Translation of Liechtenstein Law

Disclaimer

English is not an official language of the Principality of Liechtenstein. This translation is provided for information purposes only and has no legal force. The contents of this website have been compiled with utmost care and to the best of knowledge. However, the supplier of this website cannot assume any liability for the currency, completeness or accuracy of any of the provided pages and contents.

English title:	Cyber Security Ordinance (CSV) of 14 January 2025
Original German title:	Cyber-Sicherheitsverordnung (CSV) vom 14. Januar 2025
Systematic number (LR-Nr.):	784.131
First publication date:	30 January 2025
First publication no. (LGBl-Nr.):	2025-163
Last change date:	
Last change publication nr. (LGBl-Nr.):	
Translation date:	1 February 2025

Liechtenstein Law Gazette

Year 2025 No. 163 published on 30 January 2025

Cyber Security Ordinance (CSV)

of 14 January 2025

By virtue of Art. 3 (2) a) no. 5, Art. 4 (7), Art. 6 (6), Art. 11 (3), Art. 15 (3), Art. 19 (3), Art. 20 (4) and Art. 25 of the Cyber Security Act (CSG) of 5 December 2024, Liechtenstein Legal Gazette (LGBI) 2025 no. 111, the Government decrees:

I. General provisions

Art. 1

Object and scope

1) In implementation of the Cyber Security Act this Ordinance establishes more specific regulations governing the measures for ensuring a high level of security of network and information systems, in particular:

a) the risk management measures to be implemented;

b) the reporting obligations pursuant to Art. 6 and 9 of the Cyber Security Act;

c) the requirements concerning qualified third parties as referred to in Art. 11 (2) of the Cyber Security Act;

d) the cooperation and exchange of information by the National Cyber Security Unit with other domestic authorities and agencies;

e) the implementation of control measures as referred to in Art. 19 of the Cyber Security Act.

2) It serves to transpose and/or implement the following EEA legislation:

a) Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union[1];

b) Regulation (EU) 2021/887 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres[2];

c) Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification[3].

3) The current version of the EEA legislation to which this Ordinance makes reference is to be found in the publication of the decisions of the EEA Joint Committee in the Liechtenstein Legal Gazette pursuant to Art. 3 k) of the Publications Act.

Art. 2

Designations

The terms used in this Ordinance to denote persons are to be understood as applying to all persons, irrespective of their gender, unless the personal terms explicitly refer to a specific gender.

1 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333 of 27.12.2022, p. 80)

2 Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202 of 8.6.2021, p. 1)

3 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151 of 7.6.2019, p. 15)

II. Risk management measures

Art. 3

Principle

1) Essential and important entities ensure a level of security for network and information systems appropriate to the risks posed and protect them from security incidents and cyber threats, by taking the technical, operational and organisational risk management measures in the domain of cybersecurity listed in the annex.

2) If an essential or important entity considers the taking of specific technical, operational and organisational risk management measures in the field of cybersecurity set out in the annex to be inappropriate, inapplicable or impracticable, the entity concerned shall record the reasons for this in a clear and comprehensible manner.

3) The provisions of Implementing Regulation (EU) 2024/2690[4] as regards technical and methodological requirements of risk management measures for DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery service providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms and trust service providers remain reserved.

4 Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers (OJ. L 2024/2690 of 18.10.2024)

III. Reporting obligations

Art. 4

Significant security incidents

1) When assessing whether to categorise a security incident as a significant incident pursuant to Art. 6 of the Cyber Security Act, essential and important entities shall consider the following cross-sectoral factors, at the very least:

a) the importance of the network and information systems concerned for the provision of the entity's services;

b) the direct financial loss caused or possible loss which may be caused by the security incident;

c) the extent of the impact on or the disruption of economic and social activities;

d) the possibility or occurrence of damage to the health of a natural person or their death;

e) the number of natural or legal persons affected by a security incident (users);

f) the geographical reach of the territory that might be affected by a security incident;

g) the duration of the security incident or, if applicable the duration of the non-availability of the service provided by the entity in question;

h) the vulnerabilities giving rise to the security incident.

2) Several security incidents, which when considered individually pursuant to (1) are not assessed to be significant security incidents, are considered together to be a significant security incident, if they occur at least twice within six months and have the same apparent cause.

Art. 5

Handling of notifications

1) Notifications of security incidents, cyber threats or near misses as referred to in Art. 6 or 9 of the Act are handled by the Computer Security Incident Response Team (CSIRT) established at the National Cyber Security Unit.

