Pojmy
Objednatel: Krajská zdravotní, a.s.
PPK: dokument KZ06_SM0010 Požadavky na provedení a kvalitu ICT
KZ: Krajská zdravotní, a.s.
NÚKIB: Národní úřad pro kybernetickou a informační bezpečnost
Zákon: Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, případně zákon, který tento zákon nahradí

Úvodní ustanovení

- Tento bezpečnostní standard (dále také „**Standard“**) je přílohou kupní smlouvy k veřejné zakázce malého rozsahu s názvem „EKG s velkým displejem pro kardiologickou kliniku Krajské zdravotní, a.s. – Masarykovy nemocnice v Ústí nad Labem, o. z.“ (dále také „**Smlouva“**). Tato verze Standardu platí pro dodávky bezpečnostně významného hardware, obsahujícího programové vybavení nebo jiný typ kódu a je dodávaný včetně zajištění podpory.
- Účelem Standardu je zajistit plnění povinností Krajské zdravotní, a.s. podle směrnice NIS2, Zákona o kybernetické bezpečnosti a jeho prováděcích vyhlášek, soulad s publikovanými doporučeními a metodikami Národního úřadu pro kybernetickou bezpečnost a zabezpečit stanovenou kvalitu služeb Krajské zdravotní, a.s.
- Standard je účinný od 18. 11. 2024.
- Tato verze Standardu nahrazuje jakoukoliv předchozí verzi. Do účinnosti této verze zůstává předchozí verze v účinnosti a Dodavatel je povinen ji dodržovat.
- Dodavatel je povinen tento Standard dodržovat po celou účinnost Smlouvy. Jestliže je ve Smlouvě nebo Standardu uvedena doba delší než doba trvání smlouvy, je Dodavatel povinen dodržovat Standard do takto stanovené doby.
- Tento Standard doplňuje dokument KZ06_SM0010 Požadavky na provedení a kvalitu ICT (dále také **„PPK“**), který je základním souborem požadavků na kvalitu dodávek pro oblast ICT a který je pro Dodavatele závazný. PPK jsou v aktuální verzi dostupné na webových stránkách Krajské zdravotní, a.s. (www.kzcr.eu). Jestliže Standard upravuje některé okolnosti přísněji nebo stanovuje vyšší požadavky než PPK, je Dodavatel povinen dodržet přísnější úpravu.
- Jestliže je to potřebné, zejména pro zajištění souladu činností, opatření nebo služeb Krajské zdravotní, a.s. (dále také „**Objednatel**“ nebo „**KZ**“) se zákony, normami, standardy, požadavky relevantních autorit, pro odstranění nesouladu, pro snížení rizika, pro splnění požadavků KZ pro účast v obchodní soutěži, je Objednatel oprávněn vydat novou verzi Standardu. Dodavatel je povinen zajistit soulad s novou verzí Standardu bez zbytečného odkladu, nejpozději však do počátku účinnosti jeho nové verze. KZ doručí Dodavateli novou verzi Standardu bez zbytečného odkladu, nejpozději však 3 měsíce před jeho účinností.
- Dodavatel je povinen po doručení nové verze Standardu bez odkladu projednat s KZ harmonogram činností a změn, potřebných k dosažení souladu s novou verzí Standardu, nebo mu oznámit, že soulad s novou verzí Standardu dosáhne ke dni jeho účinnosti. Pokud harmonogram upraví účinnost jednotlivého ustanovení Standardu odlišně, platí termín uvedený v harmonogramu. Harmonogram má listinnou podobu a je účinný po jeho schválení KZ. Neschválí-li Objednatel harmonogram, je Standard pro Dodavatele závazný k datu, uvedenému ve Standardu jako datum účinnosti.
- Objednatel může stanovit, že věcný obsah Standardu bude zčásti nahrazen zavedením a udržováním určené normy nebo standardu třetí strany (například ISO, NIST, ČSN a podobně). Objednatel v takovém případě stanoví podmínky implementace, rozsahu, certifikace a povinností Dodavatele oznamovat změny určených okolností, zejména zánik platnosti nebo změnu podmínek certifikace. Objednatel vydá podmínky uznání takového opatření, jako součást další verze Standardu.
- Objednatel poskytne Dodavateli přiměřenou součinnost při zajišťování souladu se Standardem.

- Dodavatel nemá nárok na úhradu nákladů na zavedení opatření k zajištění souladu se Standardem, ani nákladů na implementaci ve Standardu uvedeného obecně platného právního předpisu nebo standardu nebo normy třetí strany.
- Pojmy uvedené ve Standardu mají takový význam, jaký jim přisuzuje právní řád České republiky, pokud nejsou ve Smlouvě nebo Standardu upraveny odlišně.

