10.7 Řízení dodavatelů

Tento dokument popisuje opatření, které MUSÍ nebo BY MĚLO být implementováno pro:

- **Zajištění ochrany IT a/nebo informačních aktiv organizace, které jsou přístupné dodavatelům.**
- **Udržování dohodnuté úrovně informační bezpečnosti a dodávky služeb v souladu s dodavatelskými dohodami.**
- **Předejití nejčastějších problémů vznikajících při využívání externích služeb, např. vendor lock-in, nedostatečná ochrana poskytnutých informací, nedostatečná bezpečnostní opatření při správě systému/ů atd.**
- **Směrnice je platná pro významné dodavatele. Pro ostatní dodavatele má pouze doporučující povahu.**

Tento dokument je vyhotoven v souladu s Vyhláškou o kybernetické bezpečnosti (VKB) – Řízení dodavatelů (§ 8).

1 Pravidla a principy pro výběr dodavatelů

Cíl: Zajistit ochranu IT informačních aktiv společnost, ke kterým mají přístup významní dodavatelé. Významný dodavatel je každý, kdo s povinnou osobou vstupuje do právního vztahu a je významný z hlediska bezpečnosti informačního a komunikačního systému.

1.1 Politika kybernetické bezpečnosti pro oblast vztahů s dodavateli

Požadavky kybernetické a informační bezpečnosti pro zmírnění rizik spojených s přístupem dodavatelů k IT a/nebo k informačním aktivům společnosti MUSÍ být s dodavatelem dohodnuty a zdokumentovány.

Implementační pokyny:

1.1.1 MUSÍ být zohledněny požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnuty do smlouvy uzavřené s dodavatelem.

1.1.2 Společnost MUSÍ stanovit pravidla pro významné dodavatele, která zohledňují požadavky VKB, které pokrývají veškerý hosting dat a podpůrná zařízení, na kterých jsou ukládány, zpracovávány nebo přenášeny informace společnosti.

1.1.3 Společnost MUSÍ poučit významné dodavatele o jejich povinnostech a o bezpečnostní politice (seznamovat konkrétní osoby dodavatele s bezpečnostními politikami a pravidly) a následně kontrolovat jejich dodržování.

1.1.4 Společnost MUSÍ vést evidenci svých významných dodavatelů a MUSÍ je prokazatelně písemně informovat o jejich evidenci.

1.1.5 Prokazatelné informování MUSÍ obsahovat:

a) identifikace správce (určuje účel zpracování informací a podmínky provozování informačního systému) nebo provozovatele (zajišťuje funkčnost technických a programových prostředků tvořících informační nebo komunikační systém),

b) identifikace informačního a komunikačního systému,

c) identifikace významného dodavatele,
d) vyrozumění o skutečnosti, že dodavatel je pro správce významným dodavatelem a popřípadě také o tom, že významný dodavatel je zároveň provozovatelem.

1.1.6 Dodavatel i odběratel MUSÍ umožnit bezpečnostní audit.

1.1.7 Dodavatelé IT služeb MUSÍ provádět kontroly shody s technickými požadavky uvedenými ve smlouvě a poskytovat odpovídající hlášení těchto technických kontrol.

1.1.8 Společnost MUSÍ v případě, že podmínky jejich smluvního vztahu uzavřeného s dodavatelem pro jejich informační nebo komunikační systém nesplňují požadavky podle zákona č. 181/2014 Sb. (zákon o kybernetické bezpečnosti) uvést smluvní vztah do souladu s těmito požadavky do 1 roku ode dne nabytí účinnosti tohoto zákona.

1.1.9 Je-li dodavatel vybírán prostřednictvím zadávacího řízení podle zákon č. 134/2016 Sb. (zákon o zadávání veřejných zakázek) pak MUSÍ být požadavky VKB promítnuty i do zadávacích podmínek.

1.1.10 Volba konkrétní úrovně zabezpečení systémů a konkrétních bezpečnostních opatření MUSÍ být založena především na řádně provedené analýze aktiv a s nimi souvisejících rizik a je výlučně v odpovědnosti zadavatele, který si svůj postup MUSÍ řádně odůvodnit.