2) The CSIRT may communicate information concerning reported security incidents, cyber threats or near misses, such as, in particular, indicators of compromise, to external bodies, in order to:

a) establish whether systems have been compromised;

b) find out which data or systems have been affected by a compromise;

c) evaluate the severity of security incidents;

d) provide indicators of the attack vectors and tools used by attackers, so that threats can be reduced or eliminated;

e) identify weak points in systems;

f) develop targeted counter-measures, so that future attacks can be prevented.

IV. Organisation and implementation

A. Qualified third parties

Art. 6

Requirements

1) Qualified third parties who are engaged to perform duties on behalf of the National Cyber Security Unit or the CSIRT pursuant to Art. 11 (2) of the Cyber Security Act, in particular to carry out the control measures referred to in Art. 19 of the said Act, must:

a) be unconnected with the essential or important entities to be inspected; and

b) have the necessary skills to perform the tasks assigned to them.

2) At the request of the National Cyber Security Unit they must provide evidence of the relevant qualifications for the skills required pursuant to (1) b), by the production of the appropriate certificates if applicable.

3) The National Cyber Security Unit may require qualified third parties to take a security test, carried out by a qualified, independent agency and to communicate their results. The cost of the security test is born by the qualified third parties.

B. Cooperation and exchange of information with domestic authorities

Art. 7

Cooperation and exchange of information with the FMA

1) Insofar as required for the performance of its statutory duties the National Cyber Security Unit shall work with the Financial Market Authority (FMA) with a view to ensuring a high level of security of network and information systems and may exchange information for this purpose.

2) The information exchanged may include:

a) notifications concerning security incidents as well as ICT related incidents or evidence of cyber threats received by the FMA or the National Cyber Security Unit from the banking and financial market infrastructure sectors;

b) information communicated to the FMA or the National Cyber Security Unit in the course of the performance of their respective duties;

c) information concerning unusual incidents in cyber space.

3) The National Cyber Security Unit may request assistance from the FMA in the monitoring of risk management measures and compliance with the reporting obligations pursuant to Art. 4 and 6 of the Cyber Security Act. By virtue of its powers the FMA may conduct inspections or investigations itself or instruct specialists to conduct them.

Art. 8

Cooperation and exchange of information with the Office for Communications

1) The National Cyber Security Unit shall work with the Office for Communications with a view to ensuring a high level of security of network and information systems, particularly in the following areas:

a) relating to all entities in the "digital Infrastructure", "space" and "postal and courier services" sectors; and

b) in the specialised areas for which the Office for Communications is responsible.

2) The agencies may exchange information in the course of their cooperation pursuant to (1). The information exchanged may include:

a) notifications, communications for information received by the Office for Communications or the National Cyber Security Unit concerning security incidents, cyber threats or near misses in the said sectors;

b) information on unusual incidents in cyber space.

3) The National Cyber Security Unit and the Office for Communications shall notify one another within 24 hours of receipt of notifications concerning relevant security incidents in trust service providers.

4) The National Cyber Security Unit may request assistance from the Office for Communications in the monitoring of risk management measures and compliance with the reporting obligations pursuant to Art. 4 and 6 of the Cyber Security Act. By virtue of its powers the Office for Communications may conduct inspections or investigations itself or instruct specialists to conduct them.

Art. 9

Cooperation and exchange of information with the National Police

The National Cyber Security Unit shall work with the National Police with a view to ensuring a high level of security of network and information systems, particularly in the following:

a) exchange of information about unusual incidents in cyber space;

b) technical support, with available resources being shared if required and being mutually provided;

c) participation in exercises and training.

Art. 10

Cooperation and exchange of information with the Public Prosecution Service

The National Cyber Security Unit shall work with the Public Prosecution Service with a view to ensuring a high level of security of network and information systems, particularly regarding exchange of information about unusual incidents in cyber space.

Art. 11

Cooperation and exchange of information with the Financial Intelligence Unit (FIU)

1) The National Cyber Security Unit shall work with the Financial Intelligence Unit with a view to ensuring a high level of security of network and information systems, particularly in the following areas:

a) strategic risk analysis;

b) enforcement of international sanctions, as well as brokerage of and trade in war material, nuclear goods, radioactive waste, dual-use goods and particular military goods.

2) The National Cyber Security Unit and the Financial Intelligence Unit shall provide one another with the information and documents required for the purposes listed in (1), including personal data, unless this is covered by Art. 6 (2) of the FIU Act.

