Obecná pravidla pro dodavatele ICT

Fakultní Thomayerova nemocnice

Pravidla platí pro všechny dodavatele, jejichž dodávky mohou mít přímý dopad na provoz počítačových systémů a sítí ve FTN.

1 Povinnosti dodavatele

1.1 Dodavatel se zavazuje dodržovat bezpečnostní opatření a pravidla FTN při práci s informacemi a ICT prostředky FTN.

1.2 Dodavatel se zavazuje nakládat s veškerými daty, informacemi a údaji, ke kterým se dostane v rámci Předmětu plnění takovým způsobem, aby nemohlo dojít k jejich ztrátě, vyzrazení, neoprávněné či neodborné manipulaci. Dále se zavazuje používat tato data pouze k danému účelu a neumožnit jejich zpřístupnění nepovolané osobě.

1.3 Dodavatel se zavazuje dodržovat veškerou platnou legislativu, zejména pak tu v oblasti kybernetické bezpečnosti a ochrany osobních údajů. Zaměstnanci Dodavatele mohou přistupovat k informačním a komunikačním prostředkům (ICT prostředky) FTN výhradně prostřednictvím jejich autentizačních údajů přidělených FTN (např. VPN přístup).

1.4 Na neveřejných pracovištích a prostorách FTN (např. serverovny, uzavřená oddělení,…) není dovolen pohyb cizích osob bez dozoru zaměstnance FTN.

1.5 Zaměstnanci Dodavatele mohou fyzicky přistupovat k ICT prostředkům FTN pouze v doprovodu oprávněné osoby FTN.

1.6 V případě práce Dodavatele v prostorách FTN nebo v jím využívaných prostorách v datových centrech musí Dodavatel dále dodržovat tyto zásady:

- připojovat vlastní počítač, notebook pouze se souhlasem odpovědné osoby FTN,
- v blízkosti ICT prostředků nejíst, nepít a nekouřit.

1.7 Dodavatel není oprávněn k výměně a odvozu použitých či vadných technologií bez autorizace FTN.

1.8 Dodavatel je povinen dodržovat mlčenlivost o důvěrných informacích FTN, které se dozvěděl při dodávce Předmětu plnění, a to i po ukončení smluvního vztahu založeného Smlouvou. Důvěrnou informací FTN se rozumí informace obchodní, technická, osobní údaje, zdravotnická dokumentace či jiná, která je významná pro FTN a/nebo je konkurenčně významná a není v obchodních kruzích běžně dostupná.

1.9 Pokud Dodavatel přijde do styku s osobními údaji, musí se řídit platnou legislativou na ochranu osobních údajů, především týkající se zpracování a předávání. Je-li zpracovatelem osobních údajů, podepíše zpracovatelskou smlouvu.

1.10 Dodavatel může šířit informace o Předmětu plnění či o spolupráci s FTN (web, medializace Dodavatele, publikace, tisk apod.) jen s předchozím písemným souhlasem FTN.

2 Bezpečnost informačních systémů

2.1 V případě ztráty nebo odcizení hardware, software, dat, informací FTN musí Dodavatel vždy neprodleně nahlásit tuto skutečnost FTN, a to i v případě pouhého podezření na neoprávněný přístup a manipulaci s daty.

2.2 Dodavatel hlásí skutečnosti odboru informatiky FTN vždy na e-mail: jan.cermak@ftn.cz a telefonicky na tel.: +420 261 083 714 (FTN výslovně vyžaduje duplicitní informaci, tedy telefonem a zároveň i e-mailem).

2.3 Při práci na zařízení (například: počítači, notebooku, mobilním telefonu, zdravotnickém prostředku) připojeném do sítě a/nebo k informačním systémům FTN musí Dodavatel dodržovat tyto zásady:

- umožnit přístup jen proškolenému zaměstnanci Dodavatele,
- chránit výpočetní techniku a všechna data FTN před porušením důvěrnosti, integrity či dostupnosti,
- po ukončení práce v síti a/nebo v informačním systému FTN provést neprodleně odhlášení uživatele.

2.4 **Při práci na serverech FTN** musí být splněny následující zásady, které se vztahující i na servisní (provozní) smlouvy (s ohledem na specifikace informačních systémů):

- server svěřený Dodavateli do správy musí Dodavatel pravidelně udržovat a kontrolovat zejména z pohledu bezpečnosti, dostupnosti a integrity dat,
- Dodavatel nesmí měnit jakákoliv oprávnění na serveru nebo informačním a komunikačním systému bez souhlasu odboru Správy informačního systému,
- Dodavatel nesmí měnit nastavení operačního systému serverů a jeho komponent bez souhlasu odboru Správy informačního systému,
- Dodavatel musí zajistit bezpečnostní aktualizaci operačního systému a aplikačních částí serverů; bezpečnostní aktualizace kritického charakteru, které mohou ohrozit bezpečnost sítě FTN musí aplikovat neprodleně po jejich vydání,
- Dodavatel je povinen udržovat aktuální dokumentaci k provozovaným informačních a komunikačním systémům, kterou po každé aktualizaci musí předat SIS.

