

## MINIMALŪS INFORMACIJOS SAUGOS REIKALAVIMAI PROJEKTAVIMUI IR DIEGIMUI V.1.1

### 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, pastotės laiko sinchronizavimo 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.
4. Įrangos, įskaitant ir jo operacinę sistemą, gamintojų palaikymas turi galioti ne trumpiau nei 5 metus.

### II. PAŽEIDŽIAMUMŲ VALDYMAS

5. 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.
6. Saugumo skaidrumas - Tiekėjas sužinojęs apie pažeidžiamumą, šią informaciją Užsakovui pateiks nedelsiant ir pilnoje apimtyje.
7. Jeigu nenurodyta kitaip, tuomet prieš pradedant eksploataciją, Įrenginių operacinėje sistemoje, mikrokode (angl. firmware), programinėje įrangoje turi būti įdiegtos vėliausios gamintojo saugumo pataisos ir vėliausios siūlomos programinės įrangos versijos.
8. Prieš pradedant kompleksinius bandymus teleinformacijos surinkimo ir perdavimo įrenginio (TSPĮ), pastotės laiko sinchronizavimo įrenginio (PLSĮ), operacinėje sistemoje, mikrokode (angl. firmware), programinėje įrangoje turi būti įdiegtos vėliausios gamintojo saugumo pataisos ir vėliausios siūlomos programinės įrangos versijos.

9. Prieš pradedant gamyklinius bandymus, bet ne anksčiau nei 12 mėnesių iki relinės apsaugos ir automatikos įrenginių (RAA), teleinformacijos perdavimo įrenginių (TPĮ), bendros paskirties valdiklių (BPV), perdavimo į eksploataciją, RAA, TPĮ ir BPV 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**

10. Įrangoje, kurioje yra atitinkamas funkcionalumas laikantis saugumo rekomendacijų turi būti sukonfigūruotos lokalsios ugniasienės ar kitos atitinkamos priemonės, blokuojančios visą nebūtiną įeinantį/ išeinantį duomenų srautą, bei perteklines funkcijas.
11. 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).
12. Antivirusinė programinė įranga turi būti sukonfigūruota:
- 12.1. startuoti ir įsijungti sistemos startavimo metu;
  - 12.2. tikrinti savo integralumą;
  - 12.3. vykdyti realaus laiko stebėseną;
  - 12.4. kad naudotojas jos negalėtų išjungti ar sustabdyti;
  - 12.5. kad skenuotų visus atidaromus failus prieš jų atidarymą ir paleidimą;
  - 12.6. pilnam skenavimui ne rečiau kaip kartą per mėnesį;
  - 12.7. kuomet infekuotas failas yra rastas, sistema turi:
    - 12.7.1. automatiškai išvalyti failą;
    - 12.7.2. jei failo išvalymas negalimas - blokuoti prieigą prie infekuoto failo;
    - 12.7.3. pranešti naudotojui garsiniu ir vaizdiniu pranešimu;
13. Antivirusinių žalingo kodo duomenų bazės turi būti atnaujinamos:
- 13.1. Ugniasienės, antivirusinės serveriai - ne rečiau kaip 1 kartą į valandą;
  - 13.2. Klientai (pvz. kompiuterinės darbo vietos) - ne rečiau kaip 1 kartą į 4 valandas
14. Standartiniais naudotojams draudžiamas programinės įrangos diegimas ir konfigūracijos keitimas;
15. Prieš perduodant eksploatacijai Informacinę sistemą ar įrangą, visuose jos komponentuose turi būti pašalinti arba išjungti nebūtini sisteminiai servais, vartotojai, tinklo prievadai, numatytiems užduotims nebūtina programinė įranga.
16. Sistemos ir įranga turi būti suprojektuota ir sukonfigūruota vadovaujantis gerosiomis saugos praktikomis numatytiomis CIS Security bechmarks, Security baseline for Windows dokumentuose.
17. Sistemų ir įrangos integracija į Užsakovo tinklą ar integracija su kitomis Užsakovo sistemomis neturi reikalauti sumažinti saugumo lygio esamose sistemose nukrypstant nuo gerųjų saugos praktikų.

