# Příloha č. 12

**Bezpečnostní standard pro dodavatele programového vybavení**

**Krajské zdravotní, a.s.**

(verze KZ\_DEV2503\_108)

### OBECNÉ POVINNOSTI K ZAJIŠTĚNÍ SOULADU SE ZKB

* 1. Dodavatel je povinen dodržovat zásady bezpečnosti informací a kybernetické bezpečnosti v rozsahu ujednaném s Krajskou zdravotní, a.s. (dále také jen KZ) nebo zajištěním souladu s KZ určeným standardem nebo normou třetí strany. Za základní nepominutelný rámec normativní základny   
     a regulovaných okruhů povinností Dodavatele se považuje dokument Minimální bezpečnostní standard, dostupný na www.nukib.cz v sekci „Podpůrné materiály“. Dodavatel vždy užije platnou verzi tohoto dokumentu. Dodavatel musí všechna opatření k zajištění kybernetické bezpečnosti koncipovat v souladu s architekturou zákona o kybernetické bezpečnosti a jeho prováděcích vyhlášek, zejména s ustanoveními o bezpečnostních opatřeních.
  2. Základními okruhy povinností, doporučení a zásad dokumentu Minimální standard, které musí Dodavatel řádně a prokazatelně zavést a řídit nejpozději ke dni uzavření smlouvy, jsou:
     1. zavedení bezpečnostních politik,
     2. klasifikace a ochrana informací,
     3. řízení dodavatelů,
     4. řízení lidských zdrojů,
     5. řízení změn,
     6. řízení kontinuity činností,
     7. audit kybernetické bezpečnosti,
     8. fyzická bezpečnost,
     9. řízení přístupů,
     10. ochrana před škodlivým kódem,
     11. detekce bezpečnostních incidentů,
     12. řízení reakce na bezpečnostní incidenty,
     13. aplikační bezpečnost,
     14. kryptografická ochrana,
     15. zajišťování dostupnosti informací,
     16. zálohování.
  3. Dodavatel nebude postupovat v rozporu s publikovanými doporučeními, varováními a podpůrnými materiály, dostupnými na www.govcert.cz, www.nukib.cz nebo www.kzcr.eu.
  4. 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.
  5. Dodavatel je povinen udržovat užívanou infrastrukturu a služby v bezvadném stavu tak, aby umožňovaly řádné plnění smlouvy a tento bezvadný stav průběžně monitorovat.
  6. 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.
  7. Dodavatele je povinen bez odkladu informovat KZ o všech zahájených řízeních, která mohou mít vliv na jeho schopnost plnit v ujedeném rozsahu a kvalitě smlouvu.
  8. 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 obdobné změnách, které mohou mít vliv na jeho schopnost plnit v ujedeném rozsahu a kvalitě smlouvu.
  9. Dodavatel je povinen pro komunikaci a předávání dat/aktiv využívat pouze předem schválené komunikační a přenosové kanály.
  10. 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 potřebné pro zajištění podpory, údržby nebo oprav.
  11. Dodavatel bere na vědomí, že může být KZ určen jako významný dodavatel ve smyslu zákona   
      o kybernetické bezpečnosti. Jestliže k takovému určení a oznámení dojde, zavede dodavatel bez výhrad všechna určená opatření, vyžadovaná KZ v souladu se zákonem pro významné dodavatele. Opatření Dodavatel zavede v termínu stanoveném KZ.

