Approved by 09.09.2025
Decision of the Management Board of Latvenergo AS, No 181/44

Latvenergo Group Cybersecurity Policy

1. GOAL OF THE POLICY

1.1. The Cybersecurity Policy of Latvenergo Group (hereinafter – the Group) establishes common principles for the protection of Group resources against cyber risks.

1.2. The main objective of the Policy is to ensure the effective operation of cybersecurity governance, in order to:

1.2.1. Ensure compliance with European Union and national legal acts;

1.2.2. Organise economically justified protection of resources, based on the requirements of confidentiality, integrity and availability for information systems, essential services, and critical infrastructure;

1.2.3. Support business continuity planning, maintenance and testing processes.

2. DEFINITIONS

2.1. Near-miss cyber incident – an event which could have endangered processed data or the availability, authenticity, integrity, or confidentiality of services provided by or through network and information systems, but which was successfully averted or did not fully materialise.

2.2. Vulnerability – a weakness, susceptibility to technical issues, or deficiency in information and communication technologies or their services that may be exploited by a cyber threat. A vulnerability is regarded as a subtype of a cyber incident.

2.3. Cybersecurity incident (cyber incident) – an event that endangers processed data or the availability, authenticity, integrity or confidentiality of services provided by or accessible through network and information systems.

2.4. Cyber hygiene – a set of daily practices and habits aimed at reducing cyber threats, ensuring data protection and maintaining the availability, integrity and confidentiality of information and communication technology resources.

2.5. Cyber risk – the probability of loss or service disruption caused by a cyber incident, expressed as the combination of the impact of such loss or disruption and the likelihood of the incident occurring.

2.6. Cybersecurity – measures necessary to protect network and information systems, their users and other affected persons against cyber threats.

2.7. Cyber threat – any potential circumstance, event or action that may cause harm, disruption or otherwise adversely affect network and information systems, their users or other persons.

2.8. Cybersecurity safeguards (security controls) – technical or organisational measures determined within cyber risk management to reduce cyber risks to an acceptable level.

3. POLICY GUIDELINES AND PRINCIPLES

3.1. The Group and Latvenergo capital companies maintain and continuously improve a set of cybersecurity governance documents and measures, ensuring the achievement of the Policy's objectives and compliance with the National Cybersecurity Law.

3.2. The Policy is developed in accordance with recognised best practices in cybersecurity and considering prevailing cyber risks within the industry.

3.3. The cybersecurity governance system of the Group and Latvenergo capital companies is organised based on the principles of ISO/IEC 27002[1].
3.4. The principle of "need to know" – information shall be accessible only to those persons who require it for the performance of their duties.
3.5. Everything not permitted, is prohibited – if authorisation for action with specific information, an information system resource, or part thereof is not explicitly and clearly granted, such action is prohibited.
3.6. Clean desk and desktop policy – employees shall maintain a tidy and orderly working environment, ensuring particular care in processing restricted information.
3.7. Four eyes (harmonization) principle – decisions on conflicting activities (e.g. development and maintenance, maintenance and monitoring, resource requests) must be taken by at least two employees.
3.8. Cybersecurity as shared responsibility – each employee contributes to security on a daily basis, using authorised tools and solutions, responsibly handling publicly available information. Employee inaction may also pose risks to colleagues and to Group or Latvenergo capital company resources.
3.9. Lesser evil principle – when selecting protective measures, the option that minimises potential harm to Group resources shall be preferred (e.g. restricting or blocking access to certain websites to prevent exploitation).

4. CYBERSECURITY CONTROLS

4.1. Information and communication technology (ICT) resources and their components shall be identified, classified and assessed accordance with the National Cybersecurity Law and internal normative acts of the Group, applying information security classification methodologies.
4.2. Cyber risk assessments shall be carried out at least once a year, in accordance with internal normative acts.
4.3. All Group and Latvenergo capital company resources shall be subject to proportionate protection measures applicable to critical infrastructure operators and essential service providers.
4.4. During procurement, when acquiring components or ICT resources for critical infrastructure, both the service provider and the service itself shall be subject to cyber risk assessments before contract conclusion, to ensure that the provider’s overall cybersecurity level is not lower than that maintained within the Group or Latvenergo capital companies.
4.5. Contracts for ICT resources or services concluded with selected providers must ensure that the provider, its subcontractors and the resource manufacturer (where applicable) comply with the National Cybersecurity Law and Cabinet Regulation No. 397 "Minimum Cybersecurity Requirements".
4.6. The Group and Latvenergo capital companies shall establish and maintain cybersecurity requirement documents for information systems and their components, taking into account external regulations and industry standards.

5. CYBERSECURITY GOVERNANCE STRUCTURE

5.1. Cybersecurity management in the Group and in Latvenergo capital companies is carried out by the Cybersecurity Manager, who is appointed for a three-year term.
5.2. The Cybersecurity Manager has the following responsibilities:
5.2.1. Ensure the improvement of cybersecurity controls;

[1] ISO 27002:2024 Information security, cybersecurity and privacy protection. Information security controls.