1.1.11 Při zadávání veřejných zakázek v oblasti kybernetické bezpečnosti MŮŽE společnost vycházet z metodického materiálu NÚKIB *Zadávání veřejných zakázek v oblasti ICT a kybernetická bezpečnost* (1).

1.1.12 V případě zajištění osoby provádějící audit či osoby odpovědné za kybernetickou bezpečnost externími dodavateli by se NEMĚLI uzavírat smlouvy na tyto 2 role se stejnými dodavateli či s dodavateli zajišťujícími provozní a servisní činnosti interních informačních nebo komunikačních systémů v organizaci.

1.1.13 Společnost MŮŽE pověřit provozováním informačního systému kritické informační infrastruktury jiný orgán nebo osobu, pokud to jiný zákon nevylučuje. Pověřený provozovatel, který byl prokazatelně informován MUSÍ hlásit kontaktní údaje pomocí kontaktního formuláře (2).

2 Pravidla pro hodnocení rizik souvisejících s dodavateli

Společnost MUSÍ řídit rizika spojená s dodavateli.

Implementační pokyny:

2.1.1 Významný dodavatel MUSÍ v rámci výběrového řízení a před uzavřením smlouvy provést hodnocení rizik souvisejících s plněním předmětu výběrového řízení přiměřeně v souladu s VKB.

2.1.2 Významný dodavatel MUSÍ provádět pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných plnění pomocí vlastních zdrojů nebo pomocí třetí strany.

2.1.3 Významný dodavatel MUSÍ v reakci na rizika a zjištěné nedostatky zajistí jejich řešení.

2.2 Řetězec dodavatelů informačních a komunikačních technologií

Smlouvy s dodavateli BY MĚLY zahrnovat požadavky na identifikování a řízení rizik kybernetické a informační bezpečnosti souvisejících se službami informačních a komunikačních technologií s ohledem na dodavatelské řetězce zúčastněné při dodávkách souvisejících služeb.

Implementační pokyny:

2.2.1 MUSÍ být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi společností a dodavatelem a nebudou v rozporu s požadavky společnosti na dodavatele.

2.2.2 Smlouvy s dodavateli služeb informačních a komunikačních technologií BY MĚLY zahrnovat dodatečné požadavky na kybernetickou a informační bezpečnost (nad rámec těch, které jsou zmíněné v kapitole 3.2), které jsou odlišné pro nově získávané produkty/služby informačních a komunikačních technologií, pokud je to relevantní.

2.2.3 Smlouvy s dodavateli BY MĚLY požadovat, aby dodavatel začlenil požadavky společnosti do svého dodavatelského řetězce v případě, že:

a) dodavatel řeší poskytování částí informačních a komunikačních služeb pro společnosti pomocí subdodávek,

b) služby informačních a komunikačních technologií pro společnosti zahrnují komponenty získané od dalších dodavatelů.

2.2.4 Služby informačních a komunikačních technologií, které jsou pro společnosti kritické, MUSÍ být identifikovány a MUSÍ pro ně být nastaven proces monitorování.

2.2.5 MĚLY BY být nastaveny postupy pro správu rizik bezpečnosti informací, spojené s komponenty či softwarem, které již nejsou podporovány nebo poskytovány dodavateli/výrobci kvůli technologickému pokroku.

2.2.6 K minimalizaci rizik MŮŽE být využit Supply Chain Risk Management (Řízení rizik dodavatelského řetězce) podle NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations (3).

3 Náležitosti smlouvy o úrovni služeb a způsobů a úrovní realizace bezpečnostních opatření a o určení vzájemné smluvní odpovědnosti

Cíl: Vytvořit vhodnou smlouvu s významnými dodavateli v souladu s požadavky VKB. Pro obsah smluv s ostatními dodavateli mají implementační pokyny doporučující povahu. I v případě, že je stanovena povinnost zařadit taková ustanovení do smlouvy s významným dodavatelem, lze některé požadavky označit za nerelevantní pro danou smlouvu prostřednictvím prohlášení o aplikovatelnosti.

