Příloha č. 5 smlouvy

Bezpečnostní pravidla pro práci v informačním systému (IS) Krajského úřadu Zlínského kraje (dále jen úřad)

ICT (informační a komunikační technologie) jsou veškeré informační technologie používané pro komunikaci a práci s informacemi

IS (Informační systém) je celek složený z počítačového hardwaru, souvisejícího softwaru a dat.

1. Přístup k IS úřadu

a) Přístup jiných subjektů (dále jen druhá smluvní strana) k IS úřadu je možný pouze na základě smluvně ošetřeného vztahu se Zlínským krajem.
b) Druhá smluvní strana je povinna dodržovat bezpečnostní pravidla pro práci v IS úřadu a nese v souladu s platnou legislativou a předpisy svůj díl odpovědnosti za nedodržení či porušení pravidel, případně za škody vzniklé v důsledku bezpečnostních incidentů, které zavinila.
c) Je přísně zakázáno vykonávat jiné než dohodnuté činnosti, přistupovat k jiným než povoleným prostředkům, serverům a datům. Dále je zakázáno provádět jakékoli úkony směřující k zjišťování rozsahu přidělených oprávnění, dostupnosti síťových prostředků a služeb a způsobů zabezpečení.
d) Druhá smluvní strana je povinna používat pouze jí přidělené přístupy a povolené způsoby přístupu, (fyzické přístupy, přístupové údaje, povolené časy pro přístup a přidělená oprávnění), a je odpovědná za jejich používání, za svou činnost v IS úřadu a dodržování bezpečnostních pravidel při práci s informacemi. Přidělené údaje jsou pro druhou stranu závazné, jsou důvěrné a jsou platné jen po dobu platnosti smlouvy. Tyto údaje jsou uvedeny ve smlouvě nebo v Předávacím protokolu k účtu.
e) Přístupy a přístupová oprávnění jsou přidělena pouze v rozsahu nezbytně nutném pro výkon smluvních závazků. Druhá smluvní strana nesmí do přidělených oprávnění zasahovat a měnit je. Pokud zjistí, že oprávnění jsou odlišná od dohodnutých, neprodleně na to upozorní odpovědné osoby nebo správce IS.
f) Druhá smluvní strana nesmí vytvářet žádné přístupové cesty do IS úřadu a měnit přístupová oprávnění. Tyto změny může provádět správce IS na základě písemné žádosti.
g) Přistupovat k IS úřadu mohou pouze poučení pracovníci druhé smluvní strany. Druhá smluvní strana zajistí před zahájením prací poučení a proškolení všech svých pracovníků a subdodavatelů, kteří budou přistupovat k IS úřadu.
h) Pracovníci druhé smluvní strany jsou povinni řídit se pokyny odpovědných osob (uvedených ve smlouvě) správců IS, případně dalších pracovníků oddělení informatiky.
i) Činnost druhé smluvní strany v IS úřadu je monitorována a evidována. Pověření pracovníci úřadu mohou ověřovat dodržování stanovených bezpečnostních pravidel a zakázat neoprávněné aktivity.
j) Porušení bezpečnostních pravidel je sankcionováno smluvní pokutou.
k) Druhá smluvní strana je povinna předat informace o provedených zásazích a změnách a bez zbytečného prodlení je promítnout do dokumentace.

2. Účty a hesla

a) Přidělené přihlašovací účty jsou chráněny heslem. Názvy přihlašovacích účtů a hesla nesmějí být sděleny žádné neoprávněné osobě. Heslo musí splňovat aktuální požadavky na kvalitu a platnost a musí být uchováno v tajnosti.
b) Mimo povolené časy pro přístup jsou přístupové účty neaktivní. V případě potřeby mohou jejich aktivaci schválit a zajistit odpovědné osoby.

l) Při porušení bezpečnostních pravidel druhou smluvní stranou mohou být přidělené přístupové účty zablokovány nebo zcela odebrány.

3. Vzdálený přístup a vzdálená údržba

a) Vzdálený přístup do IS úřadu je možný pouze dohodnutým způsobem. Vzdálený přístup je vždy šifrován.
b) Přístup je možný pouze z pracovní stanice, která má nainstalovaný podporovaný operační systém, nainstalovány všechny bezpečnostní záplaty operačního systému vydané výrobcem, a má aktivní a aktuální antivirovou ochranu.
c) Pro zvýšení bezpečnosti může být vzdálený přístup umožněn pouze z ověřených konkrétních předem definovaných IP adres druhé smluvní strany.
d) Přístup k systémům v oblastech s vysokou úrovní zabezpečení za účelem vzdálené údržby (např. u významných informačních systémů úřadu) musí být chráněn kromě šifrování i silnou autentizací druhé smluvní strany.
e) Pracovní stanice určené k přístupu do IS úřadu ze vzdálené lokality musí být fyzicky zabezpečeny proti přístupu neoprávněných osob.

