

Minimum information security requirements for the provision of services

1. General provisions

- 1.1. This documents 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”) who operate in 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. All duties stipulated in mandatory rules despite not being discussed in these Requirements shall be binding on the Service Provider.
- 1.4. Any provision of the Requirements may be amended by the decision of the Buyer only to the extent necessary due to changes to legal acts or mandatory instructions of competent authorities. Such changes shall be applied to the extent that they do not contradict regulatory legislation on public procurements and do not change the essential terms and conditions of the contract. The Buyer shall inform the Service Provider about any changes in the provisions of the Requirements no later than 15 days prior to their entry into force, except for the cases when legal acts or decisions of the competent authorities provide for a different time limit for entry into force.
- 1.5. The Service Provider’s actions performed in accessing and having accessed the Equipment may be monitored and recorded for the purpose of prevention of illegal disclosure, corruption and other illegal activities, as well as control of information and cyber security and control of the Requirements, as well as control of the service provision. Such information shall be stored for three years. Information on the processing of personal data by the Buyer shall be publicly available in the Privacy Statement provided on the official website of the Buyer.
- 1.6. The Service Provider must ensure that the Employees who have access to the Equipment or may be related to the granting of access or to the use of the Equipment are made aware of the Requirements prior to granting them access to the Equipment and that they comply with the Requirements.
- 1.7. The Service Provider must ensure and control that the software and hardware used do not damage, unlawfully modify or otherwise disrupt the Equipment, that the Buyer’s information, including confidential Information, is not disclosed without the Buyer’s consent, or other damage is not caused to the Buyer and (or) other persons.
- 1.8. IT and information security knowledge of the Employees of the Service Provider 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.
- 1.9. 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.

2. Communication of incidents

- 2.1. According to ISO/IEC 27001 or other equivalent standard on an information security management system, the Service

Provider shall have prepared and approved information security or cyber incident management procedures that comprise detection, analysis, localisation of information security incidents, preservation of evidence, removal of incident consequences and other important steps.

- 2.2. The Service Provider must immediately, but not later than within 24 hours from the moment it became known to it, notify the Buyer of any noticed or suspected information security or cyber incident, event or non-compliance of the Requirements that may affect or has affected the Buyer's data, information resources, the Equipment or provision of services (even if the fact of an incident has not yet been confirmed). An information security incident shall include the following events, but not limited to: detection of malicious software (viruses, etc.) in the Equipment or the Service Provider's devices; the fact of a cyber attack, hacking or likelihood that they have occurred; identification of vulnerabilities in the Equipment, systems or processes; the loss or theft of the Equipment or devices containing Buyer's information; unauthorised disclosure or leakage of the Buyer's data; the loss or compromise of login details to the Equipment; unauthorised or suspected unauthorised access to the Buyer's information resources.
- 2.3. The Service Provider must immediately take reasonable technical and organisational measures to manage the incident and/or to mitigate possible consequences (e.g. isolate affected systems in their infrastructure, change or block login details, restrict access, etc.).
- 2.4. No later than within 72 hours after becoming aware of the information security or cyber incident, the Service Provider must provide to the Buyer detailed information indicating the following: nature, cause and scope of the incident; potential or actual impact on the Buyer's data, systems, services, or activities; applied and planned incident management measures comprising identification, localisation, removal, restoration of services and indicators established during the management of the information security incident.
- 2.5. The Service Provider, at the request of the Buyer, must also submit interim information security or cyber incident reports. All submitted information must be accurate, reliable and upon the Buyer's demand, must be transmitted using encryption or other secure communications measures.

3. Ensuring security

- 3.1. The Service Provider 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. use of the producer supported software and hardware with installed all patches released by the producer;
 - 3.1.2. installation and use of antivirus software or other malicious software detection and cyber security safeguarding measures which update hacking indicators/traces at least every 24 hours after the release of the producer's updates;
 - 3.1.3. separation of user and device administrator accounts;
 - 3.1.4. application of passwords that meet the requirements specified in Chapter 6;
 - 3.1.5. use of automatic locking of the user account which is activated no later than after 15 minutes of inactivity;
 - 3.1.6. activation and use of local firewalls which control inbound and outbound traffic; as well as blocking or disabling of unsafe remote access unnecessary for the performance of works, file sharing services and ports (e.g. Telnet, FTP, VNC, SNMP, inbound SMB traffic);
 - 3.1.7. encryption of internal and, if used, external data media (e.g. BitLocker);
 - 3.1.8. search and assessment of vulnerabilities using technical measures at least once a month and after their identification, ensuring management of risks posed by them;
 - 3.1.9. use of measures that prohibit the use of unapproved devices for work;
 - 3.1.10. installation of email filtering tools: establishment of SPF, DKIM, DMARC rules, blocking spam emails, filtering of attachments by file types (e.g. it is not allowed to forward executable files by email);
 - 3.1.11. use of multi-factor authentication solutions for authentication to services accessed by the service provider via the Internet (e.g. VPN, email);
 - 3.1.12. domain controllers and the active directory must be administered from the administrator network segment which is separated from the common service user segment;
 - 3.1.13. where technically possible, control performed of the execution and running of an unauthorised software and software

