Politika bezpečnosti informací TESCO SW a.s.

Tato politika stanovuje ve společnosti TESCO SW a.s. **základní principy a východiska pro řízení bezpečnosti informací**. Dokument dále vymezuje oblasti a zásady ochrany, včetně způsobu ochrany jednotlivých oblastí.

Svým významem je politika bezpečnosti informací nezbytná pro realizaci všech standardů, směrnic, procedur a opatření ve společnosti ve vztahu k řízení systému bezpečnosti informací.

Politika bezpečnosti informací obsahuje závazek vrcholového vedení ke splnění aplikovatelných požadavků týkajících se bezpečnosti informací a k neustálému zlepšování systému řízení bezpečnosti informací ve společnosti.

Východiska a principy politiky

Společnost TESCO SW a.s. je softwarovou společností s adekvátním investičním majetkem, rozsáhlým know-how v oblasti poskytování ICT služeb, včetně poskytování outsourcingu vybraných služeb. Vzhledem k této skutečnosti si uvědomuje svoji odpovědnost za ochranu všech svých aktiv, ale současně i zákaznických dat či utajovaných informací, které jsou jí při výkonu jejich podnikatelských aktivit svěřeny.

K dosažení zamýšlených výstupů řízení bezpečnosti informací je předmětem politiky **trvalá ochrana všech aktiv** společnosti, které se ve společnosti mohou nacházet nebo k nim má společnost přístup.

Z pohledu bezpečnosti informací se za **základní oblasti ochrany** ve společnosti považuje:

- Zajištění byznys kontinuity
- Ochrana provozu – kontinuita provozu
- Ochrana hmotného majetku
- Ochrana nehmotného majetku
- Bezpečnost lidských zdrojů
- Ochrana produktů a služeb

Dokumentace a odpovědnost

Celkové pojetí řízení bezpečnosti informací ve společnosti vychází ze základního modelu dokumentace:

- **Politika bezpečnosti informací**,
- **Cíle politiky bezpečnosti informací**,
- **Bezpečnostní postupy** – soubor konkrétních bezpečnostních témat (postupy, pravidla, doporučení) pro zajištění pokynů ze strany managementu ve vztahu k systému bezpečnosti informací a zaměstnancům organizace.

Pro zajištění neustálé vhodnosti, přiměřenosti a efektivnosti je zvolený model dokumentace přezkoumáván v pravidelných intervalech, nebo pokud dojde k významným změnám ve společnosti.

Bezpečnost aktiv společnosti je věcí všech zaměstnanců. Všichni zaměstnanci se podílejí na zodpovědnosti za ochranu a dohled nad informacemi, které se vytvářejí, zpracovávají, přijímají nebo odesílají v jejich pracovním procesu.

Zásady politiky

Vrcholové vedení společnosti se zavazuje k dodržování následujících zásad:

Zajištění byznys kontinuity

Zajistit prediktivní řízení kapacit a finanční zdroje, včetně potřebných rezerv, pro plnění všech závazků v dostatečné kvalitě se zajištěním neustálé kontinuity;

Ochrana provozu – kontinuita výrobních procesů

Zajistit autorizovaný provoz všech systémů společnosti s eliminací nebo minimalizací následků případných bezpečnostních incidentů. Vyhodnocovat následky bezpečnostních incidentů a uplatňovat nápravná opatření k zamezení jejich opakování stanovením vyhodnotitelných programů a cílů;

Ochrana hmotného majetku

Zajistit trvale ochranu majetku a místa, kde společnost poskytuje služby svým zákazníkům trvalým zlepšováním úrovně havarijních a bezpečnostních plánů, jako prevenci před ekonomickými ztrátami, mimořádnými a krizovými událostmi;

Ochrana nehmotného majetku

Zachovávat a trvale chránit informační aktiva společnosti, tzn. vše, co má pro společnost nějakou hodnotu z pohledu informační bezpečnosti;

Bezpečnost lidských zdrojů

Znát rizika a pravidelným proškolováním a nacvičováním havarijních situací jako nedílné součásti přípravy, zajistit prevenci zaměstnanců před těmito riziky;

Ochrana produktů a služeb

Zajistit bezpečnost zaváděných produktů a služeb společnosti odpovědným plněním požadavků všech platných zákonných norem a předpisů. Zároveň se důsledně věnovat ochraně před zneužitím komunikačních služeb;

Informovanost

Předávat informace zákazníkům, dodavatelům a ostatním právnickým a fyzickým osobám vyskytujícím se ve společnosti i v jejím okolí o rizikách, stanovených opatřeních a jejich žádoucím chování.

