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 4 September 2023
Original German title:	Cyber-Sicherheitsverordnung (CSV) vom 4. September 2023
Systematic number (LR-Nr.):	784.131
First publication date:	6 September 2023
First publication no. (LGBl-Nr.):	2023-359
Last change date:	
Last change publication nr. (LGBl-Nr.):	
Translation date:	9 October 2023

Liechtenstein Law Gazette

Year 2023 No. 359 published on 6 September 2023

Cyber Security Ordinance (CSV)

of 4 September 2023

By virtue of Art. 4 (5), Art. 5 (7), Art. 9 (3), Art. 13 (3), Art. 18 (3), Art. 19 (3) and Art. 24 of the Cyber Security Law (CSG) of 4 May 2023, Liechtenstein Legal Gazette (LGBI) 2023 no. 269, the Government decrees:

I. General provisions

Art. 1

Object and scope

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

a) the identification of operators of essential services;

b) the specific sectors as referred to in Art. 1 (1) a) of the Law;

c) the security measures to be implemented;

d) the notification requirements pursuant to Art. 5 of the Law;

e) the requirements concerning qualified third parties as referred to in Art. 9 (2) of the Law;

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

g) the implementation of control measures as referred to in Art. 18 of the Law.

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

a) Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems 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].

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

Definition of terms and designations

1) For the purposes of this Ordinance, the following definitions apply:

a) "Internet Exchange Point (IXP)" means a network device that enables the interconnection of more than two independent, autonomous systems, primarily to facilitate the exchange of Internet traffic;

b) "Domain name system (DNS)" means a designation system divided along hierarchical lines in a network for responding to domain name queries;

c) "top-level domain name registry" means an entity that manages and operates the registration of Internet domain names within a specific top-level domain (TLD).

2) 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) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194 of 19.7.2016, p. 1)

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)

II. Operators of essential services

A. Sectors

Art. 3

Identification of operators of essential services

1) The National Cyber Security Unit identifies the operators of essential services registered in Liechtenstein that provide an essential service for each sector referred to in Art. 1 (1) a) of the Law.

2) Operators of essential services shall, when required by the National Cyber Security Unit, designate a contact point for communication with the National Cyber Security Unit or the Computer Security Incident Response Team (CSIRT). They must guarantee that they can definitely be contacted via this contact point during the period in which they provide an essential service. The National Cyber Security Unit is to be notified immediately of any changes to the contact point.

Art. 4

Energy sector

On account of their importance for the maintenance of the public energy supply the following types of entities that provide essential services are classified as falling within the energy sector:

a) in the electricity sector:
   1. electricity companies that undertake the sale, including the retail sale of electricity to consumers;
   2. distribution system operators that perform the function of distribution and are responsible for:
      aa) the operation, maintenance and if necessary, the expansion of the distribution system and, if applicable, the interconnections with other systems; and
      bb) guaranteeing the long-term ability of the system to meet reasonable demand for the distribution of electricity;
   3. transmission system operators that perform the function of transmission of electricity and are responsible for:
      aa) the operation, maintenance and if necessary, the expansion of the transmission system and, if applicable, the interconnections with other systems; and

bb) guaranteeing the long-term ability of the system to meet reasonable demand for the transmission of electricity;

b) in the natural gas sector:

1. supply companies that perform the function of supply;
2. distribution system operators that perform the function of distribution and are responsible for:
   aa) the operation, maintenance and if necessary, the expansion of the distribution system and, if applicable, the interconnections with other systems; and
   bb) guaranteeing the long-term ability of the system to meet reasonable demand for the distribution of gas;
3. transmission system operators that perform the function of transmission and are responsible for:
   aa) the operation, maintenance and if necessary, the expansion of the transmission system and, if applicable, the interconnections with other systems; and
   bb) guaranteeing the long-term ability of the system to meet reasonable demand for the transport of gas;
4. operators of a storage facility that undertake storage and are responsible for the operation of the storage facility;
5. operators of an LNG facility that undertake the liquefaction of natural gas or the import, offloading and re-gasification of liquified natural gas and are responsible for the operation of an LNG facility;
6. natural gas companies that:
   aa) undertake the production, transmission, distribution, supply, purchase or storage of natural gas, including liquified natural gas; and
   bb) perform the commercial, technical and/or maintenance-related tasks in connection with these functions, but not for end customers.

