Dílčí smlouva č. 2024/10790 o poskytnutí služeb

k Rámcové dohodě o poskytování služeb č. 2022/05974 ze dne 11.8.2022

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]

dále jen „**Objednatel**“ nebo „**ČP**“

a

Ernst & Young, s.r.o.

se sídlem:	Na Florenci 2116/15, Nové Město, 110 00 Praha 1
IČO:	26705338
DIČ:	CZ26705338
zastoupena:	[redacted]
zapsána v obchodním rejstříku u:	Městského soudu v Praze, oddíl C, vložka 108716
bankovní spojení:	[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., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**“), tuto Dílčí smlouvu o poskytnutí služeb (dále jen „**Smlouva**“) k **Rámcové dohodě o poskytování služeb** ze dne 11.8.2022 (dále jen „**Rámcová dohoda**“).

Preambule

Objednatel provedl v souladu s Rámcovou dohodou soutěž o dílčí veřejnou zakázku „Audit ISDS 2023+ na produkčním prostředí“ (dále jen „**minitendr**“). Tato Smlouva je uzavřena s Dodavatelem na základě výsledku minitendru.

1. Předmět Smlouvy a podmínky plnění

1.1. Předmětem této Smlouvy je závazek Dodavatele poskytnout Objednateli řádně a včas služby zahrnující činnosti ve smyslu ust. odst. 1.2 písm. a) Rámcové dohody, konkrétně provedení bezpečnostního auditu na produkčním prostředí Objednatele.

(dále jen „**Plnění**“).

Bližší specifikace a požadavky na Plnění, které je Dodavatel Objednateli povinen poskytnout, je obsažena v příloze č. 1 této Smlouvy.

2. Cena

2.1. Maximální cena Plnění činí **1 312 500,- Kč** (slovy: jeden milion tři sta dvanáct tisíc pět set korun českých) bez DPH. Rozklad ceny je uveden v příloze č. 1 Smlouvy.

2.2. Cena zahrnuje veškeré náklady Dodavatele spojené s plněním Dílčí smlouvy a poskytnutím plnění Objednateli. Tato cena je cenou konečnou, nejvýše přípustnou a nemůže být zvýšena bez předchozího písemného souhlasu Objednatele.

3. Práva a povinnosti Smluvních stran

3.1. Seznam osob, jejichž prostřednictvím bude Dodavatel zajišťovat plnění této Smlouvy, je uveden v Příloze č. 2 Smlouvy (dále jen „**realizační tým**“). Bude-li z důvodů vzniklých na straně Dodavatele nutné nahradit kteréhokoliv člena realizačního týmu, bude po předchozím odsouhlasení Objednatelem nahrazen novým členem týmu s odpovídající nebo vyšší kvalifikací, a to do 2 týdnů od oznámení důvodů pro nahrazení Objednateli.

4. Doba a místo plnění

4.1. Dodavatel se zavazuje poskytnout Plnění do 90 dnů ode dne nabytí účinnosti Smlouvy. Poskytování Plnění dle této Smlouvy bude zahájeno bez zbytečného odkladu po nabytí její účinnosti.

4.2. Místem poskytování Plnění je pracoviště Objednatele – Olšanská 38/9, 225 99 Praha 3.

5. Bezpečnost ICT

5.1. Objednatel zastává pozici povinné osoby ve smyslu zák. č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „ZKB“) a je provozovatelem kritické informační infrastruktury (dále jen „KII“), který je předmětem auditu ISDS2023+. Dodavatel bere na vědomí, že plnění Dodavatele dle Smlouvy se považuje za plnění významného dodavatele v souladu s § 2 písm. n) Vyhlášky 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 (dále jen „VKB“), a že jej Objednatel eviduje jako významného

dodavatele v souladu s § 8 odst. 1 písm. b) VKB. Dodavatel prohlašuje, že byl seznámen s pravidly pro Dodavatele v rozsahu a míře k předmětu plnění a bude dodržovat podmínky pro významné dodavatele, které jsou Přílohou č. 3 Smlouvy.

6. Závěrečná ustanovení

6.1. Tato Smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem uveřejnění Smlouvy v registru smluv. Případné plnění předmětu této Smlouvy v době od okamžiku platnosti Smlouvy do okamžiku nabytí její účinnosti se považuje za plnění podle této Smlouvy a práva a povinnosti z něj vzniklé se řídí touto Smlouvou.