Implementační pokyny:

3.1.1 Náležitosti smlouvy s významným dodavatelem MUSÍ vycházet z přílohy č. 7 VKB. Požadavky i s vysvětlením jsou uvedeny v příloze C.

3.1.2 Společnost MUSÍ pravidelně přezkoumávat plnění smluv s významnými dodavateli shody s VKB.

3.2 Řešení bezpečnosti v rámci smluv s dodavateli

Veškeré důležité požadavky informační bezpečnosti MUSÍ být nastaveny a dohodnuty s každým významným dodavatelem, který může přistupovat k informacím společnosti, zpracovávat je, ukládat nebo sdělovat, nebo poskytuje komponenty/služby IT infrastruktury.

Implementační pokyny:

3.2.1 Požadavky pro zmírnění rizik kybernetické a informační bezpečnosti spojené s přístupem dodavatele k informacím společnosti MUSÍ být zdokumentovány, dohodnuty a vzájemně odsouhlaseny v dodavatelských smlouvách.

3.2.2 Významný dodavatel MUSÍ v rámci uzavíraných smluvních vztahů stanovit způsoby a úrovně realizace bezpečnostních opatření a určit obsah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.

3.2.3 Společnost BY MĚLA s dodavatelem uzavřít smlouvu SLA (Service Level Agreement) - Dohoda o úrovni poskytovaných služeb. Jedná se o dokument, který vymezuje smluvní vztah mezi dodavatelem a odběratelem IT služby, tj. jaké služby je dodavatel povinen poskytovat uživateli, v jakém objemu a kvalitě a kolik za ně odběratel zaplatí.

3.2.4 Dodavatelské smlouvy BY MĚLY vyžadovat od dodavatelů, aby poskytli aktuální zprávu potvrzující, že jsou splněny požadavky na kybernetickou a informační bezpečnost definované v SLA.

3.2.5 SLA definuje rozsah, úroveň a kvalitu služby, například:

- Garantovanou časovou dostupnost (např. 24*7–24 hodin, 7 dnů v týdnu a 365 dní v roce)
- Garantovanou cenu
- Garantovanou rychlost řešení potíží se službou (např. do 30 minut po oznámení problému)

3.2.6 Struktura dokumentu SLA:

- Smluvní strany,
- Odkaz na rámcovou smlouvu,
- Předmět smlouvy – definice poskytovaných služeb,
- Objemové charakteristiky služby,
- Kvalitativní charakteristiky služby,
- Monitorování a reporting,
- Cena, slevy, sankce a bonusy,
- Fakturace a platební kalendář,
- Modifikace a upgrade služby,
- Záruky,
- Procedury řešení problémů a součinnost zákazníka,
- Odpovědnost za ztráty a škody,
- Duševní vlastnictví a autorská práva,
- Důvěrnost informací,
- Vyšší moc,
- Trvání smlouvy,
- Změny smlouvy,

- Ukončení smlouvy,
- Právo, kterým se smlouva řídí,
- Terminologický slovník.

3.2.7 Společnost MŮŽE uzavřít OLA (Operational Level Agreement) - Dohoda o úrovni poskytovaných vnitřních služeb. OLA je dokument, který vymezuje vnitřní smluvní vztah v rámci organizace na bázi IT služby. Cílem OLA je předložit jasný, stručný a měřitelný popis vztahů vnitřní podpory poskytovaných služeb. Dohoda popisuje odpovědnosti každé interní podpůrné skupiny vůči ostatním podpůrným skupinám, včetně procesu a časového rámce pro poskytování jejich služeb.

3.2.8 Společnost MŮŽE s dodavateli uzavřít Dohodu o mlčenlivosti (NDA) nebo Dohodu o důvěrnosti.

3.2.9 Správné NDA by mělo obsahovat zejména následující:

- rozsah citlivých informací, které si přejete ochránit;
- okruh osob, kterým může dodavatel citlivé informace sdělit;
- dobu, po kterou se dodavatel zaváže k mlčenlivosti; a
- smluvní pokutu, kterou bude muset dodavatel zaplatit, pokud povinnost mlčenlivosti poruší.

