# Příloha č. 5 Smlouvy – Požadavky na kybernetickou bezpečnost

*Tato příloha obsahuje Organizací používané standardní ujednání o bezpečnosti informací. Vzhledem k předmětu smlouvy, který úzce souvisí s bezpečností informací, resp. kybernetickou bezpečností, ujednání této přílohy se použijí pouze v rozsahu, v jakém jsou relevantní vzhledem k předmětu smlouvy.*

## 1. DEFINICE

Dále uvedené pojmy a zkratky mají v Příloze následující jednotný význam:

(a) **„Organizace“** – objednatel kupující apod., který je definován ve Smlouvě

(b) „**KBU**“ je kybernetická bezpečnostní událost, tedy událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.

(c) „**KBI**“ je kybernetický bezpečnostní incident, tedy narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.

(d) „**Příloha**“ je tento dokument nadepsaný „Bezpečnost informací“.

(e) „**Smlouva**“ je smlouva, ke které je přiložena Příloha.

(f) „**VKB**“ je Vyhláška č. 409/2025 Sb. a Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností), ve znění pozdějších předpisů, anebo jakoukoli jinou vyhlášku tuto vyhlášku nahrazující anebo doplňující.

(g) „**ZKB**“ je Zákon č. 264/2025 Sb., o kybernetické bezpečnosti, anebo jakýkoliv jiný zákon tento zákon nahrazující anebo doplňující.

(h) **„NÚKIB“** je Národní úřad pro kybernetickou a informační bezpečnost.

## 2. ÚČEL

2.1 V Příloze jsou stanoveny způsoby a úrovně realizace bezpečnostních opatření pro Dodavatele a určen vzájemný vztah odpovědnosti za zavedení a kontrolu bezpečnostních opatření mezi Organizací a Dodavatelem v souladu se ZKB a VKB.

2.2 Veškeré činnosti podle Přílohy jsou kontrolovány v rámci pravidelného auditu, pokud není stanoveno jinak.

## 3. ZÁKLADNÍ POVINNOSTI V OBLASTI BEZPEČNOSTI INFORMACÍ

3.1 Dodavatel musí dodržovat požadavky řízení bezpečnosti informací uvedené ve Smlouvě a Příloze a současně příslušná ustanovení interních dokumentů Organizace, zejména bezpečnostních politik,

metodik a postupů, resp. platné řídící dokumentace Organizace vycházející ze ZKB a VKB a běžných bezpečnostních standardů. V případě, že z interních dokumentů Organizace vzejde Dodavateli povinnost, která není výslovně stanovena ve Smlouvě, Příloze, právních předpisech nebo z nich jednoznačně odvoditelná, bude taková situace řešena prostřednictvím odpovídajících ustanovení o změnách obsažených ve Smlouvě, nebo, pokud taková ustanovení Smlouva neobsahuje, na základě dohody Stran.

3.2 Dodavatel musí provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění bezpečnosti informací (zajištění důvěrnosti, integrity a dostupnosti) v rámci aktiv souvisejících s plněním Smlouvy a vést o způsobu zabezpečení bezpečnostní dokumentaci.

3.3 Pokud je pro plnění Smlouvy nezbytný přenos dat z prostředí Dodavatele do prostředí Organizace nebo naopak, musí Strany dostatečně zabezpečit takový přenos a vést dokumentaci o typech přenášených dat. Takový přenos se může uskutečnit pouze na výzvu nebo se souhlasem Organizace v rozsahu a způsobem, který bude zvolen po vzájemné dohodě Stran.

