K BEZPLATNÉMU POSKYTNUTÍ LICENCE K PROGRAMU SE NA PROGRAM NEVZTAHUJE ŽÁDNÁ ZÁRUKA, V MÍŘE POVOLENÉ ZÁKONEM. POKUD NENÍ PÍSEMNĚ STANOVENO JINAK, DRŽITELÉ AUTORSKÝCH PRÁV POPŘÍPADĚ JINÉ STRANY POSKYTUJÍ PROGRAM “TAK, JAK JE”, BEZ ZÁRUKY JAKÉHOKOLI DRUHU, AŽ VÝSLOVNĚ NEBO VYPLÝVAJÍCÍ, VČETNĚ, ALE NIKOLI JEN, ZÁRUK OBCHODOVATELNOSTI A VHODNOSTI PRO URČITÝ ÚČEL. POKUD JDE O KVALITU A VÝKONNOST PROGRAMU, JE VEŠKERÉ RIZIKO NA VÁS. POKUD BY SE U PROGRAMU PROJEVILY ZÁVADY, NÁKLADY NA POTŘEBNOU ÚDRŽBU, OPRAVU ČI NÁPRAVU PADAJÍ NA VÁŠ VRUB.

12. V ŽÁDNÉM PŘÍPADĚ, S VÝJIMKOU TOHO, KDYŽ TO VYŽADUJE PLATNÝ ZÁKON, ANEBY KDYŽ TO BYLO PÍSEMNĚ ODSOUHLASENO, VÁM NEBUDE ŽÁDNÝ Z DRŽITELŮ AUTORSKÝCH PRÁV ANI ŽÁDNÁ JINÁ STRANA, KTERÁ SMÍ UPRAVOVAT NEBO ŠÍŘIT PROGRAM V SOULADU S PŘEDCHOZÍMI USTANOVENÍMI, ODPOVĚDNA ZA ŠKODY, VČETNĚ VŠECH OBECNÝCH, SPECIÁLNÍCH, NAHODILÝCH NEBO NÁSLEDNÝCH ŠKOD VYPLÝVAJÍCÍCH Z UŽÍVÁNÍ ANEBY NESCHOPNOSTI UŽÍVAT PROGRAMU (VČETNĚ, ALE NIKOLI JEN, ZTRÁTY NEBO ZKRESLENÍ DAT, NEBO TRVALÝCH ŠKOD ZPŮSOBENÝCH VÁM NEBO TŘETÍM STRANÁM, NEBO SELHÁNÍ FUNKCE PROGRAMU V SOUČINNOSTI S JINÝMI PROGRAMY), A TO I V PŘÍPADĚ, ŽE TAKOVÝ DRŽITEL AUTORSKÝCH PRÁV NEBO JINÁ STRANA BYLI UPOZORNĚNI NA MOŽNOST TAKOVÝCH ŠKOD.

Obecná veřejná licence GNU v.3 (GNU GPL v.3)

3. verze, 29. červen 2007

Copyright © 2007 [Free Software Foundation, Inc.](#)

Kopírování a distribuce doslovných kopií tohoto licenčního dokumentu jsou povoleny, ale jeho úpravy jsou zakázány.

Obsah

- [Preamble](#)
- [USTANOVENÍ a PODMÍNKY](#)
 - [0. Definice](#)
 - [1. Zdrojový kód](#)
 - [2. Základní privilegia](#)
 - [3. Ochrana zákonných práv uživatelů před Zákonem proti obcházení](#)
 - [4. Zveřejňování doslovných kopií](#)
 - [5. Zveřejňování upravených verzí zdroje](#)
 - [6. Zveřejňování nezdvořových verzí](#)
 - [7. Dodatečné podmínky](#)
 - [8. Ukončení](#)
 - [9. Přijetí Licence není povinné pro držení kopií](#)
 - [10. Automatické licencování následných příjemců](#)

- [11. Patenty](#)
- [12. Neexistuje výjimka na úkor svobody ostatních](#)
- [13. Použití s Obecnou veřejnou licencí GNU Affero](#)
- [14. Revidovaná verze této Licence](#)
- [15. Zřeknutí se záruky](#)
- [16. Omezení odpovědnosti](#)
- [17. Výklad odstavců 15 a 16](#)
- [Jak uplatnit tato ustanovení na vaše nové programy](#)

Preambule

Obecná veřejná licence GNU (v angličtině GNU General Public License, dále jen jako “GNU GPL” nebo “GPL”) je svobodná, “copyleft” (část autorských práv ponechává a části se zřídá) licence pro software a jiná díla.

Většina licencí pro software a jiná díla jsou navrženy tak, aby omezovaly svobodu jeho sdílení a úprav. Naproti tomu, Obecná veřejná licence GNU zaručuje svobodu sdílení a úprav všech verzí programu – aby byl software svobodný pro všechny jeho uživatele. My, ze Free Software Foundation, používáme Obecnou veřejnou licenci GNU pro většinu našich programů, ale licence se vztahuje i na díla jiných autorů, kteří se je rozhodli zveřejnit právě tímto způsobem. Můžete ji rovněž použít pro své programy.

Pokud mluvíme o svobodném softwaru, myslíme tím svobodu používání, nikoliv cenu. Naše Obecné veřejné licence jsou navrženy tak, abyste mohli volně šířit kopie svobodného softwaru (a pokud chcete, nechat si za to i zaplatit), abyste obdrželi zdrojový kód, nebo ho měli možnost získat, abyste mohli tento software měnit nebo jeho části použít v nových programech a abyste věděli, že tyto věci smíte dělat.

Abychom mohli chránit vaše práva, musíme zabránit tomu, aby vám kdokoliv tato práva odepíral, nebo vás žádal, abyste se těchto práv vzdali. Proto i vy máte určité povinnosti, které musíte dodržet, pokud šíříte nebo upravujete takový software, a to povinnost respektovat svobodu ostatních.

Například, šíříte-li kopie programu, ať již zdarma nebo za poplatek, příjemci musíte poskytnout stejná práva, jaké jste sami obdrželi. Musíte zaručit, že příjemci rovněž dostanou, anebo mohou získat zdrojový kód. A aby i oni znali svá práva, musíte je upozornit na tyto podmínky.

Vývojáři, kteří používají GNU GPL, chrání vaše práva ve dvou krocích: (1) zabezpečením autorských práv k softwaru, a (2) nabídkou této Licence, která vám dává právoplatné svolení k jeho kopírování, šíření a/nebo jeho úpravě.

Kvůli ochraně každého vývojáře a autora, GPL dává jasně najevo, že pro svobodný software neexistuje žádná záruka. V zájmu obou stran, uživatelů i autorů, GPL požaduje, aby upravené verze programu byly příslušně označeny, a to kvůli tomu, aby za původce případných chyb programu nebyli nesprávně označeni autoři původních verzí.

Některá zařízení uživatelům zakazují instalaci nebo spuštění upravených verzí softwaru, i když výrobce si takovou možnost ponechal. Toto je z principu neslučitelné s cílem ochrany uživatelské svobody – svobody jakkoli software měnit. Takové porušování se systematicky vyskytuje tam, kde je program určen pro jednotlivce, tedy tam, kde je to nejméně přijatelné. Abychom takovým počinem předešli, vytvořili jsme tuto verzi GPL. Jestliže problémy tohoto druhu budou nadále vznikat, jsme připraveni je podle potřeby ošetřit v následujících verzích GPL.

Závěrem, každý program je neustále ohrožen softwarovými patenty. Státy by neměly povolovat patenty pro zamezení vývoje a použití softwaru, který je určen pro všeobecné použití. Ale u těch, které tak činí, bychom rádi zamezili nebezpečí, že by distributoři svobodného programu obdrželi samostatná patentová osvědčení a tím by učinili takový program vázaným. Abychom tomu zamezili, GPL zaručuje, že patenty nemohou činit program nesvobodným.

Přesná ustanovení a podmínky pro kopírování, šíření a upravování naleznete níže.

USTANOVENÍ a PODMÍNKY

0. Definice

Označením “tato Licence” se myslí 3. verze Obecné veřejné licence GNU.

“Autorskými právy” se myslí i zákony příbuzné autorským právům, vztahující se na jiné druhy děl, jako např. polovodičové masky.

“Programem” se označuje jakékoli dílo, které může být chráněno autorskými právy a je licencováno touto Licencí. Uživatel licence se označuje jako “vy”. “Uživatelé licence” a “příjemci licence” mohou být jednotlivci nebo organizace.

“Upravováním” díla se rozumí zkopírování nebo přizpůsobení celého nebo jen části díla způsobem, který vyžaduje autorská práva. Nemyslí se tím vytvoření přesné kopie. Výsledné dílo se nazývá “upravenou verzí” původního díla nebo dílo “založené na” původním díle.

“Chráněným dílem” se myslí neupravená verze Programu nebo dílo založené na Programu.

“Šířením” díla se označuje jakákoli činnost, která by vás činila přímo či nepřímo odpovědnými za porušení Zákona o ochraně autorských práv, kromě spouštění díla na osobním počítači nebo vytváření vlastní kopie. Šíření zahrnuje kopírování, distribuci (s nebo bez úpravy), zpřístupnění veřejnosti a v některých zemích i další aktivity.

“Zveřejnit” dílo značí jakýkoliv druh šíření, které dalším stranám umožňuje výrobu nebo pořízení kopií. Běžné používání díla přes počítačovou síť, bez přenosu kopie k uživateli, se nepovažuje za zveřejnění díla.

Interaktivní uživatelské prostředí zobrazuje “Příslušné právní podmínky” v takovém rozsahu, že jsou uživateli pohodlně vnímatelné a umístěny na dobře viditelném místě a (1) oznamuje Příslušné právní podmínky a (2) oznamuje uživateli, že na dílo se nevztahuje záruka (kromě případů, kdy se záruka uděluje), že uživatelé licence mohou dílo na základě této Licence dále zveřejňovat a oznamuje, kde si mohou tuto Licenci přečíst. Pokud uživatelské prostředí obsahuje seznam uživatelských příkazů, dobře viditelné umístění v takovém menu splňuje toto kritérium.

1. Zdrojový kód

“Zdrojový kód” označuje preferovanou formu díla určenou na jeho úpravy. “Strojovým kódem” se označuje jakákoli nezdvojová forma díla.

“Standardním rozhraním” se myslí rozhraní, které je buď uznáno jako oficiální standard definován uznávanou standardizující autoritou, nebo, v případě rozhraní určených pro určitý programovací jazyk, je to rozhraní, které je uznané širokou vývojářskou veřejností daného jazyka.

“Systémové knihovny” spustitelného díla zahrnují vše (kromě díla jako celku), co (a) je zahrnuto v běžné formě balení hlavního komponentu, ale není součástí hlavního komponentu a (b) slouží pouze pro usnadnění práce s hlavní komponentou, nebo k implementaci standardního rozhraní tam, kde je implementace formou zdrojového kódu veřejnosti povolena. V tomto kontextu se “hlavní komponentou” myslí hlavní nezbytná součást (jádro, správce oken, atp.) daného operačního systému (pokud nějaký je), na kterém spustitelné dílo běží, nebo kompilátor používaný ke spuštění díla, nebo spouštěč strojového kódu používaný k běhu díla.

