

Minimum information security requirements for software development

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**”). The Requirements must be complied with in producing, developing, improving software, information systems under the Buyer’s order.
- 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. 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.

2. Security activities in the life cycle

- 2.1. The Service Provider, in consultation with the Buyer, must identify and document information and cyber security, and personal data protection risks arising for the product being produced. All security areas referred to in Clause 2.4 must be analysed during the risk assessment.
- 2.2. The Service Provider must design measures necessary for the implementation of information and cyber security and personal data protection requirements in order to manage the identified risks.
- 2.3. The Service Provider must apply a practice of developing secure software, systems during the entire period of the provision of services. Practices applied, their scope and level shall be coordinated with the Buyer taking into consideration the purpose, architecture and risks of the software being developed:
 - 2.3.1. WEB-based software and systems must comply with secure software development best practices specified in the Open Web Application Security Project (OWASP) methodology (e.g. OWASP Top 10, OWASP ASVS or equivalent).
 - 2.3.2. Other types of software, systems (non-WEB solutions, server components, microservices, libraries, integration or industrial solutions) must comply with technology-neutral secure software development practices based on recognised international standards or systems (e.g. OWASP SAMM, NIST Secure Software Development Framework (SP 800-218), ISO/IEC 27001 A.8.25 or equivalent).
- 2.4. The Service Provider shall perform the information and cyber security analysis and risk assessment of the system being programmed, as well as the testing that complies with system security requirements and software security best practices:
 - 2.4.1. CWE/SANS 25 most common programming errors (latest version);
 - 2.4.2. OWASP TOP 10 vulnerability assessment (latest version), for each of the following areas:
 - 2.4.2.1. Validation of data and coding;
 - 2.4.2.2. Authentication and session management;
 - 2.4.2.3. Access control;
 - 2.4.2.4. Error management;
 - 2.4.2.5. Registration;
 - 2.4.2.6. Interfaces with external systems;
 - 2.4.2.7. Cryptography;
 - 2.4.2.8. Accessibility;
 - 2.4.2.9. Secure configuration;
 - 2.4.2.10. Security of platforms, databases and infrastructure.

- 2.4.3. The Center for Internet Security, Inc. (CIS). According to recommendations available at <https://downloads.cisecurity.org/#/>.
- 2.5. The Service Provider must use only safe and supported components that do not have known security gaps and vulnerabilities. Software composition analysis (SCA) tools are required to be used.
- 2.6. In all cases, the Service Provider must transfer fully tested software after having satisfied itself that its installation will not disrupt the operation of the Buyer's systems and that any installed changes will work as specified in the order and other documents.
- 2.7. The Service Provider must identify security weaknesses or vulnerabilities at the earliest possible stage of product development and/or its life cycle and eliminate them. After becoming aware of possible security gaps or weaknesses in the system, the Service Provider must provide this detailed information to the Buyer immediately, but no later than within 72 hours from the moment it became aware of this.
- 2.8. If critical or high-risk security gaps or vulnerabilities are identified, the software, information system cannot be put into operation until the identified vulnerabilities have been eliminated (removal must be confirmed during a repeated verification).
- 2.9. At the request of the Buyer, the Service Provider must provide a confirmation – a declaration that the system meets the requirements for secure software development, as well as the test results for each area specified in Clause 2.4.

3. Security roles

- 3.1. To ensure security the Service Provider must delegate the Employee having information and cyber security competencies who will be responsible for ensuring compliance with the Requirements during the development of the software or information system and assessment of compliance with the Requirements before submission to the Buyer.
- 3.2. The Service Provider's employees involved in the development of the software must be familiar with secure software development methods and the Supplier must be able to provide evidence of this (e.g. to provide certificates confirming the knowledge of the employees in accordance with the Buyer's requirements).

