Pravidla pro dodavatele

Dodavatel se v rámci plnění smlouvy zavazuje dodržovat níže uvedená pravidla kybernetické bezpečnosti:

1. Řízení změn v konfiguraci systému, při realizaci aktualizací, zálohování apod., ze strany dodavatele, je vždy zahájeno navržením a zdokumentováním změny. Dodavatel poskytuje součinnost Správci IS při vyhodnocení rizik potenciálních dopadů změny. Dodavatel je povinen, v případě vyžádání Správcem IS, provést testování funkčnosti a bezpečnosti změny. Změnu provede po odsouhlasení Správcem IS, způsobem, umožňující návrat do předcházejícího stavu.
2. Dodavatel je povinen zaznamenávat přihlášení, odhlášení a činnosti administrátorů. Záznamy o přístupech administrátorů je dodavatel povinen kontrolovat min 1x za měsíc a na vyžádání je předat Správci IS.
3. Dodavatel v rámci řízení přístupů zajistí následující:
    - přístup k určeným aktivům bude realizován prostřednictvím VPN objednatele,
    - ke zpřístupněným aktivům objednatele určí příslušné administrátory, jejichž seznam předá Správci IS,
    - o vlastní zpřístupnění aktiva požádá určený administrátor dodavatele,
    - každý administrátor bude přistupovat k zpřístupněným aktivům svým jedinečným přihlašovacím jménem a heslem splňujícím min. následující podmínky:
        - minimální délka hesla: 17 znaků u privilegovaných účtů,
        - heslo musí obsahovat alespoň 4 ze 4 skupin znaků (malá písmena, velká písmena, číslice nebo speciální znaky),
        - maximální platnost hesla: 12 měsíců,
        - minimální platnost hesla: 24 hodin,
        - historie hesel: 12 hesel,
        - maximální počet neúspěšných pokusů o přihlášení: 5,
        - doba zablokování účtu po neúspěšných pokusech o přihlášení: 60 minut,
        - vynucení bezodkladné změny výchozího hesla po jeho prvním použití.
4. Dodavatel poskytne plnou součinnost Správci IS při provádění předem ohlášených bezpečnostních testů, testování zranitelností apod.
5. Dodavatel je povinen neprodleně informovat Správce IS o podezření na kybernetickou bezpečnostní událost nebo incident související s plněním smlouvy, prostřednictvím Servis Desku objednatele. Za kybernetickou bezpečnostní událost je vždy považováno podezření na např.:
    - ztrátu nebo prozrazení přístupových údajů, prostřednictvím kterých lze získat přístup k aktivům Správce IS,
    - ztrátu, odcizení nebo poškození záloh souvisejících s plněním smlouvy,
    - nedostatečnou kapacitu pro zálohování souvisejícím s plněním smlouvy,
    - neprovedení pravidelné či mimořádné aktualizace související s plněním smlouvy,
    - neoprávněný výmaz nebo změna souboru s auditními záznamy souvisejícími s plněním smlouvy,
    - neoprávněné anonymní připojení k síti dodavatele i Správce IS,
    - neoprávněné použití privilegovaných přístupových oprávnění,
    - neoprávněnou změnu dat,
    - neoprávněný logický nebo fyzický přístup k datům,

- útok na dostupnost služeb (DoS – Denial of Service, DDoS – Distributed DoS),
- útok škodlivého kódu (malware),
- možné zneužití ztráty klíčů, vstupních karet umožňujících přístup do prostor dodavatele s umístěnou výpočetní technikou nebo informacemi v listinné podobě, souvisejících s plněním smlouvy,
- další události, které mohou mít vliv na poskytované služby.