“Úplný zdroj” díla značí veškerý zdrojový kód potřebný pro generování, instalaci, spouštění (pro spustitelná díla) strojového kódu a úpravu díla, včetně skriptů pro kontrolu těchto úkonů. Nezahrnuje systémové knihovny díla, nebo obecné nástroje nebo obecně přístupné svobodné programy, které jsou používány (v neupravené podobě) k provedení těchto úkonů a nejsou součástí díla. Například, Úplný zdroj zahrnuje soubory pro definici rozhraní přidružené ke zdrojovým souborům díla, zdrojový kód sdílených knihoven a dynamicky navázané podprogramy, které dílo ke správnému fungování potřebuje – a to buď formou datové komunikace, nebo formou kontroly přenosu mezi podprogramy a jinými částmi díla.

Úplný zdroj nemusí obsahovat nic, co si mohou uživatelé automaticky vygenerovat z jiných částí Úplného zdroje.

Úplný zdroj pro dílo v podobě zdrojového kódu je dané dílo samo.

2. Základní privilegia

Všechna práva zaručená touto Licencí trvají po dobu platnosti autorského práva na Program a jsou neodvolatelné, pokud jsou dodrženy podmínky uvedené níže. Tato Licence explicitně potvrzuje vaše neomezené právo na spuštění neupraveného Programu. Výstup ze spuštění chráněného díla této Licence upravuje pouze v případě, že výstup, vzhledem ke svému obsahu, představuje chráněné dílo samo. Tato Licence zároveň uznává vaše právo na [“fair use”](#) (správné používání) nebo jiný ekvivalent daný zákonem o autorském právu.

Dokud je vaše licence platná, můžete tvořit, spouštět a šířit chráněná díla bez jakýchkoli omezení, i když díla sami nezveřejňujete. Pro účely exkluzivních úprav děl výhradně ve váš prospěch nebo vytvoření prostředků ke spuštění těchto děl, můžete chráněná díla zveřejnit pouze v případě, že v souladu s podmínkami této Licence zveřejníte všechny materiály, ke kterým nevlastníte autorská práva. A ti, kteří tvoří a spouštějí chráněná díla za vás, musí tak činit výhradně vaším jménem, s vaším usměrňováním a pod vaší kontrolou, v podmínkách, které jim mimo vztahu s vámi zakazují tvořit jakékoli kopie vašeho materiálu, ke kterému jste držitelem autorských práv.

Za jiných okolností zveřejnění díla podléhá podmínkám uvedeným níže. Sublicencování není povoleno, odstavec 10 ho činí zbytečným.

3. Ochrana zákonných práv uživatelů před Zákonem proti obcházení

Žádné chráněné dílo by nemělo být považováno za součást efektivních technologických prostředků na základě platných právních předpisů podle článku 11, Smlouvy WIPO o autorských právech, přijaté dne 20. prosince 1996, nebo obdobných zákonů zakazujících nebo omezujících obcházení takových prostředků.

Pokud zveřejníte chráněné dílo, zřikáte se jakékoliv právní moci zakázat obcházení technologických prostředků kromě případu, kdy by takové obcházení bylo provedeno na základě práva vyplývajícího z této Licence. Zároveň se zřikáte jakéhokoliv záměru omezit provoz nebo úpravu díla kvůli porušení zákonných práv (v rozporu s uživateli díla) vašich nebo třetí strany na zákaz obcházení technologických prostředků.

4. Zveřejňování doslovných kopií

Doslovné kopie zdrojového kódu Programu můžete zveřejňovat tak, jak jste jej obdržel, za pomoci libovolného média, ale pouze za předpokladu, že na každé kopii uvedete zmínku o autorovi a absenci záruky na vhodném a viditelném místě, že všechny zmínky odkazující na tuto Licenci a na jakoukoli přidanou podmínku podle odstavce 7 ponecháte beze změn a že zároveň ponecháte nedotčené všechny zmínky o absenci záruky a všem příjemcům zprostředkujete kopii této Licence spolu s Programem.

Za každou zveřejněnou kopii si můžete účtovat peníze (ale nemusíte) a také můžete nabízet služby zákaznické podpory nebo záruku za poplatek.

5. Zveřejňování upravených verzí zdroje

Dílo založené na Programu, nebo úpravy na vytvoření díla založené na Programu, můžete zveřejňovat ve formě zdrojového kódu dle platných podmínek odstavce 4, za předpokladu, že zároveň splníte všechny následující podmínky:

- a) Dílo musí obsahovat zřetelnou zmínku o tom, že bylo upraveno, spolu s datem jeho úpravy.
- b) Dílo musí obsahovat zřetelnou zmínku o tom, že bylo vydáno pod touto Licencí a zmínku o jakýchkoli přidaných podmínkách v souladu s odstavcem 7. Tento požadavek upravuje požadavek na “ponechání všech zmínek beze změn” z odstavce 4.
- c) Celé dílo musíte licencovat touto Licencí pro každého, kdo si kopii opatří, anebo s ní jinak přijde do styku. Licence se, spolu s jakýmkoli dalšími podmínkami podle odstavce 7, proto vztahuje na dílo jako celek a na všechny jeho části, bez ohledu na to, jak je dílo a jeho části balené. Tato Licence nedává povolení k licencování děl jiným způsobem, ale pokud jste toto povolení získali jinak, tato Licence takové povolení neruší.
- d) Pokud dílo obsahuje interaktivní uživatelská rozhraní, každé z nich musí zobrazovat Příslušné právní podmínky. Pokud ale Program obsahuje interaktivní uživatelská rozhraní, která nezobrazují Příslušné právní podmínky, vaše dílo nemusí přinutit Program, aby je zobrazoval.

Kompilace chráněného díla s jinými vzájemně nezávislými díly, které ze své podstaty nejsou rozšířeními chráněného díla a které s ním nejsou kombinovány tak, aby tvořily jeden větší program na paměťovém médiu, či jiném distribučním médiu, se nazývá “agregát”, pokud kompilace a její výsledné autorská práva nejsou používány k omezování přístupu nebo zákonných

práv uživatelů kompilace nad míru, kterou samostatná díla povolují. Zahrnutím chráněného díla do agregátu tato Licence nenabývá platnosti na jiné části agregátu.

6. Zveřejňování nezděrokových verzí

Dílo můžete zveřejňovat prostřednictvím strojového kódu podle odstavců 4 a 5, uvedených výše, pokud zveřejníte i strojově čitelný Úplný zdroj dle ustanovení této Licence, jedním z následujících způsobů:

- a) Zveřejníte strojový kód ve fyzickém produktu (včetně fyzického distribučního média), doplněný Úplným zdrojem uloženým na trvalém fyzickém médiu běžně používaném pro výměnu softwaru.
- b) Zveřejníte strojový kód ve fyzickém produktu (včetně fyzického distribučního média), doplněný písemnou nabídkou platnou nejméně tři roky a tak dlouho, dokud pro ten daný model produktu nabízíte náhradní díly nebo zákaznickou podporu, abyste komukoliv, kdo si strojový kód opatří, poskytli buď (1) kopii Úplného zdroje pro veškerý software obsažený v produktu a chráněný touto Licencí na trvalém fyzickém médiu běžně používaném pro výměnu softwaru, za cenu nepřesahující náklady vzniklé na fyzické vyhotovení takové kopie, nebo (2) poskytlí bezplatný přístup k Úplnému zdroji na síťovém serveru.
- c) Zveřejníte jednotlivé kopie strojového kódu s kopií písemné nabídky zpřístupnit Úplný zdroj. Tato alternativa je povolena jen výjimečně, pro nekomerční účely a jen v případě, že jste i vy přijali strojový kód s takovou nabídkou, v souladu s odstavcem 6. b).
- d) Zveřejníte strojový kód nabídkou přístupu z určeného místa (zdarma nebo za poplatek) a nabídnete rovnocenný přístup k Úplnému zdroji stejným způsobem, ze stejného místa a bez dodatečných poplatků. Od příjemců musíte vyžadovat, aby Úplný zdroj zkopírovali spolu se strojovým kódem. Pokud je tím místem na zkopírování strojového kódu síťový server, Úplný zdroj může být na jiném serveru (provozovaný vámi nebo třetí stranou), který podporuje ekvivalentní prostředky pro kopírování a za podmínky, že vedle strojového kódu zajistíte jasné instrukce o tom, jak Úplný zdroj najít. Nezávisle na tom, jaký server hostuje Úplný zdroj, jste povinen zajistit, že bude přístupný tak dlouho, dokud bude třeba tyto požadavky naplňovat.
- e) Zveřejníte strojový kód pomocí peer-to-peer přenosu, za podmínky, že jiné počítače (peers) informujete, kde je ten strojový kód a Úplný zdroj díla zveřejněn zdarma, v souladu s odstavcem 6. d).

Oddělitelná část strojového kódu, jehož zdrojový kód nespadá do Úplného zdroje jako systémová knihovna, nemusí být součástí zveřejnění strojového kódu díla.

“Uživatelský produkt” je buď (1) “zákaznický produkt”, což znamená jakékoliv soukromé vlastnictví, které je běžně používáno pro soukromé, rodinné účely a účely pro domácnost, nebo (2) cokoliv vytvořené a prodávané pro zabudování do obytných prostor. Pro určení toho, zda je produkt zákaznickým, sporné případy mají být rozhodnuty ve prospěch toho, že jimi jsou. Pro daný produkt přijat daným uživatelem, “běžné používání” znamená typické použití daného druhu produktu, nezávisle na daném uživateli nebo na konkrétním uživateli způsobu použití, jeho očekávání, nebo očekávání, které se na uživatele kladou. Produkt je zákaznickým produktem nezávisle na tom, zda má produkt podstatné komerční, průmyslové, nebo ne-zákaznické využití, pokud taková využití představují jediný signifikantní způsob použití produktu.

“Instalační informace” pro uživatelský produkt jsou jakékoliv metody, procedury, autorizační klíče, nebo jiné informace potřebné k instalaci a spuštění upravených verzí chráněného díla v daném uživatelském produktu z upravené verze Úplného zdroje. Informace musí zajistit, že se v žádném případě nebude bránit nebo zasahovat nepřerušené funkcionality upraveného strojového kódu jen proto, že byly úpravy provedeny.

Pokud budete strojový kód zveřejňovat podle tohoto odstavce v, nebo se, nebo výhradně pro použití v zákaznickém produktu a zveřejnění bude součástí transakce, v níž se právo na držení a používání uživatelského produktu převádí na příjemce na neomezenou dobu nebo na dobu určitou (bez ohledu na to, jak je transakce charakterizována), Úplný zdroj zveřejněn na základě tohoto odstavce musí být doplněn o instalační informace. Tento požadavek však neplatí, pokud ani vy, ani žádná třetí strana si neponechává možnost instalovat upravený strojový kód pro uživatelský produkt (např. dílo bylo instalováno na ROM).

Požadavek poskytnutí instalačních informací nezahrnuje požadavek na pokračování v poskytování zákaznické podpory, záruky, nebo aktualizací pro dílo, které bylo upraveno nebo instalováno příjemcům, nebo pro uživatelský produkt, ve kterém byl upraven nebo instalován. Přístup k síti může být odmítnut, pokud by měla samotná úprava věcně a nepříznivě ovlivňovat chod sítě, nebo porušuje pravidla a protokoly pro komunikaci na síti.

Zveřejněný Úplný zdroj a uvedené instalační informace musí, v souladu s tímto odstavcem, být ve formátu, který je veřejně dokumentovaný (a s veřejně dostupnou implementací ve formě zdrojového kódu) a nemůže vyžadovat žádné speciální hesla nebo klíče pro rozbalení, čtení a kopírování.

