

REIKALAVIMAI KIBERNETINIO SAUGUMO SUBJEKTAMS

KSĮ remiasi grėsmių požiūriu, kurio tikslas – apsaugoti tinklus ir informacines sistemas, taip pat šių sistemų fizinę aplinką nuo įvairių kibernetinių incidentų. Įstatymas reikalauja, kad būtų imtasi tinkamų ir proporcingų kibernetinio saugumo rizikos valdymo priemonių, kurios turi apimti bent:

Lietuvos Respublikos Vyriausybės
2024 m. lapkričio 6 d. nutarimo Nr. 945
redakcija

Rizikos analizę, tinklų ir informacinių sistemų saugumo politiką

Politikas ir procedūras, skirtas įvertinti taikomų kibernetinio saugumo rizikos valdymo priemonių efektyvumą

Tiekimo grandinės saugumą

Kibernetinių incidentų valdymą

Kibernetinės higienos ir kibernetinio saugumo mokymus

Žmogiškųjų išteklių saugumo, prieigos kontrolės politikas ir turto valdymą

Veiklos tęstinumo užtikrinimą ir krizių valdymą

Politikas ir procedūras, susijusias su kriptografija ir šifravimu

Spragų valdymo ir atskleidimo politiką

Kelių faktorių autentifikacijos užtikrinimą, saugios komunikacijos sistemas

Tinklų ir informacinių sistemų įsigijimą plėtojimą ir priežiūrą