### Specifické povinnosti dodavatele

* 1. 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.
  2. 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.
  3. 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. Za splnění této povinnosti se považuje také odpovídající certifikace podle zákona o kybernetické bezpečnosti a jeho prováděcích vyhlášek. Dodavatel může navrhnout, že se užije jiný standard, který zajistí stejnou nebo vyšší úroveň ochrany aktiv KZ.
  4. Dodavatel je povinen získat a po celou dobu platnosti smlouvy udržovat v platnosti certifikace všech výrobců nebo dodavatelů hardwaru nebo softwaru využitého pro dodávku nebo provádění podpory, jestliže to tyto osoby vyžadují pro legální užití jejich dodávky nebo pro bezvadnou záruku. Tato povinnost platí také pro fyzické osoby vykonávající činnosti podle smlouvy.
  5. Dodavatel nesmí používat v infrastruktuře nebo při přistupování k infrastruktuře KZ keyloggery, 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 schválena.
  6. Dodavatel musí zajistit, aby s využitím jemu svěřených oprávnění nebo jím vytvořené příležitosti nikdo před předchozím písemným souhlasem nepřistupoval k aktivům KZ včetně sítí, manipuloval s nimi, prováděl na nich změny nebo na nich spouštěl nebo instaloval software.
  7. Dodavatel musí zajistit, aby s využitím jemu svěřených oprávnění nebo jím vytvořené příležitosti nikdo před předchozího písemného souhlasu nepřistupoval k aktivům KZ včetně sítí, manipuloval s nimi, prováděl na nich změny nebo na nich spouštěl nebo instaloval software.
  8. Dodavatel nesmí bez předchozího písemného souhlasu KZ na aktivech KZ provádět bezpečnostní testování, skenování, zachytávání provozu, replikaci provozu, replikaci nebo zálohy dat, nebo jakékoliv další činnosti, které mohou mít vliv na stav kybernetické bezpečnosti.
  9. Dodavatel nesmí na aktivech KZ provádět konfigurační změny bez předchozího souhlasu KZ.
  10. Dodavatel nesmí na aktivech KZ, včetně dodavatelem instalovaných, spravovaných nebo podporovaných aktiv, bez předchozího souhlasu KZ vytvářet, měnil nebo rušil identity nebo účty jakéhokoliv typu.
  11. 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.
  12. 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.
  13. Dodavatel je povinen zajistit respektování pravidel fyzické bezpečnosti při pohybu v prostorách KZ.
  14. 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.
  15. Dodavatel je povinen zajistit spolupráci při řešení incidentů, hrozeb, zranitelností a patchování.
  16. Dodavatel je povinen mít zavedené mechanismy pro detekci bezpečnostních událostí, bezpečnostních incidentů a odchylek.
  17. 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“ musí být nastaven tak, aby byl provoz povolen pouze směrem z DMZ do vnitřní sítě dodavatele.
  18. Dodavatel je povinen zcela dodržovat technické a bezpečnostní standardy KZ nebo jiné osoby, které jsou uvedeny ve smlouvě nebo jiném dokumentu, zejména dokumentu KZ06\_SM0010 Požadavky na provedení a kvalitu ICT (dále také jen PPK).

### Vývoj, akvizice a údržba

* 1. Dodavatel je povinen:
     1. zavést a řádně udržovat a řídit oddělené prostředí pro vývoj a testování;
     2. zajistit, že budou použity předepsané a řádně licencované verze softwaru nebo jiného kódu, které budou kompatibilní, interoperabilní a plně funkční v prostředí KZ;
     3. zajistit, že plnění bude obsahovat jen ty součásti, které jsou nezbytné nebo potřebné a/nebo které jsou specifikovány výslovně ve smlouvě;
     4. zajistit zabezpečení aktiv užitých pro vývoj a testování proti známým zranitelnostem a testování na takové zranitelnosti po celou dobu trvání smlouvy;
     5. zajistit zabezpečení dodávaných aktiv proti zneužití známých zranitelností a testování na takové zranitelnosti po celou dobu trvání smlouvy;
     6. zajistit, že v produkčním prostředí KZ bude nasazen jen předmětem smlouvy specifikovaný kompilovaný, respektive spustitelný kód a další nezbytná data pro provozování předmětu plnění;
     7. poskytnout KZ potřebnou součinnost v případě, že vyžaduje / realizuje provedení bezpečnostních testů souvisejících s předmětem plnění;
     8. zajistit bezpečnost testovacího prostředí a ochranu poskytnutých testovacích dat poskytnutých KZ;
     9. 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;
     10. zajišťovat kontroly integrity kódu a konfiguračních dat;
     11. zajišťovat řízení přístupů ke kódu a konfiguračním datům;
     12. zajišťovat penetrační testování v rozsahu stanoveném KZ m;
     13. zajišťovat užívání vývojového, testovacího a zálohovacího prostředí odděleného od prostředí produkčního a prostředí svého vlastního dalšího provozu;
     14. zajistit bezpečnou implementaci, inovaci, aktualizaci, testování technologií, které jsou předmětem plnění;
     15. zajistit, aby migrace do provozního prostředí byla provedena až po akceptaci výsledků testů   
         v testovacím prostředí a formalizovaném a doložitelném odsouhlasení;
     16. dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru dle doporučení technických norem řady ISO/IEC 27k;
     17. umožnit audit prováděného nebo provedeného plnění a na písemnou žádost předložit vyvíjený zdrojový kód ke code review, včetně aktualizací a diagnostických nástrojů;
     18. předat ujednaným způsobem zdrojový kód nebo ho uložit do sjednané úschovy, jak je stanoveno ve smlouvě, a to bezpečnou formou zajištující 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.