Základní povinnosti Dodavatele

- Dodavatel je povinen bez odkladu informovat KZ o všech zahájených řízeních, která mohou mít vliv na jeho schopnost plnit v uvedeném rozsahu a kvalitě Smlouvu.
- Dodavatel je povinen bez odkladu informovat KZ o změnách ve své ekonomické situaci, majetkové struktuře, místě působení, změnách nebo zániku smluv s dodavateli, změně právní formy nebo obdobných změnách, které mohou mít vliv na jeho schopnost plnit v uvedeném rozsahu a kvalitě Smlouvu.
- Dodavatel je povinen udržovat užívanou infrastrukturu a služby v bezvadném stavu tak, aby umožňovaly řádné plnění Smlouvy a tento bezvadný stav průběžně monitorovat.
- Dodavatel je povinen zavést politiku bezpečnosti, řádně ji udržovat a aktualizovat.
- Dodavatel je povinen na základě bezpečnostních potřeb a výsledků hodnocení rizik zavádět a udržovat potřebná bezpečnostní opatření. Taková opatření monitorovat, vyhodnocovat jejich účinnost a v případě potřeby je modernizovat.
- Dodavatel je povinen vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného předmětu plnění, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy KZ zpřístupnit.
- Dodavatel je povinen strpět audit, kontrolu nebo bezpečnostní posouzení KZ nebo KZ určené třetí strany, poskytovat KZ informace a další podklady a součinnost pro provedení auditu či kontroly. Na pokyn KZ musí Dodavatel kontrolu nebo audit určené oblasti zajistit sám a podat o tom ve stanoveném termínu zprávu. Dodavatel je povinen provádět interní kontroly opakovaně podle pokynů KZ nebo pokud je to vzhledem k charakteru vykonávaných činností potřebné.
- Dodavatel je povinen udržovat úplnou a aktuální dokumentaci technickou, projektovou, administrátorskou, uživatelskou a bezpečnostní, archivovat předešlé verze této dokumentace, pokud byly účinné v době platnosti Smlouvy.
- Dodavatel je povinen pro komunikaci a předávání dat/aktiv využívat pouze předem schválené komunikační a přenosové kanály.
- Dodavatel je povinen zavést a udržovat pohotovostní plány pro případy neplánovaného přerušení nebo omezení činnosti nebo selhání významných třetích stran nebo poddodavatelů, zejména pokud je to potřebné pro zajištění podpory, údržby nebo oprav.
- Dodavatel je povinen dodržovat zásady bezpečnosti informací a kybernetické bezpečnosti v rozsahu ujednaném s KZ nebo zajištěním souladu s KZ určeným standardem nebo normou třetí strany, přičemž za základní nepominutelný rámec normativních základů a regulovaných okruhů Dodavatele se považuje dokument Minimální bezpečnostní standard, dostupný na www.nukib.cz v sekci „Podpůrné materiály“, kdy Dodavatel vždy užije platnou verzi tohoto dokumentu. Dodavatel musí všechna opatření k zajištění kybernetické bezpečnosti koncipovat v souladu s architekturou zákona o kybernetické bezpečnosti, zejména s ustanoveními o bezpečnostních opatřeních[1]. Dodavatel nebude postupovat v rozporu s publikovanými doporučeními, varováními a podpůrnými materiály, které jsou dostupné na www.govcert.cz. Základními okruhy povinností, doporučení a zásad dokumentu Minimální standard, které musí Dodavatel řádně zavést a řídit ve lhůtě stanovené KZ, jsou:

a) zavedení bezpečnostních politik;
b) klasifikace a ochrana informací;

[1] zejména § 5 zákona č. 181/2014 Sb.

c) řízení Dodavatelů;
d) řízení lidských zdrojů;
e) řízení změn;
f) řízení kontinuity činností;
g) audit kybernetické bezpečnosti;
h) fyzická bezpečnost;
i) řízení přístupů;
j) ochrana před škodlivým kódem;
k) detekce bezpečnostních incidentů a událostí;
l) řízení reakce na bezpečností incidenty a události;
m) aplikační bezpečnost;
n) kryptografická ochrana;
o) zajišťování dostupnosti informací;
p) zálohování.

Dodávky hardware

- Dodavatel je povinen zajistit předepsané fyzikální podmínky pro dopravu a skladování hardware (dále také „**zařízení**“).
- Dodavatel je povinen zabránit přístupu osob k zařízení, s výjimkou osob, které na něm mají vykonat potřebný pracovní úkon.
- Obal nebo schrána pro skladování nebo přepravu hardware musí být provedena nebo zajištěna tak, aby bylo bez zvláštního úsilí možné zjistit její neautorizované otevření nebo poškození. Stejným způsobem musí být zajištěn plášť, kryt nebo obdobná část zařízení.
- Každé nedodržení předepsaných fyzikálních a/nebo klimatických podmínek skladování nebo přepravy, včetně pádu nebo obdobné okolnosti způsobující vysoké zrychlení nebo otřesy, stejně jako podezření na neoprávněnou manipulaci nebo neoprávněné užití nebo převzetí zařízení v poškozeném obalu od poddodavatele, musí Dodavatel bez odkladu oznámit KZ.
- Součástí dodávky musí být pokyny nebo doporučení k bezpečnému uvedení zařízení do provozu, včetně potřebných nebo vhodných konfiguračních a aktualizačních postupů a pokyny k rozpoznání správného nebo chybového stavu zařízení.
- Jestliže bude zařízení instalovat, uvádět do provozu a/nebo konfigurovat zaměstnanec Dodavatele, musí být tato okolnost viditelně a výrazně uvedena při dodání zařízení, například na obalu.
- Dodavatel musí zajistit předání zařízení Objednateli jím předepsaným způsobem, zejména co do provedení testů, aktualizací, konfigurace, dokumentace a zaškolení určených osob. O takovém předání vyhotoví Dodavatel protokol o předání zařízení do provozu, který podpisem potvrdí určená osoba na straně Objednatele. V protokolu musí být uveden kromě technických okolností také datu, místo a čas předání zařízení do provozu. Podpisem protokolu oběma stranami se zařízení stává aktivem Objednatele a jeho kybernetická bezpečnost se řídí všemi interními a přijatými standardy Objednatele.
- Dodavatel je povinen předat KZ dokumentaci předmětu plnění minimálně v následujícím rozsahu:

