Příloha č.1 Bezpečnostní politika informací společnosti ČEZ Energetické služby, s.r.o.

BEZPEČNOSTNÍ POLITIKA INFORMACÍ

společnosti ČEZ Energetické služby, s.r.o.

Obsah:

1. Úvodní ustanovení

1) Vedení společnosti ČEZ Energetické služby, s.r.o. (dle jen ČEZ ES) vyhlašuje zásady bezpečnosti informací.
2) Tato politika je závazná pro všechny zaměstnance společnosti, kterých se systém řízení bezpečnosti informací týká ČEZ ES a spolupracující organizace.
3) K zajištění bezpečnosti informací a podpory bezpečnosti informací ve společnosti ČEZ ES se touto politikou:

   a) popisuje a vysvětluje bezpečnost informací
   b) stanovují bezpečnostní cíle
   c) stanovuje rozsah a důležitost bezpečnosti informací
   d) uvádí stručný výklad základních bezpečnostních zásad
   e) stanovují kritéria, kterými bude hodnoceno riziko a definuje struktura hodnocení rizik

4) Bezpečnost informací je charakterizována jako zachování důvěrnosti, integrity a dostupnosti informací.

   a) důvěrnost je zajištění toho, že informace je přístupná jen těm, kteří jsou oprávněni k ní mít přístup
   b) integrita je zabezpečení přesnosti a kompletnosti informací a metod jejich zpracování
   c) dostupnost je zajištění toho, že jsou informace a s nimi spojená aktiva uživatelům přístupná v době, kdy je potřebují.

5) Bezpečnostním cílem spojeným s bezpečností informací ve společnosti ČEZ ES je zajištění dostupnosti informačních aktiv jen oprávněným osobám, správnosti a kompletnosti informací, důvěrnosti a bezpečnosti jejich zpracování a ochrany informací proti náhodnému nebo neoprávněnému zničení nebo náhodné ztrátě, proti neoprávněnému přístupu, změnám nebo šíření, a to v souladu se zákony a jinými právními předpisy ČR.
6) Bezpečnost informací pokrývá celou strukturu společnosti ČEZ ES ve všech lokalitách a spolupracující organizace, které přichází do styku se zabezpečenými informacemi společnosti ČEZ Energetické služby, s.r.o. Bezpečnost informací pokrývá všechna důležitá informační aktiva společnosti ČEZ Energetické služby, s.r.o.
7) Tato politika 1x ročně podléhá posouzení aktuálnosti.
8) Za posouzení aktuálnosti dokumentu bezpečnostní politiky informací odpovídá vedoucí odboru Integrované řízení kvality.
9) Záměrem vedení společnosti ČEZ ES je udržovat přiměřenou ochranu informačních aktiv v souladu se zákony a jinými právními předpisy ČR, a to i v případech, kdy byla odpovědnost za zpracování informací přenesena na spolupracující organizace.

2. Cíle a zásady bezpečnosti informací

1) Zaměstnanci společnosti ČEZ ES v rámci dodržování bezpečnosti informací zajišťují:

   a) ochranu práv a svobod jednotlivců, zejména právo na soukromí uznané v článku 7 Úmluvy o ochraně lidských práv a základních svobod, usnesení předsednictva ČNR č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky.
   b) ochranu osobních údajů a citlivých údajů podle zákona.
   c) ochranu obchodního tajemství podle zvláštního právního předpisu a obsahu smluv obchodně závazkových vztahů, pokud se k tomu společnosti ČEZ ES v uzavřené smlouvě zavázala.
   d) ochranu listovního tajemství atd.

2) Vedení společnosti ČEZ ES podporuje stanovené cíle bezpečnosti informací. Vedení společnosti ČEZ ES vyjadřuje touto bezpečnostní politikou informací svoji strategii trvalého zajišťování bezpečnosti informací jako nedílné součásti řídicích procesů společnosti ČEZ ES.