6.2. Smluvní strany jsou oprávněny od Smlouvy odstoupit ze stejných důvodů a za stejných podmínek, jaké platí pro odstoupení od Rámcové dohody.

6.3. V otázkách touto Smlouvou neupravených se použijí ustanovení Rámcové dohody.

6.4. Kontaktní osoby Smluvních stran pro účely plnění této jsou následující:

Kontaktní osoba Objednatele: [redacted]

Kontaktní osoba Dodavatele: [redacted]

6.5. Tato Smlouva je vyhotovena v elektronické podobě, přičemž každá Smluvní strana obdrží její elektronický originál opatřený platnými elektronickými podpisy.

6.6. Nedílnou součástí Smlouvy jsou následující přílohy:

Příloha č. 1 – Specifikace Plnění a Cena

Příloha č. 2 – Složení realizačního týmu Dodavatele

6.7. Smluvní strany prohlašují, že tato Smlouva vyjadřuje jejich úplné a výlučné vzájemné ujednání týkající se daného předmětu této Smlouvy. Smluvní strany po přečtení této Smlouvy prohlašují, že byla uzavřena po vzájemném projednání, určitě a srozumitelně, na základě jejich pravé, vážně míněné a svobodné vůle. Na důkaz uvedených skutečností připojují podpisy svých oprávněných osob či zástupců.

V Praze	V Praze
Ing. Martin Götz ředitel úseku ICT a eGovernment **Česká pošta, s. p.**	[redacted] **Ernst & Young, s.r.o.**

Příloha č. 1 – Specifikace Plnění a Cena

Audit ISDS 2023+ na produkčním prostředí

1. Předmět auditu

Předmětem auditu je Provedení auditu ISDS2023+ na produkčním prostředí.

2. Účel auditu

Účelem auditu proto je poskytnout objednateli auditu objektivní a nestranné podklady o vadách ISDS 2023+.

3. Cíle auditu

Objektivně zjistit stav zabezpečení ISDS 2023+ na produkčním prostředí. Testováním, kontrolami a dalšími prověrkami provedenými v produkčním prostředí získat objektivní a ověřitelné podklady pro identifikaci a ocenění rizik, kterým bude vystaven provozovatel ISDS 2023+. Ověřit shodu respektive soulad technických bezpečnostních opatření implementovaných v produkčním prostředí ISDS 2023 + s požadavky zákona a vyhlášky o kybernetické bezpečnosti.

4. Rozsah auditu

V rámci auditu budou provedeny následující kontroly, prověrky a testy:

1. Externí penetrační testy perimetru ISDS 2023+ na produkčním prostředí.
2. Interní penetrační testy z vnitřních zón ISDS 2023+ na produkčním prostředí.
3. Kontroly nastavení bezpečnostních mechanizmů ISDS 2023+ na produkčním prostředí.
4. Kontroly nastavení přístupových oprávnění tzv. silných uživatelů ISDS 2023+ na produkčním prostředí.
5. Kontroly nastavení způsobů a postupů administrace ISDS 2023+ na produkčním prostředí.

5. Popis prostředí ISDS 2023+

V této kapitole je popsán pouze rozsah, nevysvětluje jednotlivé funkce a jejich chování.

5.1 Přístupová brána

Přístupová brána (AGW) je jednou z bezpečnostně kritických komponent ISDS. AGW je nasazena ve všech prostředích. Kromě jiného poskytuje TLS šifrování a zabezpečuje HTTPS komunikaci uživatelů

s ISDS. Zde je implementován webový aplikační firewall ModSecurity. Sestává ze tří hlavních modulů:

- AGW AS (autentizační server)
- AGW ARP (reverzní proxy)
- AGW MC (cache)

5.2 Klientský portál

Základní komponenta ISDS s kompletní funkcionalitou. Publikován je v několika subdoménách, hlavní je 'www.mojedatovaschranka.cz'. Dalšími jsou 'reg.', '.cert' pro přístup certifikátem. Přistupuje do něj největší počet uživatelů.

5.3 Informační portál

Jedná se o komponentu, která není autentizována. Obsahuje informační obsah jako články, videa, soubory atd., které jsou veřejně dávány k dispozici. Publikován je v subdoméně 'info.mojedatovaschranka.cz'.

5.4 Servisní modul

Jedná se o webovou aplikaci pro správce ISDS, která je bezpečnostně kritikou komponentou ISDS. Přístupná je z internetu.