7. Dodatečné podmínky

“Dodatečná práva” jsou podmínky, které doplňují podmínky této Licence výjimkami na jednu nebo více podmínek. Dodatečná práva, která se mohou vztahovat na celý Program, se považují za součást této Licence, ale jen dokud dodržují platné právní předpisy. Pokud se uplatní dodatečná práva pouze na část Programu, daná část se má používat zvlášť na základě těchto práv, ale na celý Program se vztahují podmínky této Licence bez dodatečných práv.

Pokud zveřejníte kopii chráněného díla, můžete z ní podle vlastní libosti odstranit kterékoli další práva, nebo jejich kteroukoliv část. (Dodatečné práva mohou být sestaveny tak, aby v některých případech úpravy díla požadovali samotné jejich odstranění.) Dodatečné práva můžete přidat na materiál, který byl ke chráněnému dílu přidán vámi, nebo pro které vlastníte, nebo můžete vydat, příslušná autorská práva.

Bez ohledu na jakákoli jiná ustanovení této Licence můžete pro materiál, který byl přidán ke chráněnému dílu (pokud vlastníte autorská práva k materiálu), rozšířit podmínky této Licence o podmínky:

- a) Popřít záruku či omezit odpovědnost jiným způsobem, než je uvedeno v odstavci 15 a 16 této Licence, nebo
- b) Požadovat uchování specifických odůvodněných zákonných vyhlášek nebo autorských příspěvků do materiálu, nebo do Příslušných právních podmínek zobrazovaných díly, které je obsahují, nebo
- c) Zakázat zavádění o původu materiálu, nebo požadovat, aby byly upravené verze tohoto materiálu označeny přiměřeným způsobem, tedy jako odlišné od originálu, nebo
- d) Omezit veřejné užívání jmen poskytovatelů licence nebo autorů materiálu, nebo
- e) Popřít přenos práv podle Zákona o ochranných známkách pro některé ochranné známky, značky a servisní známky, nebo
- f) Požadovat odškodnění poskytovatele licence a autorů materiálu od kohokoli, kdo zveřejní materiál (nebo jeho upravenou verzi) se smluvními závazky k příjemci, a za jakýkoli závazek, který smlouva přímo ukládá na poskytovatele licence a autorů.

Jiné zakazující dodatečné podmínky jsou ve smyslu odstavce 10 bráné jako “další omezení”. Pokud Program, nebo jeho část, tak jak jste jej obdrželi, obsahuje zmínku o tom, že je licencovaný touto Licencí spolu s podmínkou, která je dalším omezením, můžete tuto podmínku odebrat. Pokud licenční dokument obsahuje další omezení, ale povoluje znovu-licencování a zveřejnění pod touto Licencí, můžete ke chráněnému dílu přidat materiál podléhající podmínkám toho licenčního dokumentu, ale pouze za podmínky, že další omezení se takovýmto znovu-licencováním nebo zveřejněním zruší.

Pokud ke chráněnému dílu přidáte podmínky v souladu s tímto odstavcem, do příslušných zdrojových souborů musíte umístit prohlášení o dodatečných podmínkách vztahující se na dané soubory, nebo zmínku o tom, kde tyto platné podmínky najít.

Dodatečné podmínky, povolující nebo zakazující, mohou být podány formou zvláštní napsané licence, nebo podány jako výjimky (ale nezávisle na způsobu, platí vše, co je výše uvedeno).

8. Ukončení

Šířit nebo upravovat chráněné dílo můžete výslovně jen pod touto Licencí. Jakákoli snaha šířit nebo upravovat dílo jiným způsobem, je porušením těchto podmínek a znamená automatické ukončení vašich práv plynoucích z této Licence (včetně jakýchkoliv patentových licencí udělených podle odstavce 11.3)).

Pokud napravíte všechny porušení této Licence, pak je vaše licence z daného autorského práva obnovena (a) dočasně, pokud a dokud držitel autorských práv výslovně a s konečnou platností neukončí vaši licenci a (b) trvale, pokud se držitel autorských práv nepodaří vhodnými prostředky vás o porušení seznámit do 60 dnů po ukončení.

Navíc, vaše licence od daného držitele autorských práv se natrvalo obnovuje i v případě, že vás držitel autorských práv vhodnými prostředky informuje o porušení a toto je poprvé, co jste obeznameni o porušení této Licence (pro jakékoli dílo) od toho držitele autorských práv obdrželi a vy napravíte porušení do 30 dnů po doručení oznámení.

Ukončení vašich práv podle tohoto odstavce neukončuje licenci stran, které na základě této Licence obdržely kopie nebo práva od vás. Pokud byly vaše práva ukončeny a nebyly natrvalo obnoveny, nemáte právo přijmout nové licence pro daný materiál vyplývající z odstavce 10.

9. Přijetí Licence není povinné pro držení kopií

Pro přijímání nebo spouštění kopie Programu nejste povinen tuto Licenci přijmout. Pokud je to pouze výsledkem použití přenosu peer-to-peer, ani pomocné šíření chráněného díla nevyžaduje přijetí. Nic jiného než tato Licence vám ale nedává možnost kopírovat nebo šířit chráněné dílo. V případě, že tuto Licenci nepřijmete, tyto činnosti porušují autorská práva. Úpravou nebo šířením chráněného díla tedy vyjadřujete souhlas s Licencí a všem jejím ustanovením a podmínkám.

10. Automatické licencování následných příjemců

Po každé, když zveřejňujete chráněné dílo, získává příjemce od původního poskytovatele licence licenci pro spouštění, úpravu nebo šíření daného díla v souladu s ustanoveními této Licence. Nejste odpovědný za dodržování této Licence třetími stranami.

“Přenos entity” je přenos kontroly nad organizací, nebo v podstatě přenos všech jejích aktiv, nebo rozdělení organizace, nebo spojení organizací. Pokud šíření chráněného díla vyplývá z přenosu entity, každá strana transakce, která obdrží kopii díla, také obdrží všechny licence k dílu, které jeho předchůdce měl, nebo mohl dávat podle předchozího odstavce, plus obdrží právo na vlastní Úplný zdroj díla od předchůdce, pokud ho předchůdce vlastní nebo jej může pořídit opodstatněným úsilím.

Nesmíte klást žádné překážky výkonu zaručených práv příjemce vyplývajících z této Licence. Například, nesmíte požadovat žádné licenční poplatky nebo jiné poplatky za výkon práv udělených touto Licencí a nesmíte zahájit soudní spor (včetně příčných- a proti-pohledávek v soudním sporu) vycházející z toho, že tvorbou, používáním, prodejem, nabídnutím k prodeji, nebo dovážením Programu nebo jakékoli jeho části si nečiníte patentového nároku.

11. Patenty

“Příspěvatel” je držitel autorských práv, který touto Licencí autorizuje použití Programu nebo díla na Programu založeném. Takto licencované dílo se nazývá “verze příspěvatele”.

Příspěvatelovými “základními patentovými nároky” jsou všechny vlastněné patentové nároky nebo patentové nároky kontrolované příspěvatelem (již nabyté nebo později získané), které by tvorbou, používáním nebo prodáváním verze příspěvatele byly nějakým způsobem (povoleným touto Licencí) porušovány, ale nezahrnuje nároky, které by byly porušeny jen následkem dalších úprav verze příspěvatele. Pro potřeby této definice, “kontrolovat” znamená i právo udělit patentové sublicence způsobem konzistentním s požadavky této Licence.

Každý příspěvatel vám uděluje neexkluzivní, celosvětovou, bezplatnou patentovou licenci podle příspěvatelových základních patentových nároků k tvorbě, používání, předávání, poskytnutí k prodeji, dovážení a jinak, spouštění, úpravě a šíření obsahu verze příspěvatele.

V dalších třech odstavcích se “patentovou licencí” myslí jakýkoli výslovný souhlas nebo závazek nepožadovat patent (výslovné povolení užívání patentu nebo smlouva o nežalování za porušení patentu). “Udělit” takovou patentovou licenci nějaké straně znamená, buď takový výslovný souhlas dát, nebo závazek nevymáhat patent vůči dotyčné straně.

Pokud vědomě zveřejníte chráněné dílo, které podléhá patentové licenci a Úplný zdroj není zadarmo a podle podmínek této Licence není nikomu přístupný na kopírování přes veřejně přístupný síťový server, nebo jinak jednoduše zpřístupněný, pak musíte (1) takovým způsobem Úplný zdroj zpřístupnit, nebo (2) se sami o výhodu patentové licence pro toto konkrétní dílo připravit, nebo (3) zajistit, způsobem konzistentním s požadavky této Licence, aby se patentová licence přenášela na následně příjemce. “Vědomě” znamená, že máte skutečnou znalost o tom, že vaše zveřejnění chráněného díla v zemi nebo, že použití vašeho chráněného díla příjemcem, by porušilo jedno nebo více identifikovatelných patentů země, o kterých máte důvod se domnívat, že jsou platné.

Pokud budete zveřejňovat, nebo šířit chráněné dílo prostřednictvím pořízení jeho zveřejnění na základě jedné transakce nebo dohody a udělíte patentovou licenci jedné ze stran, které chráněné dílo přijímá a udělujete tak povolení k používání, šíření, uchování nebo zveřejnění konkrétního exempláře chráněného díla, pak patentová licence se automaticky rozšiřuje na všechny příjemce chráněného díla a na díla na něm založená.

Patentová licence je “diskriminační”, pokud do oblasti své působnosti zahrnuje zákazy výkonu, nebo je podmíněna zákazem výkonu jedné nebo více práv, která jsou touto Licencí udělena. Chráněné dílo nemůžete zveřejňovat, pokud jste uzavřeli s třetí stranou, která se zabývá obchodní distribucí softwaru, dohodu, podle níž platíte třetí straně na základě rozsahu vašeho úsilí ve zveřejňování díla a podle níž třetí strana uděluje jakékoli straně, která by přijala chráněné dílo od vás, diskriminační patentovou licenci (a) v souvislosti s kopiemi chráněného díla zveřejněného vámi (nebo kopiemi vyrobenými z těchto kopií),

nebo (b) především v souvislosti s konkrétním produktem nebo kompilací, která obsahuje chráněné dílo. To vše, pokud jste tuto dohodu uzavřeli, nebo byla patentová licence udělena před 28. březnem 2007.

Nic z této Licence by nemělo být vykládáno jako navádění k porušování nebo omezování patentů či jiných vlastnických práv, které by se na vás jinak vztahovali podle platného patentového práva.

12. Neexistuje výjimka na úkor svobody ostatních

Pokud jsou vám uloženy takové podmínky (ať již rozhodnutím soudu, smlouvou nebo jinak), které se vylučují s podmínkami této Licence, nejste tím osvobozeni od podmínek této Licence. Pokud nemůžete šířit chráněné dílo tak, abyste vyhověl zároveň svým závazkům vyplývajícím z této Licence a jiným platným závazkům, nesmíte jej v důsledku toho šířit vůbec. Pokud byste například souhlasili s podmínkami, které by vám neumožňovaly další bezplatné zveřejňování všem, komu Program zveřejňujete, pak by jediný možný způsob, jak vyhovět daným podmínkám a zároveň i této Licenci spočíval v ukončení distribuce Programu.