3. Organizace bezpečnosti

1) Záměrem vedení společnosti ČEZ ES je řídit bezpečnost informací ve společnosti ČEZ ES a koordinovat implementaci bezpečnostních opatření ve společnosti ČEZ ES dle stanovené působnosti a odpovědnosti vedoucích zaměstnanců a zlepšit řízení a koordinaci bezpečnosti informací ve společnosti ČEZ ES dle normy ČSN ISO/IEC 27 001.
2) Systém managementu bezpečnosti informaci je koordinován PV IMS a to na základě auditů, přezkoumání vedením a přezkoumáváním dokumentace
3) Povinnosti spojené s řízením bezpečnosti informací ve společnosti ČEZ ES vykonává vedoucí technik informačních řídicích systémů, který přezkoumává a sleduje bezpečnostní incidenty, sleduje významné změny zranitelnosti informačních aktiv společnosti ČEZ ES a schvaluje hlavní kroky vedoucí ke zvýšení bezpečnosti informací.
4) Dodržování a plnění bezpečnostní politiky zajišťují všichni vedoucí zaměstnanci společnosti ČEZ ES dle stanovené působnosti a odpovědnosti.

4. Politika mobilních zařízení

1) Cílem je zajistit bezpečnost informací při používání mobilních zařízení.
2) Každé mobilní zařízení je evidováno, má instalovánu proaktivní ochranu před hrozbami. Dle potřeb MDM pro případ ztráty nebo krádeže a omezení instalace SW.
3) V případě potřeby je zajištěno šifrování zařízení pro zajištění bezpečnosti dat.

5. Politika práce na dálku

1) ČEZ ESL plně podporuje moderní technologie umožňující operativní a plnohodnotnou práci mimo pracoviště.
2) Podmínkou je plně dodržet všechna bezpečnostní pravidla, aby nemohlo dojít o ohrožení informační bezpečnosti.
3) Jsou nastavena jednoznačná pravidla práce na dálku a nastaven systém důsledné kontroly.

6. Bezpečnost lidských zdrojů

1) Účelem bezpečnosti lidských zdrojů je snížení rizika lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace.
2) Bezpečnostním cílem je zajištění vhodných postupů v rámci přijímacího řízení; dále je cílem zajistit povědomí zaměstnanců o bezpečnosti informací.
3) Posuzování uchazečů o zaměstnání z hlediska bezpečnosti je součástí výkonu personálních činností dle Pracovního řádu a v souladu s obsahem pracovněprávních dokumentů.
4) Zaměstnanci společnosti podepisují prohlášení o mlčenlivosti formou závazku zaměstnance ve smyslu zákonem uložené povinnosti.
5) Zaměstnanci společnosti ČEZ ES jsou povinni zachovávat mlčenlivost o skutečnostech, se kterými se seznámili při plnění úkolů ve společnosti ČEZ ES nebo v přímé souvislosti s nimi a tato povinnost trvá i po skončení pracovního vztahu, pokud zvláštní právní předpis nestanoví jinak.
6) zaměstnanec musí být seznámen s povinnostmi a odpovědností z hlediska bezpečnosti informací při skončení nebo změně pracovního vztahu.
7) Seznámení zaměstnanců s bezpečnostní politikou je součástí vstupního školení a dalších periodických školení.
8) Zaměstnanci musí znát postupy hlášení bezpečnostních incidentů.

9) Nedodržení bezpečnostních zásad může být kvalifikováno jako porušení povinností zaměstnance příp. porušení pracovní kázně s příslušnými důsledky pro zaměstnance,
10) Šetření závažných bezpečnostních incidentů zajišťuje vedoucí technik informačních řídicích systémů včetně zpracování protokolů o bezpečnostních incidentech, jejich evidence a předložení návrhů generálnímu řediteli společnosti ČEZ ES k zajištění bezpečnosti.

