LITGRID AB informacijos saugos tvarkos aprašo patvirtinto
Generalinio direktoriaus 202-__-__ įsakymu Nr.__

MINIMALŪS INFORMACIJOS SAUGOS REIKALAVIMAI PROJEKTAVIMUI IR DIEGIMUI V.1.2

I. BENDROSIOS NUOSTATOS

1. Šiuo dokumentu yra nustatomi minimalūs reikalavimai ir principai (toliau – Reikalavimai) 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 įgyvendinimui – diegimui (toliau – Projektas).
2. Visuose Projekto įgyvendinimo etapuose turi būti laikomasi šių saugumo principų:
   2.1. Minimalių teisių – valdant prieigą prie LITGRID AB (toliau – Bendrovė) informacijos, informacinių sistemų ir Įrenginių, turi būti užtikrintas principo „būtina darbui“ ir „mažiausių teisių prieiga“ įgyvendinimas, t. y. reikalavimas, kuris reiškia, kad prieiga gali būti suteikta tik patvirtintiems asmenims ir mažiausia apimtimi, kuri yra būtina vykdant konkrečias darbo ir kitas su Bendrove 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 Bendrovei ir tiekėjui, įgyvendinančiam Projektą (toliau – Tiekėjas). Projekto metu identifikuotų rizikų pagrindu Tiekėjas kartu su Bendrove detalizuos saugumo reikalavimus ir įtrauks į Projektą.
4. Įrangos, įskaitant ir jos operacinę sistemą, gamintojų palaikymas turi galioti ne trumpiau nei 5 metus.
5. Jeigu diegiamos Informacinės sistemos ar Įrenginių gamintojas yra išleidęs saugos rekomendacijas, jos, suderinus su Bendrove, turi būti įgyvendintos. Prieš pradedant eksploataciją, Bendrovei paprašius, turi būti pateikti suderintų gamintojo saugos rekomendacijų įgyvendinimo įrodymai.

II. PAŽEIDŽIAMUMŲ VALDYMAS

6. Sistemų ir Įrangos pažeidžiamumas (saugumo spragas ar silpnos vietos, angl. vulnerabilities) yra tikėtinas. Bendrovė ir Tiekėjas skirs deramas pastangas, siekdami identifikuoti pažeidžiamumą kuo ankstesniame Projekto etape.
7. Saugumo skaidrumas – Tiekėjas, sužinojęs apie pažeidžiamumą, šią informaciją Bendrovei pateiks nedelsiant ir pilnoje apimtyje.
8. Jeigu nenurodyta kitaip, prieš pradedant eksploataciją, Įrenginių operacinėje sistemoje, mikrokode (angl. *firmware)*, programinėje įrangoje turi būti įdiegtos vėliausios gamintojo saugumo pataisos ir vėliausios siūlomos programinės įrangos versijos.
9. 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.

10. 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

11. 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.
12. Visoje įrangoje, kuri veikia Windows operacinės sistemos pagrindu, privalo būti įdiegta Bendrovės patvirtinta antivirusinė programinė įranga (kai dėl techninių apribojimų tas negali būti atlikta, išimtį tvirtina Bendrovė).
13. Antivirusinė programinė įranga turi būti sukonfigūruota:
    - 13.1. startuoti ir įsijungti sistemos startavimo metu;
    - 13.2. tikrinti savo integralumą;
    - 13.3. vykdyti realaus laiko stebėseną;
    - 13.4. kad naudotojas jos negalėtų išjungti ar sustabdyti;
    - 13.5. kad skenuotų visus atidaromus failus prieš jų atidarymą ir paleidimą;
    - 13.6. pilnam skenavimui ne rečiau kaip kartą per mėnesį;
    - 13.7. kuomet infekuotas failas yra rastas, sistema turi:
        - 13.7.1. automatiškai išvalyti failą;
        - 13.7.2. jei failo išvalymas negalimas – blokuoti prieigą prie infekuoto failo;
        - 13.7.3. pranešti naudotojui garsiniu ir vaizdiniu pranešimu.
14. Antivirusinės programos žalingo kodo duomenų bazės turi būti atnaujinamos:
    - 14.1. Ugniasienės, antivirusinės programos serveriai – ne rečiau kaip 1 kartą į valandą;
    - 14.2. Klientai (pvz. kompiuterinės darbo vietos) – ne rečiau kaip 1 kartą į 4 valandas.
15. Standartiniams naudotojams draudžiamas programinės įrangos diegimas ir konfigūracijos keitimas.
16. 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.
17. Sistemos ir Įranga turi būti suprojektuota ir sukonfigūruota vadovaujantis gerosiomis saugos praktikomis numatytomis CIS Security bechmarks, Security baseline for Windows dokumentuose.
18. Sistemų ir Įrangos integracija į Bendrovės tinklą ar integracija su kitomis Bendrovės sistemomis neturi reikalauti sumažinti saugumo lygio esamose sistemose nukrypstant nuo gerųjų saugos praktikų.