13. Použití s Obecnou veřejnou licencí GNU Affero

Bez ohledu na jakákoli jiná ustanovení této Licence, máte povolení k propojení či kombinování jakéhokoliv chráněného díla s dílem licencovaným podle 3. verze Obecné veřejné licence GNU Affero do jediného kombinovaného díla a výsledné dílo zveřejnit. Podmínky této Licence se budou nadále vztahovat na část, která je chráněným dílem, ale, pokud jde o interakci prostřednictvím sítě, na kombinované dílo jako takové budou platit zvláštní požadavky odstavce 13 Obecné veřejné licence GNU Affero.

14. Revidovaná verze této Licence

Free Software Foundation může čas od času vydávat upravené a/nebo nové verze Obecné veřejné licence GNU. Nové verze se budou svým duchem podobat současně verzi, ale v některých detailech se kvůli řešení nových problémů či zájmů mohou lišit.

Každé verzi je přiděleno jednoznačné číslo verze. Pokud Program určí číslo verze, vztahuje se na něj daná verze Obecné veřejné licence GNU nebo kterákoli "později vydaná verze", a můžete se podle uvážení řídit ustanoveními a podmínkami této konkrétní verze, nebo kterékoli pozdější verze vydanou Free Software Foundation. Jestliže program nespecifikuje číslo verze, můžete si vybrat libovolnou verzi, kterou Free Software Foundation vydala.

Pokud Program určí, že proxy-server může rozhodnout, která z budoucích verzí Obecné veřejné licence GNU může být použita, veřejné oznámení přijetí některé verze proxy-serverem vás trvale autorizuje vybrat si pro Program tu danou verzi.

Později vydané verze licence vám mohou zaručit dodatečné nebo pozměněné oprávnění. Avšak v důsledku vašeho výběru řídit se novější verzí se na žádného autora nebo držitele autorských práv neukládají žádné další závazky.

15. Zřeknutí se záruky

NA PROGRAM SE NEVZTAHUJE ŽÁDNÁ ZÁRUKA, V MÍŘE POVOLENÉ ZÁKONEM. POKUD NENÍ PÍSEMNĚ UVEDENO JINAK, DRŽITELÉ AUTORSKÝCH PRÁV POPŘÍPADĚ JINÉ STRANY POSKYTUJÍ PROGRAM "TAK JAK JE", BEZ ZÁRUKY JAKÉHOKOLI DRUHU, AŤ VÝSLOVNĚ NEBO VYPLÝVAJÍCÍ, VČETNĚ, ALE NIKOLI JEN, ZÁRUK OBCHODOVATELNOSTI A VHODNOSTI PRO URČITÝ ÚČEL. POKUD JDE O KVALITU A VÝKONNOST PROGRAMU, JE VEŠKERÉ RIZIKO NA VÁS. POKUD BY SE U PROGRAMU PROJEVILY ZÁVADY, NÁKLADY NA POTŘEBNOU ÚDRŽBU, OPRAVU ČI NÁPRAVU PADAJÍ NA VÁŠ VRUB.

16. Omezení odpovědnosti

V ŽÁDNÉM PŘÍPADĚ, S VÝJIMKOU TOHO, KDYŽ TO VYŽADUJE PLATNÝ ZÁKON, ANEBY KDYŽ TO BYLO PÍSEMNĚ ODSOUHLASENO, VÁM NEBUDE ŽÁDNÝ Z DRŽITELŮ AUTORSKÝCH PRÁV ANI ŽÁDNÁ JINÁ STRANA, KTERÁ SMÍ UPRAVOVAT NEBO ŠÍŘIT PROGRAM V SOULADU S PŘEDCHOZÍMI USTANOVENÍMI, ODPOVĚDNA ZA ŠKODY, VČETNĚ VŠECH OBECNÝCH, SPECIÁLNÍCH, NAHODILÝCH NEBO NÁSLEDNÝCH ŠKOD VYPLÝVAJÍCÍCH Z UŽÍVÁNÍ ANEBY NESCHOPNOSTI UŽÍVAT PROGRAMU (VČETNĚ, ALE NIKOLI JEN, ZTRÁTY NEBO ZKRESLENÍ DAT, NEBO TRVALÝCH ŠKOD ZPŮSOBENÝCH VÁM NEBO TŘETÍM STRANÁM, NEBO SELHÁNÍ FUNKCE PROGRAMU V SOUČINNOSTI S JINÝMI PROGRAMY), A TO I V PŘÍPADĚ, ŽE TAKOVÝ DRŽITEL AUTORSKÝCH PRÁV NEBO JINÁ STRANA BYLI UPOZORNĚNI NA MOŽNOST TAKOVÝCH ŠKOD.

17. Výklad odstavců 15 a 16

Pokud výše uvedené zřeknutí se záruk a omezení odpovědnosti nemohou být s ohledem na své podmínky místo-právně vykonatelné, příslušný soud by měl vycházet z místních zákonů, které se nejvíce přibližují zbavení veškeré občanskoprávní odpovědnosti v souvislosti s Programem, pokud není záruka nebo převzetí odpovědnosti doprovázena zpoplatněním kopií Programu.

Příloha č. 3 – Vzor formuláře požadavku na poskytnutí Podpory

Žadatel vyplní silně orámovanou část				Problém vyřešen:		ANO / NE			
Přijal:		Přijato (datum a čas):		Potvrzeno (datum a čas):		Evidenční číslo:			
Zákazník: Projekt:		Jméno žadatele:		Číslo smlouvy: Evidenční číslo žádanky:					
Místo:		Telefon:		Fax:		Datum a čas zjištění:			
				Mail:					
Je vada ANO/NE opakovatelná?		Prohlížeč: NN IE		Uživatel (role):		Označte X			
Popis požadavku:						Stav:		S	
						A		1	
						B		2	
						C		3	
						Běžný (D)		4	
								5	
						Věc:		V	
						Vada		1	
						Nový požadavek		2	
						Změna		3	
						Dotaz		4	
						Služba		5	
								6	
						Lokalizace:		L	
						HW		1	
						OS		2	
						Síť		3	
						ORACLE		4	
Aplikace		5							
		6							
Rozhraní		7							
		8							
Jméno řešitele:		Datum:		Přijal:				Odeslal:	
				dne:				dne:	
Informace o stavu vyřizování									
Přílohy řešitele:									

Příloha č. 4 – Kontaktní informace

Hot-line Dodavatele:

E-mail: [REDACTED]

Telefon: [REDACTED]

Kontaktní osoby Objednatele pověřené podáváním a přijímáním případů Podpory:

Jméno a příjmení	telefon	e-mail
[REDACTED]	[REDACTED] [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED]	[REDACTED]
[REDACTED]	[REDACTED] [REDACTED]	[REDACTED]

Příloha č. 5 – Akceptační protokol (vzor)

AKCEPTAČNÍ PROTOKOL O PŘEDÁNÍ A PŘEVZETÍ

níže specifikované části Plnění

Název:

Popis:

Splnění akceptačních kritérií

Kritérium	Splnění kritéria

Výsledek akceptace: AKCEPTOVÁNO BEZ VÝHRAD / AKCEPTOVÁNO S VÝHRADAMI / NEAKCEPTOVÁNO

Připomínky, výhrady, závady:

Předáno dne:

	Předal / Převzal	Role , funkce	Podpis
Za Dodavatele			
Za Objednatele			

Příloha č. 6 – Seznam poddodavatelů

Seznam poddodavatelů, které bude dodavatel pro plnění Smlouvy využívat:

Dodavatel v rámci předmětu plnění, poskytování podpory a rozvoje distribuce CentOS, přechodu na distribuci Alma Linux a podpory distribuce Alma Linux pro počítačové stanice na poštách, nebude mít poddodavatele.

Příloha č. 7 – Požadavky na bezpečnost ICT – Pravidla pro dodavatele

1 Úvodní ustanovení

Česká pošta (dále jen ČP) 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“). Dále pak je správcem či zpracovatelem osobních údajů dle Obecného nařízení o ochraně osobních údajů (dále jen „GDPR“) a zároveň je dle PCI DSS "merchant" (obchodník). ČP také provozuje systémy certifikování dle ISO 27001:2013 a ISO 27001:2022.

Z důvodu udržení jednotnosti kybernetické bezpečnosti jsou požadavky definované ve výše uvedených legislativách a normách přenášeny a v relevantní míře aplikovány na všechny systémy provozované v rámci ICT ČP. V rámci ČP je nutné zajistit celou ICT infrastrukturu a zabezpečit ji 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 ČP kladě důraz na efektivní implementaci opatření týkajících se kybernetické bezpečnosti a tato opatření jsou vyžadována také v rámci činnosti dodavatelů. Tímto ČP zajišťuje 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
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 komunikační technologie (ICT)	a 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, která jsou součástí Politiky ČP, a která jsou definována v dokumentu „Bezpečnostní požadavky na externí zaměstnance pro dodávky standardních systémů a technologií“.
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.), tedy Objednatel.
GDPR	General Data Protection Regulation je nařízení Evropské unie.
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
Politika ČP	Bezpečnostní politika ČP, jednotlivé dokumenty, které ji tvoří a část bezpečnostní dokumentace ČP, se kterými byl Dodavatel seznámen ze strany ČP pro účely plnění Smlouvy.
PCI DSS	Payment Card Industry Data Security Standard je soubor bezpečnostních standardů určených k ochraně údajů držitelů platebních karet.
Pravidla	Tato Pravidla pro dodavatele.
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 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, rovněž tak povinnost zachovávat důvěrnost dat, a to i po ukončení Smlouvy za podmínek dle Smlouvy.
- Dodavatel je povinen seznámit všechny své zaměstnance podílející se na plnění dle Smlouvy, 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), PCI DSS a GDPR. 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 dnů.
- 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 dnů 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 započatím 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.
- Volný pohyb pracovníků dodavatele v prostorách ČP je povolen pouze v případě, že dané osobě byla vystavena osobní přístupová karta. Pracovník dodavatele je povinen přístupovou kartu chránit, mít ji vždy při sobě na bezpečném místě, udržovat ji v místě odstíněném od potenciálního neoprávněného čtení (RFID ochrana) a není oprávněn přístupovou kartu dále zapůjčit jiným pracovníkům a/nebo třetím osobám a/nebo umožnit přístup jiných pracovníků a/nebo třetích osob do prostor 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 (jako jsou serverové místnosti, datové místnosti, technické místnosti, trezor, pokladna apod.) je povolen pouze v doprovodu oprávněného zaměstnance ČP. Doprovod je nezbytný po celou dobu fyzické přítomnosti pracovníků dodavatele v těchto prostorách a nepostačuje přístupová karta.
- V případě ztráty přístupové karty nebo v případě podezření ze ztráty přístupové karty je pracovník a/nebo dodavatel povinen bezodkladně zajistit blokaci přístupové karty.
- Před vrácením zapůjčených paměťových médií dodavateli musí být veškerá data ČP vymazána způsobem, který znemožňuje jejich opětovné obnovení; pokud toto nebylo provedeno ze strany ČP, je dodavatel povinen dané provést. O tomto je dodavatel povinen sepsat protokol a na výzvu ČP jej bezodkladně (nejdéle do 5 pracovních dnů) předložit.
- 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 na území Evropské unie nebo Evropského hospodářského prostoru či USA, pokud tomu nebrání jiná legislativa.
- 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 CIS Benchmark z 50% a nejméně zabezpečených v souladu s minimálním bezpečnostním standardem vydaný NÚKIB a NAKIT. Za důvěryhodné se považují prostředí a prostředky, které jsou určené pro použití v podnikovém prostředí a jsou odpovídající pro plnění dle Smlouvy.
- Dodavatel bere na vědomí, že ČP má vlastní infrastrukturu IT s licenčním portfoliem, které podléhá nebo může podléhat smluvním závazkům se třetí stranou k celopodnikovému pokrytí. Dodavatel v rámci řešení bude v případě dodávky sw licencí třetí strany respektovat platné celopodnikové smluvní závazky ČP s dodavateli licenčních produktů a podpory.