3.4 Dodavatel dále musí:

(a) rozvíjet bezpečnostní povědomí svých zaměstnanců a jiných osob, které se podílejí na plnění Smlouvy, a průběžně je seznamovat s prováděnými nebo plánovanými změnami;

(b) přidělovat osobám, které se podílejí na plnění Smlouvy, oprávnění k výkonu činností a přísně při tom dodržovat bezpečnostní zásadu tzv. „potřeba vědět“ (*need-to-know principle*), tedy dbát o to, aby byla minimalizována rizika nežádoucího přístupu k těm aktivům Organizace, která nesouvisí s plněním Smlouvy; jedná se například o přístupy cestou software systémů umožňujících vzdálený přístup;

(c) průběžně dokumentovat, kontrolovat a vyhodnocovat oprávněnost přístupu u všech osob na straně Dodavatele, které přistupují k aktivům souvisejících s plněním Smlouvy;

(d) průběžně detekovat obecné bezpečnostní hrozby a zranitelnosti v aktivech souvisejících s plněním Smlouvy

(e) bezodkladně informovat Organizaci o detekované bezpečnostní zranitelnosti, hrozbě nebo KBU a ve spolupráci s Organizací zajistit odstranění nebo snížení rizika hrozby, zranitelnosti nebo KBU tak, aby bylo zabráněno vzniku KBI.

3.5 V případě, kdy Organizace identifikuje KBU, která by mohla ohrozit Dodavatele, oznámí tuto skutečnost Dodavateli a společné naleznou řešení, aby nedošlo k KBI.

## 4. OPRÁVNĚNÍ UŽÍVAT DATA, PRAVIDLA PŘÍSTUPU

4.1 Dodavatel může při plnění Smlouvy užívat data předaná Organizací za účelem plnění Smlouvy, avšak vždy pouze v rozsahu nezbytném k plnění Smlouvy. Veškerá předávaná data jsou klasifikována jako informace se střední důvěrností (viz odst. 16.3 písm. (b)), pokud Organizace neurčí jinak.

4.2 Dodavatel nesmí instalovat ani používat žádné nástroje, které nebyly odsouhlaseny Organizací a jejichž užívání by mohlo ohrozit kybernetickou bezpečnost.

4.3 Dodavatel musí při plnění Smlouvy nakládat s daty (včetně osobních údajů) pouze v souladu se Smlouvou, Přílohou a právními předpisy.

4.4 Dodavatel odpovídá za aktuálnost seznamu pracovníků oprávněných přistupovat do objektů Organizace a aktiv Organizace souvisejících s plněním Smlouvy.

4.5 Dodavatel bere na vědomí, že přidělení oprávnění zaměstnanci Dodavatele nebo osobě v jiném obdobném postavení ze strany Organizace musí být řízeno principem nezbytného minima a není nárokové.

4.6 Dodavatel musí zajistit, aby žádný udělený přístup nebyl sdílen více zaměstnanci Dodavatele nebo jinými osobami a že pro přihlášení uživatele nebudou využívány účty typu *root* nebo *administrator*.

4.7 Dodavatel musí zajistit, že vzdálený přístup do aktiv souvisejících s předmětem plnění Smlouvy bude vždy uskutečněn pouze prostřednictvím zabezpečeného připojení VPN a na vyžádání ze strany Organizace a na dobu nezbytně nutnou, pokud se Strany nedohodnou jinak.

4.8 Dodavatel nesmí vyvíjet, kompilovat nebo šířit v jakékoliv části aktiv Organizace programový kód, který má za cíl nelegální ovládnutí, narušení aktiva nebo nelegální získání dat a informací. Dodavatel musí do interní sítě nebo k technologickým a komunikačním systémům Organizace výhradně s využitím zařízení Organizace, pokud se Strany nedohodnou jinak.

4.9 Dodavatel musí zajistit, aby osoby podílející se na plnění Smlouvy, kteří přistupují do interní sítě nebo technologického nebo komunikačního systému Organizace:

(a) měly v externím zařízení (např. notebook, počítač) aplikovány bezpečnostní záplaty a aktualizovanou antivirovou ochranu;

(b) chránily autentizační prostředky a údaje k systémům Organizace; Dodavatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele může být příslušný účet zablokován a řešen jako KBI;

(c) používaly v případě u administrátorských a servisních účtů hesla o délce minimálně 17 znaků obsahující velké písmeno, malé písmeno, číslici a speciální znak.