4. Zabezpečení fyzického přístupu k IS

a) Servery, síťové komponenty a další ICT zařízení jsou zabezpečeny proti fyzickému přístupu. Přístup do místností se servery s citlivými daty a přístup k síťovým zařízením je regulován a odpovídajícím způsobem monitorován. Pokud fyzické zabezpečení citlivých dat není dostatečné, musí být zabezpečena šifrováním.
b) Fyzický přístup k prostředkům IS je umožněn pouze druhým smluvním stranám (servisní a dodavatelské organizace, dohody o provedení práce apod.), u kterých udělení přístupu vyplývá z uzavřené smlouvy. Fyzický přístup k prostředkům IS je možné uskutečnit pouze se souhlasem správce IS nebo vedoucího oddělení informatiky.
c) Pohyb pracovníků druhých smluvních stran v prostorách serverovny (servisní zásah, revize zařízení apod.) je možný pouze v doprovodu odpovědných pracovníků oddělení informatiky nebo se souhlasem vedoucího oddělení informatiky.
d) Pro práci v IS úřadu smí být použita pouze přidělená technika úřadu. Připojování cizí techniky do vnitřní sítě úřadu je zakázáno. Výjimky povoluje správce IS.
e) Na přidělenou techniku úřadu nesmí být bez souhlasu pověřené osoby nahráván, instalován nebo z ní odebírán žádný software.
f) Při opuštění pracoviště je vždy nutné provést vhodným způsobem jeho zajištění (pracovní stanice, nosiče dat, papírové dokumenty).
g) Přenosná paměťová média musí být vždy uchovávána na bezpečném místě, např. v uzamčené skříni, stolu nebo místnosti. Originální datová média a záložní kopie citlivých souborů musí být ukládány na bezpečném místě, chráněném nejen proti odcizení a zneužití, ale i proti poškození nebo zničení.
h) Pracovní stanice a data na nich uložená musí být chráněna proti odcizení, proti neoprávněnému přístupu a proti poškození nebo zničení.

5. Ochrana dat a informačních aktiv

a) Druhá smluvní strana odpovídá za všechna převzatá data (elektronická a tištěná), způsob jejich použití a ochranu před neoprávněným přístupem a zneužitím. Není-li ve smlouvě stanoveno jinak, před ukončením smluvního vztahu druhá smluvní strana vrátí všechna převzatá data.
b) Druhá smluvní strana je do protokolárního předání pracovníkům úřadu odpovědná za všechna zpracovávaná aktiva a je povinna je odpovídajícím způsobem zabezpečit.
c) Ukládání pracovních dat je možné pouze na místa, která určí odpovědná osoba.
d) Druhá smluvní strana nesmí zobrazovat, měnit, mazat nebo kopírovat citlivá data, zejména pak osobní údaje, pokud to nesouvisí se schváleným účelem přístupu.
e) Opravy ICT komponent mohou být prováděny pouze na základě smluvně ošetřeného vztahu s úřadem.

f) Vadná zařízení (včetně pevných disků) s nešifrovanými citlivými daty mohou být předány externím servisním specialistům pouze po schválení správcem IS nebo vedoucím oddělení informatiky.
g) Pokud druhá smluvní strana při práci v IS úřadu přijde do styku s osobními údaji dle platné legislativy nebo jinými neveřejnými informacemi, je povinna o zjištěných skutečnostech zachovávat mlčenlivost a zajistit jejich utajení.
h) Nepotřebná data (elektronická, na mediích i papírová) musí být vždy neprodleně skartována.
i) Všechny zásahy na serverech musí být předem odsouhlaseny správcem IS a zaznamenány stanoveným způsobem.

6. Ochrana proti škodlivým kódům

a) Pokud je to možné, jsou servery a pracovní stanice vybaveny antivirovým skenerem.
b) Pokud některé aplikace nabízejí možnost zvýšené ochrany, musí být odpovídajícím způsobem nastavena. Způsob nastavení schvaluje správce IS.
c) Nebezpečné typy souborů jsou blokovány firewallem nebo skenerem v bráně. Výjimky schvaluje v řádně odůvodněných a zdokumentovaných případech správce IS.
d) Druhá smluvní strana je povinna dodržovat zásady ochrany proti virům a škodlivým kódům nejen pro nastavení a využívání prostředků úřadu, ale i na přístupových bodech a zařízeních druhé smluvní strany.

7. Bezpečnostní incidenty

a) Druhá smluvní strana je povinna neprodleně hlásit odpovědným osobám porušení těchto pravidel, všechny zjištěné neobvyklé události, které jsou, nebo mohou být bezpečnostními incidenty, zjištěná zranitelná místa, nedostatky a nesoulady. Při jejich prošetřování a odstraňování je povinna poskytnout účinnou součinnost.
b) Druhé smluvní straně není povoleno řešení bezpečnostních incidentů a odstraňování nedostatků či nesouladů vlastními silami bez předchozího schválení správcem IS.

8. Používání internetu

a) Druhá smluvní strana může používat při práci v IS úřadu internet pouze pro účely plnění smlouvy za podmínky dodržování všech bezpečnostních pravidel, platných pro práci s internetem. Stahování souborů, používání FTP a jiných služeb je možné jen po dohodě se správcem IS.
b) Pokud není ve smlouvě stanoveno jinak, není povoleno využívat elektronickou korespondenci z prostředí úřadu.

9. Tisk

a) Druhá smluvní strana může tisknout na tiskárnách úřadu pouze s povolením odpovědné osoby. Tisknout je povoleno pouze dokumenty související s předmětem smlouvy a při tisku je nutno šetřit spotřební materiál.
b) Tištěné dokumenty musí být zabezpečeny proti neoprávněnému přístupu jak během tisku, tak i po jeho vytisknutí, až do jejich bezpečné skartace.

10. Použití kryptografických technik

a) Kryptografické metody musí být použity vždy, jestliže není možné bezpečnost dat nebo komunikace zaručit jinými způsoby. Jedná se např. o přenosy citlivých dat prostřednictvím nedůvěryhodných sítí nebo přístup externích subjektů k citlivým zdrojům.
b) Použity mohou být pouze takové kryptografické algoritmy a protokoly a v takovém užití (např. odpovídající délky klíčů), které jsou podle platných standardů všeobecně považovány za bezpečné.
c) Použití proprietárních nebo obecně neuznávaných algoritmů není dovoleno, výjimky povoluje správce IS.