BEZPEČNOSTNÍ POLITIKA

PRO BEZPEČNOST INFORMACÍ V ORGANIZACI

Název organizace	Základní škola kpt. Jaroše, Trutnov, Gorkého 38
Identifikační číslo	64201112
Sídlo organizace	Maxima Gorkého 38, 541 01 Trutnov
Datum zpracování	26.4.2018
Platnost a účinnost	25.5.2018
Odpovědná osoba	Mgr. Paták Jiří

OBSAH

1. ÚVODNÍ USTANOVENÍ

Vedení Organizace vyhlašuje zásady bezpečnosti informací. Tato politika je závazná pro všechny zaměstnance Organizace, a také spolupracující organizace.

K zajištění bezpečnosti informací a podpory bezpečnosti informací v Organizaci 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.

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 uživatelům přístupná v době, kdy je potřebují.

Bezpečnostním cílem spojeným s bezpečností informací v Organizaci 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.

Bezpečnost informací pokrývá celou strukturu Organizace ve všech lokalitách a spolupracující organizace, které přichází do styku se zabezpečenými informacemi spravovaných Organizací. Bezpečnost informací pokrývá všechna důležitá informační aktiva Organizace.

Tato politika podléhá pravidelné revizi v intervalu jeden krát ročně.

Za revizi dokumentu bezpečnostní politiky informací odpovídá statutární zástupce Organizace.

Záměrem Organizace 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

Zaměstnanci Organizace 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 zvláštního 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.

Vedení Organizace podporuje stanovené cíle bezpečnosti informací. Vedení Organizace vyjadřuje touto bezpečnostní politikou informací svoji strategii trvalého zajišťování bezpečnosti informací jako nedílné součásti řídících procesů Organizace.

3. ORGANIZACE BEZPEČNOSTI

Záměrem Organizace je, řídit bezpečnost informací a koordinovat implementaci bezpečnostních opatření dle stanovené působnosti a odpovědnosti vedoucích zaměstnanců a zlepšit řízení a koordinaci bezpečnosti informací v organizaci.

Povinnosti spojené s řízením bezpečnosti informací v Organizaci vykonává statutární zástupce organizace nebo pověřený pracovník, a to ve spolupráci s Pověřencem pro ochranu osobních údajů, který přezkoumává a sleduje bezpečnostní incidenty, sleduje významné změny zranitelnosti informačních aktiv Organizace a schvaluje hlavní kroky vedoucí ke zvýšení bezpečnosti informací.

Provádění bezpečnostní politiky zajišťují všichni vedoucí zaměstnanci Organizace dle stanovené působnosti a odpovědnosti.

4. KLASIFIKACE A ŘÍZENÍ INFORMAČNÍCH AKTIV

Účelem klasifikace a řízení informačních aktiv je udržovat přiměřenou ochranu informačních aktiv.

V rámci Organizace je zavedena a udržována evidence osobních údajů, u nichž je minimálně určena, identifikace osobního údaje, jeho zdroj, kategorie, subjekt údajů, účel zpracování, operace zpracování a jednoznačně stanoveny osoby pověřené k nakládání s těmito osobními údaji v souladu s platnými předpisy.

Osobní údaje v Organizaci musí být katalogizovány tak, aby byl přesně stanoven účel jejich zpracování, zákonnost a kategorie.

Kategorizaci stanoví statutární zástupce Organizace, nebo Pověřenec pro ochranu osobních údajů, popřípadě pověření pracovníci, kteří odpovídají za periodické přezkoumávání této klasifikace a její aktualizaci.

Kategorizace určuje způsob zacházení s informacemi s ohledem na jejich ochranu a citlivost.

5. PERSONÁLNÍ BEZPEČNOST

Účelem personální bezpečnosti je snížení rizika lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace.

Bezpečnostním cílem je zajištění vhodných postupů v rámci přijímacího řízení; dále je cílem zajistit povědomí zaměstnanců o bezpečnosti informací.

Posuzování uchazečů o zaměstnání z hlediska personální bezpečnosti je součástí výkonu personálních činností dle Pracovního řádu a v souladu s obsahem pracovněprávních dokumentů v personálních šablonách.

Zaměstnanci podepisují prohlášení o mlčenlivosti formou závazku zaměstnance ve smyslu zákonem uložené povinnosti.

Zaměstnanci Organizace jsou povinni zachovávat mlčenlivost o skutečnostech, se kterými se seznámili při plnění pracovních úkolů nebo v přímé souvislosti s nimi a tato povinnost trvá i po skončení pracovního vztahu, pokud zvláštní právní předpis nestanoví jinak.

Seznámení zaměstnanců s bezpečnostní politikou je součástí vstupního školení a dalších periodických školení.

Zaměstnanci musí znát postupy hlášení bezpečnostních incidentů.

Nedodržení bezpečnostních zásad může být kvalifikováno jako porušení povinností zaměstnance příp. porušení pracovní kázně s příslušnými důsledky pro zaměstnance, ve smyslu zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, pokud se nejedná o přestupek podle § 44 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů nebo trestný čin podle § 178 zákona č. 140/1961 Sb., trestní zákon, ve znění pozdějších předpisů.

Šetření závažných bezpečnostních incidentů provádí statutární zástupce Organizace ve spolupráci s Pověřencem pro ochranu osobních údajů, včetně zpracování protokolů o bezpečnostních incidentech, jejich evidence a předložení dozorovému úřadu na jeho vyzvání.