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 §19.
- 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. Pokud existuje mezi ČP a dodavatelem více Smluv na různá nebo stejná plnění, a nedohodnou-li se ČP s dodavatelem ve Smlouvě jinak, musí dodavatel řídit oprávnění podle každé Smlouvy zvlášť a pracovníci musí mít individuální účty pro plnění každé Smlouvy zvlášť.
- 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 svého prostředí, logovat události na svém prostředí a na rozhraní komunikace směrem k systémům ČP. Dále je povinen realizovat 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.
- Logování událostí sleduje a loguje minimálně:
 - datum a čas včetně specifikace časového pásma,
 - typ prováděné činnosti,
 - identifikaci technického aktiva, které činnost zaznamenalo,
 - jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,
 - jednoznačnou síťovou identifikaci zařízení původce,
 - úspěšnost nebo neúspěšnost činnosti,
 - přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů (nebudou-li autentizovány pomocí AM - jako např. servisní účty aplikace, správcovské účty aj.),
 - úspěšné i neúspěšné manipulace s účty, oprávněními a právy,
 - neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,
 - události vzešlé z činnosti uživatelů, které mohou mít vliv na bezpečnost digitalizace nebo vytěžování a manipulace s daty,
 - zahájení a ukončení činností technických aktiv,
 - kritická i chybová hlášení technických aktiv,
 - pokusy o přístup k záznamům monitorovacího SW o událostech a také pokusy o manipulaci se záznamy o událostech v něm a změny nastavení monitorovacích nástrojů pro zaznamenávání událostí,
 - synchronizaci jednotného času (pokud ji bude provádět sám a nespolehat přitom na OS či časový server ČP).
- Dodavatel nesmí využívat přístup k systémům ČP k jakýmkoli jiným aktivitám než k činnostem, které výslovně stanoví Smlouva.

8. Bezpečnost komunikací

- Dodavatel se zavazuje k zavedení bezpečnostních mechanismů k zajištění bezpečnosti sítě ve 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 rozhraní, které je monitorováno, není-li ve Smlouvě uvedeno jinak.

9. Bezpečnost vývoje

- Dodavatel je povinen se před započítím vývojových prací seznámit se softwarovými a hardwarovými technologiemi, které jsou v prostředí ČP podporované a používané. Dále je dodavatel povinen si nechat odsouhlasit uvažované zdroje (hardware, software atd.), design/architekturu navrhovaného řešení a z toho vyplívající případné další požadavky, to vše za podmínek dle Smlouvy.
- Před započítím vývojových prací je dodavatel povinen seznámit se s bezpečnostními a auditními požadavky ČP na vyvíjený software a odpovídající Politikou ČP.
- 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 ČP.
- Dodavatel je povinen zajistit, aby veškerý vývoj byl v souladu s požadavky a pravidly bezpečného vývoje, přičemž je nutné uplatňovat osvědčené postupy (best practices) a mezinárodně uznávané standardy. Minimálním požadavkem je dodržování zásad definovaných v rámci normy ISO 27001, zaměřené na řízení bezpečnosti informací, a pravidel uvedených v OWASP (Open Web Application Security Project), které poskytují konkrétní doporučení pro prevenci zranitelnosti softwaru. Dodavatel je dále povinen pravidelně provádět bezpečnostní analýzy a testování vyvíjeného softwaru, například penetrační testy, a zajistit, že budou identifikované zranitelnosti bezodkladně odstraněny.
- Dodavatel se zavazuje v rámci vývoje a testování používat pouze testovací data vytvořená/dodaná v souladu se Smlouvou; testování na ostrých datech je vyloučeno. Testovací data zároveň musí být anonymizovaná, leda je nezbytné využít neanonymizovaných dat a takový postup je dopředu s ČP dohodnut.
- Pokud není ve Smlouvě uvedeno jinak, součástí vývojových prací je i dodání úplné dokumentace dodaného software, včetně:
 - dokumentace architektury/designu – zahrnuje vztahy k prostředí a stavebním základům, které budou použity v návrhu softwarových komponent (pokud je tvořena analýza, pak analýzu po aktualizaci dle skutečného provedení);
 - technická dokumentace – dokumentace kódu, soupis použitých open source zdrojů, popis rozhraní a API;
 - bezpečnostní dokumentace – dokumentace chyb a zranitelností dle metodiky OWASP, výsledky penetračního testování,
 - uživatelská dokumentace – manuály pro koncového uživatele, systémové administrátory a osazenstvo podpory;
 - příručka pro administraci, instalaci a údržbu;
 - programátorskou dokumentaci (vývojové postupy, diagramy apod.).
- Dodavatel musí ČP 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.
- Dodavatel odpovídá za životní cyklus programového kódu a souvisejících aktiv v tom smyslu, že ČP bude včas podrobně informována o jejich stavu, využití, potřebnosti apod., vč. zranitelností a jakýchkoli bezpečnostních rizicích.

10. 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.

11. Řízení bezpečnostních incidentů

- Dodavatel je povinen vyhodnocovat bezpečnostní události svých aplikací a nástrojů a jeho 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 (na svém prostředí a/nebo plnění dle Smlouvy) a doporučit ČP kroky k přijetí takových opatření (na ostatním prostředí ČP).
- Dodavatel je povinen oznámit ČP a evidovat každý bezpečnostní 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 bezpečnostní 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 legislativy jako je zejména GDPR, ZKB, PCI DSS, ale i smluvních požadavků svých klientů.
- Dodavatel je povinen ohlásit jednotlivý bezpečnostní incident nebo událost současně všemi následujícími způsoby:
 - e-mailem na e-mailovou adresu uvedenou ve Smlouvě;
 - telefonicky na telefonní číslo uvedené ve Smlouvě; a
 - na Helpdesk ČP.

12. Kontinuita činnosti

- Dodavatel je povinen mít zaveden plán obnovy pro aplikace a systémy provozované dodavatelem a přímo ovlivňující plnění Smlouvy.
- Pro relevantní ICT aktiva dodavatele, která jsou používána pro anebo v souvislosti s plněním Smlouvy, je dodavatel povinen zajistit vhodný cyklus zálohy dat, který splňuje smluvně ujednané požadavky dle Smlouvy. Přitom musí dodavatel posoudit minimálně následující:
 - plán zálohy;
 - umístění záloh (zálohy musí být ukládány v jiné oblasti, než zálohována data);
 - metody zálohování, formáty dat a médií;
 - retenční období pro zálohování;
 - ověřování integrity záloh;
 - postupy obnovy a testování, včetně harmonogramů obnovy v případě narušení;
 - použití šifrování;

- oddělení záloh v cloudovém prostředí s více zákazníky;
- frekvence a metody revize procesů pro zálohování a obnovu;
- dokumentace záloh a jejich obsahu, včetně označování médií.
- Zálohovaná data musí být chráněna před neoprávněným přístupem. Tato data musí být chráněna dalšími bezpečnostními opatřeními, které vyžaduje jejich klasifikace (úroveň).

13. 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 proti neautorizovanému použití vhodnými prostředky jako je PIN, heslo, biometrika.
- 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.).
- Dodavatel je povinen vrátit užívané mobilní zařízení ČP (pokud mu bylo ze strany ČP předáno) 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.

14. 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 Smlouvy.

15. Požadavky na dodávku operačního systému AlmaLinux pro kritický systém Objednatele

- Operační systém musí být upraven tak, aby podporoval provoz interně vyvíjené aplikace APOST.
- Na operačním systému musí být implementována ochrana proti škodlivému kódu aktuálně prostřednictvím produktu ESET, řízeného centrální správou ve správě Objednatele.
- OS musí generovat bezpečnostní události v souladu s požadavky minimálně Zákona o kybernetické bezpečnosti (ZoKB) a prováděcí vyhlášky č. 82/2018 Sb., § 22 (Vyhláška o kybernetické bezpečnosti, VoKB).
- Bezpečnostní události musí být zasílány do SIEM systému Objednatele, konkrétně do platformy ELISA.
- V rámci OS zakázat všechny nepotřebné služby, porty, protokoly a aplikace.
- Operační systém musí splňovat požadavky na odolnost vůči útokům, a to implementací relevantních pravidel dle CIS Benchmark s dosažením alespoň 70 % shody.
- OS bude napojen na centrální systém řízení identit Objednatele (dále jen IDM).
- Přístup do OS bude řízen na základě rolí řízených IDM.
- Dodavatel je povinen zajistit pravidelné záplatování OS:
 - Aplikace záplat pro kritické zranitelnosti musí být implementovány nejpozději do 30 kalendářních dnů od jejich zveřejnění.
- Operační systém bude podrobován pravidelnému testování skeneru zranitelnosti Tenable , a to minimálně čtyřikrát ročně. Povinností dodavatele je:
 - Vyhodnocení výsledků těchto testů, včetně analýzy identifikovaných zranitelností.

- Odstranění všech zjištěných problémů v souladu s jejich závažností, přičemž kritické a vysoké zranitelnosti musí být odstraněny bez zbytečného odkladu, nejpozději však do 90 kalendářních dnů od jejich identifikace.
- OS bude podroben pravidelnému ročnímu penetračnímu testování formou Gray boxu testu , přičemž:
 - Penetrační testování bude rovněž součástí akceptačního procesu OS.
 - Dodavatel je povinen odstranit veškeré zjištěné nedostatky, případně předložit odůvodnění nemožnosti jejich odstranění spolu s návrhem dodatečných opatření k odstranění zjištěné zranitelnosti a výsledného rizika.
 - Dodavatel je povinen spolupracovat v přípravě testování, jeho realizaci a následném odstraňování zjištěných nedostatků. Tato spolupráce zahrnuje zejména:
 - Poskytnutí potřebné dokumentace, přístupů a součinnosti pro provedení testů.
 - Podporu při interpretaci výsledků testů a návrzích opatření.
 - Aktivní účast při implementaci navržených opatření a přijetí kroků pro minimalizaci rizik.

