Bezpečnostní politika Trigema

Tuto bezpečnostní politiku vycházející z principů normy ISO 27001 přijímají společnosti koncernu Trigema s cílem minimalizovat procesní, provozní a informační rizika a dopady v případě selhání. Je zaměřena na procesy napříč koncernem, zejména pak obchodní, komunikační, personální, finanční a informační technologie. Pokrývá nejen celou strukturu koncernu Trigema ve všech lokalitách, nýbrž také spolupracující organizace, které přicházejí do styku se zabezpečenými informacemi společností koncernu Trigema.

Tento dokument definuje zajišťování bezpečnosti v klíčových oblastech v souladu s platnou legislativou pro důležitá informační aktiva společností koncernu Trigema, sumarizuje interní i externí předpisy společnosti ve vztahu k bezpečnosti a identifikuje kontrolní mechanismy společnosti.

Bezpečnostním cílem společností koncernu je zajistit bezpečnost aktiv, především informací. Bezpečnost informací je definována a uplatňována jako zachování důvěrnosti, integrity a dostupnosti informací.

1) Zajištění důvěrnosti – znamená chránit aktiva proti neautorizovanému přístupu nebo manipulaci
2) Zajištění integrity – znamená chránit aktiva před neautorizovanou nebo náhodnou modifikací a zajistit správnost a úplnost aktiv koncernu a přesnost jejich zpracování
3) Zajištění dostupnosti – znamená zajistit, aby aktiva byla dostupná vždy a tam, když to je potřebné v souladu s cíli koncernu

I. Zajišťování bezpečnosti je realizováno především v těchto oblastech:

1. Fyzická bezpečnost

- zabezpečení prostor využívaných společností, jejich technické zajištění i způsob uspořádání
- kamerové a přístupové či bezpečnostní systémy
- otázky bezpečnosti z hlediska požární ochrany a bezpečnosti práce

2. Procesní bezpečnost

- všechny klíčové procesy ve společnosti jsou tvořeny s maximální mírou pozornosti k otázkám bezpečnosti a jsou popsány v interních předpisech společnosti
- interní předpisy / směrnice jsou dobře dostupné a závazné pro všechny zaměstnance společnosti

3. Organizační bezpečnost

- je zajištěna díky organizační struktuře ve společnosti, cílenému školení, delegování odpovědnosti příslušným zaměstnancům, především s důrazem na odpovědnost vedoucích zaměstnanců a díky systému pravidelných i namátkových kontrol a testů
- dále pak zajištěním spolehlivých dodavatelských společností, které také podléhají systému kontrol a testů

4. Informační bezpečnost

- Informace jako jedno z hlavních aktiv společnosti je pomocí dílčích politik identifikována, klasifikována a řízena v souladu s normou ISO 27001.
- Přístup k informacím a nakládání s informacemi je popsán v interních předpisech

II. Interní předpisy společnosti, které řeší otázky bezpečnosti informací

Politika společnosti, Bezpečnostní politika, Cíle společnosti, Příručka IMS a dokumentace:

A. Plány obnovy procesů
Plány řešení krizových situací a následné kroky vedoucí k co nejrychlejšímu obnovení provozu firmy např. komunikační plán, plán obnovy klíčových procesů

B. Směrnice Řízení a pravidla IT

C. Interní bezpečnostní předpisy IT

D. Dokument Pravidla pro analýzu rizik a nakládání s informacemi

E. Dokument Odpovědnosti managementu a zaměstnanců organizace

F. Dokument Prohlášení o aplikovatelnosti

G. Dokument Desatero bezpečné Trigemy

H. Dokumenty Záznam z analýzy rizik a Plán zvládání rizik

I. Dokumenty nastavující pravidla ochrany osobních údajů

III. Kontrolní mechanismy koncernu

Dodržování všech závazných pravidel a předpisů, uvažování v souvislostech, dobrá komunikace a spolupráce mezi zaměstnanci i odděleními a společnostmi koncernu a celkově jednání v zájmu společnosti je samozřejmostí pro každého zaměstnance a zároveň povinností pro každého vedoucího pracovníka, čímž přispívají k efektivnosti systému řízení bezpečnosti informací. Porušení bezpečnosti informací může být považováno za hrubé porušení pracovní kázně nebo dodavatelské smlouvy.

a) Pravidelné kontroly / audity stanovené ročním plánem
b) Namátkové kontroly
c) Kontrola smluvní dokumentace před podpisem – kontrola čtyř a více očí
d) Kontrola a testování plánů obnovy procesů
e) Analýza rizik, přezkoumání incidentů, monitoring, reporting
f) Aktivita bezpečnostního týmu

Nastavení cílů bezpečnosti informací probíhá na základě výstupů z analýzy rizik, Přezkoumání IMS, bezpečnostních událostí a incidentů. Management společností koncernu Trigema podporuje dosažení stanovených cílů bezpečnosti informací a touto bezpečnostní politikou vyjadřuje svoji strategii trvalého zajišťování a zlepšování systému řízení bezpečnosti informací jako nedílné součásti procesů společností koncernu Trigema.

Dne: 15.2.2018

Zpracoval: Ing. Pavel Kouba
specialista IA, IT

Přezkoumal: Ing. Michal Tota
IT ředitel

Schválil: Ing. Marcel Soural
předseda představenstva