PARDUBICKÝ KRAJ

Základní politika bezpečnosti informací
v kontextu KrÚ Pk

a) Hlavní východiska (účel) činnosti KrÚ Pk při zabezpečení informací

- Krajský úřad Pardubického kraje (KrÚ Pk) zabezpečuje v samostatné působnosti plnění úkolů uložených mu zastupitelstvem a radou a dále výkon přenesené působnosti v rozsahu svěřeném mu příslušnými zákony. Výkon těchto činností je z velmi významné části postaven na zpracování informací občanů, jiných orgánů veřejné správy, organizací, které Pk zřizuje a dodavatelů.
- Přestože je KrÚ Pk orgánem veřejné správy, zpracovává, kromě informací přístupných široké veřejnosti, také strategické informace, obchodní tajemství a informace podléhající režimu zákona o ochraně utajovaných informací, zákona o krizovém řízení a zákona o ochraně osobních údajů.
- S ohledem na maximální zabezpečení těchto informací provádí vedení KrÚ Pk periodické, dokumentované monitorování a vyhodnocování bezpečnostních rizik a incidentů. V rámci celé organizace zajišťuje neustálé zlepšování bezpečnosti informací (tj. zabezpečení včasné dostupnosti informací, zamezení jejich modifikace, zneužití a ztráty) v souladu s obecně závaznými právními a interními předpisy a smluvními požadavky.
- Způsob zpracování informací je definován souborem cílů a zásad (dokumentované postupy jako další úroveň Základní politiky bezpečnosti informací, které jsou vedením KrÚ Pk podporovány a sdělovány v rámci celé organizace. Jedná se zejména o tyto dílčí politiky: OS Používání informačních a komunikačních technologií, Zabezpečení informačních a komunikačních technologií, Spisový řád, Pracovní řád a Ochrana utajovaných informací.
- Náklady na zajištění bezpečnosti informací musí být souměřitelné s cenou dopadů, aby byly efektivně vynaloženy finanční prostředky.

b) Hlavní zásady a strategické cíle práce s informacemi a způsob jejich zabezpečení

- Začleňovat zabezpečení informací do odpovědnosti za práci (náležitosti a podmínky zaměstnání, ochrana informací).
- Zpracovávat a aktualizovat soubor opatření pro zachování kontinuity v případě jakéhokoliv výpadku v oblasti informací. Tato opatření musí být pravidelně přezkušována a ověřována, aby byla zachována kontinuita v průběhu zpracování informací.
- Zabezpečovat informace při zaměstnání na dálku.
- Zabezpečovat elektronické administrativní systémy, veřejně dostupné systémy, elektronickou poštu a další způsoby výměny informací.
- Vytvářet a prosazovat systém řízeného přístupu k informacím a omezit přístup k informacím (používání silných hesel).
- Prosazovat politiku čistého stolu a prázdné obrazovky.
- Provádět kontrolu připojení a směrování sítě.
- Vytvářet a prosazovat bezpečnostní systém pro přenosná počítačová zařízení.
- Provádět stálé vzdělávání a zvyšování kvalifikace zaměstnanců v oblasti bezpečnosti informací.
- Zajišťovat spolehlivou antivirovou kontrolu celé interní sítě a zabezpečit celou síť proti působení každého zlomyslného softwaru.
- Provádět stálou identifikaci bezpečnostních incidentů a přijímat účinná opatření pro zlepšování bezpečnosti informací.
- Udržovat systém způsobu používání informačních aktiv a bezpečných oblastí.

c) Následky porušení informační politiky

- Porušování zásad jakékoliv úrovně politiky bezpečnosti informací ze strany zaměstnanců organizace je chápáno jako bezpečnostní incident, který má vliv na bezpečnost informací a v těchto intencích musí být řešen.
- Příčiny porušení informační politiky analyzovat a přijímat účinná opatření s cílem učení se z těchto událostí.

Závěrečné ustanovení

Tento dokument podléhá zveřejnění jako směrnice krajského úřadu a je uložen na organizačním oddělení odboru organizačního a právního KrÚ Pk.

V Pardubicích dne 20. 10. 2014

Ing. Jaroslav Folprecht v. r.
ředitel Krajského úřadu Pardubického kraje