

Politika Integrovaného systému managementu prohlášení vedení podniku

Vedení podniku Státní pokladna Centrum sdílených služeb, s. p. (dále jen „SPCSS“) si uvědomuje důležitost zajištění kvality poskytovaných služeb, bezpečnosti informací, informačních systémů, informačních a komunikačních technologií a dat v SPCSS na všech stupních řízení podniku. Dále si je SPCSS vědoma povinností vyplývajících z platného právního řádu, se zdůrazněním oblastí životního prostředí, BOZP, požární ochrany a ochrany osobních údajů.

Smyslem zavedení ISM je stanovit cíle, požadavky, zásady a opatření, která mají zajistit shodu s platným právním řádem a zvolenými normami, a omezit a minimalizovat rizika, včetně případných ztrát.

Management SPCSS se tímto zavazuje k neustálému zlepšování ISM, alokaci nezbytných zdrojů a splnění aplikovatelných požadavků na tento systém řízení.

Vedení SPCSS stanovuje následující průběžné cíle:

- Trvale rozvíjet standardizaci a zefektivnění činností spojených s poskytováním služeb i interních činností SPCSS.
- Trvale poskytovat služby vysokého standardu.
- Průběžně reagovat na potřeby zákazníků a trhu.
- Trvale plnit právní a jiné povinnosti SPCSS.
- Zvyšovat kompetence a bezpečnostní povědomí zaměstnanců SPCSS.
- Eliminovat rizika identifikovaná pro jednotlivé oblasti ISM.
- Realizovat kontinuální zlepšování kvality služeb ICT, procesů a celého ITMS prováděním pravidelných auditů a následnou aplikací nápravných a preventivních opatření, stejně jako zvyšováním kvalifikace zaměstnanců poskytujících služby ICT.
- Přiměřeně trvale zlepšovat environmentální chování s cílem snižovat dopady na životní prostředí.
- Environmentálně odpovědně přistupovat k výběru dodavatelů se zohledněním dopadu na životní prostředí, trvale udržitelný rozvoj, životní cyklus dodávky, služby nebo stavební práce.
- Vytvářet pracovní prostředí, které pozitivně ovlivňuje plnění cílů, požadavků, závazků a povinností.

V souladu s bezpečnostními cíli a novým trendem Cloud computingu, kdy dochází ke vzniku nových rizik, neboť se mění množství, původ, charakter a významnost možných hrozeb, jsou u SPCSS průběžně přizpůsobována organizační a technická bezpečnostní opatření.

V oblasti informační a kybernetické bezpečnosti a v oblasti poskytování ICT služeb se vedení SPCSS zavazuje vyvinout maximální úsilí k průběžnému dosahování cílů stanovených pro tyto oblasti. Jednotlivé cíle jsou stanovovány na základě potřeb a strategických cílů SPCSS na základě principů PDCA cyklu a tím průběžného zlepšování systému.

Integrovaný systém managementu SPCSS má nastaveny procesy a pravidla:

- pro řízení dokumentace,
- pro řízení zdrojů a provozu systému řízení bezpečnosti informací,
- pro provádění auditů integrovaného systému managementu,
- pro přezkoumání integrovaného systému managementu,
- pro nápravná opatření a zlepšování integrovaného systému managementu.

Vedení SPCSS stanovuje rovněž pro integrovaný systém managementu SPCSS následující dílčí politiky:

Politika řízení aktiv

Politika organizační bezpečnosti

Politika řízení dodavatelů

Politika bezpečnosti lidských zdrojů

Politika řízení provozu a komunikací

Politika řízení přístupu

Politika bezpečného chování uživatelů

Politika zálohování, obnovy a dlouhodobého ukládání

Politika bezpečného předávání a výměny informací

Politika řízení technických zranitelností

Politika bezpečného používání mobilních zařízení

Politika akvizice, vývoje a údržby

Politika ochrany osobních údajů

Politika fyzické bezpečnosti

Politika bezpečnosti komunikační sítě

Politika ochrany před škodlivým kódem

Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí

Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Politika bezpečného používání kryptografické ochrany

Politika řízení změn

Politika zvládnání kybernetických bezpečnostních incidentů

Politika řízení kontinuity činností

Všechny uvedené politiky se vedení SPCSS zavazuje rozpracovat ve vnitropodnikové dokumentaci, a to ve Směrnici o systému řízení bezpečnosti informací nebo ve Směrnici o systému managementu služeb ICT.

Vedení podniku od svých zaměstnanců očekává:

- aktivní spolupráci při udržování a zlepšování integrovaného systému managementu včetně bezpečnosti informací a kybernetické bezpečnosti;
- důsledné dodržování bezpečnostní politiky informační a kybernetické bezpečnosti v souladu s platnými právními předpisy a relevantní vnitropodnikovou dokumentací.

V Praze dne dle elektronického podpisu

Ing. Vladimír Dzurilla
generální ředitel