INELSEV

Politika kybernetické bezpečnosti

INELSEV s.r.o. vědom si zásadního vědomí informací, deklaruje svůj závazek pečlivě se věnovat oblasti bezpečnosti informací, poskytnout zdroje pro naplňování závazku v oblasti bezpečnosti informací.

Společnost buduje a neustále zlepšuje systém řízení kybernetické bezpečnosti (ISMS), aby chránila vlastní informační aktiva a aby všem zainteresovaným stranám, byla schopná garantovat nezbytnou míru bezpečí v této oblasti.

ISMS (Information Security Management Systém) společnosti je vybudován a neustále zlepšován dle požadavků systémové normy ČSN ISO/IEC 27001:2014.

Hlavním cílem politiky bezpečnosti informací je zajistit ochranu informačních aktiv společnosti tak, aby byla zachována důvěrnost, integrita a dostupnost informací a řízení informačních toků v souladu s platnou legislativou.

Závazek vedení INELSEV s.r.o:

společnost se zavazuje, že bude prosazovat a uskutečňovat tuto politiku zejména:

- pravidelným monitorováním a vyhodnocováním bezpečnostních rizik a přijímáním odpovídajících opatření,
- přijímáním opatření vedoucích k neustálému zlepšování bezpečnosti informací, integrity a důvěrnosti,
- zajištěním pravidelného vzdělávání zaměstnanců společnosti a ostatních uživatelů informačních aktiv,
- stanovením a prosazováním způsobu zpracování informací, který definuje souborem vnitřních předpisů,
- dbá na to, aby náklady na kybernetickou bezpečnost byly vynakládány efektivně.

Odpovědnost zaměstnanců společnosti:

- zaměstnanec, kterému byl umožněn přístup k informačním aktivům, přebírá odpovědnost za bezpečné nakládání s těmito aktivy a za jejich ochranu,
- řídící dokumentace kybernetické bezpečnosti je závazná pro všechny uživatele informačních aktiv a to bez ohledu na zastávanou funkci či pozici ve společnosti,
- všichni uživatelé informačních aktiv nesou v souladu s platnou legislativou a interními předpisy zodpovědnost za dodržení, resp. porušení pravidel, s nimiž byli seznámeni,
- všichni uživatelé informačních aktiv jsou povinni předepsaným způsobem reagovat na bezpečnostní události a incidenty, které zjistí, a upozornit na ně v souladu s příslušnými vnitřními předpisy.

Hlavní zásady práce s informacemi ve společnosti a způsob jejich zabezpečení:

- zajistit ochranu osobních údajů v souladu s platnou legislativou,
- vytvářet a prosazovat systém řízeného přístupu k informacím,
- začleňovat zabezpečení informací do odpovědnosti za práci,
- zajišťovat zvyšování bezpečnostního povědomí a zvyšování kvalifikace zaměstnanců a ostatních uživatelů informačních aktiv v oblasti bezpečnosti informací,
- provádět neustálé monitorování a identifikaci bezpečnostních událostí a incidentů a přijímat účinná bezpečnostní opatření pro jejich eliminaci, a neustále zlepšovat bezpečnost informací.

V Mostě dne 10. 12. 2021

Ing. Miroslav Kunca
ředitel a jednatel INELSEV s.r.o.