IT SECURITY RULES

1. During the Agreement period, the CUSTOMER shall ensure to the CONTRACTOR secure and encrypted data transmission within the data transmission network of the CUSTOMER, the Parties agreeing on the technological solution.
2. Information exchange which may affect the Service security shall be ensured only through mediation of contact persons specified in the Agreement, observing the type of information exchange, which ensures its confidentiality, integrity and availability:
   2.1. encrypted email;
   2.2. CUSTOMER's messaging solution;
   2.3. CUSTOMER's issue tracking system.
3. Software code or its part, and information system (hereinafter – "IS") configuration shall be supplied by the Contracting Parties agreeing on using any type of information exchange determined by the CUSTOMER – CUSTOMER's SFTP (SSH File Transfer Protocol), Version Control System or issue tracking system.
4. The CONTRACTOR shall be responsible for any action performed by their employees addressed towards security circumvention or damaging of CUSTOMER's IT systems.
5. The CONTRACTOR shall be responsible for ensuring, that actions in the CUSTOMER's IS are performed only in the amount necessary to ensure fulfilment of Agreement subject.
6. During the Agreement period, the CUSTOMER shall create User Accounts in the CUSTOMER's IS for mutually coordinated CONTRACTOR's representatives for a specified period of time, which does not exceed the term of provision of the Service specified in the Agreement, thus ensuring CONTRACTOR's access to IS production, testing and/or development environment being in possession or ownership of the CUSTOMER.
7. The CONTRACTOR shall be obliged to provide the following User Account protection measures:
   7.1. change of the initial User password on the website https://parole.latvenergo.lv not later than within 72 hours after receipt;
   7.2. secure storage and non-disclosure of the User authentication data.
8. If the CONTRACTOR's employee, whom the User Account is created for, terminates his/her employment relations and/or commitments with the CONTRACTOR, the CONTRACTOR shall immediately inform the CUSTOMER about this situation.
9. While applying technical or software means possessed by the CONTRACTOR, the CONTRACTOR shall assume responsibility for conformity of security of operating systems contained by these means, shall use updated anti-virus protection and firewall means as well as provide adequate physical security controls during provision of the Service.
10. The CONTRACTOR undertakes to use additional IT security protection software indicated by the CUSTOMER, and to ensure maintenance thereof during the Agreement period, if the CUSTOMER requests installation of such software. The CUSTOMER shall pay the costs of the software.
11. The CONTRACTOR undertakes to ensure to the CUSTOMER a possibility to permanently supervise compliance with IT security measures concerning information transferred to the CONTRACTOR. In this regard the CONTRACTOR undertakes to ensure to the CUSTOMER a possibility to inspect the CONTRACTOR's activities at its location or Service provision place in relation to provision of the Services, including to become acquainted with documents, applied technical and software means, and to request from the CONTRACTOR information related to provision of the Services, such inspection being implemented in presence of the CONTRACTOR's representative and at any time, if the CUSTOMER has informed the CONTRACTOR at least 2 (two) working days in advance.
12. The CONTRACTOR performs code review prior to the delivery of the software code or part of it.
13. All IT security vulnerabilities of software, which are among "OWASP Top 10" (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project) shall be eliminated as part of the Service. If the CUSTOMER detects any non-conformities, the CONTRACTOR shall eliminate them at its own expense within 30 (thirty) calendar days. If the identified vulnerabilities are registered in the CVE (Common Vulnerability and Exposures) database (https://cve.mitre.org) and evaluated by the criteria of CVSS v3.0 or later version (https://nvd.nist.gov/vuln-metrics/cvss), the CONTRACTOR shall eliminate them:
    13.1. Critical impact vulnerabilities – within 7 (seven) calendar days at the latest;
    13.2. High impact vulnerabilities – within 14 (fourteen) calendar days at the latest;
    13.3. Medium and low impact vulnerabilities – within 30 (thirty) calendar days at the latest.
14. The CONTRACTOR shall be obliged to acquaint own employees and/or representatives, who ensure provision of the Service, with contract annex - IT security rules.
15. If the CONTRACTOR has suspicions about any security incident or violation of IS security rules mentioned in the Agreement, the CONTRACTOR shall immediately inform the CUSTOMER's contact person or the CUSTOMER's Help Desk, phone: +371 67728888.