code from non-typical locations (e.g. temporary files folder) (e.g. using Windows Defender Application Control and/or Applocker in Windows environments);

- 3.1.14. network and information systems, where technically possible, log for a period of at least 2 weeks user, administrator, software, privileged process and other relevant events which are aggregated and analysed by dedicated cyber security solutions and tools (e.g. using security information and event management solutions (SIEM, EDR/XDR));
- 3.1.15. periodic back-up of network and information systems, servers and data necessary for the provision of the service and tests of their restoration;
- 3.1.16. The premises of the system servers intended for the provision of services and the premises in which backup copies of data are stored must be protected from unauthorised access by persons with the use of physical or electronic security measures, and access to these premises must be controlled.
- 3.2. Remote access to the Equipment, information systems or information resources shall not be carried out from countries or territories that are considered to pose an increased threat to national or cyber security in accordance with effective legislation, decisions of competent authorities or internal procedures of the Buyer, unless such access is agreed in advance in writing with the Buyer and additional security measures established by the Buyer are applied.
- 3.3. The Service Provider must ensure that measures used to service, access the Equipment, to provide services are safe, reliable and properly licensed. It is prohibited to use measures originating, produced or supplied from the countries that may pose a threat to national security, as defined in Article 37(9) and Article 47(9) of the Law on Public Procurement of the Republic of Lithuania.
- 3.4. The Buyer has the right to block, without a prior notice, the Service Provider's access and devices, including network resources, if they are/were unsafe or do not comply with the set Requirements, as well as if the Service Provider's behaviour in the Buyer's infrastructure raises suspicions or may cause threats to the Equipment or information of the Buyer and/or provided by the Buyer (e.g. DDoS attacks, spam messages, etc.).

4. Identification measures

- 4.1. An account which grants access to the Equipment shall be provided personally and only to persons about whom the Buyer was notified by the Service Provider in advance.
- 4.2. The Service Provider assumes the obligation to ensure that the Employees would use the provided login details only for their direct purpose, maintain their secrecy and do not disclose them to third parties.

5. Requirements for working with the Equipment

- 5.1. In the course of the provision of services related to the Equipment, the Service Provider shall be fully responsible for the compliance with the Requirements and must ensure protection of confidential information. If the Service Provider is unable to ensure this due to lack of information or other reasons, it must immediately suspend the provision of services and shall notify this fact to the Buyer in writing immediately, but not later than within 24 hours.
- 5.2. The provision of services shall be permitted only to the extent and only in such Equipment that are specified in or required under the service contract, in the submitted order or the Buyer's need expressed in other form. Any non-essential actions that are not in line with the ordinary practice of the provision of such services shall be prohibited.
- 5.3. When working with the Buyer's Equipment it shall be prohibited to:
 - 5.3.1. arbitrarily transfer the Equipment or the right to use it to other persons;
 - 5.3.2. remove or otherwise relocate the Equipment outside the Buyer's physical or infrastructure area by failing to agree with the Buyer's personnel responsible for the Equipment;
 - 5.3.3. disassemble, repair the Equipment or change its kitting and configuration, unless this is an expressly specified part of the provision of services or agreed with the Buyer;
 - 5.3.4. change the network settings that are provided (e.g. IP address, names of the Equipment, connection settings, etc.), if it is not necessary for the provision of services specified in the service contract;
 - 5.3.5. connect to the Buyer's Equipment data transmission network devices that are not agreed with the Buyer (e.g. 4G/5G modems, signal amplification or wireless access devices, etc.);