4 Pravidla pro provádění kontroly zavedení bezpečnostních opatření

Cíl: Udržovat dohodnuté úrovně kybernetické a informační bezpečnosti a dodávky služeb v souladu s dodavatelskými smlouvami.

4.1 Monitorování a přezkoumávání služeb dodavatelů

Společnost BY MĚLA pravidelně monitorovat, kontrolovat a provádět audit dodávky dodavatelských služeb.

Implementační pokyny:

4.1.1 Proces řízení vztahů mezi organizací a dodavatelem BY MĚL být nastaven pro:

a) monitorování úrovní výkonu služeb za účelem ověření dodržování smluv (pravidelná kontrola plnění SLA – například viz. tabulka Hodnocení dodavatelů),
b) přezkoumání servisních a, pokud je to relevantní, i bezpečnostních zpráv poskytovaných dodavatelem a průběžnou vzájemnou koordinaci,
c) provádění auditů dodavatelů ve spojení s přezkoumáním zpráv nezávislých auditorů, pokud jsou k dispozici, a navázání na identifikované problémy,
d) poskytování informací o incidentech kybernetické a informační bezpečnosti a přezkoumání těchto informací,
e) řízení dodavatelů řešením identifikovaných problémů, které by mohly vést ke vzniku rizik pro společnost.

4.1.2 MĚLA BY být udržována průběžná transparentnost bezpečnostních aktivit dodavatele, včetně činností týkajících se:

a) řízení změn,
b) řízení technických zranitelností,

c) řízení incidentů kybernetické a informační bezpečnosti.

4.1.3 Společnost MUSÍ zajistit, že dodavatelé budou oznamovat neobvyklé chování informačního a komunikačního systému a podezření na jakékoliv zranitelnosti.

4.1.4 Podmínky pro audit u dodavatele BY MĚLY být ukotveny ve smlouvě.

4.1.5 Společnost MŮŽE požadovat audit dodavatele nezávislou třetí stranou nebo MŮŽE spoléhám se na jeho deklarace/prohlášení či na jeho certifikaci.

4.1.6 Společnost MŮŽE po dodavateli požadovat doložení souladu – např. předložení auditních reportů, vyplnění dotazníků, checklistů apod.

4.2 Řízení změn služeb dodavatelů

Změny v poskytování služeb dodavateli, včetně udržování a vylepšování stávajících politik, postupů a opatření bezpečnosti informací (pokud to bylo dohodnuto) BY MĚLY být spravovány s ohledem na kritičnost firemních informací, systémů a procesů, kterých se týkají, a pokud je to relevantní, MĚLA BY být přehodnocena rizika.

Implementační pokyny:

4.2.1 Změny dodavatelských smluv BY MĚLY být řešeny prostřednictvím formálních postupů řízení změn, které zahrnují posouzení případných souvisejících rizik.

4.2.2 Významné změny týkající se dodavatelských služeb s potenciálním negativním dopadem na společnost nebo potenciálním bezpečnostním rizikem pro společnost BY MĚLY být přezkoumány a schváleny v rámci standardních schůzek s dodavatelem, včetně:

a) použití nových technologií,
b) změn fyzického místa poskytování služby,
c) změn dodavatele nebo sub-dodavatele na jiného dodavatele.

4.2.3 Jakékoliv změny týkající se požadavků na bezpečnost, které byly specificky zahrnuty ve smlouvách, MUSÍ být formálně schváleny Výborem pro KB.

5 Pravidla pro hodnocení dodavatelů

Společnost si MUSÍ stanovit postupy a zásady hodnocení dodavatelů.

5.1.1 Kritéria kvantitativní MŮŽOU být například:

A. Dodavatelé jednotlivých typů produktů:

- kvalita dodávaných produktů,
- plnění požadovaných termínů,
- cena,
- flexibilita při změně požadavku na dodávku během dodací doby,
- průběh reklamačního řízení,
- úroveň zavedeného systému řízení kvality.

B. Dodavatelé – náhradní díly:

- kvalita dodávaných dílů,

- plnění požadovaných termínů,
- cena,
- požadovaný stupeň dokonalosti dokumentace,
- spolupráce během spolupráce,
- termín opravy dílů po jejich reklamaci,
- úroveň zavedeného systému řízení kvality.

