Příloha č. 2 smlouvy: Bezpečnostní pravidla ICT

Bezpečnostní pravidla ICT (Informačních a komunikačních technologií) pro práci v informačním systému (IS) Krajského úřadu Zlínského kraje (KÚZK nebo jen úřad)

1. Přístup do IS KÚZK

- Přístup jiných subjektů k ICT úřadu (dále jen druhá smluvní strana) je možný pouze na základě smluvně ošetřeného vztahu s krajem.
- Druhá smluvní strana je povinna dodržovat bezpečnostní pravidla ICT pro práci v IS KÚZK 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.
- Jednotlivé počítače určené k přístupu do KÚZK ze vzdálené lokality (např. jsou schopny přistupovat například k centrálním aplikacím), musí být fyzicky zabezpečeny proti přístupu (např. v samostatné uzamčené místnosti s definovanými pravidly pro přístup, nebo uzamknutím nezbytných ICT komponent a zařízení potřebných pro přístup v době, kdy nejsou používána).
- Všechny povolené způsoby přístupu, povolené časy pro přístup, přístupové údaje a přidělená oprávnění musí být uvedeny ve smlouvě. Tyto údaje jsou důvěrné a jsou platné jen po dobu platnosti smlouvy.
- Druhá smluvní strana je odpovědná za používání jim přiděleného přístupu do IS KUZK, za svou činnost v IS úřadu a při práci s informacemi.
- Přistupovat k ICT úřadu mohou pouze poučení pracovníci druhé smluvní strany. Druhá smluvní strana zajistí před zahájením poučení a proškolení všech svých pracovníků a poddodavatelů, kteří budou přistupovat k ICT úřadu.
- Přístup a přístupová oprávnění jsou přidělena pouze v rozsahu nezbytně nutném pro výkon smluvních závazků.
- Pracovníci druhé smluvní strany jsou povinni řídit se pokyny oprávněných osob a dalších pracovníků oddělení informatiky.
- Činnost druhé smluvní strany v IS úřadu může být monitorována. Pověření pracovníci úřadu mohou evidovat přístupy a ověřovat dodržování stanovených bezpečnostních pravidel.
- KÚZK je oprávněn monitorovat činnost zaměstnanců Zhotovitele a zakázat neoprávněné aktivity.

2. Vzdálený přístup a vzdálená údržba

- V případě nového nastavení údržby systému, která by mohl umožňovat přístup k citlivým datům, by měl být použit šifrovaný přístup.
- Vzdálený přístup do IS KUZK je možný pouze dohodnutým způsobem z pracovní stanice která má aktivní a aktuální antivirovou ochranu a nainstalovány všechny bezpečnostní záplaty operačního systému vydané výrobcem.
- Pro zvýšení bezpečnosti je vzdálený přístup povolen pouze z konkrétních IP adres druhé smluvní strany.
- Přístup k systémům v oblastech s vysokou úrovní zabezpečení za účelem vzdálené údržby (např. u významných informačních systémů KUZK) musí být chráněn šifrováním a silnou autentizací komunikačního partnera.
- Pokud to bude technicky možné, musí být vzdálený přístup nastaven tak, aby nebylo možné zobrazovat, měnit, mazat nebo kopírovat citlivá data, zejména pak data osobní. Dále, pokud to bude technicky možné, musí být důsledně kontrolována možnost prohlížet síťové služby nebo jiné systémy, a to jak přímo, tak prostřednictvím spravovaných systémů.

3. Zabezpečení fyzického přístupu k ICT

- Servery (souborové servery, aplikační servery, databázové servery atd.) a další ICT zařízení musí být zabezpečeny proti fyzickému přístupu.

- Přístup do místností se servery s citlivými daty a přístup k síťovým zařízením musí být regulován a odpovídajícím způsobem monitorován.
- Fyzický přístup k prostředkům ICT je možný pouze na základě smluvního vztahu (servisní a dodavatelské organizace, dohody o provedení práce apod.) nebo se souhlasem určené odpovědné osoby, kterou může být vedoucí odboru, vedoucí oddělení informatiky nebo vlastník aktiva.
- Pohyb pracovníků druhých smluvních stran v prostorách serverovny (servisní zásah, revize zařízení apod.) je možný pouze v doprovodu odpovědných pracovníků oddělení informatiky a se souhlasem vedoucího oddělení informatiky.
- Pro práci v IS úřadu smí být použita pouze přidělená technika kraje. Připojování cizí techniky do vnitřní sítě úřadu je bez souhlasu správce systému zakázáno.
- Na přidělenou techniku nesmí být bez souhlasu pověřené osoby instalován nebo z ní odebírán žádný software.
- Při opuštění pracoviště je vždy nutné provést vhodným způsobem jeho zajištění.
- Citlivá data uložená, která nemohou být přiměřeně zvlášť zabezpečena proti fyzickému přístupu, musí být šifrována.
- Síťové komponenty (mosty, přepínače, řídící software atd.) používané pro výměnu citlivých dat musí být chráněny proti neoprávněnému přístupu.
- Skříně se síťovou kabeláží musí být zabezpečeny proti neoprávněnému přístupu.
- Routery nebo síťové mosty (bridges) musí být umístěny v uzamčených místnostech, aby se zabránilo změnám v konfiguraci ICT zařízení v případě neoprávněného přístupu. Pokud není toto řešení možné, musí oddělení informatiky vydat souhlas s výjimkou a poskytovatel ICT služeb si musí takovýto souhlas zajistit. Poskytovatel ICT služeb musí následně zajistit ostrahu takových komponent.
- Kabely nesmí být přístupné pro neoprávněné osoby. Pro účely kontrol kabelů síťových komponent je vyžadována dokumentace, kterou je třeba v případě změn příslušně aktualizovat.
- Oblasti sítě, ve kterých jsou přenášena mimořádně citlivá data, tj. data s „velmi vysokým“ požadavkem na zabezpečení, musí být izolována od okolní sítě.
- Záložní datová média by měla být zamčena.
- ICT systémy (jako jsou například osobní počítače nebo pracovní stanice) a data v těchto systémech uložená by měla být v maximální možné a přiměřené míře chráněna proti odcizení a proti neoprávněnému přístupu restriktivními pravidly pro přístup.

