

KERTINIO VALSTYBĖS TELEKOMUNIKACIJŲ CENTRO INFORMACIJOS SAUGUMO VALDYMO SISTEMOS POLITIKA

I SKYRIUS BENDROSIOS NUOSTATOS

1. Kertinio valstybės telekomunikacijų centro informacijos saugumo valdymo sistemos (toliau – ISVS) politika reglamentuoja pagrindinius Kertinio valstybės telekomunikacijų centro (toliau – KVTC) informacijos saugumo užtikrinimo ir valdymo principus, taikomus siekiant užtikrinti saugų ir patikimą informacinių ir ryšių technologijų paslaugų teikimą Saugiojo valstybinio duomenų perdavimo tinklo (toliau – Saugusis tinklas) naudotojams, taikant pažangias technologijas, ugdant kompetencijas ir didinant kibernetinį atsparumą.

2. ISVS politika taikoma visiems KVTC padaliniams ir veiklos procesams, susijusiems su Saugiojo tinklo ir kitomis KVTC teikiamomis informacinių ryšių ir technologijų paslaugomis bei apima žodinę ir rašytinę informaciją, informacines sistemas, tinklus, fizinę aplinką ir su jais susijusius KVTC darbuotojus, vadovybę, paslaugų KVTC teikėjus, kurie dalyvauja ir palaiko šiuos veiklos procesus.

II SKYRIUS INFORMACIJOS SAUGUMO UŽTIKIRINIMO KRYPTYS IR TIKSLAI

3. KVTC informacijos saugumo užtikrinimas vykdomas šiomis kryptimis:

3.1. Informacinio turto apsauga nuo vidinių ir išorinių, sąmoningų, atsitiktinių ar kitokių grėsmių bei informacijos saugumo rizikų mažinimas;

3.2. Sistemingas darbuotojų informacinio saugumo supratimo didinimas, jų kompetencijų ugdymas informacijos saugumo srityje;

3.3. Tinkamų, geriausių praktiką atitinkančių, saugumo priemonių įgyvendinimas nustatytoms rizikoms mažinti ir neatitiktims koreguoti;

3.4. Nuolatinis ISVS tobulinimas pagal tarptautinio LST EN ISO/IEC 27001 standarto reikalavimus.

4. KVTC informacijos saugumo tikslai:

4.1. Užtikrinti tinkamą ir efektyvų informacijos saugumo valdymą, siekiant išvengti KVTC veiklos sutrikdymo dėl informacijos konfidencialumo, vientisumo ir pasiekiamumo pažeidimų bei įgyvendinant gerąją praktiką atitinkančias organizacines ir technines saugumo priemones;

4.2. Užtikrinti reikiamas darbuotojų kompetencijas informacijos saugumo srityje;

4.3. Užtikrinti efektyvų saugos rizikos valdymą ir tinkamų rizikos valdymo priemonių naudojimą, siekiant suvaldyti rizikas iki priimtino lygio, atliekant kasmetinius saugumo rizikos ir informacinių technologijų pažeidžiamumų vertinimus bei įgyvendinant nustatytus rizikos valdymo priemonių planus;

4.4. Užtikrinti kibernetinio saugumo ir kitų specialiųjų organizacinių ir techninių saugumo reikalavimų laikymąsi, siekiant atitikti teisės aktų keliamus saugumo reikalavimus, atliekant kasmetinius atitikties vertinimus ir įgyvendinant nustatytus atitikties trūkumų šalinimo planus;

4.5. Užtikrinti Saugiojo tinklo ir kitų KVTC teikiamų paslaugų veiklos tęstinumą, atliekant periodinį veiklos tęstinumo valdymo plano veiksmingumo išbandymą ir jo peržiūrą;

4.6. Užtikrinti efektyvų KVTC ISVS atitikimą keliamiems ISO/IEC 27001:2017 standarto reikalavimams nuosekliai planuojant, vertinant ir tobulinant ISVS valdymą.

III SKYRIUS BAIGIAMOSIOS NUOSTATOS

5. KVTC vadovybės, padalinių vadovų ir kitų KVTC darbuotojų informacijos saugumo įsipareigojimai informacijos saugumo srityje nustatyti KVTC veiklai taikomuose teisės aktuose, darbuotojų pareigybių aprašymuose, Informacijos saugumo valdymo sistemos valdymo procedūros apraše VP-06-03 ir kituose susijusiuose dokumentuose.

6. KVTC nuolat gerina ISVS rezultatyvumą, įgyvendinama ISVS politiką ir tikslus, atlikdama ISVS auditus, nustatydamą neatitiktis, vykdydamą ISVS korekcinius veiksmus ir atlikdama vadovybės vertinamąją analizę.

7. Su ISVS politika KVTC darbuotojai supažindinami ne vėliau, kaip pirmąją jų darbo dieną elektroniniu paštu ir (arba) dokumentų valdymo sistemoje DokVIS.

8. ISVS politika skelbiama KVTC interneto svetainėje adresu www.kvtc.gov.lt.

9. KVTC informacijos saugumo vadybininkas užtikrina, kad ISVS politika būtų periodiškai, bet ne rečiau, kaip kartą per metus peržiūrima ir, esant poreikiui, atnaujinama.
