

Minimum information security requirements for design and installation

1. General provisions

- 1.1. This document defines information security requirements and operational principles (the “**Requirements**”) applicable to a supplier or a group of suppliers, where a supplier is composed of several entities operating under the basis of a joint arrangement, providing services to the Buyer (the “**Service Provider**”), its employees, as well as the subcontractors engaged by it and their employees (“**Employees of the Service Provider**”, “**Employees**”) in the process of the design and/or preparation and/or implementation of projects (the “**Project**”) related to information and communication technology (the “**ICT**”) and operating technology (the “**OT**”) devices and information systems of the Buyer and/or provided by the Buyer, including, but not limited to: solar power plant and electric energy storage converters, data collection, processing and transmission devices, relay protection terminals and other automation, control and monitoring devices, control panels (HMI) solutions, microprocessor-based, programmable and special purpose controllers, information systems and software, data transmission and time synchronisation devices, etc. (the “**Equipment**”).
- 1.2. In the course of the provision of the services to EPSO-G UAB, LITGRID AB, Amber Grid AB and Energy Cells, UAB, it is required to comply with information security requirements applicable to cyber security entities under the Description of Cyber Security Requirements as approved by the resolution (updated version) of the Government of the Republic of Lithuania.
- 1.3. In all stages of the Project implementation, adherence to the following security principles must be ensured:
 - 1.3.1. Minimum rights. In managing access to the Buyer’s information and to the Equipment, the implementation of the principle “necessary for work” and “minimum access rights” must be ensured, i.e. the requirement means that access may be granted only to approved persons and only to a minimum level necessary to perform specific job and other functions related to the Buyer.
 - 1.3.2. Defence in depth. Layered rather than separate security measures are employed to mitigate security threats.
 - 1.3.3. Information and cyber security decisions must be based on the risk assessment and must be adopted with the participation of the Buyer, i.e. during the provision of services, the Service Provider must submit detailed information of and agree with the Buyer specific measures and solutions which will be used in implementing the Requirements and managing the identified risks.
- 1.4. The sufficiently new Equipment, including its operating system and software, must be foreseen and installed during the project ensuring that it will be possible to receive or acquire support services from the producer of the Equipment for at least five years from its installation.
- 1.5. If security recommendations have been issued by the producer of the Equipment being installed, they must be implemented after coordination with the Buyer. Before the start of operation, upon the Buyer’s request, evidence of the implementation of the agreed security recommendations of the producer must be provided.
- 1.6. The Service Provider must ensure that the Equipment would not be used if its producers and/or suppliers and/or control systems, which use software and/or cloud services, are from the countries which according to the National Security Strategy pose threat to national security of the Republic of Lithuania and to ensuring national security interests.

2. Management of vulnerabilities

- 2.1. The Service Provider must identify the Equipment’s vulnerability, i.e. the Equipment’s security gaps or weaknesses (the “**Vulnerability**”) in an earlier stage of the Project as possible.
- 2.2. When the Service Provider becomes aware of the Vulnerability, it shall immediately, but not later than within 72 hours, provide detailed information to the Buyer about the Vulnerability.
- 2.3. The producer’s latest security patches and latest offered software versions must be installed in the operating system, firmware, software of the Equipment before the start of operation, except for the following cases:
 - 2.3.1. the producer’s latest security patches and latest offered software versions must be installed in the operating system, firmware, software of a remote terminal unit (RTU), a time synchronisation device, an emergency shutdown (ESD) system before the start of complex and/or integration tests;

2.3.2. the producer's latest security patches and latest offered software versions must be installed in the operating system, firmware, software of relay protection and automation (RPA) devices, RTUs and general purpose controllers (GPC) before the start of factory tests (conducted at the manufacturing facility of the Equipment), but not earlier than 12 months before the start of operation of RPA devices, RTUs and GPCs.