Art. 5

Transport sector

On account of their importance for the maintenance of public transport the following types of entities that provide essential services are classified as falling within the transport sector:

a) in the rail transport sector:
   1. railway infrastructure companies that undertake the building and operation of rail infrastructures, including their maintenance and renovation;
   2. railway operating companies that provide rail services for the carriage of goods and/or persons by rail and ensure traction, as well as companies that provide traction only.

b) in the road transport sector:
   1. the Office for Civil Engineering and Geoinformation which is responsible for the planning, supervision and management of highways;
   2. operators of intelligent transport systems whose function is to employ information and communications technology in road transport, including its infrastructure, vehicles and users, and in transport and mobility management and for interfaces with other modes of transport.

Art. 6

Banking sector

1) On account of their importance for the maintenance of payment transactions the following essential services and/or the systems used for their operation are classified as falling within the banking sector:

a) the operation of systems for the provision of services facilitating cash payments into a payment account;

b) the operation of systems for the provision of services facilitating cash withdrawals from a payment account;

c) the operation of systems for the execution of payment transactions, including the transfer of sums of money to a payment account with the payment services provider of the payment service user or with another payment services provider;

d) the operation of systems for the execution of payment transactions if the sums are covered by a line of credit for a payment service user.

2) The following can be identified as banks that provide essential services referred to in (1):

a) systemically relevant institutions as defined in Art. 3a (1) no. 15 of the Banking Act;

b) banks whose market share of accounts for payment transactions involving the services stated in (1) is in excess of 20 %; or

c) banks that have more than ten cash machines (ATMs).

3) There are specific provisions within the banking sector applying to banks that provide essential services as referred to in (1) concerning security requirements and notification requirements pursuant to Art. 101 and 102 of the Payment Services Act, that guarantee at least an equivalent level of security for network and information systems pursuant to Art. 4 (4) und Art. 5 (6) of the Law.

Art. 7

Financial market infrastructure sector

1) On account of their importance for the maintenance of the trading venue, the following types of entities that provide essential services are classified as falling within the financial market infrastructure sector:

a) operators of trading venues pursuant to Art. 3a (1) no. 5 of the Banking Act;

b) central counterparties as defined in Art. 2 no. 1 of Regulation (EU) no. 648/2012[3];

c) central securities depositories as defined in Art. 2 (1) no. 1 of Regulation (EU) no. 909/2014[4].

2) Essential services as referred to in (1) are:

a) with reference to trading venues as referred to in (1) a), if more than ten million transactions have taken place at this trading venue in one financial year:

   1. the technical connection of the trading and clearing participants;
   2. the provision of the electronic trading platform;
   3. market control as a technical service;

b) with reference to settlement by central counterparties as referred to in (1) b) the provision of a settlement system, if the central counterparty has been appointed as the settlement agent by a trading venue at which

3 Regulation (EU) No. 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201 of 27.7.2012, p. 1)

4 Regulation (EU) No. 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) no. 236/2012 (OJ L 257 of 28.8.2014, p.1)

more than ten million transactions have taken place in one financial year;

c) with reference to central securities depositories as referred to in (1) c):

1. providing and maintaining securities accounts at the top tier level as referred to in Section A no. 2 of the Annex to Regulation (EU) no. 909/2014, if the number of securities quoted per unit amounts to more than eight billion in the financial year;
2. operating a securities settlement system as referred to in Section A no. 3 of the Annex to Regulation (EU) no. 909/2014, if the number of settled transactions is more than one million in the financial year.

