Zpracoval: Jakub Hejma

Dne: 16.4.2018

Bezpečnostní politika společnosti společnosti BEE SITE:ES a.s.

Obsah

1. Úvod

1.1. Účel interní normy

Účelem tohoto dokumentu je stanovení bezpečnostní politiky společnosti.

1.2. Určení a platnost

Dokument je určen pouze pro vnitřní potřebu

1.3. Změny

Podněty k aktualizaci a/nebo změnám tohoto dokumentu se podávají zpracovateli – odpovědná osoba Jakub Hejma.

Aktualizace a změny se provádějí vydáním nového znění celého dokumentu.

1.4. Kontroly

Aktuálnost a efektivnost působení tohoto dokumentu kontroluje zpracovatel nejméně jednou ročně a o výsledcích kontrol vede záznamy.

1.5. Platnost výtisku

Vytištěná interní norma je platná a zveřejněna v interním informačním systému společnosti

Nahrazuje verzi: Datum vydání: 20.4.2018 Účinnost od:24.4.2018

2. Formulace bezpečnostní politiky

Tento dokument formuluje Bezpečnostní politiku informací společnosti.

Bezpečnostní politika se vztahuje na veškeré činnosti organizace v rámci působnosti (systém řízení bezpečnosti informací) a týká se informací, informačních systémů, sítě, fyzického prostředí a pracovníků, kteří uvedené činnosti zajišťují.

Tento dokument:

- Ustanovuje bezpečnostní politiku společnosti ve vztahu k ochraně důvěrnosti, integrity a dostupnosti jejích aktiv, tj. hardwaru, softwaru a informací zpracovávaných informačními systémy, a dále sítěmi a aplikacemi.
- Stanovuje odpovědnosti v oblasti bezpečnosti informací.

3. Podpora managementu, řídícího orgánu

Informace a informační systémy jsou kritická, životně důležitá aktiva společnosti. Bez spolehlivých informačních aktiv by se společnost ocitla ve vážné nevýhodě. Proto tato politika ukládá všem zaměstnancům, smluvním partnerům a vedení organizace za povinnost být s touto politikou v souladu, aby byly informace řádně zabezpečeny.

4. Cíl

Cílem této politiky je zajistit bezpečnost aktiv, zejména aktiv informačních, což znamená:

- Zajištění důvěrnosti, tj. chránit aktiva proti neautorizovanému vyzrazení.
- Zajištění integrity tj. chránit aktiva před neautorizovanou nebo náhodnou modifikací a zajistit správnost a úplnost aktiv organizace.
- Zajištění dostupnosti tj. zajistit, aby aktiva byla dostupná vždy, když to je potřebné, v souladu s cíli organizace.

5. Působnost

Tato politika stanovuje přístup k řízení bezpečnosti informací, aby zajistila, že jsou informační aktiva patřičně chráněna před rozličnými hrozbami, jako jsou chyby, podvody, sabotáže, terorismus, vydírání, špionáž, narušení soukromí, přerušení služby nebo přerušení dodávky produktů a služeb v rámci implementace, krádeže a přírodní pohromy, ať již se jedná o hrozby interní nebo externí, neúmyslné či záměrné.

Vedení společnosti má za povinnost a nese odpovědnost za zajištění ochrany informací a informačních systémů společnosti. Vedení navíc musí zajistit, že informační aktiva jsou chráněna minimálně takovým způsobem, jakým jsou chráněna v ostatních organizacích podobného typu a s přihlédnutím k přiměřenosti takových ochranných opatření.

Aby bylo dosaženo tohoto cíle, musí být v pravidelných ročních intervalech prováděny analýzy rizik, kterým jsou vystavena informační aktiva společnosti. Stejně tak, pokud bezpečnostní incident nebo výsledek auditu poukáže na nedostatečnou úroveň bezpečnosti informací a informačních systémů, musí vedení organizace okamžitě přijmout nápravná opatření k potlačení rizik, kterým je společnost vystavena.