4.10 Postup v případě nutnosti využít TeamViewer (TV):

(a) Připojení přes TV je povoleno pouze na základě požadavku Dodavatele odsouhlaseného ze strany Organizace v helpdeskovém systému Dodavatele, pokud nebude možno, tak telefonicky, což bude zaznamenáno ve výsledném reportu Dodavatele.

(b) Po odsouhlasení připojení je spuštěno nahrávání obrazovky na straně Organizace. Dobu uložení videa určí garant aktiva. V případě řešení KBI má Dodavatel právo do záznamu na vyžádání nahlédnout, a to na základě písemného požadavku směřovaného na kontaktní osoby.

(c) Dodavatel musí po skočení činností vypracovat podrobný popis toho, co bylo provedeno, do svého helpdesk systému.

# 5. MONITOROVACÍ ČINNOST

5.1 Dodavatel bere na vědomí, že veškerá aktivita Dodavatele v rámci plnění Smlouvy nebo s ním úzce související bude ze strany Organizace průběžně a pravidelně monitorována a vyhodnocována s ohledem na obsah Smlouvy, Přílohy a interních dokumentů Organizace.

Dodavatel musí průběžně monitorovat a zaznamenávat veškerou svoji aktivitu v rámci plnění Smlouvy nebo s ním úzce související. Dodavatel musí na vyžádání předkládat Organizaci záznamy/logy obsahující výsledky monitorování, úspěšná a neúspěšná přihlášení do systému Organizace (pokud nebude logováno v prostředí Organizace) a záznamy o správě uživatelů prováděná na straně Dodavatele.

# 6. AUTORSTVÍ

6.1 Dodavatel musí při plnění Smlouvy postupovat v souladu s právními předpisy upravujícími ochranu duševního vlastnictví, zejména se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

# 7. KONTROLA A AUDIT

7.1 Dodavatel je povinen poskytnout Organizaci veškeré informace nezbytné k doložení splnění povinností vyplývajících z této Smlouvy, jejích příloh, ZKB a VKB.

7.2 Dodavatel je povinen umožnit Organizaci provedení kontrol, včetně auditů, v rozsahu minimálních požadavků podle ZKB a VKB. Tyto kontroly mohou být prováděny Organizací nebo auditorem určeným Organizací. Dodavatel poskytne veškerou potřebnou součinnost, včetně umožnění vstupu do prostor Dodavatele nebo jeho poddodavatele, pokud je to relevantní vzhledem k předmětu Smlouvy.

7.3 Kontrola a audit budou probíhat minimálně jednou ročně, zpravidla formou vyplnění kontrolního dotazníku, pokud se Strany nedohodnou jinak.

7.4 Organizace oznámí Dodavateli provedení kontroly nebo auditu písemně nejméně 30 dní předem. Součástí oznámení bude seznam osob pověřených k provedení kontroly nebo auditu.

7.5 Dodavatel souhlasí s prováděním hodnocení rizik, kontrolou nebo auditem zavedených bezpečnostních opatření ze strany Organizace. Organizace poskytne Dodavateli na jeho žádost výsledek provedené kontroly nebo auditu.

7.6 Strany se zavazují zachovávat důvěrnost informací získaných v rámci kontroly nebo auditu.

# 8. ŘETĚZENÍ A ŘÍZENÍ DODAVATELŮ

8.1 Pokud Dodavatel využívá při plnění Smlouvy poddodavatele, musí zajistit, aby:

(a) poddodavatel dodržoval bezpečnostní požadavky a požadavků na ochranu osobních údajů vyplývající ze Smlouvy a Přílohy;

(b) poskytl Organizaci veškerou nezbytnou součinnost v otázkách řízení bezpečnosti informací.

8.2 Dodavatel se musí řídit požadavky Organizace na řízení bezpečnosti informací a poskytnout Organizaci veškerou nezbytnou součinnost v otázkách řízení bezpečnosti informací. Dodavatel odpovídá za to, že jeho subdodavatelé nebudou jednat v rozporu s bezpečnostními požadavky vyplývajícími ze Smlouvy nebo Přílohy. Pokud poddodavatel takové požadavky nedodrží, považuje se takové nedodržení požadavků za porušení povinnosti Dodavatele.

