TIPINIAI SAUGUMO REIKALAVIMAI PROJEKTAVIMUI IR DIEGIMUI

I. BENDROSIOS NUOSTATOS

1. Šiuo dokumentu yra nustatomi minimalūs reikalavimai ir principai taikomi Informacinių sistemų projektavimui ir/ar projektams susijusiems su Informacinių technologijų ir telekomunikacijų (toliau – **ITT**) įrenginiais, mikroprocesoriniais įrenginiais, pvz.: teleinformacijos surinkimo ir perdavimo įrenginiai, relinės apsaugos terminalai, valdymo pultai (HMI), momentinių duomenų valdikliai, bendros paskirties valdikliai, teleinformacijos surinkimo ir perdavimo sistema, komercinių duomenų valdikliai ir .t.t. (toliau – **Įranga**) ir šių projektų techniniam išpildymui – diegimui.

2. Visuose Projekto įgyvendinimo etapuose turi būti laikomasi šių saugumo principų:

2.1. Minimalių teisių – valdant prieigą prie Bendrovės projektinės Informacijos, informacinių sistemų ir Įrenginių, turi būti užtikrintas principo „būtina darbui“ įgyvendinimas, t. y. reikalavimas, kuris reiškia, kad prieiga gali būti suteikta tik patvirtintiems asmenims ir tik tokia apimtimi, kuri yra būtina vykdant konkrečias darbo ir kitas su Užsakovu susijusias funkcijas.

2.2. Kompleksiškumo (angl. defence in depth) – saugumo grėsmių mažinimui taikomos ne atskiros, o viena kitą papildančios saugumo priemonės.

3. Saugumo sprendimai turi būti grindžiami rizikų vertinimu ir priimami dalyvaujant Užsakovui ir Tiekėjui. Projekto metu Identifikuotų rizikų pagrindu Tiekėjas kartu su Užsakovu detalizuos saugumo reikalavimus ir įtrauks į projektą.

II. PAŽEIDŽIAMUMŲ VALDYMAS

4. Sistemų ir Įrangos pažeidžiamumas (saugumo spragas ar silpnos vietos, angl. vulnerabilities) yra tikėtinas. Užsakovas ir Tiekėjas skirs deramas pastangas, kad identifikuoti pažeidžiamumą kuo ankstesniame Projekto etape.

5. Saugumo skaidrumas – Tiekėjas sužinojęs apie pažeidžiamumą, šią informaciją Užsakovui pateiks nedelsiant ir pilnoje apimtyje.

6. Prieš pradedant eksploataciją Įrenginių operacinėje sistemoje, mikrokode (angl. firmware), programinėje įrangoje turi būti įdiegtos vėliausios gamintojo saugumo pataisos ir vėliausios siūlomos programinės įrangos versijos.

III. APSAUGA NUO ŽALINGO KODO

7. Įrangoje, kurioje yra atitinkamas funkcionalumas laikantis saugumo rekomendacijų turi būti sukonfigūruotos lokalios ugniasienės ar kitos atitinkamos priemonės, blokuojančios visą nebūtiną įeinantį/ išeinantį duomenų srautą, bei perteklines funkcijas.

8. Visoje įrangoje, kuri veikia Windows operacinės sistemos pagrindu, privalo būti įdiegta Užsakovo patvirtinta antivirusinė programinė įranga (kai dėl techninių apribojimų tas negali būti atlikta, išimtį tvirtina Užsakovas).

9. Antivirusinė programinė įranga turi būti sukonfigūruota:

9.1. startuoti ir įsijungti sistemos startavimo metu;

9.2. tikrinti savo integralumą;

9.3. vykdyti realaus laiko stebėseną;

9.4. kad naudotojas jos negalėtų išjungti ar sustabdyti;

9.5. kad skenuotų visus atidaromus failus prieš jų atidarymą ir paleidimą;

9.6. pilnam skenavimui ne rečiau kaip kartą per mėnesį;

9.7. kuomet infekuotas failas yra rastas, sistema turi:

9.7.1. automatiškai išvalyti failą;

9.7.2. jei failo išvalymas negalimas – blokuoti prieigą prie infekuoto failo;

9.7.3. pranešti naudotojui garsiniu ir vaizdiniu pranešimu;

10. Antivirusinių žalingo kodo duomenų bazės turi būti atnaujinamos:

10.1. Ugniasienės, antivirusinės serveriai – ne rečiau kaip 1 kartą į valandą;

10.2. Klientai (pvz. kompiuterinės darbo vietos) – ne rečiau kaip 1 kartą į 4 valandas

11. Standartiniams naudotojams draudžiamas programinės įrangos diegimas ir konfigūracijos keitimas;

12. Prieš perduodant eksploatacijai Informacinę sistemą ar įrangą, visuose jos komponentuose turi būti pašalinti arba išjungti nebūtini sisteminiai servisai, vartotojai, tinklo prievadai, numatytoms užduotims nebūtina programinė įranga.