Informace společnosti musí být chráněny adekvátně vzhledem k jejich citlivosti, hodnotě a kritičnosti. Bezpečnostní opatření se proto uplatňují bez ohledu na to, na jakém médiu je informace uchována, jakým systémem je zpracovávána nebo jakým způsobem je přenášena. Takováto ochrana zahrnuje také omezování přístupu k informacím na základě principu „need-to-know“, tj. přístup k informacím mají pouze osoby, které je nezbytně potřebují pro svou práci.

Vedení dává k dispozici dostatečné zdroje, aby bylo zajištěno, že bezpečnost informací je prosazována napříč celou společností. Je politikou společnosti využívat, kde je potřebné, služeb dodavatelů z třetích stran a externích konzultantů.

Aby bylo zamezeno narušení podnikatelských činností, musí být zavedeno řízení kontinuity. Všechny procesy musí být chráněny proti významným selháním nebo katastrofám.

Rozhodnutí provedené v rámci společnosti je také kriticky závislé na informacích, protože management potřebuje mít jistotu, že je zachována jejich integrita, důvěrnost, že jsou správné, aktuální, kompletní apod. Povědomí o takových informacích a jejich zdokonalování je důležitou činností v procesu zpracování informací.

Bezpečnost informací vyžaduje účast a podporu všech pracovníků (včetně dodavatelů). Tito lidé by měli absolvovat příslušná školení a jejich činnosti by měly být podpořeny dalšími aktivitami případně politikami (řády, směrnicemi, pokyny…), aby všechna informační aktiva byla adekvátně chráněna.

Je povinností všech pracovníků okamžitě hlásit jakékoli selhání programového vybavení, bezpečnostní incidenty, podezřelé viry, chyby, slabiny nebo hrozby, které se v systému objevily. Musí být stanoven a sledován rozsah případně i cena způsobených následků. Vyšetřování incidentů či jiných narušení bezpečnosti jsou v kompetenci bezpečnostního pracovníka.

6. Globální cíle

6.1. Ochrana provozu společnosti, ochrana provozu IT

Cílem je zvýšení spolehlivosti a bezpečnosti vedoucí k minimalizaci možných ekonomických ztrát v důsledku přerušení provozu při vzniku mimořádné události a následných mimořádných a krizových stavů včetně vytvoření záloh, vytvoření plánu krizových situací, definování krizových týmů, určení přípustné doby přerušení činnosti a určení případného náhradního řešení (pracoviště, objekt) orientace v budově.

6.2. Ochrana duševního vlastnictví – programové vybavení

- Na počítačích může být používáno pouze legální programové vybavení.
- Zaměstnanci, kteří vytvoří, získají a/nebo používají nelegální programové vybavení, mohou být potrestaní v rámci disciplinárního řízení.
- Nesmí se přehlížet nelegální kopírování programového vybavení.
- Obecně nesmí být kopírováno žádné programové vybavení bez odpovídající licence.
- Zaměstnanci jsou povinni každý incident tohoto charakteru nahlásit odpovědnému bezpečnostnímu manažerovi.

6.3. Ochrana majetku - hmotný majetek

- Přenosné počítače, PDA, MDA, Smartphones, mobilní telefony, přenosné disky apod. nesmějí být nikdy ponechány v autě, pokud v něm nikdo není.
- Stejně tak nesmějí být tato zařízení ponechána bez dozoru nikde ve veřejných dopravních prostředcích, v barech nebo restauracích či na jiných veřejných místech.
- Zaměstnanci, která tato zařízení používají na veřejných místech, si musí být vědomi, že je možné je odposlouchávat, monitorovat komunikaci nebo odezírat s displeje.
- Všechna přenosná zařízení musí být zabezpečena silným heslem a šifrována. Obecně je však mnohem důležitější chránit přenosná zařízení před ukradením a neautorizovaným přístupem, než se jen spoléhat na ochranu heslem.
- Všechna přenosná i nepřenosná zařízení na nichž může doházet ke zpracování osobních údajů jsou v době, kdy nejsou používána, a v nepřítomnosti pracovníka uzamčena.