7. Klasifikace a řízení informačních aktiv

1) Účelem klasifikace a řízení informačních aktiv je udržovat přiměřenou ochranu informačních aktiv.
2) V rámci společnosti ČEZ ES je zavedena a udržována evidence důležitých informačních aktiv, u nichž je určen vlastník a jednoznačně stanovena odpovědnost za dodržování povinností při jejich zpracování, shromažďování a uchovávání v souladu s platnými předpisy.
3) Informační aktiva společnosti ČEZ ES jsou řízena tak, aby byla identifikována, posouzena resp. ohodnocena vč. odhadu hrozeb, zranitelností a rizik.
4) Klasifikaci stanoví vlastníci informačních aktiv nebo vlastníci procesů, kteří odpovídají za periodické přezkoumávání této klasifikace a její aktualizaci.
5) Klasifikace určuje také způsob zacházení s informacemi s ohledem na jejich ochranu.
6) Jsou stanovena pravidla pro manipulaci s médii, ochraně informací na médiích a jejich likvidace.
7) Jsou stanoveny postupy při ukončení pracovního poměru nebo smlouvy týkající se ochrany informací a navrácení aktiv.

8. Fyzická bezpečnost a bezpečnost prostředí

1) Účelem fyzické bezpečnosti a bezpečnosti prostředí je předcházet neoprávněnému a neautorizovanému přístupu k informacím, poškození a narušení informací.
2) Bezpečnostním cílem je zajištění fyzické ochrany informací a prostředí, ve kterém se informace nacházejí:

   a) vymezením a využíváním zabezpečených oblastí, zahrnujících kontrolu vstupu a upřesněním způsobu práce osob v těchto oblastech, zabezpečením kanceláří, místností a zařízení, ochranou proti hrozbám působícím z vnějšího prostředí, zejména tam, kde se informace nacházejí, zpracovávají a uchovávají
   b) zabezpečením zařízení proti odcizení a zničení, poškození, zahrnujícím bezpečné umístění zařízení, zajištěním podpůrných služeb pro provoz zařízení (dodávky energie, klimatizace atd.), zabezpečením kabeláže a zajištěním pravidelné a bezpečné údržby zařízení
   c) zajištěním bezpečnosti informací mimo objekty společnosti ČEZ ES

3) Stanovení režimu vstupu a výstupu osob včetně zajištění zabezpečených oblastí a definování fyzického bezpečnostního perimetru je ve společnosti ČEZ ES stanoveno samostatnou politikou a společnou dokumentací Skupiny ČEZ.
4) Zajištění požární bezpečnosti podle zákonů a jiných právních předpisů v společnosti ČEZ ES je upraveno zvláštní vnitřní organizační politikou.
5) Vstup do budov společnosti ČEZ ES oprávněným orgánům ke zdolání požáru nebo k provedení jiných záchranných prací dle rozhodnutí velitele zásahu stanovuje dokumentace zdolávání požáru a navazující dokumentace požární ochrany ČEZ Energetické služby, s.r.o.
6) Uplatnění zásad čistého stolu a čisté obrazovky spadá do kompetence vedoucích zaměstnanců společnosti ČEZ Energetické služby, s.r.o.

9. Řízení bezpečnosti komunikací a provozu

1) Účelem řízení bezpečnosti komunikací a provozu je zajistit správný a bezpečný provoz prostředků pro zpracování informací, minimalizovat riziko selhání systému, chránit integritu a dostupnost programů, dat a informačních systémů, chránit důvěrnost informací a zajistit ochranu počítačových sítí.
2) Bezpečnostním cílem je zajištění ochrany informací prostřednictvím:

   a) ochrany proti škodlivým a automaticky spouštěným programům
   b) zálohování, aby tak byla zajištěna obnova dat a systémů ve vazbě na zachování základních funkcí společnosti ČEZ ES
   c) zpracování postupů obnovy po selhání nebo výpadku systému pro zpracování a uchování informací
   d) správy bezpečnosti počítačových sítí
   e) zajištění dostupnosti informací a služeb
   f) zajištění důvěrnosti informací při jejich přenosu pomocí kryptografické ochrany
   g) ochrany před neautorizovanými zásahy dodržováním principu oddělení povinnosti a odpovědnosti při přidělování uživatelských práv
   h) monitorování provozu a zaznamenávání událostí
   i) opatření pro zajištění bezpečnosti elektronické pošty
   j) dodržování bezpečnosti při zacházení s paměťovými médii