- 5.3.6. install and/or use software in the Equipment, unless this is agreed with the Buyer;
- 5.3.7. use the Equipment and network resources for activities not related to the performance of the service contract, as well as for the dissemination of offensive information, information promoting immoral behaviour or other illegal information. The Service Provider shall be responsible for the content of information supplied to the Buyer's networks;
- 5.3.8. conduct activities which violate legal acts of the Republic of Lithuania and international legislation;
- 5.3.9. block, disable or otherwise disrupt the operation of antivirus, firewall or other security measures on the Equipment, as well as arbitrarily change their configuration and settings;
- 5.3.10. use any measures, equipment and services (e.g. proxy, VPN, SSH tunnelling, DNS tunnelling, etc.) in order to bypass security measures used by the Buyer, access the blocked internet resources and/or services, hide the actions being performed or already performed, except for the cases when it is necessary to perform the functions specified in the service contract and has been agreed in advance with the Buyer;
- 5.3.11. scan the Equipment or the network for the purpose of detecting vulnerabilities, except for the cases when such actions are necessary to perform the functions specified in the service contract and are agreed in advance in writing with the Buyer;
- 5.3.12. browse the Internet using the Equipment, except for the guest's wireless access and other cases where such an opportunity is provided by the Buyer;
- 5.3.13. use without authorisation measures other than you own, make efforts to obtain information (e.g. to work under a name and password personally provided to another user, to search and view, to copy or use information and data, to access the Equipment which is not related to the provision of the service);
- 5.3.14. use measures that may complicate or disrupt the operation of the Buyer's Equipment (e.g., malicious software, network or system scanning, blocking, jamming measures, etc.);

6. Security requirements for passwords

- 6.1. Password security requirements shall be applicable to the Equipment, as well as to the Service Provider's devices which are intended to service the Equipment or in which the Buyer's information is stored.
- 6.2. Each Employee shall be personally provided with, if there are no technical constraints, a personal login and password to access the Equipment, which must be changed during the first login.
- 6.3. The Employees of the Service Provider shall safeguard logins, passwords and other authentication data provided to them, shall not transfer them to other persons, including to other employees of the Service Provider as well. The Employees must not use login details issued to other persons, i.e. personal accounts must not be used for work of several persons, except for service accounts which are used only in accordance with the procedure established by the Buyer.
- 6.4. The Service Provider shall be directly responsible for actions of all Employees that caused harm to the Equipment due to a login and for losses caused to the Buyer.
- 6.5. In creating, using and managing login details (including temporary and permanent passwords, technical and other authentication data), the Service Provider must comply with the following requirements:
 - 6.5.1. it is prohibited to create passwords on the basis of words provided in the Lithuanian or English language dictionary, as well as to use easily predictable sequences (e.g. qwerty, ABC123, etc.) or to use personal information (such as a birth date, names of family members, etc.);
 - 6.5.2. user and administrator passwords must consist of at least 12 and 15 characters respectively and include uppercase, lowercase letters, numbers and special characters (where technically possible);
 - 6.5.3. passwords must be changed at least once every six months. When changing the password, it is prohibited to re-use recent previous eight passwords;
 - 6.5.4. password complexity and change requirements for the OT equipment shall be established by the equipment maintenance personnel of the Buyer. If necessary, the equipment maintenance personnel of the Buyer shall familiarise the Service Provider with the requirements set for the OT passwords.
- 6.6. in all cases, it is mandatory to change production (default) login details and/or passwords before starting to use the Equipment or granting access to it, except for the cases where it is technically impossible and such risk has been assessed and accepted in accordance with the procedure established by the Buyer;
- 6.7. If passwords are required to be stored, they must be stored in dedicated encrypted password vaults (e.g. keepass). It is

forbidden to store or (if needed) transmit login passwords in an unencrypted form, written as a clear text (e.g. on paper or IT devices, in text messages, emails, etc.). Only in cases when passwords for access to Information Resources are granted (or changed), they can be given as a clear text, however in all cases this must be carried out in a secure manner:

- 6.7.1. a temporary password is created which needs to be changed during the first login;
- 6.7.2. login details are given in a secure manner, i.e. the person's identity is verified (e.g. by making a phone call) and a login and temporary password are given by different means (e.g. a login is sent by email, while a password is given directly or by phone).
- 6.8. It is prohibited to use login details and passwords used to access the Equipment anywhere else (e.g. in online systems, personal systems or devices, devices of other clients, etc.).
- 6.9. When due to technical or organizational constraints it is necessary to apply password complexity exceptions, the Buyer's approval must be obtained and additional measures must be implemented to mitigate information security risks arising from the exception.