IV. TAPATYBĖS NUSTATYMAS IR PRIEIGOS PATVIRTINIMAS

13. Prieiga prie informacinių sistemų ir įrangos (pvz.: vietinė naudojant valdymo pultą (HMI), vietinė naudojant komunikacijos/diagnostikos prievadus ar nuotolinė naudojant komunikacijų terpę) turi būti apsaugota identifikatoriumi ir slaptažodžiu atitinkančiais Litgrid AB reikalavimus (reikalavimai pateikiami projekto įgyvendinimo metu).
14. Prieigos saugumas informacinėse sistemose ir įrangoje turi būti užtikrinamas taikant vaidmenimis pagrįstą teisių sistemą (angl. Role Based Access Control) – naudotojas sistemoje turi būti priskirtas tam tikram vaidmeniui, kuriam priskirtos minimalios, darbo užduočių atlikimui būtinos teisės.
15. Tinklo prieiga prie Užsakovo resursų turi būti suteikiama tik patvirtintiems (autorizuotiems) naudotojams ir įrenginiams. Naudotojams turi būti pasiekiamos tik tos tinklo paslaugos (sąsajos, prievadai) kurie būtini jų darbui, prieiga prie administravimo/valdymo sąsajų turi būti apribota ir pasiekiama tik sistemų/įrenginių administravimo personalui.

16. Standartiniai Informacinių sistemų ir įrangos paskyrų identifikatoriai ir slaptažodžiai turi būti pakeisti į identifikatorius ir slaptažodžius atitinkančius Litgrid AB reikalavimus (reikalavimai pateikiami projekto įgyvendinimo metu) iki pradedant jų eksploataciją.
17. Iš interneto laisvai, be jokio šaltinių apribojimo pasiekiami įmonės resursai vartotojų ir administratorių tapatumui patvirtinti turi naudoti Užsakovo patvirtintą dviejų veiksnių tapatumo patvirtinimo mechanizmą.
18. Turi būti pateiktas visų sukurtų techninių/sisteminių paskyrų sąrašas su priskirtais už jų saugumą atsakingais Užsakovo darbuotojais – sistemų administratoriais.
19. Visi prisijungimo metodai (įskaitant ir nuotolinį), priemonės ir prievadai turi būti dokumentuoti ir suderinti su Litgrid AB informacijos saugos atstovu. Bet koks neautorizuotas ar nedokumentuotas prisijungimas draudžiamas.
20. Bendrovės sistemose turi būti užtikrinta, kad:

20.1. prieš prisijungiant parodomas perspėjimas dėl neautorizuoto sistemos naudojimo;

20.2. prieiga prie sistemų programinės įrangos išeities tekstų (kodo) yra apribota pagal principą „būtina darbui“.

V. DUOMENŲ PERDAVIMO TINKLAS

21. Projektuojant, diegiant ir administruojant duomenų perdavimo tinklą turi būti vadovaujamasi ISO/IEC 27033 „Informacinės technologijos. Saugumo metodai. Tinklo saugumas“ standarto rekomendacijomis.
22. Tinklo įrenginių administravimui turi būti naudojama centralizuota autentifikacijos sistema.
23. Tinklo įrenginių administravimui turi būti naudojami šifruoti protokolai.
24. Visi duomenys, perduodami viešaisiais tinklais, turi būti saugiai šifruojami (įskaitant, bet neapsiribojant SSL, AES-CCMP).
25. Visi nebūtini veiklai tinklo įrenginių valdymo prievadai turi būti panaikinti ar išjungti.
26. Nenaudojami tinklo įrenginių prievadai ir duomenų tinklo fizinės jungtys turi būti de aktyvuojamos/atjungiamos.
27. Perdavimo tinklo dispečerinio valdymo sistemos paslaugos teikimui Bevielio tinklo prieiga nenaudojama, o iškilus tokiam poreikiui jis turi būti patvirtintas Informacijos saugos vadovo ir realizuotas taip, kad atitiktų techninius kibernetinio saugumo reikalavimus numatytus teisės aktuose.