5.2.2. Ensure security testing and, based on the results, organize the elimination of identified nonconformities;
5.2.3. Attend training on cybersecurity issues;
5.2.4. Provide employees with initial, regular, and extraordinary trainings on current cyber risks, cybersecurity, and other necessary topics;
5.2.5. At least once a year, or when circumstances change (new threats, cyber risk levels, cyber incidents), ensure the review of the content of initial, regular, and extraordinary trainings;
5.2.6. Communicate with the competent cyber incident prevention authority, other competent institutions, other entities, and service recipients in cases of detected cyber incidents;
5.2.7. Within the procurement and contracting process, assess cybersecurity requirements for solutions, projects, and information systems (IS), and ensure their compliance with both internal and external regulatory requirements.

5.3. The Cybersecurity Manager has the following rights:
5.3.1. Check the list of user accounts, their assigned access rights, and their activities in IS, including changes made by users to information resources and technical resource configurations;
5.3.2. Ensure the analysis of audit logs of user activities;
5.3.3. In the event of a cyber incident, justified suspicions of a cyber incident, or failed cybersecurity training, request the blocking of user accounts related to the cyber incident;
5.3.4. Test registered users knowledge of cyber hygiene and IS usage rules, and, if necessary, organize additional training to improve such knowledge;
5.3.5. Request IS audit logs from the IS maintainer if the IS or part of it is maintained as an outsourced service.

5.4. Representatives of the Group's IT and T division and of Latvenergo capital companies functions or structural units are assigned additional cybersecurity roles, which are reviewed every three years:
5.4.1. Responsible for ensuring the IS backup management process;
5.4.2. Responsible for ensuring the IS audit log management process;
5.4.3. Responsible for cyber risk management;
5.4.4. Responsible for the development, review, and updating of the ICT business continuity plan, as well as for implementing the measures included in the plan.

5.5. Representatives of the Group's and Latvenergo capital companies core business and support functions are assigned additional responsibilities for the administrative management of IS resources: IS owner, IS resource owner, IS key user.

5.6. The technical management of IS resources is carried out by designated employees of the Group's and Latvenergo capital companies IT and T division and IT function.

5.7. Categories of administrative responsibilities for IS management are determined in accordance with the procedures established in the Group company.

5.8. The IS owner is a designated employee of the relevant core business or support function of the Group or a Latvenergo capital company.

5.9. Duties and responsibilities of the IS owner:
5.9.1. Define IS development;
5.9.2. Assess significant cyber risks;
5.9.3. Ensure IS compliance with the Policy and regulatory requirements.

5.10. The IS resource owner is an employee designated by the IS owner.

5.11. Duties and responsibilities of the IS resource owner:
5.11.1. Approve functional change requests related to IS development;

5.11.2. Manage user access rights and update the access rights register;
5.11.3. Classify IS information resources;
5.11.4. Manage cyber risks;
5.11.5. Define IS resource SLA (Service Level Agreement) criteria;
5.11.6. Define IS requirements for core business or support functions.

5.12. The IS key user is an employee designated by the IS resource owner.

5.13. Duties and responsibilities of the IS key user:

5.13.1. Evaluate and analyse IS-related requests (including requests submitted via the BURA request management system, change requests, incidents, problems);
5.13.2. Perform acceptance testing;
5.13.3. Ensure data integrity checks;
5.13.4. Provide IS user (hereinafter – User) training and support;
5.13.5. Participate in cyber risk management.

5.14. A User of the Group or Latvenergo capital company is a person who has entered into an employment relationship with the Group or Latvenergo capital company.

5.15. Duties and responsibilities of the User:

5.15.1. Comply with the cybersecurity requirements established in the Policy and related regulations;
5.15.2. Follow the rules, guidelines, and procedures relating to the protection and proper use of IS and their components;
5.15.3. Ensure IS cybersecurity and act to protect themselves and Group resources in daily operations;
5.15.4. Request and, after successfully completing cybersecurity training, obtain access rights to work with the necessary IS resources;
5.15.5. Use IS resources according to the granted access rights;
5.15.6. Treat IS resources responsibly and maintain confidentiality;
5.15.7. Immediately report to Latvenergo AS Operational Management Center (helpdesk) in cases of suspected cybersecurity incidents, near misses, suspicions of incidents, or violations of the Policy or other cybersecurity documents, which may threaten the confidentiality, integrity, or availability of IS;
5.15.8. Attend the Group company's initial, annual, and extraordinary cybersecurity training sessions.

6. COOPERATION AND POLICY MONITORING

6.1. The IT and T Security Analysis function of Latvenergo AS coordinates the implementation of the Policy across the Group and its Latvenergo capital companies, in cooperation with the Cybersecurity Manager and other organisational units.

6.2. The Cybersecurity Manager liaises with competent state authorities as provided by law.

6.3. The Cybersecurity Manager is responsible for maintaining and controlling the Policy.

6.4. The Policy shall be updated taking into account changes in regulatory enactments, documented cyber security incidents, cybersecurity audits and cyberrisk assessments, but at least once every three years.

6.5. The use of and access to the IS resources of the Group and Latvenergo capital companies is controlled by the IT and T Security Analysis function of Latvenergo AS, organising the monitoring and analysis of cybersecurity events in order to determine the adequacy, compliance and usefulness of the cybersecurity measures used, identify cybersecurity breaches and develop recommendations for improving cybersecurity testing tools and cybersecurity procedures.

6.6. External compliance audits of cybersecurity governance in the Group and Latvenergo capital companies may only be conducted by auditors included in the list of Cybersecurity Auditors (in accordance with Article 44 of the National Cybersecurity Law), who shall report on the effectiveness of cybersecurity controls and the overall cybersecurity level. Such reports shall be classified as restricted access.