# 9. DODRŽOVÁNÍ BEZPEČNOSTNÍ POLITIKY ORGANIZACE

9.1 Dodavatel musí dodržovat bezpečnostní politiku Organizace (viz odst. 3.1).

9.2 Bezpečnostní politiky Organizace jsou měněny zpravidla pouze v případě změn právních předpisů nebo v reakci na aktuální bezpečnostní situaci a dle doporučení NÚKIB.

# 10. ŘÍZENÍ ZMĚN

10.1 Dodavatel musí poskytnout Organizaci veškerou nezbytnou součinnost ke splnění povinností Organizace vyplývajících z ustanovení § 11 VKB, přijímání opatření za účelem snížení všech nepříznivých dopadů spojených se změnami, aktualizaci bezpečnostní dokumentace souvisejícím testování a zajištění možnosti navrácení do původního stavu aktiva souvisejícího s plněním Smlouvy.

10.2 Organizace musí informovat Dodavatele o výsledcích řízení změn, které mají dopady na plnění Smlouvy ze strany Dodavatele. Jde zejména o změny v bezpečnostní dokumentaci Organizace (včetně aktiv souvisejících s plněním Smlouvy) a z toho se odvíjející změny v povinnostech Dodavatele. V případě nutnosti se Strany dohodnou na změně povinností Dodavatele postupem podle Smlouvy.

10.3 Veškeré změny, které mají vliv na funkčnost primárních aktiv, podpůrných aktiv, a které mají vliv na bezpečnost informací, musí být řízeny, kontrolovány a dokumentovány ze strany Organizace. Dodavatel v této věci poskytuje součinnost. Jedná se především o následující změny:

(a) změny ovlivňující více uživatelů např. změna vzhledu systému, změna většího počtu funkcí systému, změna vyžadující dlouhodobou odstávku systém; do této kategorie nepatří pravidelné aktualizace systému;

(b) změny prováděné na základě změn platné právní úpravy;

(c) změny dle rozsahu poskytované služby;

(d) změny jednotlivých podpůrných aktiv.

10.4 Dodavatel musí v případě změn podpůrných aktiv poskytnout součinnost Organizaci v rámci přezkoumání dopadů požadovaných změn. Přezkoumání je provedeno před zahájením procesu změn a bere ohledy na následující aspekty:

(a) dopadu na funkčnost aktiv, kterých se změna týká;

(b) časová náročnost provedení změny;

(c) finanční náročnosti změny;

(d) požadavku na personální zdroje pro realizaci změny a pro provozování změněného aktiva, kterého se změna dotýká;

(e) dopadu změny na kvalitu poskytovaných služeb (SLA);

(f) dopadu na existující procesy, pracovní postupy a dokumentaci aktiva, kterého se změna dotýká;

(g) přidělení rolí a odpovědností při a po realizaci změny;

(h) identifikace a řízení rizik spojených se změnou;

(i) proces obnovy do původního stavu.

# 11. DODRŽOVÁNÍ PRAVIDEL BEZPEČNÉHO VÝVOJE

11.1 Dodavatel se zavazuje provádět veškerý vývoj, úpravy, konfigurace, integrace a údržbu v rámci aktiv souvisejících s předmětem Smlouvy po celou dobu jejich životního cyklu v souladu s uznávanými principy a postupy bezpečného vývoje (Secure Software Development), zejména zahrnujícími řízení rizik, bezpečnostní testování, řízení zranitelností a kontrolu zdrojového kódu.

11.2 Dodavatel zajistí, že vývoj bude probíhat v souladu s běžně uznávanými standardy bezpečného vývoje, jako jsou např. OWASP, NIST, ISO/IEC 27034 nebo jiné ekvivalentní standardy odpovídající povaze plnění. Užití konkrétní metodiky nebrání dodržení této povinnosti.

11.3 Dodavatel je povinen zavést a udržovat procesy, které zajistí identifikaci, odstranění a prevenci bezpečnostních zranitelností, včetně provádění pravidelných bezpečnostních testů (např. statická/dynamická analýza kódu, penetrační testy, testování závislostí a knihoven) a sledování zranitelností třetích stran (např. open-source knihoven) s jejich včasnou aktualizací.