3. Protection against malicious code

- 3.1. The Supplier must ensure that network and information systems, workstations and servers, devices used for ensuring services provided to the Buyer that are managed by the Employees are properly protected from physical security and cyber incidents by applying information security measures proportionate to the risk posed, including, but not limited to, the following measures:
 - 3.1.1. In accordance with the security recommendations, the Equipment, which contains a respective functionality, must have configured local firewalls or other respective solutions to block all unnecessary inbound / outbound traffic and excessive functions.
 - 3.1.2. The antivirus software approved by the Buyer must be installed in all Equipment that runs on the Windows operating system, except for the cases when there is no possibility to do so due to technical constraints (in the latter case the Service Provider must notify this fact to the Buyer).
 - 3.1.3. The antivirus software must be configured to:
 - 3.1.3.1. start and activate during the system start-up;
 - 3.1.3.2. check its integrity;
 - 3.1.3.3. perform real-time monitoring;
 - 3.1.3.4. operate in such a way that it cannot be switched off or stopped by the user;
 - 3.1.3.5. scan all files to be open before opening and running them;
 - 3.1.3.6. perform a full scan at least once a month;
 - 3.1.3.7. when an infected file is found, the user must be informed with a sound and visual message and the file must be cleaned up automatically, if the file cleanup is not possible, access to the infected file must be blocked.
 - 3.1.4. Antivirus malicious code databases must be updated on a regular basis:
 - 3.1.4.1. at least once an hour in firewalls, in antivirus servers;
 - 3.1.4.2. at least once in four hours in clients (e.g. in computer workstations).
 - 3.1.5. Standard users who are not granted administrator rights are not allowed to install software or change the configuration.
- 3.2. Before putting the Equipment into operation, non-essential system services, users, network ports, software unnecessary for performance of specified tasks must be removed or disabled in all its components.
- 3.3. The Equipment must be designed and configured in accordance with best security practices set forth in the CIS Security Benchmarks, Windows Security Baselines.
- 3.4. The Equipment's integration into the Buyer's network or integration with other systems of the Buyer must not require reducing a security level in the existing systems by deviating from best security practices.

4. Identification and access verification

- 4.1. Access to the Equipment (for example, a local using a control panel (HMI), a local using communication/diagnostic ports or a remote using a communication medium) must be protected by an identifier and a password that meet the requirements set by the Buyer (requirements are provided during the Project implementation).
- 4.2. Access security must be ensured in the Equipment by applying the role based access control, i.e. 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.
- 4.3. Network access to the Equipment must be granted only to approved (authorised) users and devices. Users may only have access 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.

- 4.4. Standard identifiers and passwords for the Equipment accounts must be changed to identifiers and passwords that meet the requirements set by the Buyer (requirements are provided during the Project implementation) before the start of their operation.
- 4.5. The management of the IT Equipment user accounts must be implemented using the centralised management system of the Buyer's accounts, rights and resources (the active directory).
- 4.6. A two-factor authentication mechanism approved by the Buyer must be used in the Equipment which is freely accessible from the Internet without any additional restrictions in order to authenticate users and administrators.
- 4.7. The Service Provider must submit to the Buyer the list of all created technical/system accounts with the assigned employees responsible for their security, i.e. system administrators.
- 4.8. All access methods (including a remote), tools and ports must be documented and agreed with the Buyer. Any unauthorised or undocumented access is prohibited.
- 4.9. The Buyer's IT systems must ensure that:
 - 4.9.1. before access to the system a warning is displayed regarding its unauthorised use;
 - 4.9.2. access to the source code of the systems' software is restricted according to the "necessary for work" principle.

5. Data transmission network

- 5.1. The data transmission network shall be designed, installed and administered in accordance with ISO/IEC 27033 "Information technology. Security techniques. Network security" standard recommendations.
- 5.2. A centralised authentication system must be used for administration of network devices.
- 5.3. Encrypted protocols must be used for administration of network devices.
- 5.4. All data transmitted via public networks must be securely encrypted (including, but not limited to, SSL, AES-CCMP).
- 5.5. All network device control ports which are not required for operations must be removed or disabled.
- 5.6. Network device ports and data network physical connections which are not used must be deactivated/disconnected.
- 5.7. Wireless network access must not be used in the OT Equipment and if such a need arises, it must be approved by the Buyer and implemented in a manner that complies with technical cyber security requirements established by the legal acts of the Republic of Lithuania.

6. Transmission of information

- 6.1. The Equipment's configuration files, backup copies, identifiers, passwords, instructions and other information required for the functionality restoration or agreed to during the Project must be transmitted to the Buyer in a secure manner before the start of operation.

7. Registration of events

- 7.1. The Equipment, in which it is technically possible, must log and store for a period of at least two weeks information on security and other significant events (during the design the Buyer will provide detailed requirements depending on the type of the Equipment).
- 7.2. It must be ensured that sufficient space is locally reserved for events to be logged.
- 7.3. The Equipment must be configured to send event logs to the Buyer's central log server.
- 7.4. Before putting the Equipment into operation, the table below must be filled in and emailed to the responsible persons of the Buyer who will verify whether event logs are received from the Equipment.