16. Změnové řízení

- Dodavatel je povinen vést podrobnou dokumentaci všech konfiguračních změn v informačním systému, infrastruktuře nebo softwaru.
- Dokumentace musí obsahovat:
 - Popis změny.
 - Důvod změny.
 - Očekávaný dopad na systém.
 - Datum provedení změny.
 - Osobu odpovědnou za provedení změny
 - Popis postupu pro návrat do předchozího stavu.
- Všechny změny podléhají předchozímu schválení Objednatelem prostřednictvím definovaného procesu změnového řízení.
- Dodavatel je povinen poskytnout Objednateli veškeré relevantní informace nezbytné k rozhodnutí o schválení změny.
- Dodavatel je povinen spolupracovat s Objednatelem na změnové řízení při jakékoliv plánované změně.
- Proces změnového řízení bude zahrnovat:
 - Identifikaci změny.
 - Analýzu dopadů na systém a služby.
 - Návrh opatření pro minimalizaci rizik.
 - Vyhodnocení nákladů a přínosů.
- Dodavatel je povinen aktivně spolupracovat s Objednatelem při plánování, analýze a implementaci změn.
- Dodavatel nese odpovědnost za správné provedení změn dle schváleného plánu změnového řízení.
- Veškeré změny musí být prováděny způsobem, který minimalizuje přerušení provozu.
- Dodavatel je povinen pravidelně aktualizovat dokumentaci na základě provedených změn.
- Aktualizovaná dokumentace musí být předána Objednateli v předem dohodnutém formátu a termínu.
- Veškeré kroky související s prováděním změn musí být plně auditovatelné.
- Dodavatel je povinen uchovávat záznamy o změnách po dobu stanovenou Smlouvou.
- Dodavatel musí Objednatele včas informovat o všech plánovaných změnách, jejich průběhu a případných odchylkách od plánu.
- V případě mimořádných událostí (např. havárií) musí být Objednatel neprodleně informován.
- V případě neplánovaných změn (např. reakce na kritický incident) musí být změna zpětně zdokumentována a projednána s Objednatelem.
- Dodavatel musí prokázat, že změna byla nezbytná a provedena v souladu s procesy minimalizace rizik.

- Dodavatel je povinen informovat personál Objednatele o důsledcích změn, pokud tyto změny ovlivňují provozní činnosti nebo užívání systému.

Příloha č. 8 – Požadavky na bezpečnost ICT – matice odpovědnosti

PCI DSS Requirement	Responsibility				
	Česká Pošta	Dodavatel	Sdílené	Pokrytí/Rozsah odpovědnosti	Požadavky na Dodavatele
Requirement 1: Install and Maintain Network Security Controls					
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.					
1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	X			Plně v odpovědnosti České Pošty	
1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	X			Plně v odpovědnosti České Pošty	
1.2 Network security controls (NSCs) are configured and maintained					
1.2.1 Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.	X			Plně v odpovědnosti České Pošty	

1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1. Note: Changes to network connections include the addition, removal, or modification of a connection. Changes to NSC configurations include those related to the component itself as well as those affecting how it performs its security function.	X			Plně v odpovědnosti České Pošty	
1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks. A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement.	X			Plně v odpovědnosti České Pošty	
1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment.	X			Plně v odpovědnosti České Pošty	
1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need.	X			Plně v odpovědnosti České Pošty	
1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	X			Plně v odpovědnosti České Pošty	

1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	X			Plně v odpovědnosti České Pošty	
1.2.8 Configuration files for NSCs are: - Secured from unauthorized access. - Kept consistent with active network configurations. Any file or setting used to configure or synchronize NSCs is considered to be a "configuration file." This includes files, automated and system-based controls, scripts, settings, infrastructure as code, or other parameters that are backed up, archived, or stored remotely.	X			Plně v odpovědnosti České Pošty	
1.3 Network access to and from the cardholder data environment is restricted.					
1.3.1 Inbound traffic to the CDE is restricted as follows: - To only traffic that is necessary. - All other traffic is specifically denied.	X			Plně v odpovědnosti České Pošty	
1.3.2 Outbound traffic from the CDE is restricted as follows: - To only traffic that is necessary. - All other traffic is specifically denied.	X			Plně v odpovědnosti České Pošty	
1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: - All wireless traffic from wireless networks into the CDE is denied by default. - Only wireless traffic with an authorized business purpose is allowed into the CDE.	X			Plně v odpovědnosti České Pošty	
1.4 Network connections between trusted and untrusted networks are controlled.					

1.4.1 NSCs are implemented between trusted and untrusted networks	X			Plně v odpovědnosti České Pošty	
1.4.2 Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied. The intent of this requirement is to address communication sessions between trusted and untrusted networks, rather than the specifics of protocols. This requirement does not limit the use of UDP or other connectionless network protocols if state is maintained by the NSC.	X			Plně v odpovědnosti České Pošty	
1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	X			Plně v odpovědnosti České Pošty	
1.4.4 System components that store cardholder data are not directly accessible from untrusted networks.	X			Plně v odpovědnosti České Pošty	
1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties.	X			Plně v odpovědnosti České Pošty	
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.					

1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	X			Plně v odpovědnosti České Pošty	
Requirement 2: Apply Secure Configurations to All System Components					
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood					
2.1.1 All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.			X	Pracovní stanice a lokální server APOST	Řídit se politikami a postupy České Pošty pro konfiguraci OS a Softwarových součástí lokálních APOST stanic a serverů.
2.1.2 Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.			X	Pracovní stanice a lokální server APOST	Definovat Role které budou interagovat s instalacemi.
2.2 System components are configured and managed securely.					

2.2.1 Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
2.2.2 Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
2.2.3 Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, OR • Primary functions with differing security levels that exist on the same system component are isolated from each other, OR • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.

2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
2.2.5 If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
2.2.6 System security parameters are configured to prevent misuse.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
2.2.7 All non-console administrative access is encrypted using strong cryptography.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
2.3 Wireless environments are configured and managed securely.					
2.3.1 For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-related wireless vendor defaults.	X				
2.3.2 For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary.	X				

• Whenever a key is suspected of or known to be compromised.					
Requirement 3: Protect Stored Account Data					
3.1 Processes and mechanisms for protecting stored account data are defined and understood.					
3.1.1 All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	X				
3.1.2 Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	X				
3.2 Storage of account data is kept to a minimum.					

3.2.1 Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	X				
3.3 Sensitive authentication data (SAD) is not stored after authorization.					
3.3.1 SAD is not stored after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	X				
3.3.1.1 The full contents of any track are not stored upon completion of the authorization process.	X				

3.3.1.2 The card verification code is not stored upon completion of the authorization process.	X				
3.3.1.3 The personal identification number (PIN) and the PIN block are not stored upon completion of the authorization process.	X				
3.3.2 SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	X				
3.3.3 Additional requirement for issuers and companies that support issuing services and store sensitive authentication data: Any storage of sensitive authentication data is: - Limited to that which is needed for a legitimate issuing business need and is secured. - Encrypted using strong cryptography. This bullet is a best practice until its effective date; refer to Applicability Notes below for details.	X				
3.4 Access to displays of full PAN and ability to copy cardholder data are restricted.					
3.4.1 PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	X				
3.4.2 When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.	X				
3.5 Primary account number (PAN) is secured wherever it is stored.					

3.5.1 PAN is rendered unreadable anywhere it is stored by using any of the following approaches: • One-way hashes based on strong cryptography of the entire PAN. • Truncation (hashing cannot be used to replace the truncated segment of PAN). – If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN. • Index tokens. • Strong cryptography with associated key-management processes and procedures.	X				
3.5.1.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.	X				
3.5.1.2 If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media OR • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.	X				

3.5.1.3 If disk-level or partition-level encryption is used (rather than file-, column-, or field-level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely	X				
3.6 Cryptographic keys used to protect stored account data are secured					
3.6.1 Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms.	X				

3.6.1.1 Additional requirement for service providers only: A documented description of the cryptographic architecture is maintained that includes: • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. • Preventing the use of the same cryptographic keys in production and test environments. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Description of the key usage for each key. • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.	X				
3.6.1.2 Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device. • As at least two full-length key components or key shares, in accordance with an industry-accepted method.	X				
3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	X				

3.6.1.4 Cryptographic keys are stored in the fewest possible locations.	X				
3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.					
3.7.1 Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	X				
3.7.2 Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	X				
3.7.3 Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	X				
3.7.4 Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: • A defined cryptoperiod for each key type in use. • A process for key changes at the end of the defined cryptoperiod.	X				

3.7.5 Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations	X				
3.7.6 Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control.	X				
3.7.7 Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.	X				
3.7.8 Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	X				
3.7.9 Additional requirement for service providers only: Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and	X				

updating of such keys is documented and distributed to the service providers' customers.					
Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks					
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.					
4.1.1 All security policies and operational procedures that are identified in Requirement 4 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	X				
4.1.2 Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.	X				
4.2 PAN is protected with strong cryptography during transmission					

4.2.1 Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. This bullet is a best practice until its effective date; refer to applicability notes below for details. • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.	X				
4.2.1.1 An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.	X				
4.2.1.2 Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	X				
4.2.2 PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.	X				
Requirement 5: Protect All Systems and Networks from Malicious Software					
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.					

5.1.1 All security policies and operational procedures that are identified in Requirement 5 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.			X	Pracovní stanice a lokální server APOST - Antivirová ochrana	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
5.1.2 Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.			X	Pracovní stanice a lokální server APOST - Antivirová ochrana	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
5.2 Malicious software (malware) is prevented, or detected and addressed.					
5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.			X	Pracovní stanice a lokální server APOST - Antivirová ochrana	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.			X	Pracovní stanice a lokální server APOST - Antivirová ochrana	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
5.2.3 Any system components that are not at risk for malware are evaluated periodically to include the following: • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection.			X	Pracovní stanice a lokální server APOST - Antivirová ochrana	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
5.2.3.1 The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk			X	Pracovní stanice a lokální server APOST - Antivirová ochrana	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.

analysis, which is performed according to all elements specified in Requirement 12.3.1.					
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.					
5.3.1 The anti-malware solution(s) is kept current via automatic updates			X	Pracovní stanice a lokální server APOST - Antivirová ochrana	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
5.3.2 The anti-malware solution(s): • Performs periodic scans and active or real-time scans. OR • Performs continuous behavioral analysis of systems or processes.			X	Pracovní stanice a lokální server APOST - Antivirová ochrana	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.			X	Pracovní stanice a lokální server APOST - Antivirová ochrana	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
5.3.3 For removable electronic media, the antimalware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, OR • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.			X	Pracovní stanice a lokální server APOST - Antivirová ochrana	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
5.3.4 Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.			X	Pracovní stanice a lokální server APOST - Antivirová ochrana	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.

5.3.5 Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.			X	Pracovní stanice a lokální server APOST - Antivirová ochrana	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
5.4 Anti-phishing mechanisms protect users against phishing attacks.					
5.4.1 Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks	X				
Requirement 6: Develop and Maintain Secure Systems and Software					
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.					
6.1.1 All security policies and operational procedures that are identified in Requirement 6 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	X				
6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	X				
6.2 Bespoke and custom software are developed securely.					

6.2.1 Bespoke and custom software are developed securely, as follows: • Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle.	X				
6.2.2 Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: • On software security relevant to their job function and development languages. • Including secure software design and secure coding techniques. • Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.	X				
6.2.3 Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code reviews ensure code is developed according to secure coding guidelines. • Code reviews look for both existing and emerging software vulnerabilities. • Appropriate corrections are implemented prior to release.	X				

6.2.3.1 If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:					
- Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices. - Reviewed and approved by management prior to release.	X				

6.2.4 Software engineering techniques or methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: • Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. • Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. • Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. • Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). • Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. • Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.	X				
6.3 Security vulnerabilities are identified and addressed.					

6.3.1 Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.			X	Pracovní stanice a lokální server APOST - Řízení zranitelností	Česká pošta definuje standardy pro řízení zranitelností na OS, případně dalším software, dodavatel se jimi řídí při instalaci aktualizací.
6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	X			Pracovní stanice a lokální server APOST - Řízení zranitelností	
6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Patches/updates for critical vulnerabilities (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity's assessment of the criticality of the risk to the environment as identified according to the risk ranking process at Requirement 6.3.1.			X	Pracovní stanice a lokální server APOST - Řízení zranitelností	Dodavatel připravuje aktualizací balíček na základě požadavku České Pošty. Balíček instaluje Česká Pošta. Dodavatel aktualizuje instalační image.