a) dokumentaci skutečného provedení;
b) dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;
c) dokumentaci obsahující popis autorizačních postupů a oprávnění;
d) dokumentaci obsahující zálohovací a archivační postupy;
e) dokumentaci obsahující instalační a konfigurační postupy;
f) dokumentaci zahrnující protokoly o testech zranitelností;
g) dokumentaci zahrnující protokoly o penetračních testech;
h) vyhodnocení souladu s bezpečnostními požadavky KZ;
i) dokumentaci pro zajištění kontinuity provozu a obnovy po havárii;

j) dokumentaci k řízení provozu a řízení podpory;
k) dokumentaci k odebrání nebo zneplatnění identit a účtů pro instalaci;
l) licenční a obdobná ujednání ke všem aktivům, která jsou součástí dodávky.

- Jestliže Dodavatel při zajišťování podpory, například při odstraňování závady, dodá Objednateli paměťové médium (nosič informací), nebo zařízení obsahující paměťové médium, je povinen ověřit, zda paměťové médium obsahuje výhradně pro správné užívání zařízení nezbytný a bezpečný obsah.

Specifické povinnosti Dodavatele

- Povinnosti, uvedené v článku Specifické povinnosti Dodavatele, je Dodavatel povinen aplikovat na všechna aktiva, která budou využita k plnění Smlouvy nebo mohou mít vliv na zajištění kvality dodávky nebo na kybernetickou bezpečnost Objednatele nebo další oprávněné zájmy Objednatele. Tyto povinnosti plní Dodavatel nad rámec Základních povinností.
- Dodavatel musí zajistit trvalý soulad kvality plnění s PPK.
- Dodavatel je povinen u každého dodaného aktiva písemně doporučit KZ milníky, metody a formy řízení životního cyklu a pokud dojde ke změně podstatných okolností (například v oblasti kompatibility, zranitelností, podpory nebo licenčních podmínek) bez odkladu na ně upozornit KZ.
- Pro všechna aktiva a činnosti, které budou využity pro plnění Smlouvy nebo podstatné pro kvalitu plnění Smlouvy, je Dodavatel povinen zavést standard ISO 9001 včetně akreditované certifikace a certifikaci prokazatelně udržovat platnou po celou dobu platnosti Smlouvy. Dodavatel může navrhnout, že se užije jiný standard, který zajistí stejnou nebo vyšší úroveň ochrany aktiv KZ.
- Pro všechna aktiva a činnosti, které budou využity nebo budou podstatné pro kvalitu a bezpečnost plnění Smlouvy, je Dodavatel povinen zavést standard ISO 27001 včetně akreditované certifikace a certifikaci prokazatelně udržovat platnou po celou dobu platnosti Smlouvy. S ohledem na vývoj obecně závazných právních norem a oborových regulací je Objednatel oprávněn určit, že pro Dodavatele bude závazná jiná norma nebo zákon. To oznámí KZ Dodavateli nejméně 3 měsíce před datem, od kterého bude Dodavatel povinen takový standard zavést a užívat pro řízení činností podle Smlouvy. Dodavatel může navrhnout, že se užije jiný standard, který zajistí stejnou nebo vyšší úroveň ochrany aktiv KZ.
- Dodavatel je povinen získat a po celou dobu platnosti Smlouvy udržovat v platnosti certifikace všech výrobců nebo dodavatelů hardware nebo software využitého pro dodávku zboží nebo provádění servisu, jestliže to tyto osoby vyžadují pro legální užití jejich dodávky nebo pro bezvadnou záruku. Tato povinnost platí také pro fyzické osoby, vykovávající činnosti podle Smlouvy.
- Dodavatel nesmí používat v infrastruktuře nebo při přistupování k infrastruktuře KZ keylogery, scannery, nástroje mapování sítě, neexistující identity, klony nebo kopie identit nebo identifikátorů, KZ neschválené systémy vzdáleného ovládání nebo přístupu, viry, červy nebo obdobná aktiva, která nejsou nezbytná pro zajištění potřeb KZ a KZ předem písemně schválená.
- Dodavatel musí zajistit, aby podle Objednatelem určeného vzoru vypracovali jeho zaměstnanci nebo další osoby v obdobném postavení písemný záznam o každém vstupu do režimových prostor Objednatele, o servisním zásahu nebo kontrole.
- Dodavatel musí zajistit, aby na předmětu dodávky nebo v sítích Objednatele nebyla instalována nebo spouštěna jakákoliv softwarová aktiva bez předchozího písemného souhlasu Objednatele.
- Dodavatel musí zajistit, aby s využitím jemu svěřených oprávnění nebo jím vytvořené příležitosti nikdo bez předchozího písemného souhlasu nepřistupoval k aktivům KZ včetně sítí, manipuloval s nimi, prováděl na nich změny nebo na nich spouštěl nebo instaloval software.