3) After consulting the appropriate member of the Government, the National Cyber Security Unit shall conclude an agreement with the FIU concerning further cooperation arrangements pursuant to Art. 15 (2) of the Cyber Security Act.

C. Control measures

Art. 12

General

1) The National Cyber Security Unit may conduct control measures pursuant to Art. 19 (1) of the Cyber Security Act or arrange for them to be conducted by qualified third parties at any time.

2) The National Cyber Security Unit must give advance notice of control measures pursuant to (1); except in cases where there would be a risk in delay.

Art. 13

Scope and procedure

1) Before conducting a control measure the National Cyber Security Unit shall establish its scope in agreement with the body to be inspected.

When conducting a control measure, it must be established in particular whether:

a) appropriate and proportionate technical, operational and organisational measures have been taken for the protection of network and information systems;

b) the risk management measures pursuant to the Cyber Security Act and this Ordinance have been taken;

c) the reporting obligations pursuant to Art. 6 of the Cyber Security Act have been met.

2) Where justified, the National Cyber Security Unit may extend or restrict the scope of a control measure while it is in progress.

3) The National Cyber Security Unit may inspect confidential material for evidence of compliance with risk management measures in secure premises provided by the body under inspection.

4) It shall produce a report on the results of the inspection in all cases and forward it to the body under inspection. Where justified and in consultation with the body under inspection, the National Cyber Security Unit may forward the full report or excerpts from it to third parties.

5) The working papers, documents and data media must be retained for ten years after completion of the relevant control measures; this excludes the confidential material referred to in (3).

Art. 14

Control measures by qualified third parties

1) Qualified third parties must conduct their control measures according to the requirements laid down by the National Cyber Security Unit. They are obliged:

a) to submit an inspection report to the National Cyber Security Unit upon completion of the inspection, ensuring that no essential facts are omitted. The information in the inspection report must be a truthful representation of the situation;

b) to follow the guidelines established by the National Cyber Security Unit on inspection activities and the conducting of inspections and to make all the working papers drawn up in the course of the inspection available to the National Cyber Security Unit on request;

c) to provide the National Cyber Security Unit with an interim report on the current status of the inspection at their request at any time.

2) Qualified third parties are subject to an obligation of confidentiality, without prejudice to the reporting obligation and duty of disclosure pursuant to (1).

3) When performing an inspection qualified third parties must be totally independent of the body to be inspected. In particular, they may not have acted as a consultant for the controlling body in the previous 18 months.

V. Transitional and final provisions

Art. 15

Repeal of existing law

The Cyber Security Ordinance (CSV) of 4. September 2023, Liechtenstein Legal Gazette (LGBl) 2023 No. 359, is repealed.

Art. 16

Transitional provision

Entities which at the time when this Ordinance enters into force are classified under existing legislation as operators of essential services are to be considered as essential entities pursuant to Art. 3 (2) a) no. 5 of the Cyber Security Act.

Art. 17

Entry into force

1) Subject to (2) this Ordinance enters into force on 1 February 2025.

2) Art. 1 (2) a) shall enter into force at the same time as the Decision of the EEA Joint Committee concerning the adoption of Directive (EU) 2022/2555 in the EEA Agreement.

Princely Government:

sig. *Dr. Daniel Risch*

Princely Head of Government

Annex
(Art. 3)

Risk management measures

1.	**Risk analysis and security of network and information systems**
1.1	Risk analysis: A risk analysis of the network and information systems must be carried out at regular intervals, in order to identify, assess and manage the risks to the security of network and information systems. The results of the risk analysis must be recorded and a risk management plan must be drawn up, implemented and monitored on the basis of these results.
1.2	Security policy: A security policy must be established, reviewed on a regular basis and updated if necessary.
1.3	Inspection plan for network and information systems: A plan for the regular inspection of the security of the network and information systems is to be established and implemented.
1.4	Resource management/Asset management: A full, precise, up-to-date and coherent inventory is to be conducted of the network and information systems and other associated equipment and assets, that support the operations and services of the entity concerned. All the resources that are required to ensure the security of network and information systems, are to be planned for according to short-term, medium-term and long-term capacity requirements and secured to an established level of protection.
1.5	Personnel, cyber hygiene and training: Human resources procedures must allow for and incorporate security-related considerations, including any background checks. Regular training courses and activities to raise awareness on cyber security and cyber hygiene must be held for members of staff.

