ČESKÁ TELEKOMUNIKAČNÍ INFRASTRUKTURA

BEZPEČNOST, OCHRANA MAJETKU A OSOB

PŘÍLOHA 5

Obsah

1 Rozsah dokumentu

Smluvní strany při své činnosti odpovídají za dodržování příslušných ustanovení obecně platných právních předpisů a norem upravujících jejich povinnosti v oblasti BOZP, ochrany majetku, požární ochrany, bezpečnosti technických zařízení a ochrany životního prostředí.

Smluvní strany dále odpovídají za zajištění kontinuity činností a bezpečnosti informací a plnění (včetně koordinovaného plnění) požadavků zákona č.181/2014 o kybernetické bezpečnosti.

K zajištění řádného plnění požadavků všemi svými zaměstnanci smluvní strany provedou jejich proškolení, poučení či seznámení v rozsahu odpovídajícím jejich pracovnímu zařazení.

Na základě požadavku smluvní strany mohou být do rozsahu tohoto školení zahrnuty i některé vybrané interní předpisy společností.

2 Ochrana informací

Pro poskytování služeb Přístupu ke koncovým úsekům jsou smluvní strany povinny zabezpečit ochranu informací vyplývající zejména z ustanovení zákonů č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů v platném znění (zákon o elektronických komunikacích) a zákona č. 181/2014 o kybernetické bezpečnosti.

2.1 Základní pravidla pro zaměstnance smluvních stran

Pro zabezpečení ochrany dat vyplývající z ustanovení výše uvedených zákonů, jsou zaměstnanci smluvních stran povinni dodržovat následující zásady.

Zaměstnanci smluvních stran jsou povinni zejména:

- odpovídajícím způsobem chránit veškeré informace protistrany, a to zcela bez ohledu na jejich formu uložení (flash disky, mobilní telefony, papírové dokumenty, notebooky, disky, vyměnitelná média, apod.),
- chránit výpočetní techniku (PC, notebook, telefon, PDA, flash disk apod.) před neoprávněným přístupem a poškozením,
- počínat si vždy tak, aby se minimalizovala možnost zavlečení škodlivého kódu do prvků infrastruktury informačních systémů smluvních stran,
- udržovat v tajnosti přihlašovací údaje, hesla a klíče a neprodleně učinit příslušná opatření při jejich kompromitaci, tzn. v okamžiku, kdy se tyto údaje, hesla a klíče stanou známé komukoli dalšímu kromě konkrétního zaměstnance (např. u certifikátů zažádat okamžitě o zneplatnění, u hesel provést okamžitě jejich změnu atd.),
- neprodleně hlásit bezpečnostní incidenty, a pokud jsou vyzváni, poskytovat nezbytnou součinnost při řešení jakéhokoli bezpečnostního incidentu,
- obrátit se na svého garanta nebo zaměstnance jednotky Bezpečnost s žádostí o pomoc, pokud by hrozilo, že jakýmkoli způsobem bude ohroženo plnění povinností dle této přílohy.

- Zaměstnanci smluvních stran se musí zdržet zejména:
- takového jednání, které je v rozporu s dobrými mravy a platnými zákony České republiky,
- zneužívání jakýkoliv případných bezpečnostních slabin informačních systémů nebo jejich vyhledávání (pokud nesouvisí s výkonem práce zaměstnance),
- instalace a spouštění programového vybavení, které nebylo schváleno pro prostředí dané smluvní strany nebo nesouvisí s výkonem jeho práce,
- předávání chráněných informací druhé smluvní strany jakýmkoli neoprávněným osobám,
- volby jednoduchých hesel, resp. hesel, která jsou v rozporu s příslušnou politikou, s níž byl zaměstnanec seznámen,
- sdělování hesel, klíčů a dalších přihlašovacích údajů jakýmkoli jiným osobám,
- nedůsledné ochrany hesel a dalších přihlašovacích údajů, zejména v podobě zapisování na papírky a jejich umisťování na volně přístupná místa (monitory, klávesnice apod.),
- modifikace nastavení prvků sítě (pokud nesouvisí s výkonem jeho práce),
- ponechání jakékoliv výpočetní techniky nebo jakýchkoliv materiálů obsahující informace smluvních stran bez dozoru (např. v automobilech),
- výkonu takové činnosti, která nesouvisí s výkonem práce (a kde hrozí nebezpečí stažení škodlivého kódu) zejména:
  - návštěvy neznámých WWW stránek nebo stránek, kde hrozí nebezpečí stažení škodlivého kódu,
  - stahování a přenášení souborů informačních systémů neznámého původu nebo zdroje (včetně otevírání příloh e-mailu, kde si uživatel není jist původem e-mailu či obsahem přílohy) a souborů, u kterých hrozí zavlečení škodlivého kódu,
  - využívání jakýchkoliv dalších komunikačních nástrojů, kde výše popsané nebezpečí hrozí.