6.4. Obecné bezpečnostní zásady

- Jakákoli aktiva společnosti by neměla být odnášena v jakékoli podobě z prostor společnosti bez povolení a vědomí odpovědného manažera.
- Sdílené skupinové adresáře, kalendáře apod. musejí být chráněny odpovídajícím způsobem, aby nebyly prozrazeny citlivé projektové informace.
- Mělo by být zajištěno, že žádné citlivé informace nejsou prozrazeny při používání mobilních telefonů na veřejných místech, při používání mobilních prostředků, při používání hlasitého odposlechu (zapnutý telefonní reproduktor), při používání automatických telefonních operátorů.
- Zaměstnanci by si měli být vědomi, že citlivé informace mohou být také prozrazeny při diskusi ve veřejných dopravních prostředcích nebo na veřejných místech.
- Zaměstnanci při kontaktu s klienty by si měli být vědomi skutečnosti, že může dojít k odposlechnutí verbální komunikace jinými klienty přítomnými ve společných prostorech

- Při práci s kopírkami a tiskárnami, scanery se má dbát na to, aby vytištěné, zpracované dokumenty nezůstaly v zařízení.
- Zaměstnanci, pověřené osoby, smluvní partneři ctí politiku „need to know".
- Zaměstnanci, pověřené osoby, smluvní partneři ctí politiku „prázdného stolu".
- Zaměstnanci, pověřené osoby, smluvní partneři ctí politiku „prázdné obrazovky".

6.5. Bezpečnostní zásady užívání online aplikací

- Pro přístup do online aplikací využívají zaměstnanci, pověřené osoby, smluvní partneři pouze silná hesla – alfanumerická hesla se speciálními znaky o minimální délce 10 znaků
- Pro přístup k těmto aplikacím využívají zaměstnanci, pověřené osoby, smluvní partneři pouze zařízení, která jsou definována v „NDA-smlouva-se-zamestnanci"
- Zaměstnanci, pověřené osoby, smluvní partneři nesmí své přihlašovací údaje do aplikace nikomu vyzradit a zároveň nesmí tyto přihlašovací údaje ukládat v prohlížeči

7. Platnost Bezpečnostní politiky

Tento dokument je obecně závaznou interní normou platnou pro všechny zaměstnance, pověřené osoby, smluvní partnery. Tato politika bude revidována jednou ročně pod vedením výkonného představitele organizace. Související bezpečnostní normy jsou součástí průběžného rozvoje a programu revizí.

7.1. Legislativní požadavky

Tam, kde to je relevantní, bude společnost udržovat soulad s:

- zákon 101 – 2000 Sb. O ochraně osobních údajů;
- zákon 106 – 99Sb. Svobodný přístup k informacím;
- zákon 227 – 2000 Sb. O elektronickém podpisu;
- zákoník práce 262-2006 Sb. v aktuálním znění;
- Nařízení Evropského parlamentu a Rady (EU) 679/2016 – tzv. GDPR
- ostatní platné a aktuální interní normy, předpisy, procesy a postupy.

7.2. Bezpečnostní provozní směrnice

Musí být vytvořeny bezpečnostní provozní směrnice pro systém a plány obnovy funkčnosti, odrážející bezpečnostní politiku. Všichni uživatelé systémů si musejí uvědomovat obsah a smysl odpovídajících provozním směrnicím.

7.3. Odpovědnosti vedoucí osoby

Zabezpečuje v každém projektu odpovědnost za to, že budou tvořeny podmínky pro efektivní implementaci bezpečnostních protiopatření, že bude tvořena odpovídající bezpečnostní dokumentace, bezpečnostní provozní směrnice a plány obnovy funkčnosti podle požadavků systémové bezpečnostní politiky. Tyto požadavky budou nedílnou součástí každého projektu.

7.4. Odpovědnosti uživatelů

Všem uživatelům informačních systémů, aplikací, sítí a fyzických datových zdrojů je poskytováno potřebné bezpečnostní poradenství, zvyšováno jejich bezpečnostní povědomí a podle potřeby poskytováno školení pro zvýšení jejich bezpečnostní odpovědnosti.

Neodpovědné nebo nesprávné jednání může vést ke kázeňským postihům dle platných pravidel – legislativní rámec, Provozní řád.

7.5. Schválení informačních systémů

Společnost zajišťuje, že před uvedením do provozu jsou všechny informační systémy, aplikace, sítě a fyzické datové zdroje schváleny odpovědnou osobou.

V této roli je odpovědná osoba podporována jednatelem, který je odpovědný za to, že informační systémy nebudou pro organizaci představovat žádné zvýšené bezpečnostní riziko.