4. Environment and code management

- 4.1. Separate development, testing, and production environments ("Environments") must be used in designing, developing, and improving software, systems.
- 4.2. Environments must be logically and technically separated.
- 4.3. Real, confidential and personal data shall not be used in the testing environment, unless this is necessary and agreed in advance with the Buyer's representatives, by applying appropriate data anonymisation or pseudonymisation measures.
- 4.4. Environments must ensure that user actions are logged to determine who, when, and what actions have been taken. Logs must be protected from unauthorised modification.
- 4.5. Configuration and code management is applicable in all Environments, for this the Service Provider must use specialised configuration and/or code management systems that:
- 4.5.1. authenticate persons involved in the development, testing or support of the system;
- 4.5.2. record and ensure the traceability of their actions;
- 4.5.3. allow to identify who, when, and what changes have been made in a particular environment.
- 4.6. The Service Provider must use a software code version control system (e.g., Private Git, Fossil, Perforce Helix Core, Azure DevOps Server, or other) that ensures the tracking, auditing, and reproducibility of code changes.
- 4.7. Each change to the software code must be documented by indicating the changes made and the reasons for making them.
- 4.8. It shall be prohibited to make changes to software code or configurations in the production environment by omitting code versioning, configuration, or change management processes and systems.
- 4.9. The Service Provider must store at least the last three stable versions of the software and ensure the rollback possibility.
- 4.10. It is mandatory to use a branching strategy (e.g. Git Flow, trunk-based development) to ensure secure development and

testing.

- 4.11. Environment and software code repositories and the related infrastructure must be physically stored in the European Economic Area (EEA). The data must not be moved outside this territory.
- 4.12. The infrastructure for storing the Environments and software code must be protected from unauthorised access by applying at least two-factor authentication and role-based access rights management. Code repositories must be backed up and checked for recoverability.
- 4.13. The Service Provider must ensure that software code repositories do not store passwords, API keys or other sensitive data. Key management solutions must be used for this purpose.
- 4.14. All software code and configurations created by AI tools must be verified and approved by a human.

5. Third-party components

- 5.1. The Service Provider must indicate all third-party components, libraries, and schemes used in the system, irrespective of whether it is a commercial, free, open source, or closed source software.
- 5.2. The Service Provider shall take appropriate measures to ensure that a third-party software used in the system complies with the Requirements set for the system.
- 5.3. The Service Provider undertakes to provide the developed software that does not contain any hidden, security-compromising features, including malicious software, viruses, “worms”, “time mines”, unauthorised access or features (Trojans, backdoors, easter eggs).

6. Personal data protection

- 6.1. If personal data is processed in the information system under development, the Service Provider must ensure that the information system complies with the requirements of the effective personal data protection legislation, including those of General Data Protection Regulation (EU) 2016/679.
- 6.2. To ensure security of personal data, the following functionalities must be implemented in the information system:
 - 6.2.1. possibility to process personal data only for those users who have been granted relevant roles and access rights;
 - 6.2.2. possibility to automatically anonymise according to the established rules, where this does not contradict effective legal acts, all or specific personal data of a selected person or a group of persons by ensuring data integrity;
 - 6.2.3. possibility to automatically prepare an extract of personal data processed in the information system by person selected (an employee, a subcontractor or other data subject);
 - 6.2.4. possibility for the information system administrator to remove selected sensitive and/or confidential personal data, the collection of which is not mandatory, or which is not necessary for the operation of the information system;
 - 6.2.5. possibility to manage time limits for the storage of personal data and, after the expiry of the time limit laid down in legislation or set by the Buyer, to automatically delete personal data.
- 6.3. A detailed list of personal data protection and security requirements, including technical and organisational measures, shall be specified at the analysis and/or design stage, taking into consideration the functionality of the solution being developed, the nature, scope and risks of personal data processed, and shall be coordinated with the Buyer.

7. Securing compliance

- 7.1. 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.
- 7.2. 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.

- 7.3. 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.
- 7.4. If the Service Provide 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.
- 7.5. The Buyer, having assessed the risk posed by the identified defects, may unilaterally suspend the Service Provider's access to the infrastructure and/or information of the Buyer 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.
- 7.6. 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.