No.	Region	Object	Device type	Model	IP address	Syslog enabled (Yes/No)	dispatch Comment

Table 1. Event log testing form

8. Security testing

- 8.1. Before the start of operation of information systems, the Service Provider must perform security testing in order to determine the system's compliance with the Requirements and to eliminate the system's technical vulnerabilities. Upon a separate demand of the Buyer, the Service provider shall submit documents supporting the test results. The testing shall include the assessment (but not be limited to) of compliance:
- 8.1.1. OWASP 10 most common technical vulnerabilities in online systems;
 - 8.1.2. CWE/SANS 25 most common software errors.

9. Third-party components

- 9.1. Upon the Buyer's demand, the Service Provider must indicate all third-party components, libraries, and schemes used in the Equipment, irrespective of whether it is a commercial, free, open source, or closed source software.
- 9.2. The Service Provider shall take appropriate measures to ensure that a third-party software used in the Equipment complies with the security requirements set for the system and is properly licensed.
- 9.3. The Service Provider undertakes to provide the Equipment that does not contain any hidden, security-compromising features, including malicious software, viruses, "worms", "time mines", unauthorised access or features (Trojans, backdoors, easter eggs).

10. Security roles

- 10.1. To ensure security the Service Provider will delegate the Employee having cyber security competencies who will review the results of the Project before submitting them to the Buyer and will confirm compliance with the security requirements.
- 10.2. The Employees participating in the Project must be familiar with the Requirements.
- 10.3. The knowledge of the Employees must be sufficient to perform the job duties. The Service Provider must be able to prove the qualification of the Employees, e.g. by providing diplomas, licenses, certificate of the completed training. The Service Provider must assess the level of this knowledge and ensure that the knowledge of the Employees would be periodically updated.
- 10.4. The Buyer may demand that the Employees of the Service Provider prior to being granted access to the Equipment complete the Buyer's electronic information security training course related to ensuring compliance with these Requirements and pass the knowledge test (the total duration is around one hour). The knowledge test may be repeated until it is passed by the Employee. Access may not be granted to those Employees who failed the knowledge test. The knowledge test shall be repeated at least once in three years.

11. Securing compliance

- 11.1. The Buyer shall have the right to verify the Service Provider's compliance with the Requirements at any time during the validity term of the contract, including, but not limited to, verification of compliance with the Requirements of the work equipment used by the Service Provider to access the Buyer's Equipment without a prior notice, verification of the software

code created for the Buyer.

- 11.2. Upon the submission of an official request by the Buyer, once a year and/or upon the occurrence of an information security or cyber incident, in order to confirm that the Service Provider complies with the Requirements, the Service Provider must grant the Buyer or a third party selected by the Buyer acting under the authorisation of the Buyer a permission to carry out the assessment, audit, inspection or review of all control measures applied in the environment of the Service Provider related to the processing of the Buyer's data and/or the provision of services to the Buyer. In performing such assessment, the Service Provider shall fully cooperate, i.e. shall make a possibility to familiarise with the responsible Employees, documents, infrastructure and software which is directly used in the provision of services. The Service Provider shall submit necessary information not later than within five working days from the date of the receipt of the request. The Buyer shall not be obliged to cover any costs of the Service Provider which are incurred by the Service Provider due to cooperation during the audit or due to elimination of identified defects.
- 11.3. If non-compliance with the Requirements or defects are identified, the Service Provider is notified of this and must eliminate them within a reasonable time specified by the Buyer. If the Service Provider is late in correcting non-compliance or defects, the Buyer shall charge the Supplier a default interest of 0.02 (two hundredths) per cent of the value of the contract, excluding VAT, for each day of the delay from the date following the due date until the fulfilment of the obligation.
- 11.4. If the Service Provider repeatedly breaches the Requirements (i.e. within a period of 12 months after a written notice) or if the breach of the Requirements causes a significant risk to the Buyer's activities, it shall be obliged, upon the Buyer's demand, to pay a fine of EUR 1,000, excluding VAT, for each case of identification of a breach and to compensate all direct losses incurred by the Buyer as a result of such a breach, to the extent that they are not covered by the fine paid. This fine shall be deemed minimal damages of the Buyer not subject to prove. If non-essential breaches committed for the first time are identified, the Buyer has the right to give a warning and to establish a deadline for the elimination of breaches.
- 11.5. The Buyer, having assessed the risk posed by the identified defects, may unilaterally suspend the Service Provider's access to the Equipment and/or to the Buyer's information until the defects are eliminated or other measures are applied to manage risks arising from the defects. Delay in the performance of works due to suspension of access shall be considered a circumstance under the Service Provider's control, therefore a default interest provided for in the contract is applied for it.
- 11.6. The payment of the fine and/or default interest does not release the Service Provider from the obligation to comply with the Requirements, to eliminate the identified breaches or defects and to properly fulfil the contractual obligations.