7. Requirements for the granting of rights

- 7.1. The Service Provider must immediately, but not later than within 24 hours, inform about changes related to its Employees and other changes in order to ensure that access to the Equipment is removed and/or the provided Equipment is returned not later than on the last day of the validity of the contract with these individuals.
- 7.2. Prior to the start of the provision of services, the Service Provider shall have implemented a formal procedure for granting and removing access rights and shall apply it in managing access to the Equipment, and upon the Buyer's demand, shall be able to provide evidence of this.
- 7.3. A formal procedure for the Service Provider's access control shall include and ensure compliance with the following requirements:
 - 7.3.1. access rights of the Employees to all information resources must be removed not later than on the last day of the contract validity or of the provision of services for which access was required, as well as immediately after the termination of the Employee's employment for the Service Provider's benefit, discontinuance of the participation in the service provision or when access is no longer required for the performance of his/her functions;
 - 7.3.2. access rights to the Equipment would be granted to the Employees only after the fulfilment of all the requirements specified below:
 - 7.3.2.1. on the basis of a signed contract, for a time period not longer than required and to the minimum extent required for the performance of specific actions;
 - 7.3.2.2. after a confidentiality obligation is signed that complies with the terms of the confidentiality agreement with the Buyer, unless it is specified in the above-mentioned contract;
 - 7.3.2.3. after obligations are assumed to fulfil the requirements that meets these Requirements.

8. Requirements for remote access

- 8.1. Only secure access methods and means provided by the Buyer may be used for remote access. Arbitrary remote access to the Equipment is strictly prohibited and is possible only if the Buyer grants the right for such access. Remote access shall be granted strictly in cases when it is necessary for the performance of direct duties or is stipulated in the service contract.
- 8.2. The use of remote access for purposes other than job duties is strictly prohibited.
- 8.3. Remote access to the Buyer's network resources and to the Equipment via public networks (Internet) must be realised only using VPN or equivalent measures approved by the Buyer. Remote access is implemented on the principle of at least two-factor authentication, therefore, in order to additionally verify the identity of the person requesting access, it shall be mandatory to use an authentication measure which is personally assigned to a specific Employee (e.g. the mobile phone number, authentication application, hardware security key).
- 8.4. Employees shall be responsible for ensuring that during access to the Equipment other persons do not access the Buyer's information, network and the Equipment (e.g. it is mandatory to disconnect from the Buyer's network, lock the computer, etc. when leaving the workplace).

8.5. Remote access shall be granted to the Service Provider under the following conditions:

- 8.5.1. after the submission of a form for ordering remote access to the Buyer's resources signed by the person authorised by the Service Provider;
- 8.5.2. after the completion of the training indicated by the Buyer and successful passing of the test by the persons for whom access is requested;
- 8.5.3. after the confirmation of a remote access order by the Buyer's authorised representatives and provision of login details;
- 8.5.4. for a time period not longer than required for the provision of services, but not longer than one year upon the expiry of which the procedure is repeated.

9. Management of technical vulnerabilities

- 9.1. If the Service Provider provides a service relating to information systems, services relating to the design, development and maintenance of the Equipment, it shall be responsible for eliminating technical security vulnerabilities (security gaps) and installing security patches or applying other measures to manage the risk posed by vulnerability.
- 9.2. Before installing security patches on the Equipment, all necessary precautionary measures must be taken to avoid disrupting the operation of the Equipment, including but not limited to: patches must be tested, installation must be agreed with the Buyer before fixing security vulnerabilities in the Equipment.
- 9.3. Unless other time limits are provided in the contract, including the technical specification of the services, critical and high-level vulnerabilities of the Equipment shall be eliminated and any security patches released by the producers shall be installed as soon as possible, but no later than:
 - 9.3.1. within 10 working days after the release on the Equipment accessible from the Internet (e.g. firewalls) as well as on the equipment that has a direct interface to the Internet (e.g. computer workstations);
 - 9.3.2. within 30 working days after the release on the Equipment accessible from the Intranet;
 - 9.3.3. within the time limits agreed with the Buyer on the OT Equipment.

10. Securing compliance

- 10.1. The Buyer shall have the right to verify the Service Provider's compliance with the Requirements at any time during the period of the validity 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.
- 10.2. 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.
- 10.3. 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 Service Provider 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.
- 10.4. 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, upon the Buyer's demand, pay a fine of EUR 1,000, excluding VAT, for each case of identification of a breach and shall 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.

- 10.5. 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.
- 10.6. 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.