2.2 Výměna informací a jejich klasifikace

Smluvní strany jsou si vzájemně povinny vyměnit si řídicí dokumenty upravující ochranu informací respektive uvést klasifikační stupně smluvních stran a zajistit adekvátní ochranu informací protistrany.

Uvést, které informace lze předávat případným subdodavatelům bez souhlasu a které klasifikace pouze se souhlasem smluvní strany.

2.3 Kontinuita činností a ochrana bezpečnosti informací

Obě strany zajistí kontinuitu činností a ochranu bezpečnosti informací v souladu s touto přílohou a obecně uznávanými mezinárodními standardy řady ISO/IEC 27000 dle následujícího seznamu:

a) ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements,

b) ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls,

c) ISO/IEC 27011 Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002,

d) ISO/IEC 27031 Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity,

e) ISO/IEC 27033 1-5 Information technology — Security techniques — Network security,

f) ISO/IEC 27035 Information technology — Security techniques — Information security incident management

g) ISO 22301 Societal security -- Business continuity management systems --- Requirements

h) ISO 22313 Societal security -- Business continuity management systems – Guidance

3 Fyzická bezpečnost, ochrana osob a majetku, požární ochrana a ochrana životního prostředí

3.1 Vstupy do objektu

Smluvní strana umožní oprávněným osobám protistrany a jeho smluvních dodavatelů vstup do prostor nacházejících se v jeho objektech v souladu s interními pravidly, která ke vstupu do objektů vydala a se kterými byla protistrana seznámena, v časech podle požadavků protistrany, pokud tomu nebrání omezení vyplývající z ochranných opatření a režimů uplatňovaných smluvní stranou v předmětném objektu a tato omezení byla protistraně známa před podpisem této Smlouvy o Přístupu ke koncovým úsekům, nebo s ním byla projednána v souvislosti s jejich vznikem.

Protistrana zajistí, a to i u svých dodavatelských nebo jiných smluvních subjektů, dodržování pravidel vstupu do budov smluvní strany a podmínek přítomnosti či regulace pohybu v nich stanovených smluvní stranou. V tomto smyslu budou osoby protistrany používat stanovené vstupní doklady a protistrana k jejich vydání předá smluvní straně potřebné údaje. Obě smluvní strany určí kontaktní osoby, odpovědné za přímé administrativní vyřizování potřebných vstupních dokladů a souvisejících náležitostí.

Pokud se zaměstnanci smluvní strany nebo jeho dodavatelů nacházejí v objektech některé smluvní strany, musí být označeni svou identifikační/vstupní kartou připevněnou na viditelném místě. Tyto osoby mohou vstupovat a pohybovat se pouze v prostorech, pro které jim bylo uděleno vstupní oprávnění.

Osoby nacházející se mimo určený prostor nebo bez řádného označení, mohou být požádány, aby opustily objekt. Při opakovaném porušování stanovených pravidel bude osobám, které se tohoto přestupku dopustily, povolení přístupu do objektů smluvní strany odebráno. Smluvní strany si při podpisu Smlouvy o Přístupu ke koncovým úsekům předají veškeré své interní předpisy vydané v oblasti vstupu do objektů a zajistí předávání aktualizací těchto předpisů.

3.2 Ochrana majetku

Obě Strany přijmou opatření k tomu, aby při své činnosti nezpůsobily škodu či jinou újmu na majetku a zařízení druhé Strany nebo třetích stran a jejich zaměstnanců.

V případě, že zaměstnanci jedné Strany způsobí poškození nebo poruchu na zařízení druhé Strany, musí o tom ihned informovat druhou Stranu telefonicky na stanovenou kontaktní linku (Helpdesk) druhé Strany.

Úmyslné poškození zařízení používaného k poskytování služeb sítě je považováno za závažné porušení smluvních pravidel s možností vyvození příslušných sankcí.

3.3 Požární ochrana

Obě Strany se zavazují, že jejich zaměstnanci i zaměstnanci jejich smluvních dodavatelů jsou proškoleni podle zákona o požární ochraně a budou dodržovat bezpečnostní pravidla a zásady požární ochrany, stanovené příslušnými obecnými právními předpisy a interními předpisy CETIN, vydanými v této oblasti.