2.5 **Při práci v interní sítí FTN** odpovídají zaměstnanci Dodavatele, kteří mají přidělen přístup do interní sítě FTN, za své činnosti prováděné v rámci této sítě. Zaměstnanci Dodavatele nesmí, zejména:

- zneužívat síťové prostředky pro osobní účely a zatěžovat kapacitu sítě,
- šířit či jinak nakládat se škodlivým malwarem,
- využívat nástroje sloužící k maskování identity,
- provádět bezdůvodné skenování portů či jiných parametrů sítě a síťových zařízení,
- provádět jakoukoliv formou monitorování sítě, které může vést k zachycení dat, pokud není Předmětem plnění smlouvy s FTN,
- obcházet autentizaci uživatele nebo obcházet zabezpečení jakéhokoliv počítače, sítě nebo uživatelského účtu,
- provádět jakékoliv nepracovní aktivity vedoucí k omezování nebo odepírání služeb jiným uživatelům,
- užívat jakékoliv programy, skripty nebo příkazy, nebo zasílat zprávy v jakékoliv formě s úmyslem omezit nebo znemožnit poskytování služeb nebo terminálových relací lokálně nebo přes síť, internet nebo intranet,
- využívat bezpečnostních mezer nebo vytvářet útoky na komunikaci v počítačových sítích (např. přístup k datům, jichž není zaměstnanec zamýšleným příjemce, přihlašování na server nebo účet zaměstnancem, který není k tomuto přístupu výslovně oprávněn, s výjimkou případů, kdy tyto aktivity jsou součástí řádných pracovních úkolů),

- předávat informace o konfiguraci a topologii sítě cizím osobám; tyto informace je oprávněn předat pouze odpovědný zaměstnanec FTN, pokud jsou takové informace nutné z hlediska přípravy či Předmětu plnění.

2.6 Dodavatel musí vyvinout maximální úsilí pro odvracení bezpečnostních hrozeb a kybernetických útoků pro informační a komunikační systémy FTN.

2.7 Dodavatel musí zajistit maximální součinnost při analýze kybernetických bezpečnostních událostí a incidentů FTN a následně zavádět vhodná nápravná opatření určená FTN.

2.8 V případě podezření či potvrzení vzniku bezpečnostní hrozby pro informační a komunikační systém FTN je Dodavatel povinen neprodleně písemně (e-mailem) či telefonicky (a následně také písemně) informovat o této skutečnosti Manažera kybernetické bezpečnosti FTN.

3 Požadavky na dodávané informační systémy

3.1 Požadavky na dodávané informační systémy

- Informační systém musí být vytvářen tak, aby dostatečně chránil data před porušením důvěrnosti, dostupnosti a integrity.
- Informační systém musí být vytvořen tak, aby byla každá operace uložena v provozním záznamu (logu) s jedinečným identifikátorem uživatele, který tuto operaci vykonal. Musí být zajištěno, aby nemohlo dojít k provádění operací pod cizím identifikátorem uživatele.
- Možnosti nastavení autentizace uživatelů informačního systému musí umožňovat 2FA, autentizaci pomocí AD nebo IDM, případně musí umožnit nastavit minimálně složitost a délku hesla, vynucení změny hesla a oddělené nastavení pro privilegované účty.
- Informační systém musí být vytvořen tak, aby byl počet neúspěšných pokusů o přihlášení omezen. Po daném počtu neúspěšných pokusech o přihlášení musí být další zadávání dočasně zablokováno nebo spojení rozpojeno.
- V případě, že je povolen přístup do informačního systému, v němž určuje vstupní heslo administrátor, je povinností autora informačního systému vynutit si změnu tohoto inicializačního hesla.
- Dodavatel nesmí používat jedno přihlašovací jméno pro několik svých zaměstnanců, každý účet musí být jmenný.
- Dodavatel musí zajistit integraci informačního systémů na IDM FTN, pokud je to technicky možné.

3.2 V informačních systémech musí být pořizovány auditní záznamy obsahující alespoň:

- identifikaci uživatele;
- datum a čas přihlášení a odhlášení;
- identifikaci místa, odkud se uživatel přihlašoval (pokud je to možné);
- záznamy o přístupu (úspěšném i neúspěšném), případně o prováděných operacích;
- záznamy musí být možné vzdáleně číst a následně zpracovávat nebo je systém musí automaticky odesílat na vzdálený SIEM FTN.