5.5 Redakční systém

Jde o webovou aplikaci. Navazuje na Servisní modul, pomocí kterého je editorům zřizován účet a jsou jim přidělována oprávnění. RS slouží pro editaci obsahu Informačního portálu. Přístupný je z internetu.

5.7 Hostované spisové služby

Hostované spisové služby jsou dvojího druhu. Existují hostované spisové služby (HSS) jako aplikace, které se mohou certifikátem přihlašovat („jako stroj“, bez konkrétního účtu) do cizích schránek (schránek svých klientů) a tam za ně konat (číst nebo odesílat zprávy). Vedle toho existují Hostované spisové služby pro uživatele (HSSU), alias Přístupové rozhraní dle §14b zákona 300/2088 Sb. To jsou externí internetové aplikace (aktuálně dvě - Portál občana a Portál dopravy), které mají vlastní uživatelské osobní účty a tyto jejich externí účty lze spárovat s účty v ISDS a umožnit pak, aby externí aplikace přistupovala do schránky přes tento spárovaný externí účet.

5.8 Autentizační služba

Jde o součást přístupové brány AGW. Autentizační služba (ExtISO) slouží převážně pro autentizaci uživatelů (předání vybraných atributů schránek a uživatelů) do externích aplikací, resp. ve speciálním případě jako prostředek ke komfortnímu předání autentizačního tokenu.

5.9 Odesílací brána

Odesílací brána je součástí přístupové brány AGW, umožňující schválení či zamítnutí konceptu (návrhu) datové zprávy a její fyzické odeslání tak, že ISDS přijme požadavek od externí aplikace a po úspěšné autentizaci uživatele zprávu odešle přímo z jeho schránky.

5.10 Notifikační brána

Notifikační brána ISDS (aplikace na APP serveru) zajišťuje odesílání SMS a e-mailových notifikací událostí.

5.11 Systémové schránky

Systémové schránky správce a provozovatele jsou speciální schránky zřízené nad rámec zákona 300/2008 Sb. Lze z nich pouze odesílat. Zprávy z nich odeslané se nazývají systémové zprávy a nepočítají se do statistik provozu.

Systémová schránka správce (s ID = aaaaaaa, interní název ROOT) vznikla při inicializaci systému, pod ní jsou vedeni interní uživatelé ISDS. Z této schránky odcházejí systémové provozní zprávy.

Systémová schránka provozovateleje speciální schránka s pevným ID = zzzzzzq a názvem Systémová schránka provozovatele ISDS. Schránka je založena zevnitř ISDS a rovnou aktivována (nastaven stav = 1). Nečeká se tedy s aktivací na první přihlášení.

Ze schránky se posílají tyto typy zpráv:

- notifikační systémové zprávy (pro komerční události)
- uvítací zprávy (pro nové schránky)
- výběrové systémové zprávy (výjimečně – zpráva zasílaná provozovatelem do vybraných, případně do všech schránek).

5.12 Statistický modul

Datová základna pro statistiky datových zpráv je tvořená zejména databázovým schématem BILL, umístěným na produkčním SQL serveru. V menší míře se jako zdroj pro statistiky využívá databáze eDirectory (např. registrované metody přihlašování či notifikací), resp. databáze Sentinelu (skutečné

způsoby přihlášení apod.). Veškerá data ve schématu BILL jsou neměnná (tzn. jsou zde uložena pouze ta data, která se v čase nemění). Výjimku ze statistických tabulek, uložených ve schématu BILL, tvoří tabulky DM_AGGREG, které jsou umístěné ve schématech ISDS na zprávových SQL serverech.

5.13 Katalog webových služeb

Z pohledu pracnosti auditu se jedná o 122 aktivně používaných.

Webové služby ISDS se rozdělují na dvě skupiny - veřejné a neveřejné.

- veřejné: znamená, že jsou publikovány a popsány ve veřejné dokumentaci
- neveřejné: znamená jsou uvedeny pouze v neveřejných dokumentech pro specifické adresáty, často jej pro jednoho. Všechny služby jsou chráněny systémem oprávnění.

5.14 Napojení na ISZR

Informační systém základních registrů je klíčovým zdrojem dat pro ISDS.

Komunikace s ISZR prostřednictvím webových služeb z rozhraní ISZR je obousměrná.

5.15 Napojení na Identitu občana

Identita občana (NIA – národní bod pro identifikaci - https://www.identitaobcana.cz) je IS veřejné správy, sloužící jako nástroj pro bezpečné a zaručené ověření totožnosti uživatele online služeb

5.16 Verifier

Verifier je důležitým bezpečnostním mechanismem. K zákonu č. 300/2008 Sb. existuje provozní vyhláška, která definuje povolené formáty příloh datové zprávy. V době, kdy vzniká tento podklad pro audit, jsou povoleny zde uvedené formáty příloh datových zpráv.