- Dodavatel nesmí bez předchozího písemného souhlasu Objednatele na aktivech Objednatele provádět bezpečnostní testování, skenování, zachytávání provozu, replikaci provozu, replikaci nebo zálohy dat, nebo jakékoliv další činnosti, které mohou mít vliv na stav kybernetické bezpečnosti.
- Dodavatel nesmí na aktivech Objednatele provádět konfigurační změny bez předchozího souhlasu Objednatele.
- Dodavatel nesmí na aktivech Objednatele bez předchozího souhlasu Objednatele vytvářet, měnit nebo rušit identity nebo účty jakéhokoliv typu.
- Dodavatel je povinen zajistit, aby migrace nebo nasazení aktualizací, konfiguračních dat nebo jiných aktiv do provozního prostředí byla provedena až po akceptaci výsledků testů v testovacím prostředí a formalizovaném a doložitelném odsouhlasení KZ.
- Dodavatel je povinen zajistit zavedení politiky bezpečnosti a její pravidelnou aktualizaci.
- Dodavatel je povinen zajistit prokazatelné proškolení zaměstnanců a třetích stran o zajištění bezpečnosti plynoucí ze Smlouvy.
- Dodavatel je povinen zajistit při přístupu do systémů KZ využívat jen zařízení, která vyhovují bezpečnostním, technickým a provozním požadavkům KZ a jsou jím schválená, zejména jsou aktualizovaná, patchovaná, vybavená bezpečnostním softwarem, je na nich užito výhradně legální programové vybavení a přístup k nim je řízen.
- Dodavatel je povinen zajistit respektování pravidel fyzické bezpečnosti při pohybu v prostorách KZ.
- Dodavatel je povinen zajistit součinnost při stanovení pravidel a provedení penetračních testů, zejména povinnost testy provést a povinnost na své náklady bez odkladu přijímat opatření k vyřešení kritických nálezů.
- Dodavatel je povinen zajistit spolupráci při řešení incidentů, hrozeb, zranitelností a patchování.
- Dodavatel je povinen mít zavedené mechanismy pro detekci bezpečnostních událostí, bezpečnostních incidentů a odchylek.
- Dodavatel je povinen zajistit povinnost, zajistit nebo umožnit nezávislou revizi zdrojového kódu, jestliže bude předmětem dodávky, včetně aktualizací nebo diagnostických nástrojů.
- Dodavatel je povinen zajistit, v případě exponování části jeho prostředí pro vývoj, testování nebo ukládání datových celků, spravovaných podle Smlouvy, prostředí DMZ, přičemž první firewall musí plnit funkci „perimeter“ a musí být nastaven tak, aby byl provoz povolen pouze směrem do DMZ. Druhý firewall musí plnit funkci „back-end“ a musí být nastaven tak, aby byl provoz povolen pouze směrem z DMZ do vnitřní sítě Dodavatele.
- Dodavatel je povinen zcela dodržovat technické nebo bezpečnostní standardy Objednatele nebo jiné osoby, které jsou uvedeny ve Smlouvě nebo Standardu.
- Dodavatel je povinen v případě použití bezdrátových technologií zajistit, že nebude použitá bezdrátová technologie rušit či jinak omezovat ostatní bezdrátová připojení/zařízení.

Řízení bezpečnosti poddodavatelů

- Dodavatel smí pro potřeby plnění Smlouvy používat pouze takové poddodavatele, které předem notifikoval KZ a ta s jejich využitím vyjádřila souhlas. KZ může odmítnout poddodavatele, který je subjektem varování Národního úřadu pro kybernetickou a informační bezpečnost nebo je uveden na sankčních seznamech oprávněných orgánů ČR nebo Evropské Unie nebo by jeho zapojení mohlo být zdrojem neakceptovatelného rizika pro KZ nebo existují vážné pochybnosti o jeho způsobilosti zajistit dodávku v souladu s PPK, Standardem nebo zákonnými povinnostmi KZ.
- Dodavatel je povinen smluvně a věcně zajistit, aby řízení a výkon bezpečnosti poddodavatelů a jimi poskytovaného plnění, prováděných činností a dalších okolností naplňovala potřebné normy, nejméně však tento Standard, a to po celou dobu, kdy je to potřebné k plnění Smlouvy.

- Změnu nebo ztrátu schopnosti či vůle poddodavatele naplňovat bezpečnostní standard je Dodavatel povinen bez odkladu oznámit KZ. Dodavatel musí KZ bez odkladu oznámit i další podstatné okolnosti na straně poddodavatele, jako je například změna struktury, právní formy, sídla, personální změna na pozici podstatné pro dodávku.
- Dodavatel musí KZ oznámit změnu licenčních nebo obdobných podmínek poddodavatele kódu nebo služeb, které využil, využívá nebo hodlá využít pro plnění Smlouvy, jestliže taková změna může mít vliv na bezpečnost dodávky, na oprávnění nebo odpovědnosti.
- Dodavatel je povinen předávat Objednateli informaci o změnách dodavatelů svého poddodavatele, jestliže takové změny mohou mít vliv na stav kybernetické bezpečnosti aktiv Objednatele.

