Cybersecurity Rules

1. **Terms and abbreviations**
   1.1. **Information system** (hereinafter – IS) – an organised system intended for the management and electronic processing of information resources using technical resources.
   1.2. **Vulnerability**: a weakness or susceptibility to technical problems, or a flaw in information and communication technologies or their services, that can be exploited by cyber threats.
   1.3. **Cybersecurity incident** (hereinafter – cyber incident) — an event that compromises the availability, authenticity, integrity or confidentiality of processed data or services offered by or accessible through networks and information systems.
   1.4. **Cybersecurity** refers to the actions that must be taken to protect networks and information systems, their users and other individuals affected by cyber threats.
   1.5. **Cyber threats** are any possible circumstances, events, or actions that could damage, disrupt, or otherwise negatively affect networks and information systems, their users, and other individuals.
2. **Secure communication and distribution of responsibilities**
   2.1. During the contract period, the Customer shall ensure that data is transmitted securely and encrypted to the Contractor via the Customer's data transmission network. The technological solution shall be agreed by both parties.
   2.2. Any exchange of information that may affect the security of the service shall only be carried out with the authorised contact persons specified in this contract, using secure communication channels that ensure the confidentiality, integrity and availability of information:
      2.2.1. Encrypted email;
      2.2.2. A messaging solution (chat or instant messaging) specified by the Customer.
      2.2.3. A ticket management IS specified by the Customer.
   2.3. Software code, or parts thereof, and IS configuration information shall be delivered as agreed by the Parties, using one of the information exchange methods specified by the Customer, such as the Customer's SFTP (SSH File Transfer Protocol), Version control system or Ticket management IS.
   2.4. Before delivering the software code, the Contractor shall perform a code security check based on OWASP Secure Coding Practices or other comparable industry best practice principles.
   2.5. The Contractor shall ensure that operations in the Customer's IS are performed only to the extent necessary to fulfil the terms of the Contract.
3. **Access rights control and account management**
   3.1. During the Contract period, the Customer shall create user accounts in the Customer's IS for mutually agreed Contractor representatives for a specified period of time, but no longer than the service provision term specified in the Contract. This will give the Contractor access to the Customer's IS production, testing and/or development environment owned or controlled by the Customer.
   3.2. The Contractor shall implement the following cybersecurity control measures for user account management:
      3.2.1. Change the initial user password on the website https://parole.latvenergo.lv within 72 hours of receipt.
      3.2.2. Subsequent password changes in accordance with IS password change settings and security notifications.
      3.2.3. Secure storage and confidentiality of IS authentication data.

3.3. If an employee of the Contractor who has a User account leaves the Contractor's employment and/or ceases their relationship with the Contractor, the Contractor shall immediately notify the Customer.

4. Cybersecurity compliance

4.1. The Contractor shall ensure the implementation of technical and organisational measures in accordance with the National Cyber Security Law of the Republic of Latvia and related Cabinet of Ministers regulations. These measures its ownership, possession, or use shall include secure IT configuration, protection against malware, network security management, timely updates, vulnerability management and appropriate physical and environmental security measures. These controls shall be maintained throughout the entire period of service provision.

4.2. The Contractor undertakes to use and maintain additional cyber security protection software specified by the Customer during the term of the Contract, provided that the Customer requests its installation. The Customer shall bear the costs of the software.

4.3. The Contractor undertakes to provide the Customer with the opportunity to continuously monitor information transferred to the Contractor and compliance with cybersecurity measures. The Customer shall also have the right to verify compliance with applicable cybersecurity requirements regarding the processing, management and protection of information entrusted to the Contractor. To this end, the Customer has the right to conduct audits, either independently or through a third party, at the Contractor's premises and at any other location where Services are provided. The Customer must notify the Contractor in written form at least two (2) working days in advance.

4.4. The audit process includes, but is not limited to, checking relevant documentation, physical and technical security measures, and software and IT system configurations, as well as obtaining any information necessary to assess compliance with the contract and applicable cybersecurity requirements.

4.5. The Contractor is obliged to cooperate with the Customer during the audit process.

5. Vulnerability management

5.1. The Contractor shall ensure that the service provided does not pose any security risks defined in the current "OWASP Top 10", "OWASP Mobile Top 10" and "OWASP API Security Top 10" lists (www.owasp.org).

5.2. The Contractor shall eliminate any vulnerabilities registered in the CVE (Common Vulnerabilities and Exposures) database1 and assessed according to the CVSS v3.0 or a newer version[2] criteria at their own expense:

5.2.1. Critical impact vulnerabilities – within seven calendar days at the latest;

5.2.2. High-impact vulnerabilities – within 14 calendar days at the latest.

5.2.3. Medium and low-impact vulnerabilities: within 30 calendar days at the latest.

5.3. 5.3. The Contractor shall eliminate any vulnerabilities or security risks identified by the Customer at their own expense within 30 calendar days at the latest.

6. Security training and awareness

6.1. The Contractor shall ensure that all persons involved in providing the Service are familiar with, and comply with, the cybersecurity requirements set out in the Contract.

6.2. The Contractor shall provide regular training on best cybersecurity practices, cyber hygiene, the protection of confidential information and compliance with applicable legal and contractual cybersecurity requirements.

7. Cyber incident management

7.1. The Contractor shall notify the Customer immediately by email at palidzibas.dienests@latvenergo.lv or by phone on +371 67728888 of any cyber incident, including but not limited to security breaches, identified vulnerabilities, threats

[1] https://cve.mitre.org

[2] https://nvd.nist.gov/vuln-metrics/cvss

or other suspicious activities that may affect the security, confidentiality, integrity or availability of the Service.

7.2. In the case of a cyber incident, the Contractor shall provide the Customer with detailed information about the nature, extent and possible impact of the incident, as well as the immediate protective measures taken to mitigate its consequences.

7.3. The Contractor shall cooperate with the Customer in investigating cyber incidents by providing all necessary support, including access to relevant audit logs and personnel, to facilitate resolution in accordance with regulatory procedures.

7.4. The Contractor shall ensure that all audit records and security events relating to the cyber incident are securely stored for at least 18 months from the cyber incident or event date.