

## Informacinio saugumo reikalavimai

1. Teisiniai reikalavimai. Visuose įgyvendinimo etapuose (projektavimas, diegimas, priežiūra ir kt.) turi būti laikomasi informacinio saugumo reikalavimų patvirtintų:
  - 1.1. Lietuvos Respublikos energetikos ministro 2013-05-07 d. įsakyme Nr. 1-89 „Dėl Strateginę ar svarbią reikšmę nacionaliniam saugumui turinčių energetikos ministro valdymo sričiai priskirtų įmonių ir įrenginių informacinės saugos reikalavimų patvirtinimo“;
  - 1.2. Lietuvos Respublikos kibernetinio saugumo įstatyme ir lydinčiuose teisės aktuose.Bet kokios išimtys turi būti suderintos su Užsakovu.
2. Visuose įgyvendinimo etapuose turi būti laikomasi šių saugumo principų:
  - 2.1. Minimalių teisių (būtina žinoti) - vartotojams ir sistemos komponentams suteikiamos minimalios, būtinos teisės konkrečių funkcijų atlikimui;
  - 2.2. Kompleksiškumo (angl. defence in depth) - saugumo grėsmių mažinimui taikomos ne atskiros, o viena kitą papildančios saugumo priemonės;
  - 2.3. Rezervavimo - atskiro sistemos komponento sutrikimas neturi iš esmės pažeisti sistemos saugumo.
3. Saugumo stiprinimas (angl. system hardening). Prieš pradedant eksploatuoti sistemą, visuose jos komponentuose turi būti pašalinti arba deaktivuoti nebūtini sisteminiai servisai, vartotojai, tinklo prievadai, numatytais užduotims nebūtina programinė įranga.
4. Prieš pradedant eksploataciją įrenginiuose - operacinėje sistemos, mikrokode (firmware), programinėje įrangoje turi būti įdiegtos vėliausios gamintojo saugumo pataisos.
5. Prieš pradedant eksploataciją įrenginių standartiniai (gamintojo) prisijungimo identifikatoriai ir slaptažodžiai turi būti pakeisti į identifikatorius ir slaptažodžius atitinkančius Užsakovo saugumo reikalavimus (saugumo reikalavimai pateikiami atskirai).
6. Bet kokia prieiga prie įrenginių - pvz. vietinė naudojant valdymo pultą (HMI), vietinė naudojant komunikacijos/diagnostikos prievadus ar nuotolinė naudojant komunikacijų terpę turi būti apsaugota vartotojo identifikatoriumi ir slaptažodžiu.
7. Vartotojų paskyrų valdymas turi būti užtikrinamas rolėmis, atskiriant šias roles:
  - 7.1. Administratorius - vartotojas prižiūrintis, instaliuojantis programinę/aparatinę įrangą ir administruojantis sistemą;
  - 7.2. Operatorius - vartotojas valdantis sistemą, turintis teisę keisti operacinius parametrus;
  - 7.3. Informacijos peržiūra - vartotojas turintis teisę matyti duomenis.
8. Sistemose/įrenginiuose turi būti registruojami ir vėlesnei analizei saugomi žurnaliniai įrašai apie vartotojų veiksmus, įvykius, klaidas ir saugumo pranešimus.
9. Atsarginis kopijavimas ir veiklos tęstinumas. Prieš pradedant eksploataciją, turi būti pateikti visų įrenginių konfigūraciniai failai, identifikatoriai, slaptažodžiai ir kita funkcionalumo atstatymui reikalinga informacija.
10. Pastotės duomenų perdavimo tinklo komponentai turi būti grupuojami į skirtingas saugumo zonas, t.y. segmentuojami:
  - 10.1. Vertikaliai - atskiriami skirtingos funkcinės paskirties komponentai;
  - 10.2. Horizontaliai - atskiriami teritoriniai segmentai.
11. Duomenų srautų filtravimui tarp skirtingų segmentų turi būti naudojamos ugniasienės.
12. Tinklo įrenginių administravimui turi būti naudojami tik saugūs protokolai, užtikrinantys autentifikaciją ir šifravimą - pvz. SSHv2, SNMPv3, HTTPS.

13. Visi nuotolinio ir vietinio prisijungimo metodai, priemonės ir prievadai turi būti dokumentuoti ir suderinti su perdavimo tinklo operatoriaus informacijos saugos atstovu. Bet koks neautorizuotas ar nedokumentuotas prisijungimas draudžiamas.