5.17 Antivirová ochrana

V souladu se zákonem 300/2008 Sb. musí být v ISDS prováděna vstupní kontrola příloh datových zpráv. Antivirová kontrola je prováděna pomocí produktu Symantec Protection Engine.

5.18 Logování a bezpečný log

HCAP neboli Hitachi Content Archive Platform je řešení úložiště pro dlouhodobou archivaci dat s neměnným obsahem pod pevně definovanými zásadami průkaznosti takto archivovaných dat (bezpečný log). V rámci ISDS neboli Informačního Systému Datových Schránek je nutné zálohovat data tak, aby byla zachována soudní a transakční průkaznost a nepopiratelnost informací.

5.19 Bezpečnostní dohled

Řešen ze strany dodavatele

5.20 Řízení technických zranitelností

Výstupy ze skenů zranitelností pomocí Virtuální appliance Greenbone

5.21 Provozní dohled

Zejména Zabbix

5.22 Zodolněná infrastruktura

V oblasti auditu technologické a aplikační infrastruktury bude zapotřebí pro ucelený audit počítat s rozsahem:

a) zodolnění operačních systémů na vybraných RHEL a Windows serverech z množiny:

- AGW servery (ASS, ARP, MC)
- APP servery
- EDR servery
- FAS servery (Win)
- APE servery
- OTP servery
- NGW servery (Win)
- Sentinel servery
- AV servery
- Zabbix servery

b) kontrola infrastruktury úložišť

- produkční disková pole (NetApp MetroCluster)
- archivní pole (HCAP)
- SAN switche
- zálohovací pole (nezávislá)

c) kontrola síťových prvků:

- síťové switche
- loadbalancer
- firewally (vč. IPS)
- VPN

d) konfigurace komponent softwarové infrastruktury

- přístupová brána (AGW ARP, AS, MC)
- adresářový systém (eDirectory, LDAPGate)
- virtualizační prostředí (VMware vSphere s vCenter Server)
- databázové stroje (Oracle19c v RAC)
- antivirus (Symantec Protection Engine)
- provozní dohled (Zabbix, MariaDB)
- bezpečnostní dohled (Sentinel)

- zálohování (Backup Manager)
- vyhledávání Search server

e) administrátorské prostředky

- samoobslužný PWM (součást eDirectory)
- SSH
- Task Status
- dedikované pracovní stanice (nebo VM) administrátora

5.23 Fyzická bezpečnost

HC (Chodov, Jihozápadní město, Malešice)

Lze připravit návštěvu auditora a provést kontrolu na místě. Je nutné respektovat obecné podmínky pro pohyb a chování se v těchto prostorách (např. není dovoleno fotografování aj.).

5.24 Doménová infrastruktura, CMS a TSA

ISDS kriticky závisí na těchto externích komponentách/konfiguracích:

- farma časových razítek (CA PostSignum)
- správa doménových záznamů (MV, NAKIT)
- správa CMS konfigurací (MV, NAKIT).

6. Předávaná dokumentace

Výstupem z auditu KB budou následující dokumenty, jejichž finální verze bude odsouhlasena ČP:

- Plán auditu
- Závěrečná zpráva
- Zpráva, kterou může ČP využít pro poskytnutí informací dle zákona 106/1999 Sb, o svobodném přístupu k informacím ve verzi, která může být poskytnuta veřejnosti, tj. v redukovaném rozsahu. Zpráva bude obsahovat vyznačení informací a odůvodnění k těm částem, které nelze vydat/zveřejnit, resp. které auditor nedoporučuje zveřejňovat.

Cena

Sazba (cena) za 1 člověkoden (MD)[1] v Kč bez DPH	7 500,00
Počet člověkodní za vypracování plánu auditu, včetně jeho provedení	140
Počet člověkodní za vypracování závěrečné zprávy	34
Počet člověkodní za vypracování zprávy dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím	1
Maximální celková cena za Plnění v Kč bez DPH	1 312 500,00

[1] Jedním člověkodnem (MD) se rozumí 8 hodin výkonu práce jednoho pracovníka Dodavatele pro Objednatele.