IV. TAPATYBĖS NUSTATYMAS IR PRIEIGOS PATVIRTINIMAS

19. 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 Bendrovės nustatytus reikalavimus (reikalavimai pateikiami projekto įgyvendinimo metu).
20. 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.
21. Tinklo prieiga prie Bendrovės 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.
22. Standartiniai informacinių sistemų ir Įrangos paskyrų identifikatoriai ir slaptažodžiai turi būti pakeisti į identifikatorius ir slaptažodžius atitinkančius Bendrovės nustatytus reikalavimus (reikalavimai pateikiami Projekto įgyvendinimo metu) iki pradedant jų eksploataciją.
23. Sistemose naudotojų paskyrų valdymas turi būti realizuotas naudojant centralizuotą Bendrovės paskyrų, teisių ir resursų valdymo sistemą – katalogų tarnybą.
24. Iš interneto laisvai, be jokio papildomo apribojimo pasiekiami Bendrovės resursai vartotojų ir administratorių tapatumui patvirtinti turi naudoti Bendrovės patvirtintą dviejų veiksnių tapatumo patvirtinimo mechanizmą.
25. Turi būti pateiktas visų sukurtų techninių/sisteminių paskyrų sąrašas su priskirtais už jų saugumą atsakingais Bendrovės darbuotojais – sistemų administratoriais.
26. Visi prisijungimo metodai (įskaitant ir nuotolinį), priemonės ir prievadai turi būti dokumentuoti ir suderinti su Bendrovės Informacijos saugos grupės atstovu. Bet koks neautorizuotas ar nedokumentuotas prisijungimas draudžiamas.
27. Bendrovės sistemose turi būti užtikrinta, kad:
    27.1. prieš prisijungiant parodomas perspėjimas dėl neautorizuoto sistemos naudojimo;
    27.2. prieiga prie sistemų programinės įrangos išeities tekstų (kodo) yra apribota pagal principą „būtina darbui“.

V. DUOMENŲ PERDAVIMO TINKLAS

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

31. Visi duomenys, perduodami viešaisiais tinklais, turi būti saugiai šifruojami (įskaitant, bet neapsiribojant SSL, AES-CCMP).
32. Visi nebūtini veiklai tinklo įrenginių valdymo prievadai turi būti panaikinti ar išjungti.
33. Nenaudojami tinklo įrenginių prievadai ir duomenų tinklo fizinės jungtys turi būti deaktyvuojamos/atjungiamos.
34. Perdavimo tinklo dispečerinio valdymo sistemos paslaugos teikimui bevielio tinklo prieiga nenaudojama, o iškilus tokiam poreikiui jis turi būti patvirtintas Bendrovės Informacijos saugos grupės vadovo ir realizuotas taip, kad atitiktų techninius kibernetinio saugumo reikalavimus numatytus Lietuvos Respublikos teisės aktuose.