Oznamování incidentů

- Dodavatel je povinen bez prodlení hlásit KZ veškerá podezření na kybernetické bezpečnostní události nebo jakékoliv bezpečnostní události nebo zjištěné zranitelnosti, související s použitou službou, řešením nebo jeho částmi, o kterých se dozví, bez ohledu na to, kde nastaly nebo byly zjištěny.
- Oznámení se provádí telefonicky nebo osobně a dodatečně podle pokynů KZ písemnou zprávou. Součástí oznámení musí být datum a čas zjištění, povaha události, zdroj detekce události, cíle/oběti/událostí dotčená aktiva, možný dopad, zamýšlený další postup a odborná doporučení.
- Povinnost oznamovat incidenty se vztahuje zejména na aktiva KZ, Dodavatele, aktiva poddodavatelů, dodávaná aktiva, aktiva stejného typu jako dodávaná aktiva, subjekty technologicky nebo jinak obdobné jako Objednatel.

Užívání kryptografické ochrany

- Pokud je v rámci plnění Smlouvy vyžadováno použití kryptografických prostředků:

a) šifrování se provádí symetrickým heslem nejméně metodou AES 256. Heslo musí být vždy předáno jiným komunikačním kanálem než chráněný obsah;

b) šifrování pomocí digitálních certifikátů vydaných obecně uznávanou certifikační autoritou nebo KZ určenou autoritou;

c) pokud nelze ověřit platnost certifikátu, je certifikát považován za neplatný a nelze jej použít k šifrování nebo podpisu;

d) pro VPN přístup se užije AES256/SHA256 nebo silnější;

e) pro webové servery prezentující provozní nebo jiná určená data KZ nebo indikující stav aktiv KZ se užije HTTPS protokol minimálně s TLS 1.2.

Řízení změn

- Dodavatel musí zavést a po celou dobu účinnosti Smlouvy udržovat systém řízení změn u všech aktiv, procesů a/nebo opatření, která jsou předmětem dodávky nebo která mohou mít přímý nebo nepřímý vliv na stav kybernetické bezpečnosti Objednatele. Zejména dodavatel musí:
  a) Identifikovat změny;
  b) přezkoumávat možné dopady změn;
  c) určovat významné změny

  přičemž kteroukoliv změnu může v odůvodněných případech jako významnou určit Objednatel.
- Dodavatel u významných změn
  a) plánuje jejich provádění;
  b) určuje odpovědné osoby;
  c) dokumentuje jejich řízení;
  d) eviduje je;
  e) provádí analýzu rizik;

f) přijímá opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami;

g) reviduje a v případě potřeby aktualizuje bezpečnostní politiku a bezpečnostní dokumentaci;

h) zajišťuje jejich testování;

i) zajišťuje možnost navrácení do původního stavu;

j) informuje Objednatele a navrhuje opatření.

- Objednatel na základě výsledků analýzy rizik podle tohoto článku rozhoduje o provedení penetračního testování nebo testování zranitelností; pokud rozhodne o provedení penetračního testování nebo testování zranitelností, Dodavatel je povinen podle pokynů Objednatele reagovat na zjištěné nedostatky.

Personální bezpečnost

- Dodavatel je povinen ověřovat totožnost osob, které se podílejí nebo mají podílet na plnění Smlouvy nebo které vstupují nebo mají získat oprávnění vstupovat do objektů KZ nebo přistupovat k jeho aktivům. Dodavatel je povinen vést evidenci takových osob nejméně po dobu účinnosti Smlouvy.
- Dodavatel je povinen zajistit prokazatelné seznámení osob, které se podílejí nebo mají podílet na plnění Smlouvy nebo které vstupují nebo mají získat oprávnění vstupovat do objektů KZ nebo přistupovat k jeho aktivům, s KZ určenými předpisy, normami nebo standardy a ověřit, že tyto osoby určené texty znají a pochopily je. Dodavatel je povinen zajistit takové prokazatelné seznámení, například formou proškolení, v KZ určené periodě.
- Dodavatel musí mít stanoven plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí v rozsahu nejméně poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice.
- Dodavatel musí systematicky provádět potřebná teoretická i praktická školení uživatelů, administrátorů a osob zastávajících bezpečnostní role.
- Dodavatel musí určit osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny.
- Dodavatel v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a poddodavatelů o jejich povinnostech, oprávněních a o bezpečnostní politice.
- Dodavatel pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje pravidelná odborná školení včetně praktického procvičování, přičemž vychází z aktuálních potřeb v oblasti kybernetické bezpečnosti.
- Dodavatel v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje pravidelné zevrubné školení a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní.
- Dodavatel zajišťuje kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a má nastaven proces disciplinárního nebo obdobného řízení pro své zaměstnance.
- Dodavatel v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajišťuje předání odpovědností.
- Dodavatel hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí.
- Dodavatel určuje pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.
- Dodavatel vede o provedených školení přehledy, které obsahují předmět školení, obsah školení, identifikaci lektora nebo technického řešení a seznam osob, které školení absolvovaly.
- Dodavatel alespoň jedenkrát ročně předává KZ informace, týkající se osob souvisejících s poskytovaným předmětem plnění Smlouvy, o provedených školeních a jejich obsahu.

- Objednatel má právo vést záznamy a prověřovat činnosti Dodavatele, vést záznamy o incidentech a nestandardních činnostech zaměstnanců a dalších osob působících ve prospěch Dodavatele.