Zaměstnanci obou Stran musí neustále udržovat na pracovišti v objektech CETIN pořádek a zajistit, aby požární východy a evakuační cesty byly trvale volné. Po skončení prací musí být odstraněny všechny nebezpečné předměty.

Poskytovatel nesmí v objektech CETIN používat bez povolení vlastní tepelné spotřebiče. V případě, že by Poskytovatel chtěl provádět činnosti se zvýšeným požárním nebezpečím nebo práce, které mohou ovlivnit provozuschopnost elektrické požární signalizace, musí tuto skutečnost předem ohlásit a projednat s odborně způsobilou osobou CETIN. CETIN vydává k těmto činnostem souhlas a stanovuje protipožární opatření, za nichž lze tyto činnosti vykonávat. Zaměstnanci obou Stran odpovědné za plnění povinností na úseku požární ochrany jsou uvedené v Přílohy 3 – Seznam kontaktních osob

Pokud činnost Poskytovatele vznikne v objektech CETIN požár a Poskytovatel se o tom dozví, vyrozumí bez zbytečného odkladu CETIN. Tím není dotčena povinnost Poskytovatele ohlásit požár hasičskému záchrannému sboru. Požáry a další požární incidenty (zahoření, zadýmení apod.) je Poskytovatel povinen ohlásit na Security HELP CETIN. Kontaktní telefony jsou uvedeny na Požární poplachové směrnici.

V objektech CETIN je zakázáno kouřit.

Pokud bude vyhlášen na pracovištích CETIN vyhlášen požární poplach a nařízena evakuace, jsou všechny osoby pracující pro Poskytovatele povinny neprodleně opustit ohroženou budovu. Při evakuaci se řídí požárními poplachovými směrnicemi.

3.4 Bezpečnost a ochrana zdraví při práci

Obě Strany se zavazují, že jejich zaměstnanci i zaměstnanci jejich smluvních dodavatelů jsou proškoleni podle zákoníku práce a prováděcích předpisů o bezpečnosti a ochraně zdraví při práci.

Poskytovatel odpovídá za to, že všichni jeho zaměstnanci, kteří budou provádět práce, jsou k práci zdravotně a odborně způsobilí, mají platné zdravotní prohlídky v rozsahu kategorizací prací a na vyžádání je schopen CETIN předložit. Poskytovatel garantuje, že veškeré stroje, strojní zařízení, el. nářadí, el. prodlužovací kabely a zařízení, jichž užívá v souvislosti s plněním této smlouvy, jsou v dobrém technickém stavu, odpovídají příslušným ČSN a ČSN EN normám a všechny tyto stroje, strojní zařízení, el. nářadí, el. prodlužovací kabely a zařízení jsou podrobovány pravidelnému servisu v souladu s doporučenými lhůtami výrobce a dle platných ČSN a ČSN EN a ISO norem.

Poskytovatel je povinen dodržovat opatření vyplývající z právních a ostatních předpisů k zajištění BOZP, opatření CETIN a rovněž svá vlastní opatření, která mají za cíl předcházet rizikům, odstraňovat je nebo minimalizovat působení neodstranitelných rizik. V případě vzniku úrazu nebo jakéhokoli zranění zaměstnance Poskytovatele v prostorách CETIN, ohlásí Poskytovatel tuto skutečnost CETIN. Obě strany budou navzájem spolupracovat při šetření příčin a okolností vzniku úrazu. Záznam o úrazu sepisuje Poskytovatel a výsledek šetření projedná s CETIN.

Pokud Poskytovatel zjistí jakékoli riziko vedoucí k úrazu v prostorách CETIN, oznámí tuto skutečnost na Security HELP CETIN.

3.5 Ochrana životního prostředí

Poskytovatel se zavazuje, že jeho zaměstnanci i pracovníci jeho smluvních dodavatelů se budou chovat v souladu s platnými právními předpisy ČR i EU na ochranu životního prostředí.

Poskytovatel je rovněž povinen dodržovat interní environmentální předpisy CETIN, se kterými byl prokazatelně seznámen.

V prostorách, pro které je vypracován provozní řád, místní provozní předpis, havarijní plán závadných látek nebo jiné pokyny pro případ poruch a havárií, je povinností Poskytovatele se s těmito předpisy prokazatelně seznámit a zaměstnanci Poskytovatele i jeho smluvních dodavatelů jsou povinni je dodržovat.