1.6	Evaluation of the effectiveness of risk management measures: Plans are to be put in place and procedures are to be established to assess whether the cyber security risk management measures taken have been effectively implemented.
2.	**Authorisation management (identity and access management)**
2.1	Identification and authentication: Procedures must be implemented using the appropriate technology to guarantee logical and physical control of access to network and information systems through identification and authentication of users and services. The allocation of access and entry rights is to be reviewed on a regular basis and adjusted if necessary.
2.2	Privileged accounts: Administrative access and entry rights are to be allocated on a restricted basis according to the principle of least privilege. These allocations must be periodically reviewed and adjusted if necessary.
2.3	Systems and applications for system administration: Systems and applications for system administration are to be used exclusively for the purposes of system administration.
2.4	Multi-factor authentication: Authentication methods are appropriate to the critical nature of the network and information systems, one such method being multi-factor authentication.
3.	**Security measures in ongoing operation and maintenance**
3.1	Security of network and information systems: Technical, operational and organisational measures are to be introduced to ensure the secure operation of network and information systems and are to be inspected on a regular basis. These measures must include protection against malware.
3.2	Remote access: Remote access must be granted on a restricted basis according to the principle of least privilege and for a limited period of time. The remote access rights must be periodically reviewed and adjusted if necessary. The security of remote access must be guaranteed.

3.3	Configuration management: Network and information systems must be configured securely and the configuration must be documented, with the documentation being kept up to date.
3.4	Network segmentation: Segmentation must be carried out within the network and information systems depending on the protection requirements.
3.5	Cryptography: Confidentiality, authenticity and integrity of information must be ensured through appropriate and effective use of cryptographic procedures and technology.
3.6	Update management: Available security updates must be tested, assessed and incorporated in a timely manner.
3.7	Vulnerability management: Possible data leaks and publicly known security vulnerabilities in the hardware and software employed must be identified. Appropriate action is to be taken against vulnerabilities and known weaknesses in the network and information systems during ongoing operations.
4.	**Security measures for acquisition and development**
4.1	Procurement management: Procedures and measures are to be established, and reviewed on a regular basis for the management of the risks arising from the procurement of ICT services or ICT products that have an impact on the security of the network and information systems of the entities concerned.
4.2	Project and development management: The security of network and information systems must be appropriately considered in project management procedures, particularly in development.
4.3	Modification management: The security of network and information systems must be appropriately considered in modification management procedures. Modifications to the network and information systems, in particular security-related configuration modifications must be recorded, assessed, tested, approved, implemented and reviewed.

5.	**Security of the supply chain**
5.1	List of distributors, suppliers and service providers: A list containing distributors, direct suppliers and service providers, together with contact details, is to be drawn up and kept up to date.
5.2	Relationships with direct suppliers and service providers: Requirements for direct suppliers and service providers must be established, and reviewed on a regular basis, for the operation of, secure entry to and access to network and information systems.
5.3	Service agreements with distributors, suppliers and service providers: Service agreements with distributors, direct suppliers and service providers must be reviewed and monitored on a regular basis.
6.	**Physical security**
	The physical protection of the network and information systems, in particular physical protection against natural disasters or unauthorised entry and access, must be guaranteed.
7.	**Management of security incidents (detection and handling)**
7.1	Logging and monitoring: Mechanisms must be implemented for logging and monitoring of activities in the network and information systems.
7.2	Detection, correlation and analysis: Mechanisms must be implemented for the detection and evaluation of security incidents, if applicable through the correlation and analysis of the data recorded.
7.3	Security incident response: Incident response procedures must be drawn up (blueprint for the management of security incidents), reviewed periodically, updated when necessary and tested.
7.4	Security incident reporting: Procedures for internal and external reporting of security incidents must be established, maintained and tested.

7.5	Security incident analysis: Procedures for analysing and evaluating security incidents and collecting relevant information must be established, maintained and tested to promote a continuous process of improvement.
8.	**Maintenance of operations and restoration after an emergency**
8.1	Supporting utility services: Loss, damage or disruption of network and information systems or interruption of their operation due to the failure of or disruption to supporting utility services must be avoided.
8.2	Operational continuity management: The restoration of the provision of the network and information systems to a predetermined level of quality after a security incident must be guaranteed.
8.3	Emergency management: Contingency plans are to be drawn up, applied, reviewed on a regular basis and tested for the maintenance and restoration of operations after a security incident.
8.4	Backup management: Backup copies are to be made of all relevant data (including configuration data). Restoration within an established timeframe must be guaranteed. Regular integrity checks of the backup copies must be carried out.
9.	**Crisis management**
	Parameters and processes for crisis management in respect of network and information systems must be defined, implemented, tested, and reviewed on a regular basis, before and during a security incident.