Řízení provozu a přístupu

- Dodavatel je povinen zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění v souladu s požadavky vyhlášky č. 82/2018 Sb., (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů a v souladu s PPK.
- Na vyžádání je Dodavatel povinen poskytnout KZ přehled o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře, kterými plní předmět Smlouvy.
- Při přístupu do systémů KZ smí Dodavatel využívat jen zařízení, která vyhovují bezpečnostním požadavkům KZ a jsou jím schválená, zejména jsou aktualizovaná, patchovaná, vybavená bezpečnostním softwarem, je na nich užito výhradně legální programové vybavení a přístup k nim je řízen.
- Jestliže se předpokládá síťová komunikace dodaného zařízení, musí být plně interoperabilní se síťovým prostředím KZ podle dokumentu PPK, a podporovat řízení přístupů s využitím služby Active Directory nebo obdobným nástrojem používaným Objednatelem. Zařízení musí být vybaveno schopností odesílat logy a alerty do bezpečnostních a dohledových systémů Objednatele. Veškeré okolnosti síťové komunikace, tedy zejména její fyzické provedení, protokoly, doménové politiky, autentizace, autorizace, routování a další domény relevantní pro bezpečnost síťového provozu musí být bezvýhradně provedeny podle pokynů Objednatele, v souladu s jeho interními standardy, obecně závaznými právními normami a určenými technickými standardy.
- Jestliže bude Dodavateli umožněn přístup k aktivům KZ svěřením přístupových údajů, certifikátů a zanesením technických a uživatelských identit do systémů a seznamů KZ (dále také autentifikační prostředky), musí Dodavatel zajistit, aby autentifikační prostředky nebyly sdíleny mezi uživateli, aby byly chráněny proti vyzrazení nebo ztrátě a je povinen KZ bezodkladně oznámit jejich ztrátu, podezření na porušení jejich bezpečnosti nebo podezření na jejich zneužití.
- Dodavatel zajistí dodržování zásady okamžitého odhlašování účtů a minimalizace činností.
- Každý zaměstnanec Dodavatele, který přistupuje k aktivům KZ má u Objednatele, přidělen a evidován jedinečný uživatelský účet, kterému jsou v jednotlivých systémech nebo aplikacích přiřazeny specifické role související výhradně s plněním předmětu Smlouvy.
- K jednoznačné identifikaci privilegovaných uživatelů se při přihlašování zásadně používá vícefaktorová autentizace. Jestliže to není možné, je použita autentizace pomocí kryptografických klíčů se zaručením obdobné úrovně bezpečnosti nebo použití hesla s definovanými pravidly.
- Dodavatel bere na vědomí, že přístup k aktivům Objednatele je možné povolit pouze schválené technické identitě nebo identitě odvozené od fyzické identity zaměstnance dodavatele nebo poddodavatele s vygenerovaným jednoznačným identifikátorem a zaevidované v registru identit KZ, na základě požadavku Dodavatele na přístup. Pro zaevidování v registru identit je nezbytné sdělení osobních údajů: jméno, příjmení, rodné příjmení, pohlaví, datum narození, email, mobilní telefon nebo případně pevná linka. Dodavatel se zavazuje informovat své zaměstnance a poddodavatele, kterým bude přidělen přístup k aktivům Objednatele o účelu a způsobu zpracování jejich osobních údajů. Objednatel osobní údaje užije výhradně v souladu s platnou právní úpravou.
- Dodavatel je povinen zavést a dodržovat opatření fyzické bezpečnosti prostor nebo objektů, kde se nakládá s aktivy KZ nebo pro KZ podstatnými, včetně přepravních schrán, vozidel a přenosných médií.

Monitorování provozu

- Objednatel je oprávněn nepřetržitě zaznamenávat, monitorovat a vyhodnocovat přístup zaměstnanců a aktiv Dodavatele k vybraným chráněným interním informacím, k informačním a komunikačním systémům v souladu s PPK.
- Dodavatel je povinen na svém informačním systému a infrastruktuře, kterými plní předmět Smlouvy zajistit monitorování a zaznamenávání událostí nejméně v tomto rozsahu:
  a) úspěšné a neúspěšné přihlášení a odhlášení uživatelů nebo technických účtů;
  b) činnosti provedené administrátory;
  c) úspěšné a neúspěšné manipulace s účty, oprávněními a právy;
  d) neprovedení činností v důsledku nedostatku přístupových oprávnění;
  e) činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému;
  f) zahájení a ukončení činností technických aktiv;
  g) automatická varovná nebo chybová hlášení technických aktiv;
  h) mazání, změna, přesun, kopírování nebo nedostupnost KZ určených datových aktiv;
  i) přístupy k logům, pokusy o manipulaci s logy a změny nastavení nástroje pro zaznamenávání činností a použití mechanismů autentizace včetně změny údajů, které slouží k přihlášení

  a ke každé události v logu přiřadit nejméně tyto údaje: datum a čas; typ činnosti nebo události; identifikaci technického aktiva; identifikaci uživatele nebo jiného účtu; identifikaci síťového zařízení původce; úspěšnost nebo neúspěšnost provedení činnosti; klasifikaci závažnosti.
- Jestliže budou indikace některých provozních stavů nebo hodnot přenášeny mimo prostory KZ, předloží Dodavatel Objednateli ke schválení projekt takového přenosu, analýzu rizik a opatření k detekci selhání přenosu nebo ztráty viditelnosti aktiv.