4. Ochrana dat a informačních aktiv

- Mobilní paměťová média vždy uchovávejte na zabezpečeném místě, tj. v uzamčené skříni, stolu nebo místnosti. V této souvislosti platí, že originální datová média a záložní kopie citlivých souborů musí být ukládány na bezpečném místě chráněném proti požáru.
- Nezbytné opravy ICT komponent mohou být prováděny pouze na základě smluvně ošetřeného vztahu s krajem nebo poddodavatelem.
- Vadná zařízení a pevné disky s nešifrovanými citlivými daty mohou být předány externím servisním specialistům pouze po konzultaci s oddělením informatiky.
- 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.
- Druhá smluvní strana je do protokolárního předání pracovníkům úřadu odpovědná za všechna zpracovávaná aktiva a je povinna je odpovídajícím způsobem zabezpečit.
- Pracovní data se ukládají pouze na místa, určená pověřenou osobou.
- Pokud druhá smluvní strana při práci v IS úřadu přijde do styku s osobními údaji dle zákona č. 101/2000 Sb. nebo jinými neveřejnými informacemi, je povinna o zjištěných skutečnostech zachovávat mlčenlivost a zajistit jejich utajení.
- Nepotřebná data (elektronická, na mediích i papírová) musí být vždy neprodleně zlikvidována.
- Druhá smluvní strana je povinna dodržovat zásady ochrany proti virům a škodlivým kódům
- Všechny zásahy na serverech musí být předem odsouhlaseny správcem IS a zaznamenány stanoveným způsobem.

5. Ochrana proti virům

- Pokud to bude možné, všechny servery (ale přinejmenším centrální servery) musí být vybaveny antivirovým skenerem. Na poštovních a groupware serverech musí být použity specializované skenery, které jsou rovněž schopny vymazat zlomyslné programy zpětně.
- Pokud některé aplikace (např. aplikace Office) nabízejí ochranu proti makrovirům, musí poskytovatel ICT služeb tuto ochranu odpovídajícím způsobem nastavit.
- Tam, kde to bude možné, musí skener obsahu využívající virových definic umožňovat stahování těchto definic z Internetu nebo z centrálních serverů dostupných v rámci sítě. Skenovací nástroj a zejména virové definice musí být pravidelně obnovovány. Navíc musí být pravidelně prováděny dodatečné aktualizace, například pokud jsou vydány nové definice z důvodu rychlého šíření nového nebezpečného viru.
- Nebezpečné typy souborů, které se nesmějí dostat do místních sítí úřadu, musí být blokovány firewallem nebo skenerem v bráně. Výjimky (např. pro administrátory) jsou povoleny pouze v řádně odůvodněných a zdokumentovaných případech.

6. Bezpečnostní incidenty

- Druhá smluvní strana je povinna neprodleně hlásit odpovědným osobám porušení těchto pravidel, všechny zjištěné neobvyklé události, které jsou, nebo mohou být bezpečnostními incidenty a zranitelná místa, a účinně pomáhat při jejich prošetřování a odstraňování.
- Druhá smluvní strana je povinna hlásit všechny zjištěné nedostatky nebo nesoulad se skutečností.
- Druhé smluvní straně není povoleno řešení bezpečnostních incidentů a odstraňování nedostatků či nesouladů vlastními silami bez předchozího schválení bezpečnostním správcem ICT.

7. Používání internetu

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

8. Tisk

- Pokud bude druhé smluvní straně umožněn tisk na tiskárnách kraje, je povinna šetřit spotřební materiál a tištěné dokumenty zabezpečit proti neoprávněnému přístupu jak během tisku, tak i po jeho vytisknutí až do jejich bezpečné likvidace.

9. Účty a hesla

- Druhá smluvní strana smí používat pouze jim přidělené přihlašovací účty. Tyto účty jsou chráněny heslem.
- Přístupová práva k datům nebo ICT komponentám mohou být udělena pouze na základě žádosti a v rozsahu nezbytném pro splnění konkrétního úkolu.
- Heslo musí splňovat aktuální požadavky na kvalitu a platnost a musí být uchováno v tajnosti.
- Názvy přihlašovacích účtu a hesla nesmějí být sděleny žádné neoprávněné osobě.
- V případě porušení bezpečnostních pravidel mohou být druhé straně přístupové účty zablokovány nebo zcela odebrány.

10. Použití kryptografických technik

- Kryptografické metody musí být použity vždy, jestliže není možné bezpečnost dat nebo komunikace zaručit jinými způsoby. Jako příklad je možno uvést přenosy citlivých dat prostřednictvím nedůvěryhodných sítí, nebo přístup externích subjektů k citlivým zdrojům atd.

- Použity mohou být pouze takové kryptografické algoritmy a protokoly, které jsou podle platných standardů všeobecně považovány za bezpečné (např. Příloha č. 3 k vyhlášce č. 316/2014 Sb., Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti).
- Použití proprietárních nebo obecně neuznávaných algoritmů není dovoleno.
- Kromě kvality kryptografického algoritmu je pro sílu kryptografické metody rozhodující délka klíče. Aby bylo také zde dosaženo bezpečnosti odpovídající současnému stavu techniky, musí být použity obecně uznávané minimální délky.