VI. INFORMACIJOS PERDAVIMAS

35. Prieš perduodant eksploatacijai, Bendrovei 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

36. Visose informacinėse sistemose ir Įrangoje, kuriose tai techniškai įmanoma, turi būti registruojama ir ne mažiau kaip 2 savaites išsaugoma saugumo ir kitų svarbių įvykių informacija (Bendrovė projektavimo metu pateiks detalius reikalavimus priklausomai nuo Įrangos tipo).
37. Turi būti užtikrinta, kad registruojamiems įvykiams lokaliai rezervuota pakankamai laisvos vietos.
38. Informacinė sistema ir visa Įranga turi būti sukonfigūruota siųsti įvykių įrašus į Bendrovės centrinį žurnalinių įrašų serverį.
39. Prieš pradedant Įrangos eksploataciją privaloma užpildyti žemiau pateiktą lentelę ir el. laišku išsiųsti Bendrovės Informacijos saugos grupės specialistui, kuris patikrins ar žurnaliniai įrašai iš Įrangos gaunami. Bendrovės Informacijos saugos grupės specialistą nurodys už Įrangos eksploataciją atsakingas Bendrovės darbuotojas.

Eil. Nr.	Regionas	Pastotė	Įrenginio tipas ir gamintojas	Modelis	IP adresas	Įjungtas Syslog siuntimas (Taip/ Ne)	Pastaba

1 lentelė. Žurnalinių įrašų testavimo forma

VIII. SAUGUMO TESTAVIMAS

40. Prieš pradedant eksploatuoti informacines sistemas Tiekėjas turi atlikti saugumo testavimą, siekdamas nustatyti sistemos atitiktį saugumo reikalavimams ir pašalinti sistemos techninius

pažeidžiamumus. Pagal atskirą Bendrovės nurodymą Tiekėjas privalo pateikti dokumentus, pagrindžiančius testavimo rezultatus. Testuojant turi būti įvertinama (bet neapsiribojant) atitiktis:

40.1. OWASP 10 dažniausiai pasitaikančių internetinių sistemų techninių pažeidžiamumų;

40.2. CWE/SANS 25 dažniausiai pasitaikančios programinės įrangos klaidos.

IV. TREČIŲ ŠALIŲ KOMPONENTAI

41. Skaidrumas. Tiekėjas privalo nurodyti visus sistemoje naudojamus trečių šalių komponentus, bibliotekas ir schemas nepriklausomai ar tai komercinė, nemokama, atviro ar uždaro kodo programinė įranga.
42. Vertinimas. Tiekėjas turi imtis deramų priemonių užtikrinant, kad sistemoje naudojama trečių šalių programinė įranga atitinka saugumo reikalavimus keliamus sistemai ir yra tinkamai licencijuota.
43. 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 (angl. *Trojans, backdoors, easter eggs*).

X. SAUGUMO VAIDMENYS

44. Tiekėjas saugumo užtikrinimui deleguos kibernetinio saugumo kompetencijas turintį darbuotoją (saugumo architektą), kuris peržiūrės Projekto rezultatus iki pateikiant Bendrovei ir patvirtins atitikimą saugumo reikalavimams.
45. Saugumo mokymai. Tiekėjo darbuotojai dalyvaujantys Projekte turi būti susipažinę su Reikalavimais, praėję Bendrovės parengtus mokymus ir sėkmingai išlaikę Bendrovės parengtą testą.

XI. SAUGUMO AUDITAS

46. Audito teisė. Užsakovas turi teisę atlikti Projekto auditą. Teikėjas privalo suteikti deramą pagalbą Bendrovei atliekant saugumo auditą, įskaitant išeities kodo pateikimą ir prieigos prie testavimo aplinkos suteikimą. Tuo atveju, jeigu audito metu nustatomi trūkumai, Tiekėjas privalo per Bendrovės nurodytą protingą terminą trūkumus pašalinti.