3) Within the financial market infrastructure sector there are specific provisions that guarantee at least an equivalent level of security for network and information systems pursuant to Art. 4 (4) of the Law, applying to entities that provide essential services pursuant to:

a) (2) a) concerning security requirements in Art. 30s (1) a) and (3) as well as Art. 30t (1) a) of the Banking Act in connection with Art. 15, 16 and 23 (1) and (2) of Delegated Regulation (EU) 2017/584[5];

b) (2) b) concerning security requirements in Art. 26 (1), (3) and (6) as well as Art. 34 of Regulation (EU) no. 648/2012 in connection with Art. 4 and 9 of Delegated Regulation (EU) no. 153/2013[6];

c) (2) c) concerning security requirements in Art. 45 of Regulation (EU) no. 909/2014 in connection with Art. 75 of Delegated Regulation (EU) 2017/392[7].

5 Commission Delegated Regulation (EU) 2017/584 of 14 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying organisational requirements of trading venues (OJ L 87 of 31.3.2017, p. 350)

6 Commission Delegated Regulation (EU) No. 153/2013 of 19 December 2012 supplementing Regulation (EU) no. 648/2012 of the European Parliament and of the Council with regard to regulatory technical standards on requirements for central counterparties (OJ L 52 of 23.2.2013, p. 41)

7 Commission Delegated Regulation (EU) 2017/392 of 11 November 2016 supplementing Regulation (EU) no. 909/2014 of the European Parliament and of the Council with regard to regulatory technical standards on authorisation, supervisory and operational requirements for central securities depositories (OJ L 65 of 10.3.2017, p. 48)

Art. 8

Healthcare sector

On account of their importance for the maintenance of the public health service, healthcare facilities used for inpatient, day unit, or outpatient treatment of acute medical conditions or for the provision of medical rehabilitation services, in particular clinics and hospitals, and which thereby provide an essential service are classified as falling within the healthcare sector.

Art. 9

Drinking water supply sector

1) On account of their importance for the maintenance of the public supply of drinking water, suppliers of and undertakings involved in the supply of water in its original state or after treatment, intended for drinking, boiling, meal preparation or for other household purposes, irrespective of whether it is supplied via a distribution network, in tankers, in bottles or other containers, which thereby provide an essential service, are classified as falling within the drinking water supply sector.

2) Suppliers for whom the supply of water for consumption as described in (1) only forms part of the business of supplying other raw materials and goods that are not classified as essential services, are not included.

Art. 10

Digital infrastructure sector

On account of their importance for the maintenance of the functionality of public information and communications technology, the following categories of entities that provide essential services are classified as falling within the digital infrastructure sector:

a) DNS service providers that perform the function of provision of DNS services on the Internet;

b) top-level domain name registries;

c) IXP's (Internet hubs/exchanges);

d) providers of electronic communications networks as defined in communications legislation;

e) providers of publicly accessible electronic communications services as defined in communications legislation.

B. Security requirements

Art. 11

Security measures

1) In order to ensure the level of security of network and information systems pursuant to Art. 4 of the Law, operators of essential services shall take the security measures listed in the Annex in the following areas:

a) governance and risk management;

b) user authorisation management (identity and access management);

c) operational management (continuous operation and maintenance);

d) project, modification and update management;

e) interaction with service providers, suppliers and third parties;

f) physical security;

g) management of security incidents (detection and handling);

h) business continuity; and

i) crisis management (contingency plan).

2) From a technical and organisational point of view, security measures in the areas referred to in (1) are to be implemented as far as possible on the basis of a risk analysis, determining the operational impact of security incidents and assessing that impact in the light of the paramount importance of the operator of essential services for the functioning of the community.

III. Notification requirements

Art. 12

Notification procedure

1) The National Cyber Security Unit will provide an electronic form for reporting security incidents pursuant to Art. 5 of the Law.