VI. INFORMACIJOS PERDAVIMAS

28. Prieš perduodant eksploatacijai, Užsakovui saugiu būdu turi būti perduoti Informacinių sistemų ir Įrangos konfigūraciniai failai, atsarginės kopijos, identifikatoriai, slaptažodžiai, instrukcijos ir kita funkcionalumo atstatymui reikalinga ar projekto metu suderinta informacija.

VII. ĮVYKIŲ REGISTRAVIMAS

29. Visose informacinėse sistemose ir Įrangoje, kuriose tai techniškai įmanoma, turi būti registruojama ir ne mažiau kaip 6 mėnesius išsaugoma saugumo ir kitų svarbių įvykių informacija (Užsakovas projektavimo metu pateiks detalius reikalavimus priklausomai nuo įrangos tipo).
30. Turi būti užtikrinta, kad registruojamiems įvykiams lokaliai rezervuota pakankamai laisvos vietos.
31. Informacinė sistema ir visa Įranga turi būti sukonfigūruota siųsti įvykių įrašus į Bendrovės centrinį žurnalinių įrašų serverį.

VIII. SAUGUMO TESTAVIMAS

32. Prieš pradedant eksploatuoti informacines sistemas turi būti atliekamas saugumo testavimas, siekiant nustatyti sistemos atitiktį saugumo reikalavimams ir pašalinti sistemos techninius pažeidžiamumus. Testuojant turi būti įvertinama (bet neapsiribojant) atitiktis:
    32.1. OWASP 10 dažniausiai pasitaikančių internetinių sistemų techninių pažeidžiamumų;
    32.2. CWE/SANS 25 dažniausiai pasitaikančios programinės įrangos klaidos.

IV. TREČIŲ ŠALIŲ KOMPONENTAI

33. Skaidrumas. Tiekėjas privalo nurodyti visus sistemoje naudojamus trečių šalių komponentus, bibliotekas ir schemas nepriklausomai ar tai komercinė, nemokama, atviro ar uždaro kodo programinė įranga.
34. Vertinimas. Tiekėjas turi imtis deramų priemonių užtikrinant, kad sistemoje naudojama trečių šalių programinė įranga atitinka saugumo reikalavimus keliamus sistemai ir yra tinkamai licencijuota.
35. Kenksminga programinė įranga. Tiekėjas įsipareigoja pateikti sistemą, kurioje nėra jokių paslėptų, saugumą silpninančių funkcijų, įskaitant: kenksmingos programinės įrangos, virusų, „kirminų“, „laiko minų“, neautorizuotų prieigų ar funkcijų (Trojans, backdoors, easter eggs).

X. SAUGUMO VAIDMENYS

36. Tiekėjas saugumo užtikrinimui deleguos saugumo kompetencijas turintį darbuotoją (saugumo architektą), kuris peržiūrės rezultatus iki pateikiant Užsakovui ir patvirtins atitikimą saugumo reikalavimams.

37. Saugumo mokymai. Visi Tiekėjo darbuotojai dalyvaujantys projekte turi būti susipažinę su šiais reikalavimais.

XI. SAUGUMO AUDITAS

38. Audito teisė. Užsakovas turi teisę atlikti sistemos saugumo auditą. Teikėjas privalo suteikti deramą pagalbą Užsakovui atliekant saugumo auditą, įskaitant išeitinio kodo pateikimą ir prieigos prie testavimo aplinkos suteikimą.

XII. PAPILDOMI REIKALAVIMAI PRAMONINIŲ PROCESŲ VALDYMO SISTEMAI IR JOS DALIMS

39. Visuose Įrangos įgyvendinimo etapuose (projektavimas, diegimas, priežiūra ir kt.) turi būti laikomasi informacinio saugumo reikalavimų patvirtintų:

    39.1. Lietuvos Respublikos energetikos ministro 2013-05-02 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“.

    39.2. Lietuvos Respublikos Vyriausybės nutarimu 2018 m. gruodžio 5 d. Nr. 1209 patvirtintame Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams apraše