XII. PAPILDOMI REIKALAVIMAI PRAMONINIŲ PROCESŲ VALDYMO SISTEMAI IR JOS DALIMS

47. Visuose Įrangos įgyvendinimo etapuose (projektavimas, diegimas, priežiūra ir kt.) turi būti laikomasi informacijos saugumo reikalavimų nustatytų Lietuvos Respublikos Vyriausybės nutarimu patvirtintame Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše (aktualioje jo redakcijoje).

XIII. ATSAKOMYBĖ

48. Bendrovė turi teisę tikrinti kaip Tiekėjas laikosi Reikalavimų, įskaitant, bet neapsiribojant, Tiekėjo Projekto įgyvendinimui naudojamų darbo priemonių atitikties Reikalavimams patikrinimą be išankstinio įspėjimo.
49. Tiekėjas, pažeidęs Reikalavimus, Bendrovei pareikalavus privalo sumokėti 1 000 eurų baudą ir atlyginti visus dėl tokio pažeidimo patirtus tiesioginius Bendrovės nuostolius, kiek jų nepadengia sumokėta bauda. Ši bauda laikoma minimaliais Bendrovės nuostoliais ir jų įrodinėti nereikia.

MINIMUM INFORMATION SECURITY REQUIREMENTS FOR PROJECT DESIGNMENT AND IMPLEMENTATION V.1.2

I.GENERAL PROVISION

1. This document sets out the minimum requirements and principles (hereinafter referred to as Requirements) 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 principles (hereinafter referred to as the Project).
2. The following security principles must be complied at all stages of the Project implementation:
   2.1. Minimum rights. When managing access to the LITGRID AB (hereinafter referred to as the Company) 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 Company.
   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 Company and the supplier implementing the Project (hereinafter referred to as the Supplies). During the Project, based on the identified risks, the Supplier together with the Company 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.
5. If the manufacturer of the installed Information System or Equipment has issued safety recommendations, they must be implemented after coordination with the Company. Prior to the start of operation, upon the Company's request, evidence of the implementation of manufacturer's safety recommendations must be provided.

II.VULNERABILITY MANAGEMENT

6. Vulnerabilities in the Systems and Equipment (security vulnerabilities or vulnerabilities) are likely. The Company and the Supplier will make reasonable efforts to identify the vulnerability at the earliest possible stage of the Project.
7. Security Transparency. Upon becoming aware of the vulnerability, the Supplier will provide this information to the Company immediately and in full.

8. 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.
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 telecommunication collection and transmission device (RTU), substation time synchronization device before the start of complex tests.
10. 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

11. In accordance with security recommendations, Equipment must contain properly configured local firewall or other appropriate solution to block all unnecessary inbound / outbound traffic.
12. All Equipment that runs on the Windows operating system requires the installation of antivirus software approved by the Company (when due to technical limitations, an exception is approved by the Company).
13. Antivirus software must be configured:
    - 13.1. to start and turn on during system startup;
    - 13.2. to check its integrity;
    - 13.3. to perform real-time monitoring;
    - 13.4. to operate in such a way that it cannot be switched off or stopped by the user;
    - 13.5. to scan all open files before opening and executing them;
    - 13.6. to perform a full scan at least once a month;
    - 13.7. when an infected file is found, the system must:
        - 13.7.1. automatically clean the file;
        - 13.7.2. if file cleanup is not possible - block access to the infected file;
        - 13.7.3. notify the user by audio and visual message.
14. Antivirus malicious code databases must be updated on regular basis:
    - 14.1. Firewalls, antivirus servers - at least once an hour;
    - 14.2. Clients (eg computer workstations) - at least once in 4 hours.
15. Standard users are not allowed to install software or change the configuration.
16. 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.
17. Systems and Equipment must be designed and configured in accordance with the best security practices set forth in the CIS Security bechmarks, Security baseline for Windows.