Poskytovatel je původcem odpadů vzniklých z jeho činnosti dle této smlouvy v předmětných prostorách. Je povinen s odpady nakládat (shromažďování, soustřeďování, sběr, třídění, přeprava a doprava, skladování, evidence) v souladu se zákonem č. 185/2001 Sb., o odpadech a o změně některých dalších zákonů, ve znění pozdějších předpisů, a jeho prováděcími vyhláškami.

CETIN má právo na náhradu škody, včetně škody vzniklé uložením sankcí od orgánů státní či veřejné správy, kterou by druhá smluvní strana porušením takových platných právních předpisů prokazatelně způsobila.

4 Bezpečnostní postupy

4.1 Proces hlášení řešení bezpečnostních incidentů

CETIN bude hlásit bezpečnostní události a incidenty na kontaktní místo Poskytovatele. Poskytovatel bude hlásit bezpečnostní incidenty spojené s jím užívanými službami na kontaktní místo Security HELP CETIN viz 5.8 Kontaktní místa pro řešení problémů.

V případě incidentu, který je smluvní stranou hodnocen jako kritický, bude druhá smluvní strana spolupracovat na jeho řešení tak, aby nebyly narušeny procesy a kontinuita činností obou smluvních stran a nebyla ohrožena bezpečnost kritické infrastruktury.

4.2 Řízení přístupů k IS

Pro řízení přístupu k informačním systémům a technologiím sloužícím k realizaci a služeb Poskytovatelem musí být použit transparentní systém řízení přístupu.

4.3 Propojování informačních systémů a rušení propojení

Pro propojování informačních systémů pro účely výměny dat a jejich rušení jsou použity transparentní mechanismy na základě postupů na straně poskytovatele i objednatele. Mechanismy připojení musí zajistit, že kromě předávání určených dat bude zamezeno možnosti vzájemného ovlivnění informačních prostředí.

4.4 Řízení zranitelností

Poskytovatel i objednatel mají ustaveny procesy řízení zranitelností.

4.5 Bezpečnostní monitoring

Pro potřeby bezpečnostního monitoringu na straně objednatele budou ze strany CETIN poskytovány potřebné logové extrakty v dohodnuté časové periodicitě

4.6 Proces hlášení ohrožení bezpečnosti a ochrany sítě

Poskytovatel, který zjistí jakékoliv aktivity či skutečnosti ohrožující bezpečnost osob nebo které mohou způsobit škodu na objektu, zařízení nebo mít dopad na poskytované služby, musí tyto aktivity ohlásit prostřednictvím formuláře Hlášení o porušení bezpečnosti a ochrany sítě. CETIN podnikne kroky k nápravě.

Hlášení o porušení bezpečnosti a ochrany sítě/ochrany osobních údajů

Vyplní Strana (CETIN nebo Poskytovatel) podávající stížnost

Datum podání stížnosti	
Společnost podávající stížnost	
Adresa firmy	
ID firmy (jde-li o Poskytovatele)	
Kontaktní osoba firmy:	
Kontaktní adresa firmy	
Datum vzniku případu	
Popis ohrožení nebo hmotné škody	
Důsledek ohrožení	

5 Kontaktní místa pro řešení problémů

K řešení vzniklých problémů v oblasti bezpečnosti, ochrany majetku a osob zřídí obě Strany kontaktní místa s nepřetržitou 24 hodinovou službou.

V rámci CETIN plní funkci tohoto kontaktního místa Security HELP podle Přílohy 3 – Seznam kontaktních osob

Kontaktním místem Poskytovatele je pracoviště uvedené v Příloze 3 – Seznam kontaktních osob.

Na tato kontaktní místa budou obě Strany vzájemně oznamovat všechny případy porušení bezpečnosti, vznik úrazu, požáru, poškození majetku a zařízení, ztráty vstupních karet nebo klíčů, případy vandalizmu, nebezpečné situace, které ohrožují osobní bezpečnost zaměstnanců nebo mohou způsobit škody na objektu, zařízení nebo službách.

Jestliže konkrétní pracovní aktivita představuje bezprostřední ohrožení bezpečnosti zaměstnanců druhé Strany, přímý zásah do plnění závazků při poskytování služeb, nebo bezprostředně ohrožuje fyzickou integritu zařízení druhé Strany, pak tato Strana provede příslušná opatření k nápravě vzniklé situace na náklady Strany, která tuto situaci způsobila.

Strany zodpovídají za seznámení svých zaměstnanců a zaměstnanců svých smluvních dodavatelů a partnerů s uvedenými bezpečnostními požadavky a možnými sankcemi při jejich nedodržení.