7.6. Autorizace změn

Společnost zajišťuje, že všechny změny v informačních systémech, aplikacích a sítích jsou posuzovány projektovým/systémovým manažerem. Všechny tyto změny musí být posouzeny a schváleny manažerem bezpečnosti. Manažer bezpečnosti informací a/nebo manažer bezpečnosti informačních systémů může požadovat prověření nebo přehodnocení aktuální implementace na základě implementovaných změn.

7.7. Připojení na externí sítě

Společnost zajišťuje, že všechna propojení na další (cizí) sítě jsou dokumentována a mají schválenou systémovou bezpečnostní politiku. Bezpečnostní tým musí všechna propojení na další sítě schválit před jejich uvedením do provozu.

7.8. Řízení konfigurace

Společnost zajišťuje, že existuje efektivní systém řízení konfigurace pro všechny informační systémy, aplikace a sítě. Manažer bezpečnosti informací může vyžadovat prověrku efektivnosti systému řízení konfigurací.

7.9. Plány obnovy funkčnosti

Společnost zajišťuje, že pro všechny kritické aplikace, systémy a sítě jsou vytvořeny plány obnovy funkčnosti a havarijní plány. Plány musí být posouzeny manažerem bezpečnosti informací a manažerem bezpečnosti informačních systémů a musí být pravidelně testovány.

7.10. Bezpečnostní povědomí

Všichni zaměstnanci musí být pravidelně školeni, aby získali povědomí o bezpečnosti a aby si byli vědomi následků při nedodržení povinností vyplývajících z této bezpečnostní politiky nebo dalších směrnic.

7.11. Hlášení incidentů

Každé podezření na bezpečnostní selhání musí být hlášeno a vyšetřeno.

8. Bezpečnostní odpovědnosti

8.1. Odpovědnost vedení společnosti

Vedení společnosti je odpovědné za:

- Vytvoření podmínek pro bezpečnost informací ustanovením celkové politiky bezpečnosti informací v organizaci.
- Jmenování manažera bezpečnosti informací, je-li nezbytné.
- Jmenování DPO – Pověřence ochrany osobních údajů zajišťujícího soulad se zákonem o ochraně osobních údajů, požaduje-li tento krok platná právní úprava.
- Zajištění vhodných školení a zvyšování bezpečnostního povědomí zaměstnanců.

8.2. Odpovědnost manažera bezpečnosti informací, odpovědné osoby

Manažer bezpečnosti informací popř. odpovědná osoba je odpovědný za:

- Práci na pozici ústředního místa pro informační bezpečnost v rámci společnosti ve vztahu k zaměstnancům i externím organizacím.
- Implementaci efektivního způsobu řízení bezpečnosti informací.
- Pomoc při formulaci politiky bezpečnosti informací.
- Poradenství ohledně obsahu a implementace programu zajištění bezpečnosti informací.
- Tvorbu návrhů organizačních norem, postupů a doporučení v oblasti informační bezpečnosti, předkládaných ke schválení bezpečnostní radou/výborem.
- Koordinaci bezpečnostních aktivit zejména při sdílení informačních systémů a IT infrastruktury více subjekty.
- Udržování kontaktů s externími organizacemi ve věci informační bezpečnosti, včetně reprezentace organizace v relevantních výborech.

8.3. Odpovědnost jednotlivých manažerů

Manažeři jsou přímo odpovědní za:

- Zajištění bezpečnosti aktiv společnosti, tj. informací, hardwaru a softwaru v užití zaměstnanců a případně třetích stran a to konzistentním způsobem a v souladu s právními požadavky a s požadavky a závazky vedení.
- Zajištění odpovídajícího povědomí vlastních podřízených o jejich bezpečnostních odpovědnostech.
- Vhodná bezpečnostní proškolení vlastních podřízených.

8.4. Obecná odpovědnost

Všichni zaměstnanci nebo další subjekty působící ve prospěch organizace musí:

- chránit hardware, software a informace, které jsou jim svěřeny;
- chránit průnik škodlivého programového vybavení do IT systémů organizace;

- hlásit veškerá podezření na bezpečnostní ohrožení.