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

IV. IDENTIFICATION AND ACCESS VERIFICATION

19. 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 the Company (requirements are provided during the Project implementation).
20. 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.
21. Network access to Company'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.
22. Standard identifiers and passwords for Information Systems and Equipment accounts must be changed to identifiers and passwords that meet the requirements of the Company (requirements are provided during the Project implementation).
23. In the systems, the management of user accounts must be implemented using the centralized management system of the Company's accounts, rights and resources (the active directory service).
24. The Company's resources freely accessible from the Internet without any additional restrictions, must use a two-factor authentication mechanism approved by the Company to authenticate users and administrators.
25. A list of all created technical / system accounts, with the assigned Company's employees responsible for their security (system administrators), must be provided.
26. All connection methods (including remote), tools and ports must be documented and agreed with the information security representative of the Company. Any unauthorized or undocumented connection is prohibited.
27. The Company's systems must ensure that:

    27.1. a warning about unauthorized use of the system is displayed before connecting;

    27.2. access to the source code of the systems software is restricted according to the "necessary for work" principle.

V. DATA TRANSMISSION NETWORK

28. 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.
29. A centralized authentication system must be used for the administration of network devices.
30. Encrypted protocols must be used to administer network devices.
31. All data transmitted over public networks must be securely encrypted (including but not limited to SSL, AES-CCMP).
32. All non-essential network device control ports must be removed or disabled.
33. Network device ports and physical data network connections that are not used, must be deactivated / disconnected.
34. 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 Company Information Security Group representative and implemented in such way, that it meets the technical requirements of cyber security provided by law of Republic of Lithuania.

VI. PROVISION OF INFORMATION

35. 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 Company in a secure manner.

VII. EVENT REGISTRATION

36. In all information systems and Equipment, information on security and other important events must be recorded and stored for at least 2 weeks (the Company will provide detailed requirements during design depending on the type of equipment).
37. It must be ensured that sufficient space is reserved locally for the events to be recorded.
38. The information system and all Equipment must be configured to send event logs to the Company's central log server.
39. Before commissioning, the table below must be filled ant and e-mailed to the specialist of the Company's Information Security Group, who will check whether event logs are received from the Device. The specialist of the Company's Information Security Group will be specified by the Company's employee responsible for the operation of the Device.

No.	Region	Substation	Type ant manufacturer of the Device	Model	IP adress	Syslog Sending Enabled (Yes/No)	Comment

1 table. Form of event logs test

VIII. SECURITY TESTING

40. 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. According to a separate request of the Company, the Supplier shall submit documents justifying the test results. The testing shall assess (but not be limited to) compliance with:
    40.1. OWASP 10 most common technical vulnerabilities in online systems;
    40.2. CWE / SANS 25 most common software errors.

IX. THIRD PARTY COMPONENTS

41. 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.
42. 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.
43. 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

44. The Supplier will delegate an employee with security competencies (security architect) to ensure security, who will review the results before submitting them to the Company and confirm compliance with security requirements.
45. Security training. All employees of the Supplier participating in the Project must be familiar with Requirements, having completed the training and successfully passed the test prepared by the Company.

XI. SECURITY AUDIT

46. Audit rights. The Company has the right to perform an information system and Equipment security audit. The Supplier must provide appropriate assistance to the Company during the security audit. In case deficiencies are identified during the audit, the Supplier must eliminate them within a reasonable period specified by the Company.

XII. ADDITIONAL REQUIREMENTS FOR INDUSTRIAL PROCESS MANAGEMENT SYSTEM AND PARTS THEREOF

47. At all stages of the implementation of the Equipment (design, installation, maintenance, etc.) the approved information security requirements shall be complied with the Description of

Organizational and Technical Cyber Security Requirements for Cyber Security Entities approved by the Resolution of the Government of the Republic of Lithuania (valid edition).

XIII.LIABILITY

48. The Company has the right to check how the Supplier complies with the Requirements, including, but not limited to, checking the compliance of the work tools and assets used for the implementation of the Project with the Requirements without prior notice.
49. The Supplier, in violation of the Requirements, shall, upon the request of the Company, pay a fine of EUR 1,000 and compensate for all direct losses incurred as a result, to the extent that they are not covered by the paid fine. This fine is considered a minimum loss of the Company and does not need to be proven.