11.4 Dodavatel prohlašuje, že do aktiv souvisejících s předmětem Smlouvy, ani jiných systému Organizace neúmyslně ani úmyslně nevloží žádné prvky, které by mohly ohrozit bezpečnost, dostupnost, integritu nebo důvěrnost dat nebo systémů Objednatele, zejména škodlivý kód, backdoory, neautorizované moduly nebo prvky umožňující neoprávněný přístup.

11.5 Na žádost Organizace poskytne Dodavatel bez zbytečného odkladu přiměřenou dokumentaci potvrzující dodržování postupů bezpečného vývoje, zejména záznamy o provedených testech, výsledky analýz, informace o použitých verzích knihoven a komponent, a to v rozsahu nezbytném pro ověření souladu.

# 12. SOULAD S PRÁVNÍMI PŘEDPISY

12.1 Dodavatel musí při plnění Smlouvy postupovat v souladu s právními předpisy.

12.2 Organizace má právo jednostranně odstoupit od Smlouvy bez výpovědní doby v případě, že dojde k významné změně kontroly nad Dodavatelem nebo ke změně kontroly nad zásadními aktivy využívanými Dodavatelem k plnění podle Smlouvy. Dodavatel je povinen Organizaci takovou změnu oznámit bezodkladně, nejpozději do 3 pracovních dnů od jejího uskutečnění.

# 13. INFORMAČNÍ POVINNOST

13.1 Dodavatel musí informovat (například formou dotazníku v rámci auditu) Organizaci o tom, jakým způsobem řídí bezpečnostní rizika spojená s plněním Smlouvy a dále jaká jsou zbytková rizika s tím související (postup přiměřeně podle Přílohy č. 3 a č. 4 VKB).

13.2 Dodavatel musí Organizaci neprodleně, nejpozději do druhého pracovního dne, v případě závažného KBI ihned, informovat o všech nově vzniklých KBU nebo KBI souvisejících s plněním Smlouvy, a to prostřednictvím kontaktních osob uvedených v odst. 13.3. Součástí oznámení musí být popis povahy KBU nebo KBI s ohledem na následující klasifikaci:

(a) **slabé místo nebo KBU** – nedošlo ke KBI, ale KBU související se systémem, procesem nebo Organizací může dříve či později vést ke KBI;

(b) **méně závažný KBI** – KBI, který nemůže významně ovlivnit důvěrnost nebo integritu informací a nemůže způsobit dlouhodobou nedostupnost informací nebo procesů.

(c) **závažný KBI** – KBI, který může způsobit značnou škodu v důsledku ztráty důvěrnosti nebo integrity informací nebo může způsobit nepřijatelné časové období přerušení dostupnosti informací a/nebo procesů.

V případě nedodržení povinnosti informovat Organizaci dle tohoto odstavce do 24 hodin poté, co se o nežádoucí události dozví, je Dodavatel povinen uhradit Objednateli smluvní pokutu ve výši 100.000,- Kč za každý případ porušení zajišťované smluvní povinnosti. Zaplacením smluvní pokuty není dotčen nárok Organizace na náhradu škody vzniklé v důsledku nesplnění této povinnosti Dodavatele.

13.3 Dodavatel musí oznámení zaslat e-mailem oběma kontaktním osoby. V případě, že by měl popis obsahovat informace s vysokou nebo kritickou důvěrností, musí být prostřednictvím e-mailu předán pouze obecný popis. Následný postup bude řešen individuálně. V případě závažného KBI musí Dodavatel oznámení provést také telefonicky minimálně na jednu z kontaktních osob.

Kontaktní osoby pro hlášení KBU/KBI:

Jméno a pozice:
E-mail:
Tel.:

Organizace musí Dodavateli bezodkladně oznámit změnu kontaktních osob nebo jejich kontaktních údajů.