6. FYZICKÁ BEZPEČNOST A BEZPEČNOST PROSTŘEDÍ

Účelem fyzické bezpečnosti a bezpečnosti prostředí je předcházet neoprávněnému a neautorizovanému přístupu k informacím, poškození a narušení informací.

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 Organizace.

Stanovení režimu vstupu a výstupu osob včetně zajištění zabezpečených oblastí a definování fyzického bezpečnostního perimetru je v Organizaci stanoveno samostatnou směrnicí pro řízení přístupů a dokumentací související s pověřením osob.

Zajištění požární bezpečnosti podle zákonů a jiných právních předpisů v Organizaci je upraveno zvláštní vnitřní organizační směrnicí.

Vstup do budov Organizace oprávněným orgánům ke zdolání požáru nebo k provedení jiných záchranných prací dle rozhodnutí velitele zásahu stanovuje dokumentace zdolávání požáru a navazující dokumentace požární ochrany Organizace.

Uplatnění zásad čistého stolu a čisté obrazovky spadá do kompetence vedoucích zaměstnanců Organizace.

7. ŘÍZENÍ BEZPEČNOSTI KOMUNIKACÍ A PROVOZU

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.

Bezpečnostním cílem je zajištění ochrany informací prostřednictvím:

a) ochrany proti škodlivým a automaticky spouštěným programům;
b) zálohování, tak aby byla zajištěna obnova dat a systémů ve vazbě na zachování základních funkcí Organizace;
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.

8. ŘÍZENÍ PŘÍSTUPU

Účelem řízení přístupu k informacím a prostředkům informačních systémů Organizace 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.

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. Řízení přístupu k síti, operačním systémům, aplikacím a informacím – systém správy přístupu zajistí definované postupy řízení přístupu uživatelům ke zmíněným prostředkům informačního systému
b) mobilní výpočetní prostředky a práce na dálku – zvláštní pozornost musí být věnována mobilním výpočetním prostředkům a prostředkům umožňujícím práci na dálku, aby bylo zabráněno jejich zneužití.

9. VÝVOJ A ÚDRŽBA SYSTÉMŮ

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 Organizace jsou spojeny se stanovením vhodných bezpečnostních požadavků.

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.

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

10. ŘÍZENÍ KONTINUITY ČINNOSTÍ

Záměrem vedení Organizace je zajistit připravenost Organizace k řešení krizových situací a zachování základních funkcí v rozsahu fungování kritické infrastruktury.

Bezpečnostním cílem je zajištění přípravy, proškolení a připravenosti určených zaměstnanců Organizace po odborné stránce k výkonu činností spojených s řešením krizových situací, ochranou zdraví a života zaměstnanců a ochranou majetku.

Do kompetence Organizace spadá:

a) přechod na krizové řízení v případě vzniku bezpečnostního incidentu;
b) přijetí preventivních opatření k zachování základních funkcí.

11. SOULAD S POŽADAVKY

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

Organizace dodržuje ustanovení o autorském právu a podmínky licenčních ujednání dodavatelů programového vybavení.

K posouzení shody bezpečnostní politiky informací v Organizaci a navazujících předpisů se skutečným stavem bezpečnosti informací a k zajištění souladu informačního systému Organizace s příslušnými technickými normami je prováděno posouzení shody.

Organizace přijímá a provádí opatření k zajištění ochrany osobních údajů a citlivých údajů v souladu se zákony a jinými právními předpisy.

12. REGULATORNÍ, LEGISLATIVNÍ A SMLUVNÍ POŽADAVKY NA BEZPEČNOST INFORMACÍ

Zajištění bezpečnosti informací Organizace se realizuje v souladu s regulatorními, legislativními a smluvními požadavky zákonů a jiných právních předpisů s důrazem na povinnosti při ochraně informací.

Vyjádřené specifické bezpečnostní požadavky Organizace zpřesňují výběr opatření ke snížení rizika na přijatelnou úroveň s ohledem na jejich implementaci v Organizaci.

13. KRITÉRIA HODNOCENÍ RIZIK

Bezpečnostní opatření jsou vybrána na základě prováděného hodnocení rizik v Organizaci s přihlédnutím k citlivosti osobních údajů.

Hodnocení rizik je prováděno na základě následujících kritérií:

a) stanovení citlivosti osobních údajů z hlediska požadavků na jejich dostupnost, důvěrnost a integritu;

b) určení možných dopadů identifikovaných hrozeb, reálné pravděpodobnosti jejich uskutečnění a určení úrovně rizik pro osobní údaje;
c) určení akceptovatelné úrovně rizika pro osobní údaje ve správě Organizace.

14. STANOVENÍ OBECNÝCH A SPECIFICKÝCH ODPOVĚDNOSTÍ PRO OSOBNÍ ÚDAJE

Obecné odpovědnosti pro oblast bezpečnosti informací vyplývají pro zaměstnance Organizace ze směrnic EU, zákonů a jiných právních předpisů ČR.

Specifické odpovědnosti pro oblast bezpečnosti informací v Organizaci vyplývají pro zaměstnance Organizace zejména z vnitřních organizačních směrnic, povinností uložených nadřízenými vedoucími zaměstnanci a dle pracovního zařazení.

Bezpečnostní politiku informací jsou povinni dodržovat všichni zaměstnanci Organizace; její plnění kontrolují vedoucí zaměstnanci Organizace v rozsahu stanovené působnosti a odpovědnosti.

Kontrolní činnost v oblasti bezpečnosti informací metodicky usměrňuje statutární zástupce Organizace.

15. ZÁVĚREČNÁ USTANOVENÍ

Tato politika nabývá účinnosti dnem 25. 5. 2018