5.1.2 Kritéria kvalitativní MŮŽOU být například:

- Kvalitativní kritéria slouží k evidenci a sledování environmentálních a bezpečnostních aspektů u jednotlivých dodavatelů.

5.1.3 Kritéria pro dodavatele MŮŽOU být například:

- sledování Environmentálního aspektu (viz tabulky),
- sledování Bezpečnostního aspektu.

5.1.4 Hodnocení dodavatelů se MŮŽE provádět pololetně v tabulkové formě (viz příloha B), přičemž se využívá bodové hodnocení jednotlivých relevantních kvantitativních kritérií podle následující stupnice:

1 - výborný,
2 - velmi dobrý,
3 - dobrý (průměrný),
4 - podprůměrný,
5 - nekvalitní

5.1.5 Hodnocení / sledování kvalitativních kritérií:

A - ano (je třeba sledovat a vyhodnocovat kvalitu tohoto aspektu u dodavatele)
N - ne (tento aspekt je pro naše dodávky a plnění kvality nesignifikantní u dodavatele a nebude specificky sledován)

5.1.6 Na základě hodnocení se určuje pořadí kvality dodavatelů pro následující půlrok a na základě tohoto pořadí se dodavatelé určují.

Použité zdroje

(1) *ZADÁVÁNÍ VEŘEJNÝCH ZAKÁZEK V OBLASTI ICT A KYBERNETICKÁ BEZPEČNOST: Metodický materiál* [online]. Verze 1.3. Brno: NÚKIB, 2020 [cit. 2022-04-18]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

(2) *Hlášení kontaktních údajů* [online]. In: . NÚKIB [cit. 2022-04-20].

(3) *SP 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. Revision 1. Gaithersburg: NIST, 2015.

(4) ČESKÁ REPUBLIKA. Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti. In: *Sbírka zákonů*. 2018, Ročník 2018, Částka 43, č. 82. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=82&r=2018

Příloha A Interpretace klíčových slov

Klíčové slovo	Interpretace
MUSÍ	Naprostý požadavek (**bez výjimek**).
NESMÍ	Naprostý zákaz (**bez výjimek**).
MĚLY BY	Doporučený požadavek, mohou existovat platné důvody pro částečné nebo úplné odchýlení od uvedeného, ale MUSÍ být pochopeny a pečlivě zváženy plné důsledky takového chování dříve, než dojde k volbě odlišného postupu (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
NEMĚLO BY	Doporučený zákaz, záporná forma MĚLO BY (**výjimky jsou možné po zhodnocení rizik a přijetí zbytkových rizik**).
MŮŽE	Plně volitelné (není sledováno v rámci monitorování shody)

Příloha B Hodnocení dodavatelů

	Hodnocení dodavatelů								
Služba:									
Název firmy nebo osoby	jakost	Systém jakosti	flexibilita	cena	spolehlivost	dodržování termínů	bodů	hodnocení	
									Datum hodnocení
									Jméno a podpis
Pro období							Schválil		
									Datum hodnocení
									Jméno a podpis
Pro období							Schválil		
									Datum hodnocení
									Jméno a podpis
Pro období							Schválil		
									Datum hodnocení
									Jméno a podpis
Pro období							Schválil		

Příloha C Smluvní požadavky kybernetické a informační bezpečnosti a jejich výklad

Při uzavírání smlouvy s dodavatelem s ohledem na jeho důležitost společnost MUSÍ zvážit, které z následujících oblastí jsou relevantní a ty zohlednit ve smlouvě (obsah přílohy č. 7 vyhlášky o kybernetické bezpečnosti):