#### **IV. TAPATYBĖS NUSTATYMAS IR PRIEIGOS PATVIRTINIMAS**

18. 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).
19. 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.
20. 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 pasiekama tik sistemų/įrenginių administravimo personalui.
21. 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.
22. Sistemose naudotojų paskyrų valdymas turi būti realizuotas naudojant centralizuotą Užsakovo paskyrų, teisių ir resursų valdymo sistemą - katalogų tarnybą.
23. Iš interneto laisvai, be jokio papildomo apribojimo pasiekiami įmonės resursai vartotojų ir administratorių tapatumui patvirtinti turi naudoti Užsakovo patvirtintą dviejų veiksmų tapatumo patvirtinimo mechanizmą.
24. Turi būti pateiktas visų sukurtų techninių/sisteminių paskyrų sąrašas su priskirtais už jų saugumą atsakingais Užsakovo darbuotojais - sistemų administratoriais.
25. 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.
26. Bendrovės sistemose turi būti užtikrinta, kad:
  - 26.1. prieš prisijungiant parodomas perspėjimas dėl neautorizuoto sistemos naudojimo;
  - 26.2. prieiga prie sistemų programinės įrangos išeities tekstų (kodo) yra apribota pagal principą „būtina darbui“.

#### **V. DUOMENŲ PERDAVIMO TINKLAS**

27. Projektuojant, diegiant ir administruojant duomenų perdavimo tinklą turi būti vadovaujama ISO/IEC 27033 „Informacinės technologijos. Saugumo metodai. Tinklo saugumas“ standarto rekomendacijomis.
28. Tinklo įrenginių administravimui turi būti naudojama centralizuota autentifikacijos sistema.

- 29. Tinklo įrenginių administravimui turi būti naudojami šifruoti protokolai.
- 30. Visi duomenys, perduodami viešaisiais tinklais, turi būti saugiai šifruojami (įskaitant, bet neapsiribojant SSL, AES-CCMP).
- 31. Visi nebūtini veiklai tinklo įrenginių valdymo prievadai turi būti panaikinti ar išjungti.
- 32. Nenaudojami tinklo įrenginių prievadai ir duomenų tinklo fizinės jungtys turi būti deaktyvuojamos/atjungiamos.
- 33. 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**

- 34. 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**

- 35. 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).
- 36. Turi būti užtikrinta, kad registruojamiems įvykiams lokaliai rezervuota pakankamai laisvos vietos.
- 37. Informacinė sistema ir visa įranga turi būti sukonfigūruota siųsti įvykių įrašus į Bendrovės centrinį žurnalinių įrašų serverį.

## **VIII. SAUGUMO TESTAVIMAS**

- 38. 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:
  - 38.1. OWASP 10 dažniausiai pasitaikančių internetinių sistemų techninių pažeidžiamumų;
  - 38.2. CWE/SANS 25 dažniausiai pasitaikančios programinės įrangos klaidos.

#### **IV. TREČIŲ ŠALIŲ KOMPONENTAI**

39. Skaidrumas. Tiekėjas privalo nurodyti visus sistemoje naudojamus trečių šalių komponentus, bibliotekas ir schemas nepriklausomai ar tai komercinė, nemokama, atviro ar uždaro kodo programinė įranga.
40. Vertinimas. Tiekėjas turi imtis deramų priemonių užtikrinant, kad sistemoje naudojama trečių šalių programinė įranga atitinka saugumo reikalavimus keliamus sistemai ir yra tinkamai licencijuota.
41. 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**

42. Tiekėjas saugumo užtikrinimui deleguos saugumo kompetencijas turintį darbuotoją (saugumo architektą), kuris peržiūrės rezultatus iki pateikiant Užsakovui ir patvirtins atitikimą saugumo reikalavimams.
43. Saugumo mokymai. Visi Tiekėjo darbuotojai dalyvaujantys projekte turi būti susipažinę su šiais reikalavimais.

#### **XI. SAUGUMO AUDITAS**

44. Audito teisė. Užsakovas turi teisę atlikti sistemos saugumo auditą. Tiekėjas 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**

45. Visuose įrangos įgyvendinimo etapuose (projektavimas, diegimas, priežiūra ir kt.) turi būti laikomasi informacinio saugumo reikalavimų patvirtintų Lietuvos Respublikos Vyriausybės nutarimu 2018 m. gruodžio 5 d. Nr. 1209 patvirtintame Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams apraše.