6.4 Public-facing web applications are protected against attacks.					
6.4.1 For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections OR • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.	X				

6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.	X				
6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written business or technical justification as to why each is necessary	X				
6.5 Changes to all system components are managed securely.					

6.5.1 Changes to all system components in the production environment are made according to established procedures that include: - Reason for, and description of, the change. - Documentation of security impact. - Documented change approval by authorized parties. - Testing to verify that the change does not adversely impact system security. - For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. - Procedures to address failures and return to a secure state			X	Pracovní stanice a lokální server APOST - Změnové řízení	Česká Pošta vytváří změnové požadavky včetně důvodu a popisu změny. Dodavatel je odpovědný za provedení základních bezpečnostních testů, posouzení zdali mají dopad na bezpečnost a dokumentaci tohoto dopadu. Dodavatel nesmí nasadit změnu do produkce bez autorizovaného a dokumentovaného schválení Českou Poštou. Dodavatel také musí popsat postup pro "rollback" změny v případě problémů.
6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	X				
6.5.3 Pre-production environments are separated from production environments and the separation is enforced with access controls.	X				
6.5.4 Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.	X				
6.5.5 Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.	X				

6.5.6 Test data and test accounts are removed from system components before the system goes into production.	X				
Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know					
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.					
7.1.1 All security policies and operational procedures that are identified in Requirement 7 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	X				
7.1.2 Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.	X				
7.2 Access to system components and data is appropriately defined and assigned.					
7.2.1 An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.	X				

7.2.2 Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.	X				
7.2.3 Required privileges are approved by authorized personnel.	X				
7.2.4 All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	X				
7.2.5 All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use	X				
7.2.5.1 All access by application and system accounts and related access privileges are reviewed as follows: • Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). • The application/system access remains appropriate for the function being performed. • Any inappropriate access is addressed.	X				

• Management acknowledges that access remains appropriate					
7.2.6 All user access to query repositories of stored cardholder data is restricted as follows: • Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. • Only the responsible administrator(s) can directly access or query repositories of stored CHD.	X				
7.3 Access to system components and data is managed via an access control system(s).					
7.3.1 An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.	X				
7.3.2 The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.	X				
7.3.3 The access control system(s) is set to "deny all" by default.	X				
Requirement 8: Identify Users and Authenticate Access to System Components					
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.					

8.1.1 All security policies and operational procedures that are identified in Requirement 8 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	X				
8.1.2 Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.	X				
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.					
8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed.	X				
8.2.2 Group, shared, or generic ID, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • ID use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.	X				
8.2.3 Additional requirement for service providers only: Service providers with remote access to customer premises use unique	N/A				

authentication factors for each customer premises					
8.2.4 Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval. • Implemented with only the privileges specified on the documented approval.	X				
8.2.5 Access for terminated users is immediately revoked.	X				
8.2.6 Inactive user accounts are removed or disabled within 90 days of inactivity.	X				
8.2.7 Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: • Enabled only during the time period needed and disabled when not in use. • Use is monitored for unexpected activity.	X				
8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	X				
8.3 Strong authentication for users and administrators is established and managed.					
8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card.	X				

• Something you are, such as a biometric element.					
8.3.2 Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	X				
8.3.3 User identity is verified before modifying any authentication factor.	X				
8.3.4 Invalid authentication attempts are limited by: • Locking out the user ID after not more than 10 attempts. • Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.	X				
8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use.	X				
8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).	X				

• Contain both numeric and alphabetic characters.					
8.3.7 Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	X				
8.3.8 Authentication policies and procedures are documented and communicated to all users including: • Guidance on selecting strong authentication factors. • Guidance for how users should protect their authentication factors. • Instructions not to reuse previously used passwords/passphrases. • Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	X				
8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	X				

8.3.10 Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single factor authentication implementation), then guidance is provided to customer users including: • Guidance for customers to change their user passwords/passphrases periodically. • Guidance as to when, and under what circumstances, passwords/passphrases are to be changed.	N/A				
8.3.10.1 Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly	N/A				
8.3.11 Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access.	X				
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE					

8.4.1 MFA is implemented for all non-console access into the CDE for personnel with administrative access.	X				
8.4.2 MFA is implemented for all non-console access into the CDE.	X				
8.4.3 MFA is implemented for all remote access originating from outside the entity's network that could access or impact the CDE.	X				
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.					
8.5.1 MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks. • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. • At least two different types of authentication factors are used. • Success of all authentication factors is required before access is granted.	X				
8.6 Use of application and system accounts and associated authentication factors is strictly managed.					

8.6.1 If accounts used by systems or applications can be used for interactive login, they are managed as follows: • Interactive use is prevented unless needed for an exceptional circumstance. • Interactive use is limited to the time needed for the exceptional circumstance. • Business justification for interactive use is documented. • Interactive use is explicitly approved by management. • Individual user identity is confirmed before access to account is granted. • Every action taken is attributable to an individual user.	X				
8.6.2 Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.	X				
8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.	X				

Requirement 9: Restrict Physical Access to Cardholder Data					
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.					
9.1.1 All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	X				
9.1.2 Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	X				
9.2 Physical access controls manage entry into facilities and systems containing cardholder data.					
9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	X				
9.2.1.1 Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: • Entry and exit points to/from sensitive areas within the CDE are monitored. • Monitoring devices or mechanisms are protected from tampering or disabling. • Collected data is reviewed and correlated with other entries. • Collected data is stored for at least three months, unless otherwise restricted by law	X				

9.2.2 Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	X				
9.2.3 Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	X				
9.2.4 Access to consoles in sensitive areas is restricted via locking when not in use.	X				
9.3 Physical access for personnel and visitors is authorized and managed.					
9.3.1 Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: - Identifying personnel. - Managing changes to an individual's physical access requirements. - Revoking or terminating personnel identification. - Limiting access to the identification process or system to authorized personnel.	X				
9.3.1.1 Physical access to sensitive areas within the CDE for personnel is controlled as follows: - Access is authorized and based on individual job function. - Access is revoked immediately upon termination. - All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.	X				

9.3.2 Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering. • Visitors are escorted at all times. • Visitors are clearly identified and given a badge or other identification that expires. • Visitor badges or other identification visibly distinguishes visitors from personnel.	X				
9.3.3 Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.	X				
9.3.4 Visitor logs are used to maintain a physical record of visitor activity both within the facility and within sensitive areas, including: • The visitor's name and the organization represented. • The date and time of the visit. • The name of the personnel authorizing physical access. • Retaining the log for at least three months, unless otherwise restricted by law.	X				
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.					
9.4.1 All media with cardholder data is physically secured.	X				
9.4.1.1 Offline media backups with cardholder data are stored in a secure location.	X				
9.4.1.2 The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.	X				
9.4.2 All media with cardholder data is classified in accordance with the sensitivity of the data.	X				

9.4.3 Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged. • Media is sent by secured courier or other delivery method that can be accurately tracked. • Offsite tracking logs include details about media location.	X				
9.4.4 Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	X				
9.4.5 Inventory logs of all electronic media with cardholder data are maintained.	X				
9.4.5.1 Inventories of electronic media with cardholder data are conducted at least once every 12 months.	X				
9.4.6 Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction.	X				
9.4.7 Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed. • The cardholder data is rendered unrecoverable so that it cannot be reconstructed.	X				
9.5 Point of interaction (POI) devices are protected from tampering and unauthorized substitution.					

9.5.1 POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: • Maintaining a list of POI devices. • Periodically inspecting POI devices to look for tampering or unauthorized substitution. • Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	X				
9.5.1.1 An up-to-date list of POI devices is maintained, including: • Make and model of the device. • Location of device. • Device serial number or other methods of unique identification.	X				
9.5.1.2 POI device surfaces are periodically inspected to detect tampering and unauthorized substitution	X				
9.5.1.2.1 The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	X				

9.5.1.3 Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. • Procedures to ensure devices are not installed, replaced, or returned without verification. • Being aware of suspicious behavior around devices. • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	X				
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data					
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.					
10.1.1 All security policies and operational procedures that are identified in Requirement 10 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy pro konfiguraci logování, dodavatel se jimi řídí při nastavování.
10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	X				
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.					

10.2.1 Audit logs are enabled and active for all system components and cardholder data.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy pro konfiguraci logování, dodavatel se jimi řídí při nastavování.
10.2.1.1 Audit logs capture all individual user access to cardholder data.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy pro konfiguraci logování, dodavatel se jimi řídí při nastavování.
10.2.1.2 Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy pro konfiguraci logování, dodavatel se jimi řídí při nastavování.
10.2.1.3 Audit logs capture all access to audit logs.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy pro konfiguraci logování, dodavatel se jimi řídí při nastavování.
10.2.1.4 Audit logs capture all invalid logical access attempts.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy pro konfiguraci logování, dodavatel se jimi řídí při nastavování.
10.2.1.5 Audit logs capture all changes to identification and authentication credentials including, but not limited to: • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy pro konfiguraci logování, dodavatel se jimi řídí při nastavování.
10.2.1.6 Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy pro konfiguraci logování, dodavatel se jimi řídí při nastavování.
10.2.1.7 Audit logs capture all creation and deletion of system-level objects.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy pro konfiguraci logování,

					dodavatel se jimi řídí při nastavování.
10.2.2 Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy pro konfiguraci logování, dodavatel se jimi řídí při nastavování.
10.3 Audit logs are protected from destruction and unauthorized modifications.					
10.3.1 Read access to audit logs files is limited to those with a job-related need.	X				
10.3.2 Audit log files are protected to prevent modifications by individuals.	X				
10.3.3 Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	X				
10.3.4 File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy pro konfiguraci logování, dodavatel se jimi řídí při nastavování.
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.					

10.4.1 The following audit logs are reviewed at least once daily: • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).	X				
10.4.1.1 Automated mechanisms are used to perform audit log reviews.	X				
10.4.2 Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.	X				
10.4.2.1 The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1	X				
10.4.3 Exceptions and anomalies identified during the review process are addressed.	X				
10.5 Audit log history is retained and available for analysis.					
10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	X				
10.6 Time-synchronization mechanisms support consistent time settings across all systems.					

10.6.1 System clocks and time are synchronized using time-synchronization technology.	X			Pracovní stanice a lokální server APOST	Česká pošta definuje standardy pro konfiguraci synchronizace času, dodavatel se jimi řídí při nastavování.
10.6.2 Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use. • Only the designated central time server(s) receives time from external sources. • Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). • The designated time server(s) accept time updates only from specific industry-accepted external sources. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time. • Internal systems receive time information only from designated central time server(s).			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy pro konfiguraci synchronizace času, dodavatel se jimi řídí při nastavování.
10.6.3 Time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business need. • Any changes to time settings on critical systems are logged, monitored, and reviewed.	X				
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.					

10.7.1 Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).	N/A				
10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls • IDS/IPS • Change-detection mechanisms • Anti-malware solutions • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) • Audit log review mechanisms • Automated security testing tools (if used)	X				

10.7.3 Failures of any critical security controls systems are responded to promptly, including but not limited to: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls	X				
Requirement 11: Test Security of Systems and Networks Regularly					
11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.					
11.1.1 All security policies and operational procedures that are identified in Requirement 11 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.			X	Pracovní stanice a lokální server APOST - Bezpečnostní testování	Česká pošta definuje standardy a postupy pro bezpečnostní testování (zranitelnosti, penetrační testy), dodavatel poskytuje součinnost, předání informací, odstranění nálezů.
11.1.2 Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	X				
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.					