Požadavek přílohy č. 7 vyhlášky o kybernetické bezpečnosti	Výklad požadavku
Ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity)	Jedná se o ustanovení smlouvy, které reflektuje, zejména, s jakými informacemi dodavatel nakládá a jakým způsobem tak má činit z pohledu důvěrnosti, dostupnosti a integrity (např. pro provozní údaje tzv. logy je klíčová integrita; pro osobní údaje či obchodní tajemství je klíčová zejména důvěrnost apod.). Minimální úrovní splnění tohoto požadavku je ustanovení o uložení těchto dat v souladu s účelem smlouvy a o technických a organizačních opatřeních s tím spojených. Toto ujednání může být obsaženo v samostatné smlouvě tzv. non-disclosure agreement (NDA).
Ustanovení o oprávnění užívat data	Jde o ustanovení smlouvy o právech k datům. Zejména je potřeba stanovit, komu data náleží, kdo k nim má primárně užívací právo. Dále by pak takové ustanovení mělo obsahovat, jakým způsobem má dodavatel s daty nakládat, jak k nim řídit přístup apod. Je vhodné upravit, jak bude s daty a provozními údaji naloženo po ukončení spolupráce, zejména zda a v jaké podobě dojde k předání dat povinnému subjektu nebo zda budou zlikvidována, což připadá v úvahu zejména právě u provozních údajů.
Ustanovení o autorství programového kódu, popřípadě o programových licencích	Jedná se o ustanovení smlouvy upravující zejména, kdo je autorem programového kódu, jakou licencí je kód poskytnut (výhradní/nevýhradní), jaké jsou podmínky užívání programového kódu dle této licence (jak může subjekt s kódem nakládat, např. zda má právo provádět v kódu změny či jej poskytnout třetí osobě, jak bude s programovým kódem naloženo po ukončení spolupráce apod.). Dále se jedná i o ustanovení upravující úpravu a nakládání s dokumentací ke zdrojovému kódu.
Ustanovení o kontrole a auditu dodavatele (pravidla zákaznického auditu)	Jedná se o ustanovení smlouvy stanovující pravidla pro provádění zákaznického auditu. Zejména jde o samotnou možnost provést zákaznický audit. Dále by obsahem tohoto ustanovení mělo být jak často, jakým způsobem a za jakých podmínek (přítomnost některých osob, ohlášení auditu apod.) lze audit provést. Dále pak rozsah auditu, kam budou mít auditoři přístup apod. Audit může být proveden také třetí stranou a tento audit může být doložen např. auditní zprávou či jiným dokumentem.
Ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou v rozporu s požadavky povinné osoby na dodavatele	Jedná se o ustanovení smlouvy zabezpečující promítnutí požadavků na dodavatele i směrem k subdodavatelům. Jde zejména o ujednání, že subdodavatel je povinen dodržovat stejná smluvní ujednání, jaká má sjednána povinný subjekt s dodavatelem.
Ustanovení o povinnosti dodavatele dodržovat bezpečnostní politiky povinné osoby nebo ustanovení o odsouhlasení bezpečnostních politik dodavatele povinnou osobou	Jedná se o ustanovení smlouvy, které zabezpečuje dodržování bezpečnostních politik povinného subjektu ze strany dodavatele. Toto ustanovení může být (a obvykle tomu tak bude) obsaženo ve všeobecných obchodních podmínkách či jsou tyto politiky přikládány ke smlouvě ve formě jejích příloh.
Ustanovení o řízení změn	Jde o ustanovení smlouvy, které reflektuje způsob, jakým dochází k řízení změn, a to ve dvou rovinách: a) Jakým způsobem probíhá vzájemné schvalování změn obsahu smlouvy. b) Tzv. change management – tedy stanovení přezkumu možných dopadů změn (např. prostřednictvím analýzy rizik), akceptačního procesu (jakým způsobem je změna přijata), testování před nasazením do provozu, promítnutí do bezpečnostních politik, dokumentování změny, možnost navrácení do původního stavu apod. Blíže se této problematice věnuje také § 11 vyhlášky o kybernetické bezpečnosti.