Příloha č. 2: Složení realizačního týmu Dodavatele

Realizační tým Dodavatele bude složen z následujících členů:

jméno a příjmení	role (pozice) v realizačním týmu
[redacted]	Auditor
[redacted]	Konzultant
[redacted]	Manažer zakázky

Příloha č. 3: Pravidla pro dodavatele

1. Pravidla pro zabezpečení informací

1.1. Základní ustanovení

• Veškeré informace, které jsou v rámci smluvního vztahu Dodavateli poskytovány ze strany Objednatele nebo vzniknou během plnění smluvních činností, jsou informačním aktivem Objednatele (dále jen informace Objednatele), které je třeba chránit z pohledu bezpečnosti informací.

• Dodavatel se řídí obecně závaznými právními předpisy.

• Dodavatel musí informovat Objednatele o významných změnách týkajících se ovládání dodavatele podle zákona o obchodních korporacích, o změnách týkajících se vlastnictví či práva nakládání se zásadními aktivy Dodavatele, zejména pokud mohou mít dopad na plnění smluvních závazků vůči Objednateli.

1.2. Řízení rizika, změnové řízení.

• Dodavatel musí mít nastaven proces řízení rizik.

• Dodavatel je povinen informovat Objednatele o jakémkoli vzniklém riziku či hrozícím riziku, které by mohlo mít dopad na bezpečnost informací Objednatele. Dodavatel je dále povinen přijmout vhodná opatření k odstraňování takových rizik a informovat Objednatele o přijatých opatřeních a stavu jejich realizace.

1.3. Kontrola a audit Dodavatele

• Objednatel je oprávněn provést u Dodavatele a jeho případných poddodavatelů kontrolu plnění povinností týkajících se bezpečnosti informací. Dodavatel je povinen Objednateli takovou kontrolu umožnit do 10 dnů od nahlášení. Kontrola může zahrnovat přezkoumávání dokumentace, implementaci bezpečnostních opatření a kontrolu prostor, v kterých jsou prováděny činnosti, které mohou mít vliv na bezpečnost informací Objednatele. Dodavatel je povinen poskytnout součinnost pro provedení kontroly, zahrnující umožnění vstupu do požadovaných prostor (včetně prostor poddodavatelů), přístupu k příslušným dokumentům. Kontrola může být provedena zaměstnanci Objednatele nebo prostřednictvím další strany pověřené Objednatelem.

• Dodavatel je povinen udržovat aktuální dokumentaci všech opatření přijatých pro zajištění bezpečnosti informací Objednatele a poskytnout tuto dokumentaci osobám pověřeným Objednatelem v rámci kontroly plnění povinností Dodavatele.

1.4. Systém řízení bezpečnosti informací

• Dodavatel musí nakládat s informacemi Objednatele dle jejich klasifikace. Klasifikaci primárně určuje Objednatel. V případě, že data nejsou označena, má se za to, že se jedná o interní informace

Objednatele. Žádné informace, vyjma veřejných, není možné předávat třetím stranám bez vědomí a souhlasu Objednatele.

- Dodavatel musí zajistit, aby přístup k informacím Objednatele měly pouze osoby, které tyto informace potřebují pro výkon smluvních činností (dle zásad need to know – „potřeba vědět“) a že informace budou použity pouze pro účely plnění Smlouvy.

- Dodavatel jmenuje zodpovědnou kontaktní osobu pro potřeby zajištění plnění bezpečnostních požadavků vyplývajících ze Smlouvy a této Přílohy a pro potřeby související komunikace mezi Smluvními stranami ohledně tohoto tématu (dále také jen „Kontaktní osoba“). Kontaktní osoba na straně dodavatele je:

[redacted]

- V případě, že Dodavatel pro plnění smluvních závazků vůči Objednateli využívá služeb třetí strany (poddodavatele), musí zajistit, aby se tito zavázali plnit všechny relevantní bezpečnostní požadavky ve stejném rozsahu jako jsou smluvně stanoveny mezi Dodavatelem a Objednatelem.

- Dodavatel musí zajistit, aby zaměstnancům, či zaměstnancům třetích stran, kteří mohou mít přístup k informacím Objednatele, byl tento umožněn s ohledem na rizika spojená s důvěrností informací (klasifikačním stupněm), byli náležitě proškoleni a poučeni a aby mezi nimi a Dodavatelem byla uzavřena dohoda o mlčenlivosti.

1.5. Řízení přístupu

- Systémy a prvky systémů musí být nakonfigurovány takovým způsobem, aby umožňovaly přístup pouze autorizovaným uživatelům.