10. Řízení přístupu

1) Účelem řízení přístupu k informacím a prostředkům informačních systémů společnosti ČEZ ES je zajistit, aby k nim měli přístup pouze oprávnění uživatelé. Pro přístup k těmto prostředkům jsou stanovena pravidla, která určují postupy pro autorizaci, zřizování, změny a odebírání přístupových práv.
2) Bezpečnostním cílem je zajištění řízení přístupu realizací opatření v následujících oblastech:

   a) správa přístupu uživatelů a odpovědnost uživatelů – systém správy přístupu zajistí definovaný postup přidělování, změny a odebírání přístupu, správu hesel a kontrolu přístupových práv.
   b) Řízení přístupu k síti, operačním systémům, aplikacím a informacím – systém správy přístupu zajistí definované postupy řízení přístupu uživatelům ke zmíněným prostředkům informačního systému

11. Politika bezpečnosti informací pro dodavatelské vztahy

1) Součástí smluvních vztahů musí být podmínky dodržování bezpečnosti informací v souladu s ustanovenými politikami a postupy
2) Dodavatel smí mít přístup pouze k těm informacím, které potřebuje pro realizaci díla
3) Musí existovat analýza příslušných rizik a návrhy na jejich eliminaci
4) Po ukončení smluvního vztahu musí být provedeno vyhodnocení z hlediska dodržování bezpečnosti informací.

12. Vývoj a údržba systémů

1) Účelem je prosadit bezpečnost informací do celého životního cyklu provozovaných informačních systémů od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu. Implementace a změny informačních systémů společnosti ČEZ ES jsou spojeny se stanovením vhodných bezpečnostních požadavků.

2) Bezpečnostním cílem je zajištění ochrany prostřednictvím opatření v následujících oblastech:

   a) analýza a specifikace bezpečnostních požadavků – určení bezpečnostních požadavků v klíčových fázích životního cyklu informačního systému zajistí, aby bezpečnost byla nedílnou součástí informačních systémů
   b) zajištění přesnosti a spolehlivosti zpracování dat v aplikacích a kryptografická opatření – validace a kontrola dat má spolu s kryptografickými opatřeními za cíl předcházet ztrátě, neoprávněné modifikaci nebo zneužití dat v aplikacích;
   c) bezpečnost systémových souborů a procesu vývoje a podpory – je nutné zabezpečit systémové soubory a zdrojový kód a kontrolovat postupy vývoje a podpory, včetně formalizovaného postupu řízení změn;
   d) správa zranitelností – je nutné vhodnými opatřeními omezit rizika vyplývající ze zneužití publikovaných zranitelností.

3) Vývoj a údržba informačních systémů v rozsahu infrastruktury společnosti ČEZ ES a uživatelsky vyvinutých aplikací je podle stanovené působnosti zajišťována dodavateli jednotlivých systémů včetně zajišťování implementace bezpečnostní politiky v oblasti procesů IT.

13. Politika kryptografických prostředků

1) Cílem je zajistit ochranu informací před zneužitím a neoprávněnou modifikací.
2) Všechny informace, které mohou být takto ohroženy, musí být chráněny vhodnými kryptografickými prostředky.
3) Kryptografické klíče, postupy používání, principy ochrany musí být zajištěny po celou dobu životnosti informací a klíčů.
4) Pro systém používání kryptografických prostředků musí být zpracována příslušná dokumentace.

14. Řízení projektů

1) Cílem je zajistit, aby každý projekt realizovaný ve společnosti ČEZ ESL odpovídal požadavkům bezpečnosti informací.
2) Součástí projektů libovolného typu musí být implementace systému bezpečnosti informací.
3) Za implementaci systému v rámci projektu odpovídá příslušný projektový manažer.