### Užívání kryptografické ochrany

* 1. Pokud je v rámci plnění smlouvy vyžadováno použití kryptografických prostředků, užije dodavatel standard, uvedený v dokumentu PPK.

### Řízení provozu a přístupu

* 1. Dodavatel je povinen zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění v souladu s požadavky vyhlášky o kybernetické bezpečnosti ve znění pozdějších předpisů.
  2. Na vyžádání je dodavatel poskytnout KZ přehled o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře, kterými plní předmět smlouvy.
  3. 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.
  4. 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 Zadavatelem. Zařízení musí být vybaveno schopností odesílat logy a alerty do bezpečnostních a dohledových systémů Zadavatele. 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 zadavatele, v souladu s jeho interními standardy, obecně závaznými právními normami   
     a určenými technickými standardy.
  5. 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.
  6. Dodavatel zajistí dodržování zásady okamžitého odhlašování účtů a minimalizace činností.
  7. Každý zaměstnanec dodavatele, který přistupuje k aktivům KZ, má u KZ přidělen a evidován jedinečný uživatelský účet, kterému jsou v jednotlivých systémech nebo aplikacích přiřazeny specifické role související výhradně s plněním předmětu smlouvy.
  8. 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.
  9. Dodavatel bere na vědomí, že přístup k aktivům dodavatele 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, e-mail, mobilní telefon nebo případně pevná linka. Dodavatel se zavazuje informovat své zaměstnance a poddodavatele, kterým bude přidělen přístup k aktivům KZ, o účelu a způsobu zpracování jejich osobních údajů. Objednatel osobní údaje užije výhradně v souladu s platnou právní úpravou.
  10. 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

* 1. KZ je oprávněna nepřetržitě zaznamenávat, monitorovat a vyhodnocovat přístup zaměstnanců a aktiv dodavatele k vybraným chráněným interním informacím, k informačním a komunikačním systémům.
  2. Dodavatel je povinen na svém informačním systému a infrastruktuře, kterými plní předmět smlouvy, zajistit monitorování a zaznamenávání událostí nejméně v tomto rozsahu:
     1. úspěšné a neúspěšné přihlášení a odhlášení uživatelů nebo technických účtů;
     2. činnosti provedené administrátory;
     3. úspěšné a neúspěšné manipulace s účty, oprávněními a právy;
     4. neprovedení činností v důsledku nedostatku přístupových oprávnění;
     5. činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému;
     6. zahájení a ukončení činností technických aktiv;
     7. automatická varovná nebo chybová hlášení technických aktiv;
     8. mazání, změna, přesun, kopírování nebo nedostupnost KZ určených datových aktiv;
     9. 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.

* 1. Všechna dodaná aktiva musí podporovat monitorování a logování v souladu s dokumentem PPK a musí být interoperabilní se zavedeným SIEM.
  2. Jestliže budou indikace některých provozních stavů nebo hodnot přenášeny mimo prostory KZ, předloží dodavatel KZ ke schválení projekt takového přenosu, analýzu rizik a opatření k detekci selhání přenosu nebo ztráty viditelnosti aktiv.

### Dodávky hardware

* 1. Jestliže dodavatel při zajišťování podpory, například při odstraňování závady, dodá KZ 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.
  2. Jestliže dodavatel je předá KZ paměťové médium, zejména k provedení potřebných činností při správě dodaného aktiva, není povinností KZ toto paměťové médium dodavateli vracet, a leda že by to bylo zcela bezpečné a nebyly by s takovým vrácením spojeny náklady KZ, například na bezpečné zničení dat.

### Oznamování incidentů

* 1. 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.
  2. 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.
  3. 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.