11.2.1 Authorized and unauthorized wireless access points are managed as follows: • The presence of wireless (Wi-Fi) access points is tested for, • All authorized and unauthorized wireless access points are detected and identified, • Testing, detection, and identification occurs at least once every three months. • If automated monitoring is used, personnel are notified via generated alerts.	X				
11.2.2 An inventory of authorized wireless access points is maintained, including a documented business justification.	X				
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.					
11.3.1 Internal vulnerability scans are performed as follows: • At least once every three months. • Vulnerabilities that are either high-risk or critical (according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high-risk and all critical vulnerabilities (as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists.			X	Pracovní stanice a lokální server APOST - Bezpečnostní testování	Česká pošta definuje standardy a postupy pro bezpečnostní testování (zranitelnosti, penetrační testy), dodavatel poskytuje součinnost, předání informací, odstranění nálezů.

11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk vulnerabilities or critical vulnerabilities according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows: • Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. • Rescans are conducted as needed.			X	Pracovní Pracovní stanice a lokální lokální server APOST - Bezpečnostní testování	Česká pošta definuje standardy a postupy pro bezpečnostní testování (zranitelnosti, penetrační testy), dodavatel poskytuje součinnost, předání informací, odstranění odstranění nálezů.
11.3.1.2 Internal vulnerability scans are performed via authenticated scanning as follows: • Systems that are unable to accept credentials for authenticated scanning are documented. • Sufficient privileges are used for those systems that accept credentials for scanning. • If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.			X	Pracovní Pracovní stanice a lokální lokální server APOST - Bezpečnostní testování	Česká pošta definuje standardy a postupy pro bezpečnostní testování (zranitelnosti, penetrační testy), dodavatel poskytuje součinnost, předání informací, odstranění odstranění nálezů.
11.3.1.3 Internal vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are either high-risk or critical (according to the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).			X	Pracovní Pracovní stanice a lokální lokální server APOST - Bezpečnostní testování	Česká pošta definuje standardy a postupy pro bezpečnostní testování (zranitelnosti, penetrační testy), dodavatel poskytuje součinnost, předání informací, odstranění odstranění nálezů.

11.3.2 External vulnerability scans are performed as follows: • At least once every three months. • By a PCI SSC Approved Scanning Vendor(ASV). • Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.	N/A				
11.3.2.1 External vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	N/A				
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.					

11.4.1 A penetration testing methodology is defined, documented, and implemented by the entity, and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope-reduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. • Retention of penetration testing results and remediation activities results for at least 12 months.				X Pracovní stanice a lokální server APOST - Bezpečnostní testování	Česká pošta definuje standardy a postupy pro bezpečnostní testování (zranitelnosti, penetrační testy), dodavatel poskytuje součinnost, předání informací, odstranění nálezů.
---	--	--	--	--	---

11.4.2 Internal penetration testing is performed: • Per the entity's defined methodology, • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third-party • Organizational independence of the tester exists (not required to be a QSA or ASV).			X	Pracovní stanice a lokální server APOST - Bezpečnostní testování	Česká pošta definuje standardy a postupy pro bezpečnostní testování (zranitelnosti, penetrační testy), dodavatel poskytuje součinnost, předání informací, odstranění nálezů.
11.4.3 External penetration testing is performed: • Per the entity's defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester exists (not required to be a QSA or ASV).	N/A				
11.4.4 Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections.			X	Pracovní stanice a lokální server APOST - Bezpečnostní testování	Česká pošta definuje standardy a postupy pro bezpečnostní testování (zranitelnosti, penetrační testy), dodavatel poskytuje součinnost, předání informací, odstranění nálezů.

11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	X				
--	---	--	--	--	--

11.4.6 Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every six months and after any changes to segmentation controls/methods. • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	N/A				
11.4.7 Additional requirement for multi-tenant service providers only: Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4.	N/A				
11.5 Network intrusions and unexpected file changes are detected and responded to.					

11.5.1 Intrusion-detection and/or intrusion prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date	X				
11.5.1.1 Additional requirement for service providers only: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	N/A				
11.5.2 A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.			X	Pracovní stanice a lokální server APOST	Česká pošta definuje standardy, dodavatel se jimi řídí při nastavování.
11.6 Unauthorized changes on payment pages are detected and responded to.					

11.6.1 A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the security impacting HTTP headers and the script contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP headers and payment pages. • The mechanism functions are performed as follows: – At least weekly OR – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	X				
Requirement 12: Support Information Security with Organizational Policies and Programs					
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.					
12.1.1 An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.			X	Politika informační bezpečnosti	Dodavatel musí mít dokumentovanou a implementovanou alespoň základní politiku pro řízení informační bezpečnosti (třeba ISO27001).
12.1.2 The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment.			X	Politika informační bezpečnosti	Dodavatel musí mít dokumentovanou a implementovanou alespoň základní politiku pro řízení

					informační bezpečnosti (třeba ISO27001).
12.1.3 The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.			X	Politika informační bezpečnosti	Dodavatel musí mít dokumentovanou a implementovanou alespoň základní politiku pro řízení informační bezpečnosti (třeba ISO27001).
12.1.4 Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management			X	Politika informační bezpečnosti	Dodavatel musí mít dokumentovanou a implementovanou alespoň základní politiku pro řízení informační bezpečnosti (třeba ISO27001).
12.2 Acceptable use policies for end-user technologies are defined and implemented.					
12.2.1 Acceptable use policies for end-user technologies are documented and implemented, including: • Explicit approval by authorized parties. • Acceptable uses of the technology. • List of products approved by the company for employee use, including hardware and software			X	Politika informační bezpečnosti	Dodavatel musí mít dokumentovanou a implementovanou alespoň základní politiku pro řízení informační bezpečnosti (třeba ISO27001).
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.					

12.3.1 For each PCI DSS requirement that specifies completion of a targeted risk analysis, the analysis is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how the frequency or processes defined by the entity to meet the requirement minimize the likelihood and/or impact of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review	X				
12.3.2 A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: • Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). • Approval of documented evidence by senior management. • Performance of the targeted analysis of risk at least once every 12 months.	X				

12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • Documentation of a plan, to respond to anticipated changes in cryptographic vulnerabilities.	X				
12.3.4 Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive security fixes from vendors promptly. • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.	X				
12.4 PCI DSS compliance is managed.					

12.4.1 Additional requirement for service providers only: Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance. • Defining a charter for a PCI DSS compliance program and communication to executive management.	N/A				
12.4.2 Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: • Daily log reviews. • Configuration reviews for network security controls. • Applying configuration standards to new systems. • Responding to security alerts. • Change-management processes.	N/A				

12.4.2.1 Additional requirement for service providers only: Reviews conducted in accordance with Requirement 12.4.2 are documented to include: • Results of the reviews. • Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2. • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.	N/A				
12.5 PCI DSS scope is documented and validated.					
12.5.1 An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.	X				

12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). • Updating all data-flow diagrams per Requirement 1.2.4. • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. • Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. • Identifying all connections from third-party entities with access to the CDE. • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.	X				
--	---	--	--	--	--

12.5.2.1 Additional requirement for service providers only: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2.	N/A				
12.5.3 Additional requirement for service providers only: Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management.	N/A				
12.6 Security awareness education is an ongoing activity.					
12.6.1 A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	X				
12.6.2 The security awareness program is: - Reviewed at least once every 12 months, and - Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data.	X				
12.6.3 Personnel receive security awareness training as follows: - Upon hire and at least once every 12 months. - Multiple methods of communication are used. - Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	X				

12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: • Phishing and related attacks. • Social engineering.	X				
12.6.3.2 Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.	X				
12.7 Personnel are screened to reduce risks from insider threats.					
12.7.1 Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.	X				
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.					
12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	X				

12.8.2 Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that TPSPs are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that the TPSP could impact the security of the entity's cardholder data and/or sensitive authentication data.	X				
12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement	X				
12.8.4 A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	X				
12.8.5 Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity	X				
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.					
12.9.1 Additional requirement for service providers only: TPSPs provide written agreements to customers that include acknowledgments that TPSPs are responsible for the security of account data the TPSP possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that the TPSP could impact the security of the customer's cardholder data and/or sensitive authentication data.		X			Dodavatel je povinen smluvně akceptovat odpovědnost za bezpečnost dodávaných služeb které mohou ohrozit bezpečnost systémů objednatele.

12.9.2 Additional requirement for service providers only: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: • PCI DSS compliance status information (Requirement 12.8.4). • Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5), for any service the TPSP provides that meets a PCI DSS requirement(s) on behalf of customers or that can impact security of customers' cardholder data or sensitive authentication data		X			Dodavatel musí poskytnout součinnost v případě potřeby při bezpečnostních auditech poskytnutím relevantních informací předmětu plnění.
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately					
12.10.1 An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system			X	Pracovní stanice a lokální server APOST	Dodavatel je povinen hlásit všechny u něho vzniklé bezpečnostní incidenty které zahrnují všechny systémy podílející se na plnění nebo zahrnují citlivé informace České Pošty vzniklé v rámci smluvního plnění.

components. • Reference or inclusion of incident response procedures from the payment brands.					
12.10.2 At least once every 12 months, the security incident response plan is: • Reviewed and the content is updated as needed. • Tested, including all elements listed in Requirement 12.10.1.	X				
12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.	X				
12.10.4 Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.	X				
12.10.4.1 The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in	X				

Requirement 12.3.1.					
12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. This bullet is a best practice until its effective date; refer to Applicability Notes below for details. • Detection of unauthorized wireless access points.	X				
12.10.6 The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	X				

12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected.	X				
A1 Additional PCI DSS Requirements for Multi-Tenant Service Providers					
A1.1 Multi-tenant service providers protect and separate all customer environments and data.	N/A				
A1.1.1 Logical separation is implemented as follows: • The provider cannot access its customers' environments without authorization. • Customers cannot access the provider's environment without authorization.	N/A				
A1.1.2 Controls are implemented such that each customer only has permission to access its own cardholder data and CDE.	N/A				
A1.1.3 Controls are implemented such that each customer can only access resources allocated to them.	N/A				

A1.1.4 The effectiveness of logical separation controls used to separate customer environments is confirmed at least once every six months via penetration testing.	N/A				
A1.2 Multi-tenant service providers facilitate logging and incident response for all customers.	N/A				
A1.2.1 Audit log capability is enabled for each customer's environment that is consistent with PCI DSS Requirement 10, including: • Logs are enabled for common third-party applications. • Logs are active by default. • Logs are available for review only by the owning customer. • Log locations are clearly communicated to the owning customer. • Log data and availability is consistent with PCI DSS Requirement 10.	N/A				
A1.2.2 Processes or mechanisms are implemented to support and/or facilitate prompt forensic investigations in the event of a suspected or confirmed security incident for any customer.	N/A				
A1.2.3 Processes or mechanisms are implemented for reporting and addressing suspected or confirmed security incidents and vulnerabilities, including: • Customers can securely report security incidents and vulnerabilities to the provider. • The provider addresses and remediates suspected or confirmed security incidents and vulnerabilities according to Requirement 6.3.1.	N/A				