2) It must be possible, on the basis of the information concerning the security incident communicated in the initial notification, for the CSIRT to establish whether such an incident has any cross-border implications.

3) Follow-up notifications must include an update of the information concerning the security incident communicated in the initial notification, in particular information on its severity, its impact and any indicators of compromise (IOCs).

Art. 13

Significance of the impact of a security incident

When assessing the extent of a security incident operators of essential services must consider the following cross-sectoral factors at the very least:

a) the number of users who use the service provided by the entity in question;

b) the duration of the security incident;

c) the extent of the interruption to the provision of the service;

d) the extent of the impact on economic and social activities;

e) the market share of the entity concerned;

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

g) the importance of the entity concerned for the maintenance of the service to a sufficient level, taking in to account the availability of alternative resources for the provision of the service in question.

Art. 14

Handling of notifications

1) Notifications of security incidents as referred to in Art. 12 (1) are handled by the CSIRT using its own IT infrastructure.

2) The CSIRT may communicate information concerning reported security incidents, 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. 15

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. 9 (2) of the Law, in particular to carry out the control measures referred to in Art. 18 of the Law must:

a) be unconnected with the operators of essential services and providers of digital services 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), if applicable by the production of the corresponding certification.

B. Cooperation and exchange of information with domestic authorities

Art. 16

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) Exchange of information may include:

a) notifications concerning security incidents from the banking and financial market infrastructure sectors received by the FMA pursuant to Art. 101 and 102 of the Payment Services Act and by the National Cyber Security Unit pursuant to Art. 5 or 8 of the Law;

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 verification of security requirements and compliance with the notification requirements pursuant to Art. 4 and 5 of the Law. By virtue of its powers the FMA may conduct the inspections or investigations itself or instruct specialists to conduct them.

Art. 17

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 areas:

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. 18

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 in the following areas:

a) secure communication of information by the creation of secure transmission channels;

b) exchange of information about unusual incidents in cyber space.

Art. 19

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. 13 (2) of the Law.

C. Control measures

Art. 20

General

1) The National Cyber Security Unit may conduct control measures pursuant to Art. 18 (1) of the Law 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 imminent danger.

Art. 21

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 reasonable technical and organisational measures have been taken for the protection of network and information systems;

b) the security requirements pursuant to the Law and this Ordinance have been met;

c) the notification requirement pursuant to Art. 5 or 7 of the Law 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 security requirements in secure premises provided by the body under inspection.

4) It will 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. 22

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. Essential facts may not be omitted from this report. 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 conduct 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.

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 independent of the body to be inspected. In particular, they may not have acted as a consultant for the body to be inspected in the previous 18 months.

V. Final provision

Art. 23

Entry into force

1) Subject to (2) this Ordinance shall enter into force on the day after promulgation.

2) Art. 1 (2) a) shall enter into force at the same time as the Decision of the EEA Joint Committee no. 21/2023 of 3 February 2023 amending Annex XI (Electronic communication, audio-visual services and information society) to the EEA Agreement.

Princely Government:

sig. *Dr. Daniel Risch*

Princely Head of Government

Annex
(Art. 11(1))

Security measures

1.	**Governance and risk management**
1.1	Risk analysis: A risk analysis of the network and information systems must be carried out at regular intervals. Specific risks must be identified, based on an analysis of the operational impact of security incidents and assessed in terms of the importance of the operator of essential services for the functioning of the community.
1.2	Security policy: A security policy must be established and updated periodically.
1.3	Inspection plan for network and information systems: A plan for the regular inspection of network and information system security is to be established and scheduled.
1.4	Resource management: All the resources that are required to ensure the functional capability of the network and information systems are to be allocated and secured according to short-term, medium-term and long-term capacity requirements.
1.5	Information security management system audit: A regular audit of the information security management system is to be set up and carried out.
1.6	Human resources: Security-related factors have to be considered and implemented in the procedures of human resources practices. Regular training courses on cyber security must be held for members of staff.
2.	**User authorisation management (identity and access management)**
2.1	Identification and authentication:

