PATVIRTINTA
Biudžetinės įstaigos Kertinio valstybės
telekomunikacijų centro direktoriaus
2020 m. birželio 16 d. įsakymu Nr. V - 34

KERTINIO VALSTYBĖS TELEKOMUNIKACIJŲ CENTRO

INFORMACIJOS SAUGUMO VALDYMO SISTEMOS POLITIKA

Įstaiga, siekdama užtikrinti teikiamų paslaugų ir informacijos saugumą, pagal standarto LST EN ISO/IEC 27001:2017 reikalavimus, formuoja Informacijos saugumo valdymo sistemos politiką, kuri nustato pagrindines kryptis ir tikslus, kuriais privalo vadovautis visi įstaigos darbuotojai ir vadovybė siekiant apsaugoti turimą informacinį turtą.

Pagrindinis informacijos saugumo valdymo tikslas – užtikrinti tinkamą ir efektyvų informacijos saugumo valdymą ir išvengti veiklos sutrikdymo dėl informacijos konfidencialumo, vientisumo bei prieinamumo pažeidimų. ISVS politika taikoma visiems Įstaigos padaliniams ir veiklos procesams, susijusiems su Saugiuoju valstybiniu duomenų perdavimo tinklu (toliau – Saugusis tinklas) ir apima žodinę ar rašytinę informaciją, informacines sistemas, tinklus, fizinę aplinką ir su jais susijusius darbuotojus, kurie dalyvauja ir palaiko šiuos veiklos procesus. Siekiant įvertinti informacijos konfidencialumo, vientisumo ir prieinamumo praradimų potencialias pasekmes bei įvertinti galimą žalą veiklai, kurią gali sukelti informacijos saugos pažeidimai, vieną kartą metuose atliekama Saugiojo tinklo rizikos analizė ir informacinių technologijų pažeidžiamumų vertinimas. Įvertinama informacinio turto įtaka, pažeidžiamumai ir grėsmės, galinčios iškilti turtui. Įvertinus rizikas, jos yra mažinamos diegiant parinktas valdymo priemones.

INFORMACIJOS SAUGUMO UŽTIKIRINIMO KRYPTYS

- Saugiojo tinklo informacinio turto apsauga nuo vidinių ir išorinių, sąmoningų, atsitiktinių ar kitokių grėsmių bei informacijos saugumo rizikų mažinimas;
- Sistemingas darbuotojų informacinio saugumo supratimo didinimas, jų kompetencijų ugdymas elektroninės informacijos saugumo srityje;
- Tinkamų, geriausią praktiką atitinkančių, saugumo priemonių įgyvendinimas nustatytoms rizikoms mažinti, atsižvelgiant į periodinius elektroninės informacijos saugumo rizikos vertinimus;
- Nuolatinis Informacijos saugumo valdymo sistemos tobulinimas pagal tarptautinio LST EN ISO/IEC 27001 standarto reikalavimus.

INFORMACIJOS SAUGUMO UŽTIKRINIMO TIKSLAI

- Užtikrinti valstybės informacinių išteklių apsaugą nuo galimų grėsmių;
- Užtikrinti nuolatinį informacijos saugumo valdymo ciklą, atliekant kasmetinį informacijos saugumo auditą, siekiant identifikuoti gerinimo galimybes;
- Užtikrinti tinkamą saugumo valdymo priemonių parinkimą;
- Užtikrinti reikiamą darbuotojų kompetenciją informacijos saugumo srityje;
- Užtikrinti atitikimą keliamiems ISO/IEC 27001:2017 standarto reikalavimams.