## **MINIMUM INFORMATION SECURITY REQUIREMENTS FOR PROJECT DESIGNMENT AND IMPLEMENTATION**

### **I.GENERAL PROVISION**

1. This document sets out the minimum requirements and principles applicable to the design of Information Systems and / or projects related to Information Technology and Telecommunications (ITT) equipment, microprocessor equipment, such as: telecommunication data acquisition and transmission equipment (RTU), substation time synchronization equipment, relay protection terminals (IED), control panels (HMI), metering data controllers, general purpose controllers, telecommunication collection and transmission system, commercial data controllers, Supervisory control and data acquisition system (SCADA) etc. (hereinafter referred to as the Equipment) and for the technical execution and implementation of these projects.
2. The following security principles must be complied at all stages of the Project implementation:
  - 2.1. Minimum rights. When managing access to the Company's project Information, information systems and Equipment, the implementation of the principle “necessary for work” must be ensured, for example: requirement that means that access may be granted only to approved persons and only to the extent necessary for the performance of specific work and other functions related to the Customer.
  - 2.2. Complexity (defense in depth). To reduce cyber security threats risk, measures that supplement each other must be used.
3. Technical and organizational security decisions must be based on a risk assessment and taken in the presence of the Customer and the Supplier. During the project, based on the identified risks, the Supplier together with the Customer will detail the security requirements and include them in the project.
4. Manufacturer support period for the information system and Equipment, including operating system, shall be at least 5 years.

### **II.VULNERABILITY MANAGEMENT**

5. Vulnerabilities in the Systems and Equipment (security vulnerabilities or vulnerabilities) are likely. The Customer and the Supplier will make reasonable efforts to identify the vulnerability at the earliest possible stage of the Project.
6. Security Transparency. Upon becoming aware of the vulnerability, the Supplier will provide this information to the Customer immediately and in full.
7. Unless otherwise noted, the latest firmware fixes and the latest software versions offered by the manufacturer must be installed in the software operating system, microcode (firmware), before putting equipment into operation.

8. The latest security patches and the latest software versions offered by the manufacturer must be installed in the operating system, microcode (firmware), software of the telecommunication collection and transmission device (RTU), substation time synchronization device before the start of complex tests.
9. The latest security patches and the latest software versions offered by the manufacturer must be installed in the operating system, microcode (firmware), software of the relay protection and automation devices (IED), telecommunication devices, general purpose controllers before factory testing, but not earlier than 12 months before putting equipment into operation.

### **III. PROTECTION AGAINST MALICIOUS CODE**

10. In accordance with security recommendations, Equipment must contain properly configured local firewall or other appropriate solution to block all unnecessary inbound / outbound traffic.
11. All Equipment that runs on the Windows operating system requires the installation of antivirus software approved by the Customer (when due to technical limitations, an exception is approved by the Customer).
12. Antivirus software must be configured:
  - 12.1. to start and turn on during system startup;
  - 12.2. to check its integrity;
  - 12.3. to perform real-time monitoring;
  - 12.4. to operate in such a way that it cannot be switched off or stopped by the user;
  - 12.5. to scan all open files before opening and executing them;
  - 12.6. to perform a full scan at least once a month;
  - 12.7. When an infected file is found, the system must:
  - 12.8. automatically clean the file;
  - 12.9. if file cleanup is not possible - block access to the infected file;
  - 12.10. notify the user by audio and visual message;
13. Antivirus malicious code databases must be updated on regular basis:
  - 13.1. Firewalls, antivirus servers - at least once an hour;
  - 13.2. Clients (eg computer workstations) - at least once in 4 hours;
14. Standard users are not allowed to install software or change the configuration;
15. Unused system services, users, network ports must be removed or disabled in all its components before the Information System or Equipment is put into operation.
16. Systems and Equipment must be designed and configured in accordance with the best security practices set forth in the CIS Security benchmarks, Security baseline for Windows.

17. Systems and Equipment integration into the Customer's network or integration with other Customer's systems must not call a security level reduction of existing systems or deviation from good security practices.