Ustanovení o souladu smluv s obecně závaznými právními předpisy	Jedná se o ustanovení smlouvy obsahující ujednání, že smlouva je v souladu s aktuálními právními předpisy a směřuje k tomu, že smlouva musí plnit aktuální legislativní požadavky a v případě významných legislativních změn musí být upraven způsob, jakým bude těmto požadavkům přizpůsobena.
Ustanovení o povinnosti dodavatele informovat povinnou osobu o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy	Jde o ustanovení smlouvy upravující, že v případě bezpečnostního incidentu souvisejícího s plněním smlouvy u dodavatele se o něm povinný subjekt doví. Zejména je třeba stanovit povinnost dodavatele informovat povinný subjekt o výskytu incidentu (např. jakým způsobem a v jaké lhůtě povinný subjekt dodavatel informuje).
Ustanovení o povinnosti dodavatele informovat povinnou osobu o způsobu řízení rizik na straně dodavatele a o zbytkových rizicích souvisejících s plněním smlouvy	Jedná se o ustanovení smlouvy, které zavazuje dodavatele, aby povinnému subjektu podal informaci o tom, jakým způsobem řídí rizika a o tom, jaká jsou zbytková rizika související s plněním smlouvy. (např. riziko = špatná konfigurace, opatření = před ostrým provozem otestování, zbytkové riziko = jaké riziko zbyde po nasazení opatření). Je třeba počítat s tím, že i po nasazení bezpečnostního opatření riziko není nulové a vždy tu zbytkové riziko bude.
Ustanovení o povinnosti dodavatele informovat povinnou osobu o významné změně ovládání tohoto dodavatele podle zákona o obchodních korporacích nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy, využívaných tímto dodavatelem k plnění podle smlouvy se správcem	Jde o ustanovení smlouvy o tom, že je třeba povinný subjekt informovat o významné změně ovládání dodavatele. Ovládáním se zde rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení.
Ustanovení o právu jednostranně odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem k plnění podle smlouvy	Jedná se o ustanovení smlouvy navazující na povinnost zmíněnou výše, které zabezpečuje, aby se povinný subjekt o změně kontroly nad dodavatelem dověděl a mohl následně reagovat. Obsahem tohoto ujednání je pak možnost odstoupit od smlouvy v případě, že dojde k významné změně kontroly nad dodavatelem, přičemž kontrolou se zde rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení.

Specifikace podmínek z pohledu bezpečnosti při ukončení smlouvy (například přechodné období při ukončení spolupráce, kdy je třeba ještě udržovat službu před nasazením nového řešení, migrace dat a podobně)	Jde o ustanovení smlouvy, kterým je stanoven postup při ukončení spolupráce s dodavatelem. Jde zejména o stanovení délky přechodného období při ukončení spolupráce (dostatečně dlouhé období, po které má dodavatel povinnost provozovat systém i po ukončení spolupráce), pravidel migrace dat (v jakém formátu a do kdy data a provozní údaje předat povinnému subjektu či novému dodavateli nebo provést jejich likvidaci atd.), poskytování součinnosti budoucímu dodavateli (její rozsah a podmínky), poskytování know-how nasazených řešení budoucímu dodavateli apod. Je třeba myslet i na předání dokumentace spojené s provozem systému.
Specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností)	Jedná se o ustanovení smlouvy upravující zapojení dodavatele do řízení kontinuity činností a specifikace povinností, které má v takovém případě nad rámec běžných povinností. Jedná se také o úpravu změny režimu jeho fungování vůči objednateli, například o zahrnutí (a jeho způsob) dodavatele do plánů kontinuity či do havarijních plánů povinné osoby.
Specifikace podmínek pro formát předání dat, provozních údajů a informací po vyžádání správcem	Jde o ustanovení smlouvy, kterým je ujednán formát předávaných dat a provozních údajů tak, aby byly pro povinný subjekt použitelná. Data v nesystematizované podobě či strojově nečitelném formátu jsou často pro povinný subjekt či nového dodavatele neupotřebitelná.
Pravidla pro likvidaci dat	Jedná se o ustanovení smlouvy reflektující postup a způsob likvidace dat a provozních údajů. Způsob likvidace dat by měl být stanoven v návaznosti na jejich citlivost a důležitost, někdy postačí pouhé smazání, někdy naopak bude potřeba protokolárně zničit i hmotný nosič, na kterém jsou data zachycena.
Ustanovení o sankcích za porušení povinností	Jde o ustanovení smlouvy, která stanovují sankce za porušení smluvních povinností. Sankce by měly být úměrné k ceně poskytované služby i dopadu případného porušení, aby jejich význam nebyl marginální.