6. Dodavateli je zakázáno provádět jakoukoliv formou monitorování síťové komunikace, které neslouží k plnění Předmětu smlouvy se Správcem IS.
7. Dodavatel je povinen řídit rizika související s předmětem dodávané služby a na požádání, nejméně však jedenkrát do roka, Správce IS mu předložit přehled akceptovatelných rizik souvisejících s předmětem plnění smlouvy.
8. Dodavatel je povinen udržovat aktuální provozní dokumentaci technických a programových prostředků související s plněním smlouvy. Provozní dokumentace mimo jiné musí obsahovat postupy pro spuštění a ukončení chodu systému, restart nebo jeho obnovu v případě selhání systému, nestandardního stavu nebo po kybernetickém bezpečnostním incidentu. V případě aktualizace provozní dokumentace je dodavatel povinen, informovat Správce IS a aktuální verzi předat minimálně jednou do roka.
9. Dodavatel je povinen vytvořit a průběžně aktualizovat Plán zálohování aktiv, souvisejících s plněním dodavatele, který bude obsahovat zálohované prostředky, zálohovací média, periodu, způsob zálohování a způsoby ověřování záloh. Minimální doba aktualizace Plánu zálohování je jeden rok.
10. Dodavatel vede seznam kontaktů svých odpovědných zaměstnanců, pro případ vzniku neočekávaných provozních nebo technických problémů. Změny hlásí neprodleně Správci IS. Aktualizace je nutná při každé změně odpovědných zaměstnanců.
11. Dodavatel pro zajištění provozní a komunikační bezpečnosti je povinen:
    a) Provádět pravidelné sledování a analýzy technických zranitelností a následné ošetření slabin technických a programových prostředků. Pro proces řízení a správy technických zranitelností musí mít určeny role a odpovědnosti.
    b) Je prováděna autentizovaná synchronizace času.
    c) Programové vybavení dodavatele na prostředcích používaných pro plnění Předmětu smlouvy musí být instalováno v aktuální verzi a mít implementovány aktuální bezpečnostní záplaty pro danou technologii.
    d) Kontrolu plnění povinností dodavatele prověří objednatel prostřednictvím zákaznického auditu.
12. V případě použití programového vybavení třetích stran vede dodavatel evidenci programového vybavení (instalovaného software) v rozsahu:
    a) dodavatele a výrobce programového vybavení;
    b) přehledu platných licencí;
    c) aktuální nasazenou verzi;
    d) umístění programového vybavení;
    e) kontrolu plnění povinností dodavatele prověří objednatel prostřednictvím zákaznického auditu.
13. Dodavatel je povinen u prostředků používaných pro přístup k IS dodržet minimálně tato bezpečnostní opatření:
    a) Provozovat příslušné prostředky pro ochranu před škodlivým kódem s odpovídající mírou účinnosti bezpečnostního opatření.
    b) Zajistit ochranu používaného prostředku před neoprávněným přístupem nebo manipulací.
    c) Zaměstnanci dodavatele využívající privilegované oprávnění pro přístup k IS jsou povinni chránit toto oprávnění a nesmí ho sdílet s jinými využívanými oprávněními.
    d) Chránit data získaná a zpracovávaná při správě IS.

14. Dodavatel je povinen zajistit přiměřenou ochranu informací, v datové anebo listinné podobě, které od Správce IS obdržel pro potřebu plnění předmětu díla nebo které vytvořil v rámci plnění předmětu díla. Dodavatel je povinen takové informace evidovat a po předání díla Správci IS prokazatelně předat, nebo je, dle rozhodnutí Správce IS, prokazatelně zlikvidovat. Dodavatel je povinen zajistit, že takové informace nebudou poskytnuty třetí straně s výjimkou explicitního souhlasu Správce IS.
15. Dodavatel zajistí požadovanou účast na školení bezpečnostního povědomí objednatele svých zaměstnanců, kteří se podílejí na plnění smlouvy.
16. Při likvidaci prostředků pro zpracování informací, které jsou nahrazeny v rámci díla, budou dodavatelem v likvidovaných prostředcích obsažená data nenávratně odstraněna. O likvidaci bude pro objednatele vytvořen likvidační protokol.
17. Dodavatel se na výzvu zavazuje umožnit Správci IS provedení kontroly zavedení bezpečnostních opatření. Dodavatel v této věci poskytne Správci IS, nebo jím určené třetí straně, nutnou součinnost. Při těchto kontrolách bude vždy přihlédnuto k povaze a rozsahu plnění dle smlouvy.
18. Požadavky, hlášení událostí, záznamy a ostatní komunikace související s bezpečným provozem a funkčností dodaných technických prostředků je vedena ze strany dodavatele prostřednictvím tiketovacího systému objednatele nebo případně prostřednictvím elektronické pošty na e-mailovou adresu stanovenou objednatelem.