#### **IV. IDENTIFICATION AND ACCESS VERIFICATION**

18. Access to information systems and Equipment (example: local using the control panel (HMI), local using the communication / diagnostic ports or remote using the communication medium) must be protected by an identifier and password that meet the requirements of Litgrid AB (requirements are provided during the project implementation).
19. The security of access to the information systems and Equipment must be ensured by applying a Role Based Access Control - the user must be assigned to a certain role in the system to which the minimum rights necessary for the performance of work tasks have been assigned.
20. Network access to Customer's resources must be granted only to approved (authorized) users and devices. Users must have access only to those network services (interfaces, ports) that are necessary for their work. Access to administration / management interfaces must be restricted and accessible only to system / device administration personnel.
21. Standard identifiers and passwords for Information Systems and Equipment accounts must be changed to identifiers and passwords that meet the requirements of Litgrid AB (requirements are provided during the project implementation).
22. In the systems, the management of user accounts must be implemented using the centralized management system of the Customer's accounts, rights and resources (the active directory service).
23. The company's resources freely accessible from the Internet without any additional restrictions, must use a two-factor authentication mechanism approved by the Customer to authenticate users and administrators.
24. A list of all created technical / system accounts, with the assigned Customer's employees responsible for their security (system administrators), must be provided.
25. All connection methods (including remote), tools and ports must be documented and agreed with the information security representative of Litgrid AB. Any unauthorized or undocumented connection is prohibited.
26. The company's systems must ensure that:
- 26.1. a warning about unauthorized use of the system is displayed before connecting;
  - 26.2. access to the source code of the systems software is restricted according to the "necessary for work" principle.

#### **V. DATA TRANSMISSION NETWORK**



27. The design, implementation and administration of the data transmission network shall be in accordance with ISO / IEC 27033 „Information technology. Security methods. Network Security“ standard.
28. A centralized authentication system must be used for the administration of network devices.
29. Encrypted protocols must be used to administer network devices.
30. All data transmitted over public networks must be securely encrypted (including but not limited to SSL, AES-CCMP).
31. All non-essential network device control ports must be removed or disabled.
32. Network device ports and physical data network connections that are not used, must be deactivated / disconnected.
33. Wireless network must not be used for the provision of the transmission network or dispatching management system service. In case of such need it must be approved by the LITGRID Information Security Manager and implemented in such way, that it meets the technical requirements of cyber security provided by law.

## **VI. PROVISION OF INFORMATION**

34. Before commissioning, the configuration files, backup copies, identifiers, passwords, instructions and other information required for the restoration of functionality or agreed upon during the project must be provided to the Customer in a secure manner.

## **VII. EVENT REGISTRATION**

35. In all information systems and Equipment, information on security and other important events must be recorded and stored for at least 2 weeks (the Customer will provide detailed requirements during design depending on the type of equipment).
36. It must be ensured that sufficient space is reserved locally for the events to be recorded.
37. The information system and all Equipment must be configured to send event logs to the Company's central log server.

## **VIII. SECURITY TESTING**

38. Prior to the commissioning of information systems, security testing shall be performed in order to determine the compliance of the system with the security requirements and to eliminate the technical vulnerabilities of the system. The testing shall assess (but not be limited to) compliance with:
  - 38.1. OWASP 10 most common technical vulnerabilities in online systems;
  - 38.2. CWE / SANS 25 most common software errors.

#### **IX. THIRD COUNTRY COMPONENTS**

- 39. Transparency. The Supplier must identify all third-party components, libraries, and schemas used in the system, whether commercial, free, open source, or closed source software.
- 40. Evaluation. The Supplier shall take appropriate measures to ensure that the third-party software used in the System complies with the security requirements of the System and is properly licensed.
- 41. Malicious software. The Supplier undertakes to provide a system that does not contain any hidden, security-compromising features, including malware, viruses, worms, "time mines", unauthorized access or features (Trojans, backdoors, easter eggs).

#### **X. SECURITY ROLES**

- 42. The Supplier will delegate an employee with security competencies (security architect) to ensure security, who will review the results before submitting them to the Customer and confirm compliance with security requirements.
- 43. Security training. All employees of the Supplier participating in the project must be familiar with these requirements.

#### **XI. SECURITY AUDIT**

- 44. Audit rights. The customer has the right to perform an information system and Equipment security audit. The Provider must provide appropriate assistance to the Client during the security audit.

#### **XI. ADDITIONAL REQUIREMENTS FOR INDUSTRIAL PROCESS MANAGEMENT SYSTEM AND PARTS THEREOF**

- 45. At all stages of the implementation of the Equipment (design, installation, maintenance, etc.) the approved information security requirements shall be complied with the Resolution of the Government of the Republic of Lithuania in 2018. December 5 No. 1209 in the approved Description of Organizational and Technical Cyber Security Requirements for Cyber Security Entities.