	Procedures must be established and implemented, using the appropriate technology, to ensure that users and services can be identified and authenticated. The allocation of user authorisations is to be reviewed on a regular basis and adjusted if necessary.
2.2	Authorisation: Procedures must be established and implemented, using the appropriate technology, to prevent unauthorised access to network and information systems.
2.3	Multi-factor authentication: Authentication methods are commensurate with the critical nature of the network and information systems. One such method is multi-factor authentication.
3.	**Operational management (continuous operation and maintenance)**
3.1	System maintenance and operation: Processes and procedures guaranteeing secure system operation of network and information systems are to be introduced and reviewed on a regular basis.
3.2	Systems and applications for system administration: Systems and applications for system administration are to be used exclusively for activities for the purpose of system administration.
3.3	Administrative access rights: Administrative access rights are to be allocated on a restricted basis according to the minimum rights principle. These allocations must be periodically reviewed and adjusted if necessary.
3.4	Remote access: Remote access must be restricted according to the minimum rights principle and granted for a limited time. The remote access rights must be periodically reviewed and adjusted if necessary. The security of remote access must be guaranteed.
3.5	System configuration: Network and information systems must be configured securely and the configuration must be documented, with the documentation being kept up to date.

3.6	Network segmentation: Segmentation must be carried out within the network and information systems depending on the protection requirements.
3.7	Cryptography: Confidentiality, authenticity and integrity of information must be ensured through appropriate and effective use of cryptographic procedures and technology.
4.	**Project and modification management**
4.1	Project management: The security of network and information systems must be considered accordingly in project management processes.
4.2	Modification management: The security of network and information systems must be considered accordingly in modification management processes. Modifications to the network and information systems, in particular security-related configuration modifications must be recorded, tested, assessed, approved, implemented and reviewed.
4.3	Update management: Possible data leaks and publicly known security vulnerabilities in the software and hardware employed must be identified. Available security updates must be tested, assessed and incorporated in a timely manner.
5.	**Interaction with service providers, suppliers and third parties**
5.1	Relationships with service providers, suppliers and third parties: Requirements for service providers, suppliers and third parties for the operation of, secure entry to and access to network and information systems must be established and reviewed periodically.
5.2	Vulnerability management: Specific vulnerabilities of the individual service providers and suppliers, as well as the overall quality of the products used with reference to cyber security must be taken into account during operation.
5.3	Service agreements with service providers and suppliers:

	Service agreements with service providers and suppliers must be periodically reviewed and monitored.
6.	**Physical security**
	The physical protection of the network and information systems, in particular physical protection against unauthorised entry and access, must be guaranteed.
7.	**Management of security incidents (detection and handling)**
7.1	Detection: Mechanisms for detecting and evaluating security incidents must be implemented.
7.2	Logging and monitoring: Mechanisms for logging and monitoring, in particular of activities and processes crucial for the provision of the essential service, must be implemented.
7.3	Correlation and analysis: Mechanisms for the detection and appropriate assessment of security incidents through the correlation and analysis of the recorded data must be implemented.
7.4	Security incident response: Incident response processes must be created, maintained and tested.
7.5	Security incident reporting: Processes for internal and external reporting of security incidents must be created, maintained and tested.
7.6	Security incident analysis: Processes for analysing and evaluating security incidents and collecting relevant information must be created, maintained and tested to promote a continuous process of improvement.
8.	**Business continuity**
8.1	Business continuity management: The restoration of the provision of the essential service to a predetermined level of quality after a security incident must be guaranteed.
8.2	Emergency management:

	Emergency plans must be created, applied, regularly evaluated and tested.
9.	**Crisis management (contingency plan)**
	Parameters and processes for crisis management must be defined, implemented and tested to maintain essential services before and during a security incident.