### Personální bezpečnost

* 1. 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.
  2. 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.
  3. Dodavatel musí určit osoby odpovědné za realizaci jednotlivých činností, které jsou v plánu uvedeny.
  4. Dodavatel v souladu s plánem rozvoje bezpečnostního povědomí specificky zajišťuje poučení a školení uživatelů, administrátorů, osob zastávajících bezpečnostní role a poddodavatelů o jejich povinnostech, oprávněních a o bezpečnostní politice.
  5. Dodavatel pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje pravidelná odborná školení včetně praktického procvičování.
  6. Dodavatel je povinen zajistit prokazatelné proškolení zaměstnanců a třetích stran o zajištění bezpečnosti plynoucí z uzavřené smlouvy.
  7. 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.
  8. Dodavatel hodnotí účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených se zlepšováním bezpečnostního povědomí.
  9. Dodavatel vede o provedených školeních přehledy, které obsahují předmět školení, obsah školení, identifikaci lektora nebo technického řešení a seznam osob, které školení absolvovaly.
  10. Dodavatel je povinen zavést a udržovat pohotovostní plány pro případy neplánovaného přerušení nebo omezení činnosti nebo selhání určených rolí vykonávaných zaměstnanci, zejména pokud je potřebné pro zajištění podpory, údržby nebo oprav. Dodavatel je povinen udržovat je po celou dobu platnosti smlouvy počet a kvalifikaci zaměstnanců potřebných pro plnění smlouvy na takové úrovni, aby nedostupnost některého ze zaměstnanců, například z důvodu nemoci nebo ukončení pracovního poměru, nemohla způsobit neschopnost dodavatele plnit řádně povinnosti dané smlouvou nebo jejími přílohami, a to zejména v oblastech vývoje, řízení změn a poskytování podpory.
  11. 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.
  12. Dodavatel v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajišťuje předání odpovědností.
  13. Dodavatel určuje pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.
  14. Dodavatel alespoň jednou ročně předává KZ informace týkající se osob souvisejících s poskytovaným předmětem plnění smlouvy o provedených školeních a jejich obsahu.
  15. 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 bezpečnosti poddodavatelů

* 1. Dodavatel smí pro potřeby plnění smlouvy používat pouze KZ schválené poddodavatele.
  2. 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.
  3. 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.
  4. 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.
  5. Dodavatel je povinen předávat KZ informaci o změnách dodavatelů svého poddodavatele, jestliže takové změny mohou mít vliv na stav kybernetické bezpečnosti aktiv KZ.

### Audit dodavatele

* 1. KZ má právo provést nebo nařídit provedení auditu dodavatele.
  2. KZ alespoň 5 pracovních dnů předem oznámí dodavateli provedení auditu. Obě strany projednají obsah, potřebnou součinnost a časový plán auditu. KZ bude postupovat tak, aby nad nezbytnou míru nenarušil provozní potřeby dodavatele.
  3. 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 této smlouvy může KZ provést neohlášený audit u dodavatele s přihlédnutím k provozní situaci dodavatele.
  4. Dodavatel je povinen nápravná opatření realizovat v plném rozsahu nálezem zjištěných neshod,   
     v požadovaném termínu.
  5. Záznamy týkající se auditu jsou vždy označeny stejným identifikátorem.
  6. Jednotlivé záznamy auditů tvoří nejméně:
     1. plán auditu
     2. oznámení o auditu;
     3. dotazník k auditu;
     4. zprávy nebo záznamy z auditních činností;
     5. zpráva z auditu;
     6. písemné, fotografické nebo jiné záznamy provozu, postupů nebo zařízení, které souvisí s auditem, pokud je to relevantní;
     7. záznam o zjištěních (závěrečná zpráva);
     8. návrhy nápravných opatření;
     9. dokumenty dodavatele;
     10. záznam o projednání výsledků auditu;
     11. záznam o následné kontrole.
  7. Dodavatel obdrží k vyjádření závěrečnou zprávu auditu, navrhne nápravná opatření včetně termínů (plán nápravných opatření) a předá je KZ ke schválení. Pokud je KZ neschválí, vrátí s připomínkami dodavateli k přepracování nebo stanoví plán nápravných opatření sám.
  8. Dodavatel je povinen v určeném čase zajistit realizaci plánu nápravných opatření a bez odkladu o tom zprávu KZ.

### Důvěrnost dat

* 1. 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 kdykoli možná tato data identifikovat, kontrolovat, řídit jejich zálohování, obnovu nebo ničení.
  2. Uložení chráněných informací KZ do datových úložišť, na přenosná média a případný transport médií je možný pouze po předchozím prokazatelném schválení KZ.
  3. 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.
  4. Jestliže Dodavatel při zajišťování podpory, například při odstraňování závady, vyjme ze zařízení KZ paměťové médium (nosič informací) nebo zařízení obsahující paměťové médium, je povinen postupovat podle pravidel a pokynů KZ pro převoz, používání a ničení nosičů informací. Dodavatel musí postupovat v součinnosti s KZ a plně ho informovat o nakládání s daty na vyjmutém paměťovém médiu.
  5. Dodavatel je povinen zajistit likvidaci dat KZ ihned po pominutí účelu jejich zpracování nebo uložení. Likvidace dat musí být provedena způsobem dle standardu určeného KZ tak, aby po likvidaci dat na elektronickém médiu nebylo možné data obnovit. O provedení likvidace dat musí Dodavatel vést protokol nebo jiné záznamy ve formě schválené KZ.
  6. 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 jakékoli podobě, nebo předložit důkaz o jejich bezpečné likvidaci v souladu s 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.