15. Řízení kontinuity činností

1) Záměrem vedení společnosti ČEZ ES je zajistit připravenost společnosti ČEZ ES k řešení krizových situací a zachování základních funkcí v rozsahu fungování kritické infrastruktury.
2) Bezpečnostním cílem je zajištění přípravy, proškolení a připravenosti určených zaměstnanců společnosti ČEZ ES po odborné stránce k výkonu činností spojených s řešením krizových situací, ochranou zdraví a života zaměstnanců a ochranou majetku.
3) Přechod na krizové řízení spadá do kompetence společnosti ČEZ Energetické služby, s.r.o..
4) Přijetí preventivních opatření k zachování základních funkcí spadá do kompetence společnosti ČEZ ES

16. Soulad s požadavky

1) Pro zabezpečení informací společnosti ČEZ ES jsou jednoznačně definovány a zdokumentovány všechny relevantní zákonné a smluvní požadavky. V rámci společnosti ČEZ ES musí být veden přehled platných právních norem a předpisů vztahujících se k problematice bezpečnosti informací.

2) Společnost ČEZ ES dodržuje ustanovení o autorském právu a podmínky licenčních ujednání dodavatelů programového vybavení.
3) K posouzení shody bezpečnostní politiky informací v společnosti ČEZ ES a navazujících předpisů se skutečným stavem bezpečnosti informací a k zajištění souladu informačního systému společnosti ČEZ ES s příslušnými technickými normami je prováděno posouzení shody.
4) Společnost ČEZ ES přijímá a provádí opatření k zajištění ochrany osobních údajů a citlivých údajů v souladu se zákony a jinými právními předpisy.

17. Regulatorní, legislativní a smluvní požadavky na bezpečnost informací

1) Zajištění bezpečnosti informací společnosti ČEZ ES se realizuje v souladu s regulatorními, legislativními a smluvními požadavky zákonů a jiných právních předpisů s důrazem na povinnosti při ochraně informací.
2) Vyjádřené specifické bezpečnostní požadavky společnosti ČEZ ES zpřesňují výběr opatření ke snížení rizika na přijatelnou úroveň dle normy ČSN ISO/IEC 27001 s ohledem na jejich implementaci ve společnosti ČEZ Energetické služby, s.r.o.

18. Kritéria hodnocení rizik

1) Bezpečnostní opatření jsou vybrána na základě prováděného hodnocení rizik a požadavků zákonných norem.
2) Hodnocení rizik je prováděno na základě následujících kritérií:

   a) stanovení hodnot informačních aktiv společnosti ČEZ ES z hlediska požadavků na jejich dostupnost, důvěrnost a integritu,
   b) určení možných dopadů identifikovaných hrozeb, reálné pravděpodobnosti jejich uskutečnění a určení úrovně rizik pro aktiva,
   c) určení akceptovatelné úrovně rizika pro informační aktiva společnosti ČEZ ES.

19. Stanovení obecných a specifických odpovědností pro bezpečnost informací

1) Obecné odpovědnosti pro oblast bezpečnosti informací vyplývají pro zaměstnance společnosti ČEZ ES ze směrnic EU, zákonů a jiných právních předpisů ČR.
2) Specifické odpovědnosti pro oblast bezpečnosti informací v společnosti ČEZ ES vyplývají pro zaměstnance společnosti ČEZ ES zejména z vnitřních organizačních dokumentů, povinností uložených nadřízenými vedoucími zaměstnanci a dle pracovního zařazení.
3) Bezpečnostní politiku informací jsou povinni dodržovat všichni zainteresovaní zaměstnanci společnosti ČEZ ES; její plnění kontrolují vedoucí zaměstnanci společnosti ČEZ ES v rozsahu stanovené působnosti a odpovědnosti.
4) Kontrolní činnost v oblasti bezpečnosti informací metodicky usměrňuje vedoucí technik informačních řídicích systémů.

20. Závěrečná ustanovení

1) Tato politika nabývá účinnosti dnem 1. 9. 2015.