Nástroje politiky

K nástrojům politiky bezpečnosti informací patří cokoli, co je schopno s vynaložením určitých nákladů snížit nebo vyloučit nebezpečí újmy vzniklé na straně společnosti.

Klasifikace informací

Cílem klasifikace je rozdělení všech informací, se kterými společnost pracuje, do tříd dle stupně jejich důvěrnosti. Z toho pak vyplývá způsob nakládání s těmito informacemi a jejich nosiči (osoby oprávněné k manipulaci, způsob skladování, způsob skartace, …).

Systém pro podporu řízení bezpečnosti

Jedná se o centrální sběrný systém, který zpracovává všechny bezpečnostní incidenty a rizika v organizaci (narušení bezpečnostních politik, trestně právní události, rizika trestně právního jednání atd.). Výsledkem je pak adekvátní reakce na příslušné incidenty, případné vyčíslení způsobených škod, zastupování organizace v trestním řízení, přijímání protiopatření a návrh preventivních postupů.

Zabezpečení zaváděných produktů a služeb

Jedná se o prvotní posouzení zaváděné služby nebo produktu (obchodního záměru) z pohledu bezpečnosti již ve fázi přípravy prováděním bezpečnostních testů apod.

IT ochrana

Úkolem IT ochrany je zajistit požadovanou úroveň v charakteristikách - dostupnost, integrita a důvěrnost odpovídajících systémů, aplikací a dat vlastních i zákaznických.

Fyzická ochrana

Fyzická ochrana jako nástroj obsahuje veškerá fyzická zabezpečení provozu, hmotného majetku i osob. Mezi prostředky fyzické ochrany organizace patří prvky technické ochrany, speciální technické ochrany, požární ochrany, mechanické ochrany a režimové ochrany.

Personální ochrana

Jedná se o zajištění povinností, práv a bezpečnosti práce zaměstnance podle požadavků platných právních předpisů (zejména Zákoníku práce, Listiny základních práv a svobod) a ochranu zaměstnanců formou pravidelných školení, vybavení a zajištění pracovních podmínek.

Krizové řízení

Krizové řízení lze definovat jako systém a metody řešení krizových situací. Krizové řízení je tvořeno širokým spektrem činností, mezi něž patří zejména plánování, podpora rozhodování v mimořádných / krizových situacích, simulace krizových situací a jejich řešení, civilní nouzové plánování, monitorování, modelování a analýza situací.

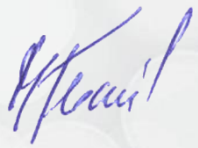
Podniková kultura z pohledu bezpečnosti

Zaměstnanci jsou s podnikovou kulturou seznamováni zároveň s Etickým kodexem v rámci individuálních školení, jejichž výsledkem je osobní rozvoj zaměstnanců a jejich seznámení se zákonnými, interními a obecně platnými bezpečnostními pravidly – interními normami.

Prohlášení managementu

Vrcholové vedení společnosti TESCO SW a.s. se tímto zavazuje, v souladu s přijatou a schválenou strategií společnosti, jejíž nedílnou součástí je trvalá ochrana aktiv společnosti a výše uvedenou politikou bezpečnosti informací, k plnění všech aplikovatelných požadavků a k neustálému zlepšování řízení bezpečnosti informací ve společnosti.

V Olomouci dne: 11. 11. 2014



RNDr. Josef Tesařík
generální ředitel TESCO SW a.s.

TESCOSW

TESCO SW a.s.
Tř. Kosmonautů 1288/1, 779 00 Olomouc – Hodolany
tescosw@tescosw.cz / www.tescosw.cz