13.4 Dodavatel musí v souvislosti s plněním Smlouvy stanovit činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání KBU a KBI. Dodavatel musí podle takto stanovených a popsaných pravidel postupovat a hlásit všechny KBU a KBI související s plněním Smlouvy, včetně případů porušení zabezpečení osobních údajů ve výše stanovené lhůtě.

13.5 Dodavatel musí realizovat opatření pro snížení zranitelnosti aktiva souvisejícího s plněním Smlouvy vůči KBI a omezení dostupnosti způsobených Dodavatelem a vycházet při tom zejména z požadavků stanovených VKB.

13.6 Dodavatel musí dále Organizaci informovat o:

(a) významné změně ovládání Dodavatele nebo jeho poddodavatele;

(b) změně vlastnictví zásadních aktiv využívaných Dodavatelem k plnění Smlouvy nebo změně oprávnění nakládat s těmito aktivy, a to nejpozději do 3 pracovních dnů od uskutečnění této změny.

(c) žádosti cizozemského orgánu o zpřístupnění nebo předání dat zpracovávaných na území cizího státu, vyjma situace, kdy by takové informování bylo v rozporu s právním řádem, v jehož působnosti dochází ke zpracování dat nebo podle kterého byla žádost podána,

(d) fyzických osobách přicházejících do kontaktu s důvěrnými informacemi Organizace.

# 14. POVINNOSTI PŘI UKONČENÍ SMLOUVY

14.1 V případě, že dojde k ukončení Smlouvy, musí Dodavatel i nadále dodržovat veškeré bezpečnostní požadavky stanovené právními předpisy, Smlouvou a Přílohy.

14.2 Dodavatel musí po ukončení Smlouvy v rozsahu pokynů Organizace:

(a) vrátit Organizaci veškerou dokumentaci označenou jako důvěrnou, která mu byla předána;

(b) provést prokazatelnou likvidaci dat, kterými disponuje v souvislosti se Smlouvou, pokud se nejedná o dokumenty, které musí Strana uchovávat podle právních předpisů;

(c) předat Organizaci prohlášení o vhodné likvidaci dat;

(d) předat Organizaci nezbytné informace, které:

(i) Organizaci umožní provedení migrace dat zpracovávaných na prostředcích dodaných či zajišťovaných podle Smlouvy na jiné systémy;

(ii) jsou do ukončení migrace nezbytné za účelem zajištění kontinuity služeb dodaných či zajišťovaných prostředky podle Smlouvy; rozsah a formu těchto informací musí Strany projednat v rámci ukončovacího období Smlouvy;

(e) účastnit se podle pokynů Organizace jednání s Organizací nebo třetí osobou za účelem plynulého a řádného převedení všech činností souvisejících s provozem, údržbou a rozvojem předmětu Smlouvy na Organizaci nebo třetí osobu.

14.3 Dodavatel je povinen spolupracovat na tvorbě a aktualizaci exit plánu, který stanoví postupy pro ukončení poskytování služeb, migraci dat, jejich bezpečné předání a likvidaci u dodavatele.

# 15. ŘÍZENÍ KONTINUITY

15.1 Organizace může zapojit Dodavatele do řízení kontinuity činností, zejména jej může zahrnout do:

(a) plánu kontinuity činností, který souvisí s aktivy souvisejícími s p plnění Smlouvy a souvisejících služeb;

(b) havarijního plánu Organizace.

Organizace musí Dodavatele o této skutečnosti informovat a poskytnou související dokumenty k připomínkám s dostatečným předstihem před jejich vydáním. Jakmile budou Stranami ujednány veškeré kroky, budou zapracovány do výpisu bezpečností dokumentace, jehož aktualizace bude předána Dodavateli podle čl. 16.

# 16. PODMÍNKY PŘEDÁVÁNÍ DAT

16.1 Veškeré provozní údaje, soubory, obsah logů, ostatní data a informace poskytnuté a zpracovávané v souvislosti s plněním Smlouvy (s výjimkou dat Dodavatele, která jsou jeho duševním vlastnictví) jsou ve výhradním vlastnictví Organizace.