3.3 Řízení přístupu k informačním systémům

- Před umožněním přístupu musí být každý uživatel identifikován a autentizován.
- Informační systém by měl po určité době nečinnosti uživatele (doporučeno 15 minut) tohoto uživatele odhlásit.
- Po určitém množství neúspěšných autentizačních pokusů (doporučeno 10) se musí ukončit přihlašovací proces.

- V případě neúspěšné autentizace nesmí informační systém poskytnout uživateli informaci o tom, která část autentizace je chybná.
- Pro každého uživatele informačního systému musí být možné identifikovat, jaká má přístupová práva.
- Pro každý prostředek musí být možné vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku s rozlišením druhu přístupových práv (čtení, úprava atd.).
- Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo skupině.

3.4 Data vstupující do informačních systémů musí být kontrolována tak, aby byla zajištěna jejich správnost. V informačních systémech se musí evidovat identifikátor uživatele, který změny provedl. Pro kontrolu dat musí Dodavatel aplikovat opatření:

- vstupní kontrola (neplatné znaky, rozsah, přetečení, kompletnost, souvislost...),
- kontrola vnitřního zpracování dat,
- kontrola oprávněnosti běhu programů,
- kontrola integrity dat,
- kontrola obsahu generovaných dat.

3.5 Vývoj software musí probíhat:

- legálním softwarem,
- autorská a licenční ujednání musí být smluvně řešena před samotným vývojem,
- na testovacím prostředí odděleném od prostředí produkčního,
- na testovacích datech, která nejsou převzata z provozní databáze; pokud je nutné použít data z provozní databáze, je nutné je anonymizovat,
- migrace do provozního prostředí může být provedena až po akceptaci výsledků testů ve vývojovém či testovacím prostředí.

4 Předání plnění

4.1 Je-li informační systém vyvíjen na zakázku, musí splňovat všechny níže uvedené body a jedná-li se o již vyvinutý informační systém, musí být tyto požadavky zohledněny v hlavní smlouvě.

4.2 Dodávka software

- Dodávka software musí být řádně smluvně zajištěna a průběžně kontrolována a dokumentována. Pokud není stanoveno ve smlouvě jinak, je Dodavatel povinen software dodat se zdrojovými kódy.
- U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený software nebo program podléhající licenční a registrační politice. Pracuje-li počítačový program nebo aplikace, s daty, musí být specifikováno s jakými daty a musí být provedena jejich kategorizace.

4.3 Dodávka hardware

- Ke každé dodávce musí existovat kromě účetních dokladů I předávací protokol podepsaný Dodavatelem a FTN. Způsob předání závisí na konkrétním hardware a na smlouvě s Dodavatelem.

4.4 Dodávka služeb

- Způsob předání závisí na konkrétní službě a na smluvních podmínkách dohodnutých ve Smlouvě.

- Dodavatel zajistí monitorování služby tak, aby bylo možné porovnání jejich parametrů, rozsahu a kvality stanovených Smlouvou.

4.5 Dokumentace

- Nedílnou součástí dodávky Předmětu plnění je projektová a bezpečnostní dokumentace Předmětu plnění. Rozsah a náplň dokumentace musí být specifikován ve smlouvě s Dodavatelem. Chybějící, neúplná nebo neaktuální dokumentace je důvodem k reklamaci dodávky a v případě, že ji Dodavatel ve lhůtě stanovené FTN neopraví, důvodem k odstoupení od Smlouvy.
- Pokud má být měněn Předmět plnění, musí Dodavatel aktualizovat dokumentaci.

4.6 Akceptace

- Každý dodávaný prvek Předmětu plnění musí být plně a široce Dodavatelem otestován, zda splňuje očekávané a smluvně definované parametry, a zda jeho používání nepředstavuje neočekávaná bezpečnostní rizika (penetrační test, práce s daty).
- Každý prvek Předmětu plnění je předán až podpisem písemného předávacího protokolu oprávněnými zástupci smluvních stran.
- Akceptace díla ze strany FTN přenáší odpovědnost na FTN pouze za vlastnosti, které byly prokazatelně předvedeny.

4.7 Porušení těchto pravidel představuje porušení Předmětu plnění. Pokud Dodavatel poruší tato pravidla hrubým způsobem nebo opakovaně, je FTN oprávněna uplatnit sankce uvedené ve smlouvě nebo odstoupit od smluvního vztahu s Dodavatelem.

V Praze 1. 1. 2025

Ing. Lumír Kučaba
náměstek pro informatiku a komunikaci
Fakultní Thomayerova nemocnice