Důvěrnost informací

- Dodavatel je povinen bez časového omezení zachovávat v tajnosti a nesdělit žádné třetí osobě žádné informace, které nejsou dosud legálně přístupné veřejnosti, tedy nejsou přístupné v důsledku jejich zveřejnění KZ, které se dozví o KZ, v souvislosti s ním, zejména žádné informace o jeho činnosti, organizaci, vnitřních poměrech, orgánech, zaměstnancích, veškeré informace obsažené v dokumentech nebo jiných písemnostech či materiálech, na datových nosičích, jakož i informace ústně předávané, jakkoliv související s KZ, její činností, bez ohledu na to, zda jsou nebo nejsou výslovně označené jako důvěrné informace; zejména veškeré poznatky provozní, technické povahy související s činností KZ; software, jeho nastavení, přístupová práva, stupně, úrovně a prostředky zabezpečení, diagnostika, dokumentace včetně příruček, návodů; vstupní a přístupová hesla, vnitřní předpisy a interní dokumenty KZ, informace týkající se vnitřního uspořádání KZ, kontrolních nebo bezpečnostních mechanismů a opatření, jakož i veškeré další informace, které jsou nebo budou označeny jako důvěrné informace.
- Dodavatel je povinen do 30 dnů od podpisu Smlouvy předložit analýzu potřebných nebo nezbytných zpracování osobních údajů jím nebo KZ a návrh, jak takové zpracování bude provedeno bezpečně a zákonně.
- Dodavatel je povinen ukládat veškerá data, včetně verzí kódu, testovacích dat a provozní dokumentace odděleně od svých provozních dat nebo dat jiných projektů tak, aby bylo kdykoliv možné tato data identifikovat, kontrolovat, řídit jejich zálohování, obnovu nebo ničení.
- Uložení chráněných informací KZ do datových úložišť, na přenosná média a případný transport médií je možné pouze po předchozím prokazatelném schválení KZ.
- V případě ukládání chráněných informací KZ do datových úložišť a na přenosná média má Dodavatel povinnost ukládat, případně vyžadovat uložení těchto dat v šifrované podobě a vést evidenci těchto médií.

- Jestliže Dodavatel při zajišťování podpory, například při odstraňování závady, vyjme ze zařízení Objednatele paměťové médium (nosič informací), nebo zařízení obsahující paměťové médium, je povinen postupovat podle pravidel a pokynů Objednatele pro převoz, používání a ničení nosičů informací. Dodavatel musí postupovat v součinnosti s Objednatelem a plně ho informovat o nakládání s daty na vyjmutém paměťovém médiu.
- Dodavatel je povinen zajistit likvidaci dat KZ ihned po pominutí účelu jejich zpracování nebo uložení. Likvidace dat musí být provedena způsobem dle standardu NIST 800-88 tak, aby po likvidaci dat na elektronickém médiu nebylo možné data obnovit. O provedení likvidací dat musí Dodavatel vést protokol nebo jiné záznamy ve formě schválené KZ.
- Dodavatel nesmí veřejně komentovat a/nebo negativně hodnotit KZ, svoji spolupráci s KZ či třetími osobami na základě Smlouvy, ani výsledky vzniklé na základě Smlouvy. Jakékoliv rozhovory a informace pro média týkající se předmětu Smlouvy nebo jejího plnění je Dodavatel oprávněn poskytnout pouze po předchozím písemném souhlasu KZ nebo na jeho výzvu.
- Dodavatel je povinen zachovávat mlčenlivost ohledně důvěrných informací a skutečností a osobních údajů i po ukončení Smlouvy.
- Dodavatel nesmí pořizovat jakékoli fotografie a/nebo obrazové, zvukové a/nebo zvukově obrazové záznamy v prostorách KZ nebo záznamy osob, které se jakýmkoli způsobem podílí na plnění Smlouvy.
- Po ukončení Smlouvy je Dodavatel povinen podle pokynů KZ předat anebo vrátit aktiva, která náleží KZ nebo byla KZ Dodavateli svěřena, zejména pak data a informace v jakékoliv podobě, nebo předložit důkaz o jejich bezpečné likvidaci v souladu se Smlouvou a příslušnými právními předpisy. Nosiče, zapůjčené Dodavateli, které informace nesou nebo nesly, a nejsou již potřebné, má Dodavatel povinnost bez odkladu vrátit KZ. Z vlastních nosičů musí Dodavatel uložené informace bezpečně, nenávratně a prokazatelně vymazat a toto vymazání písemně potvrdit KZ. Na výzvu KZ je Dodavatel povinen poskytnout spolehlivý důkaz o bezpečné likvidaci nosičů. Jestliže Objednatel nevydá pokyn ke vrácení nebo zničení dat a informací, je Dodavatel povinen si ho neprodleně vyžádat.
- Ujednání obsažená v samostatně uzavřené dohodě nebo smlouvě o mlčenlivosti nebo ochraně důvěrných, interních nebo neveřejných informací mezi účastníky Smlouvy tímto nejsou dotčena.