16.2 Předávání dat musí probíhat tak, aby je nemohly neoprávněné osoby číst, kopírovat, měnit ani mazat. Pokud Organizace neurčí jinak, běžné informace, klasifikované jako informace s nízkou nebo střední důvěrností, budou zpravidla předávány prostřednictvím e-mailové komunikace, informace klasifikované jako informace s vysokou nebo kritickou důvěrností zpravidla prostřednictvím zabezpečeného cloudového úložiště Organizace. Organizace musí oznámit stupeň klasifikace informací oznámí Dodavateli před vlastním přenosem. Klasifikace informací Organizace je specifikována v následujícím odstavci.

16.3 Klasifikace informací Organizace:

(a) Informace s nízkou důvěrností:

(i) jsou veřejně přístupné bez omezení;

(ii) nenarušují důvěrnost primárních aktiv a neohrožují zájmy Organizace;

(b) Informace se střední důvěrností:

(i) nejsou veřejně přístupné bez omezení;

(ii) jsou bez omezení přístupné zaměstnancům Organizace;

(iii) jsou poskytovány nebo šířeny s definovaným omezením;

(iv) jsou přenášeny po veřejných komunikačních sítích jen určeným příjemcům;

(c) Informace s vysokou důvěrností:

(i) nejsou veřejně přístupné;

(ii) jsou sdíleny pouze mezi vymezeným oprávněným okruhem příjemců;

(iii) jsou sdíleny tak, že je vyhotoven záznam o přístupu nebo přenosu;

(iv) jsou přenášeny po veřejných komunikačních sítích jen určeným příjemcům s použitím ochranných kryptografických prostředků;

(d) Informace s kritickou důvěrností:

(i) nejsou veřejné přístupné;

(ii) jsou sdíleny pouze mezi taxativně vymezeným oprávněným okruhem příjemců;

(iii) jsou sdíleny tak, že je vyhotoven záznam o přístupu nebo přenosu;

(iv) jsou přenášeny po veřejných komunikačních sítích jen určeným příjemcům s použitím ochranných kryptografických prostředků a současně zabraňující zneužití jinými subjekty.

16.4 Pokud Organizace neurčí jinak, Strany nesmí uchovávat předávaná data s výjimkou informací s nízkou důvěrností na přenosných datových nosičích.

## 17. PRAVIDLA PRO LIKVIDACI DAT

17.1 V případě, kdy Dodavatele disponuje daty Organizace, musí se řídit pokyny Organizace pro mazání dat a likvidaci technických nosičů, provozních údajů nebo informací a jejich kopií přiměřeně hodnotě a důležitosti aktiv a dále přiměřeně podle přílohy č. 2 VKB.

17.2 Likvidaci dat nepodléhají dokumenty, které musí Strana uchovávat podle právních předpisů.

## 18. DOKUMENTACE INFORMAČNÍHO SYSTÉMU

18.1 V případě, že je Dodavatel provozovatelem informačního systému, jehož narušení by významně ohrozilo poskytování regulované služby Organizace, musí Dodavatel k takovému systému vypracovat a předat Organizaci bezpečnostní dokumentaci alespoň v následujícím rozsahu:

(a) systémová příručka obsahující alespoň následující:

(i) popis funkcí, včetně bezpečnostních, které používá správce systému pro provádění určených činností a návod na používání těchto funkcí;

(ii) podrobný popis nebo odkaz na dokument, ve kterém je popis uveden a který je správci systému dostupný;

(iii) popis jednotlivých činností vykonávaných při správě a oprávnění nezbytných pro výkon těchto činností, definování uživatelů nebo skupin uživatelů a jejich oprávnění a povinnosti při využívání předmětu plnění;

(b) uživatelská příručka obsahující alespoň následující:

(i) popis funkcí, včetně bezpečnostních, které používá uživatel pro svou činnost a návod na použití těchto funkcí např. formou nápovědy v SW;

(c) potřebná provozní dokumentace v rozsahu vyplývajícím z předmětu Smlouvy, zejména:

(i) dokumentace strategie obnovy (pokud není řešeno na straně Organizace);

(ii) dokumentace skutečného provedení;

(iii) dokumentace obsahující popis autorizačního konceptu a oprávnění (pokud není řešeno na straně Organizace);

(iv) dokumentace obsahující zálohovací a archivační postupy (pokud není řešeno na straně Organizace);

(v) dokumentace obsahující instalační a konfigurační postupy (pokud se nejedná o know-how Dodavatele);

(vi) dokumentace obsahující bezpečností nastavení související s plněním Smlouvy.