- • Dodavatel musí zajistit používání dostatečně silných hesel, jejichž tvorba a užití bude v souladu s VKB. a Hesla (včetně dalších autentizačních prostředků, jako jsou prvky vícefaktorové autentizace) budou dostatečně chráněna před zneužitím.

- Pro autentizaci musí být používány unikátní účty pro každého uživatele, které nesmí být sdíleny.

- Jestliže jakékoliv oprávnění k přístupu do systémů a k informacím Objednatele již není platné (například při změně pracovní pozice nebo při ukončení práce zaměstnance, případně zaměstnance třetí strany), je Dodavatel povinen bezodkladně o této skutečnosti informovat Objednatele a zajistit zrušení přístupových oprávnění.

- Dodavatel musí zajistit logování všech úspěšných i neúspěšných přístupů k systémům a informacím Objednatele. Do logů musí být zaznamenány informace umožňující jednoznačnou informaci toho, kdo přistoupil nebo se pokusil přistoupit k těmto informacím. Záznamy musí být vyhodnocovány za účelem odhalení případného neoprávněného přístupu a musí být ukládány minimálně po dobu vyžadovanou VKB.

1.6. Bezpečnost informací a jejich předávání.

- Dodavatel musí zajistit, že informace DIA, jako jsou dokumenty a data nebudou předávány prostřednictvím nezabezpečených kanálů a ukládány na nezabezpečených úložištích. Informace nesmí být zejména: o ukládány na veřejných úložištích,
    - ukládány na soukromých zařízeních uživatelů (například princip BYOD),
    - ukládány na firemních zařízeních uživatelů, která nejsou zabezpečena šifrováním,
    - posílány prostřednictvím veřejné sítě bez zabezpečení (například bez pomoci VPN, TLS apod.),
    - posílány na emailové adresy uživatelů, které nejsou spravovány Dodavatelem anebo smluvní třetí stranou (např. freemailové služby, soukromý email zaměstnance apod.).

1.7. Fyzická bezpečnost a bezpečnost prostředí

- Dodavatel musí zajistit, aby do prostor, ve kterých jsou zpracovávány informace Objednatele, měly přístup pouze osoby, které jsou autorizovány k přístupu k těmto informacím.

- Prostředí, v kterém jsou umístěny informační systémy Objednatele, musí mít implementována opatření proti následkům vnějších vlivů, jako jsou například havárie, přírodní katastrofy nebo úmyslné poškození či zneužití.

1.8. Bezpečnost zařízení

- Dodavatel musí zajistit, aby na všech zařízeních byl používán pouze jím schválený legální software a přijmout opatření zamezující instalaci neschváleného softwaru uživateli.

- Dodavatel musí zajistit, aby na všech zařízeních, na kterých jsou zpracovávány informace Objednatele, probíhalo pravidelné přezkoumání zranitelností a včasná instalace oprav a bezpečnostních zásad.

- Na všech počítačích Dodavatele musí být provozována softwarová ochrana před škodlivým kódem, která je pravidelně aktualizována. Tato musí být nastavena tak, aby nemohla být vypnuta uživatelem.

1.9. Řízení bezpečnostních incidentů

- Dodavatel je povinen stanovit a dodržovat procesy pro řízení bezpečnostních událostí a incidentů a jmenovat role zodpovědné za tyto procesy.
- Dodavatel musí Objednateli bezodkladně po jejich detekci oznámit bezpečnostní události a incidenty, i ve stádiu podezření, prostřednictvím sjednaných ohlašovacích kanálů.
- Při řešení bezpečnostního incidentu je dodavatel povinen:
  - poskytnout veškerou potřebnou součinnost týmům Objednatele;
  - použít otestovaný postup zahrnující požadavky na zajištění důkazů;
  - navrhnout, implementovat a dokumentovat opatření, která zajistí minimalizaci dopadu incidentu na aktiva Objednatele;
  - provést analýzu příčin a navrhnout a implementovat opatření s cílem zamezit opakování incidentu.

1.10. Zálohování dat a jejich likvidace

- Dodavatel musí zajistit, aby na zálohované informace Objednatele byla aplikována minimálně stejná bezpečnostní opatření jako na data v provozním prostředí.
- V případě, že Dodavatel již nepotřebuje informace Objednatele k plnění smluvních závazků, anebo informace Objednatele nejsou součástí jejich plnění, je Dodavatel povinen zajistit bezpečnou likvidaci informací.