Příloha č. 3

Bezpečnostní pravidla pro práci v informačním systému (IS) Zlínského kraje (ZK)

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.

Správce IS ZK je pracovník Odboru informačních a komunikačních technologií, Oddělení serverové a síťové infrastruktury. Je uveden jako odpovědná osoba předávajícího v předávacím protokolu o předání přihlašovacích údajů.

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

1. Přístup k IS ZK

a) Přístup jiných subjektů (dále jen druhá smluvní strana) k IS ZK je možný pouze na základě smluvně ošetřeného vztahu se Zlínským krajem.

b) 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. 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.

c) Přístupy a přístupová oprávnění jsou přidělena pouze v rozsahu nezbytně nutném pro výkon smluvních závazků. Druhá smluvní strana nesmí bez souhlasu správce IS vytvářet nové přístupové účty a do přidělených účtů a oprávnění zasahovat a měnit je. Pokud druhá strana zjistí, že skutečná oprávnění jsou odlišná od dohodnutých, neprodleně na to upozorní odpovědné osoby nebo Správce IS.

d) Přistupovat k IS ZK 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 ZK.

2. Práce v IS ZK

a) Druhá smluvní strana je povinna dodržovat bezpečnostní pravidla a stanovené postupy pro práci v IS ZK a nese v souladu s platnou legislativou a předpisy svůj díl odpovědnosti za nedodržení či porušení pravidel, případně za škody které zavinila.

b) 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 a provádět pokusy o jejich překonání.

c) Druhá smluvní strana nesmí vytvářet žádné přístupové cesty do IS ZK a měnit přístupová oprávnění. Tyto změny může provádět Správce IS na základě písemné žádosti.

d) Činnost druhé smluvní strany v IS ZK je monitorována a evidována. Pověření pracovníci ZK mohou ověřovat dodržování stanovených bezpečnostních pravidel a zakázat neoprávněné aktivity.

e) Pracovníci druhé smluvní strany jsou povinni řídit se pokyny odpovědných osob (uvedených ve smlouvě), Správců IS a dalších pracovníků Odboru informačních a komunikačních technologií.

f) Druhá smluvní strana je povinna předávat informace o provedených zásazích a změnách, a bez zbytečného prodlení je promítnout do dokumentace. Všechny změny, které mohou ovlivnit bezpečnost IS ZK, musí být předem projednány a schváleny Správcem IS.

g) Druhá smluvní strana je povinna chránit data ZK. Používat ostrá data pro zkušební a testovací účely je zakázáno. Výjimku může na základě písemné žádosti v odůvodněných případech povolit pouze vedoucí Odboru informačních a komunikačních technologií.

3. Účty a hesla

a) účty jsou chráněny heslem. Názvy účtů a hesla nesmějí být sděleny žádné neoprávněné osobě. Heslo musí splňovat aktuální požadavky ZK na kvalitu a platnost a musí být uchováno v tajnosti. Hesla musí být vždy předávána bezpečným způsobem. Pokud je to možné, musí být použita vícefaktorová autentizace.

b) Standardně jsou přístupové účty neaktivní. V případě potřeby mohou jejich aktivaci schválit a zajistit odpovědné osoby. Žádost musí obsahovat informace o prováděných činnostech a předpokládané době prací. Druhá strana nesmí bez předchozího upozornění provádět jiné než nahlášené práce.

4. Vzdálený přístup a vzdálená údržba

a) Vzdálený přístup do IS ZK 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 ZK) musí být chráněn kromě šifrování i silnou autentizací druhé smluvní strany.

e) Pracovní stanice určené k přístupu do IS ZK ze vzdálené lokality musí být fyzicky zabezpečeny proti přístupu neoprávněných osob.

5. 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) Opravy ICT komponent mohou být prováděny pouze na základě smluvně ošetřeného vztahu se ZK.

c) 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 serverové a síťové infrastruktury, Odboru informačních a komunikačních technologií.

d) Pohyb pracovníků druhých smluvních stran v prostorách serverovny (servisní zásah, revize zařízení apod.) je možný pouze v doprovodu odpovědných pracovníků Odboru informačních a komunikačních technologií nebo jimi pověřených osob.

e) Pro přímé připojení (v prostorách ZK) do IS ZK smí být použita pouze přidělená technika ZK. Připojování cizí techniky do vnitřní sítě ZK je zakázáno. Výjimky povoluje Správce IS.

f) Na přidělenou techniku ZK nesmí být bez souhlasu pověřené osoby nahráván, instalován nebo z ní odebírán žádný software.

g) Při opuštění pracoviště musí být provedeno jeho zajištění (pracovní stanice, nosiče dat, papírové dokumenty) před neoprávněným přístupem.

h) 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 chráněna nejen proti odcizení a zneužití, ale i proti poškození nebo zničení.

i) Pracovní stanice a data na nich uložená musí být chráněna proti odcizení, proti neoprávněnému přístupu a proti poškození nebo zničení.

6. 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 a všechny jejich kopie bezpečně zlikviduje.
b) Druhá smluvní strana je do protokolárního předání pracovníkům ZK 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) Vadná zařízení (včetně pevných disků) s nešifrovanými citlivými daty mohou být předány externím servisním specialistům pouze po schválení Správcem IS nebo vedoucím Oddělení serverové a síťové infrastruktury, Odboru informačních a komunikačních technologií.
f) Pokud druhá smluvní strana při práci v IS ZK přijde do styku s osobními údaji dle platné legislativy nebo jinými neveřejnými informacemi, je povinna o zjištěných skutečnostech zachovávat mlčenlivost a zajistit jejich utajení.
g) Nepotřebná data (elektronická, na mediích i papírová) musí být vždy neprodleně skartována.
h) Všechny zásahy na serverech musí být předem odsouhlaseny Správcem IS a zaznamenány stanoveným způsobem.

7. Ochrana proti škodlivým kódům

a) Všechny servery a pracovní stanice jsou vybaveny antivirovým skenerem. Výjimky schvaluje Správce IS.
b) Pokud některé aplikace nabízejí možnost zvýšené ochrany, musí být odpovídajícím způsobem nastavena. Způsob nastavení schvaluje Správce IS.
c) Nebezpečné typy souborů jsou blokovány na hranicích bezpečnostního perimetru. 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 ZK, ale i na přístupových bodech a svých vlastních zařízeních.

8. 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.

9. Používání internetu

a) Druhá smluvní strana může používat při práci v IS ZK internet pouze pro účely plnění smlouvy a za podmínky dodržování všech všeobecně uznávaných 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 ZK.

10. Tisk

a) Druhá smluvní strana může tisknout na tiskárnách ZK 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.

11. 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.