## 19. ZPŘÍSTUPNĚNÍ NEBO PŘEDÁNÍ DAT NA ZÁKLADĚ ŽÁDOSTI CIZOZEMSKÉHO ORGÁNU

19.1 Smluvní strany se dohodly, že v případě, kdy jedna ze Stran zpracovávajících data podle této smlouvy obdrží žádost cizozemského orgánu veřejné moci o zpřístupnění nebo předání dat, která jsou zpracovávána na území cizího státu, postupuje následovně:

(a) Žádost bude vyřízena až po provedení přezkoumání její zákonnosti, a to s ohledem na právní řád státu, v jehož působnosti se data zpracovávají, jakož i na právní řád, podle něhož byla žádost podána.

(b) Povinný subjekt vynaloží veškeré úsilí, které lze dle relevantního právního řádu spravedlivě požadovat, k zabránění zpřístupnění nebo předání dat, pokud takový postup není nezákonný nebo neproveditelný.

(c) Jakékoli zpřístupnění nebo předání dat bude provedeno pouze v nezbytném rozsahu, který je nutný k naplnění zákonné povinnosti plynoucí z příslušné žádosti.

(d) O přijetí takové žádosti a jejím výsledku bude druhá smluvní strana informována bez zbytečného odkladu, pokud to právní předpisy umožňují.

## 20. NÁLEŽITOSTI SMLOUVY O ÚROVNI SLUŽEB

20.1 V případě, že předmětem této Smlouvy je mimo jiné i poskytování služeb, jsou požadavky na úroveň poskytovaných služeb popsány v dalších přílohách této Smlouvy.

20.2 Pokud se jedná o jiný typ smlouvy (např. kupní smlouvu), u které není relevantní sjednání SLA, toto ustanovení se neuplatní.

## 21. SANKCE ZA PORUŠENÍ POVINNOSTÍ

21.1 Smluvní strany berou na vědomí, že za porušení povinností stanovených touto Přílohou se uplatní ustanovení o smluvních sankcích stanovená ve Smlouvě, pokud taková ustanovení existují.

21.2 V případě, že Smlouva neobsahuje ustanovení o smluvních sankcích vztahujících se k povinnostem dle této Přílohy, zavazuje se Dodavatel uhradit Objednateli smluvní pokutu ve výši

**0,1 % z hodnoty plnění, kterého se porušení týká**, za každé jednotlivé porušení povinnosti stanovené touto Přílohou.

21.3 Není-li možné hodnotu dotčeného plnění jednoznačně určit, sjednávají smluvní strany smluvní pokutu ve výši 0,**1 % z ceny Smlouvy** (nebo ceny příslušné části plnění, pokud je cena členěna, včetně DPH).

21.4 Za porušení povinnosti Dodavatele zakládající právo Objednatele na smluvní pokutu podle odst. 21.2. resp. 21.3. tohoto článku se nepovažuje porušení povinností Dodavatele, pro které tato Příloha stanovuje speciální smluvní pokutu v odst. 21.5. tohoto článku ve spojení s čl. 13 odst. 13.2. této Přílohy.

21.5 V případě porušení informační povinnosti dle čl. 13 odst. 13.2. této Přílohy se uplatní smluvní pokuta dle čl. 13 odst. 13.2. této Přílohy.

21.6 Smluvní pokuta je splatná do 14 dnů od doručení výzvy k úhradě straně, která smluvní povinnost porušila.

Uplatněním smluvní pokuty není dotčeno právo Objednatele požadovat náhradu škody v plném rozsahu, přesahuje-li škoda výši smluvní pokuty, ani právo požadovat odstranění závadného stavu.