Vývoj, akvizice a údržba

- Jestliže bude součástí dodávky zařízení nebo podpory dodávka software nebo jiného typu kódu, je Dodavatel povinen:

a) zajistit, že budou použity předepsané a řádně licencované verze software nebo jiného kódu, které budou kompatibilní, interoperabilní a plně funkční v prostředí KZ;

b) zajistit, že plnění bude obsahovat jen ty součásti, které jsou nezbytné nebo potřebné a/nebo které jsou specifikovány výslovně ve Smlouvě;

c) zajistit zabezpečení systémů proti známým zranitelnostem a testování na takové zranitelnosti;

d) zajistit, že v produkčním prostředí KZ bude nasazen jen předmětem Smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění;

e) poskytnout KZ potřebnou součinnost v případě, že vyžaduje / realizuje provedení bezpečnostních testů souvisejících s předmětem plnění;

f) zajistit bezpečnost testovacího prostředí a ochranu poskytnutých testovacích dat poskytnutých KZ;

g) aplikovat zásady bezpečného vývoje a řízení životního cyklu systému v souladu s dobrou praxí, včetně užívání metod peer-review kódu, přičemž tato zásada musí být uplatněna také na konfigurační a obdobné změny;

h) zajišťovat kontroly integrity kódu a konfiguračních dat;

i) zajišťovat řízení přístupů ke kódu a konfiguračním datům;

j) zajišťovat penetrační testování v rozsahu stanoveném Objednatelem;

k) zajišťovat užívání vývojového, testovacího a zálohovacího prostředí odděleného od prostředí produkčního a prostředí svého vlastního dalšího provozu;

l) zajistit zabezpečení dodávaných systémů proti zneužití známých zranitelností a testování na takové zranitelnosti;

m) zajistit bezpečnou implementaci, inovaci, aktualizaci, testování technologií, které jsou předmětem plnění;

n) zajistit, aby migrace do provozního prostředí byla provedena až po akceptaci výsledků testů v testovacím prostředí a formalizovaném a doložitelném odsouhlasení;

o) zajistit, že budou dodrženy všechny zásady a povinnosti podle PPK.

- Jestliže bude součástí dodávky vývoj nebo úpravy kódu, je Dodavatel navíc povinen:

a) dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru dle doporučení technických norem řady ISO/IEC 27k;

b) pokud jsou softwarové auditní činnosti a předání zdrojového kódu k řešení součástí plnění dle Smlouvy, umožnit audit prováděného nebo provedeného plnění a na písemnou žádost předložit vyvíjený zdrojový kód ke code review;

c) předat zdrojový kód, je-li tak stanoveno ve Smlouvě, a to bezpečnou formou zajišťující jeho integritu a zajistit řízení verzí zdrojového kódu, zajistit zálohování zdrojového kódu a jeho uložení mimo produkční prostředí a zajistit, aby distribuce zdrojových kódů obsahovala soubor z vývojového prostředí na řízenou kompilaci těchto zdrojových kódů.

Audit dodavatele

- Objednatel má právo provést nebo nařídit provedení auditu Dodavatele.
- KZ alespoň 5 pracovních dnů předem oznámí Dodavateli provedení auditu. Obě strany projednají obsah, potřebnou součinnost a časový plán auditu. Objednatel bude postupovat tak, aby nad nezbytnou míru nenarušil provozní potřeby Dodavatele.
- V případě závažných důvodů (zejména při podezření na porušení Smlouvy, Standardu, Zákona nebo určené normy, případně při detekci rizikového chování Dodavatele) v souvislosti s plněním Smlouvy může Objednatel provést neohlášený audit u Dodavatele s přihlédnutím k provozní situaci Dodavatele.
- Dodavatel je povinen nápravná opatření realizovat v plném rozsahu nálezem zjištěných neshod, v požadovaném termínu.
- Záznamy, týkající se auditu jsou vždy označovány stejným identifikátorem. Jednotlivé záznamy auditů tvoří nejméně:

  a) plán auditu;

  b) oznámení o auditu;

  c) dotazník k auditu;

  d) zprávy nebo záznamy z auditních činností;

  e) zpráva z auditu;

  f) písemné, fotografické nebo jiné záznamy provozu, postupů nebo zařízení, které souvisí s auditem, pokud je to relevantní;

  g) záznam o zjištěních (závěrečná zpráva);

  h) návrhy nápravných opatření;

  i) dokumenty Dodavatele;

  j) záznam o projednání výsledků auditu;

  k) záznam o následné kontrole.
- Dodavatel obdrží k vyjádření závěrečnou zprávu auditu, navrhne nápravná opatření včetně termínů (plán nápravných opatření) a předá je Objednateli ke schválení. Pokud je Objednatel neschválí, vrátí s připomínkami Dodavateli k přepracování nebo stanoví plán nápravných opatření sám.

- Dodavatel je povinen v určeném čase zajistit realizaci plánu nápravných opatření a bez odkladu o tom předat zprávu KZ.

Kontaktní údaje

- Pokud je Dodavatel podle Standardu povinný oznamovat události, stavy, změny, incidenty, žádat o pokyny nebo pokud je třeba jakákoliv komunikace o Standardu nebo bezpečnostních aspektech plnění Smlouvy, užije tyto kontakty:

a) KZ_Ex_Kyberbezpecnost@kzcr.eu, +420 477 114 336

- Jestliže se nezdaří prokazatelná, dostatečná a efektivní komunikace s využitím uvedených kontaktů, využije Dodavatel bez odkladu spojení na operační středisko

a) +420 477 117 890

- Jakákoliv komunikace ve věci bezpečnosti Aktiv KZ musí být vedena jednoznačně, srozumitelně a prokazatelně. Jestliže je vedeno osobní jednání, může KZ stanovit, že se o něm pořídí písemný záznam.