NATIONAL CYBERSECURITY UNIT
PRINCIPALITY OF LIECHTENSTEIN

National Strategy For Protection Against Cyber Risks

February 2025

Contents

Summary

Liechtenstein has a National Strategy for Protection Against Cyber Risks.[1] This broad-based national strategy, co-developed with the help of an expert monitoring group, was adopted by the government on 20 October 2020 to protect Liechtenstein against cyber risks. The National Cyber Security Unit[2] coordinates the periodic review and update of this strategy and has been working on the first full revision of it since spring 2024.

The result of this review, the present follow-up strategy, defines Liechtenstein's vision in connection with protection against cyber risks, it defines the stakeholders and sets out the goals and principles of action. The strategy also takes into account the latest developments in the field of cybersecurity and the current legal obligations.

Liechtenstein is developing and fostering digitalisation in all areas of life for the benefit of the population, the economy and the administration. Liechtenstein is protecting itself against cyber risks. This protection is based on networking, collaboration and mutual support between all parties involved as well as know-how and personal responsibility. Protection ensures resilience, security, trust in the institutions and the continued attractiveness of Liechtenstein in the future.[3]

The national strategy to protect Liechtenstein against cyber risks covers all the key cybersecurity issues. It is aimed at the following stakeholders: the population, the economy and the financial centre, critical infrastructures and government bodies.

The strategy has four main objectives, namely all stakeholders (1.) know their cyber risks, (2.) are resilient, (3.) are organised in networks and (4.) make their contribution.

The strategy includes the following principles, which the stakeholders follow when dealing with cyber risks:

- informing, raising awareness and educating;
- pooling and strengthening resources - working together in the country;
- cross-border cooperation;
- working efficiently and effectively;
- measurable and effective implementation.

The need for action set out in this strategy is divided into five fields of activity. In each field of activity (chapters 6.1 to 6.5), the starting point and intention as well as the respective goals to be achieved are expressed. The resources required to achieve the goals, including any political and regulatory measures for protection against cyber risks, are set out in an Implementation and Action Plan.

The National Cyber Security Unit plays a central role in implementing this strategy. It serves as a contact and liaison centre for all matters relating to cyber risks and as a hub for all the stakeholders. It draws on its national and international network and can therefore provide stakeholders with the best possible advice on cyber risks.

The strategy is implemented on a rolling basis. The National Cyber Security Unit coordinates the Implementation and Action Plan and all activities connected with this strategy and its realisation in consultation with the government. It is supported by an advisory board.[4]

[1] https://www.llv.li//serviceportal2/amtsstellen/stabstelle-cyber-sicherheit/nis-strategie/2020-10-08_schutz-cyber-risiken_strategie_li_v1.1.pdf.
[2] https://scs.llv.li.
[3] Vision, see chapter 2, p. 5.
[4] See chapter 0, p. 13.

Liechtenstein's cybersecurity policy is based on personal responsibility, networking, cooperation and efficiency. It relies on fostering close cooperation and exchanging information with neighbouring countries and the relevant authorities in the European Economic Area. Liechtenstein networks specifically with countries that have similar conditions regarding the economy and digitalisation and are facing comparable challenges. Wherever possible, existing organisations, structures, processes and synergies are used to protect against cyber risks. Decisions are taken in such a way that the resources available and deployed have the greatest possible impact.

This strategy will apply from as of 1 February 2025. It will be evaluated after five years at the latest on the basis of essential key performance indicators and updated if necessary.

1. Introduction

The Principality of Liechtenstein is supporting, developing and shaping digitalisation for the benefit of the population and the economy in all areas of life. The government is aware of the associated risks and actively promotes protection against these risks.

This National Strategy for Protection Against Cyber Risks defines Liechtenstein's vision in connection with protection against cyber risks, it defines the stakeholders and sets out the goals and principles of action. It also takes into account the latest developments in the field of cybersecurity and the current legal obligations.

What is cyber risk?

Cyber risks are different types of hazards that can arise during or through the use of information and communication technologies. They impair the availability, authenticity, integrity or confidentiality of network and information systems, for example, i.e. we are talking about hazards that affect a device or a group of interconnected or related devices, but also electronic communication networks and digital data that are, inter alia, stored, processed, retrieved or transmitted.

Cyber risks also affect intangible assets, such as an organisation's or a person's reputation or public trust.

Cybersecurity refers to all activities that are necessary to protect network and information systems, users of such systems and other individuals affected by cyber threats.

Features of the strategy

The strategy takes into account Liechtenstein's particular strengths and characteristics. It relies on a high degree of personal responsibility, short, unbureaucratic channels, the advantages of personal networks and strong cooperation. It is intended to lead to approaches and solutions that are in keeping with Liechtenstein's size and therefore strengthen all stakeholders.

The strategy is drafted in an open and technologically neutral manner so that the goals, principles and fields of activity can also be applied to new developments, technologies and issues connected with cyber risks, such as the advancing digitalisation of work and administrative processes, the Internet of Things, intelligent (electricity) grids (known as smart grids) and artificial intelligence. The strategy itself does not assess cyber risks, but this will be part of the implementation of the strategy.

The strategy forms the basis for the government to make coherent and prudent decisions in connection with the challenges of protecting against cyber risks and to involve all the stakeholders according to their responsibilities. It is the basis for Liechtenstein to have comprehensive and good protection against cyber risks.

2. Vision

Liechtenstein is developing and fostering digitalisation in all areas of life for the benefit of the population, the economy and the administration. Liechtenstein is protecting itself against cyber risks. This protection is based on networking, collaboration and mutual support between all parties involved as well as know-how and personal responsibility. Protection ensures resilience, security, trust in the institutions and the continued attractiveness of Liechtenstein in the future.

3. Stakeholders

This national strategy is all-encompassing and covers the key cybersecurity issues. Only together can we succeed in protecting against cyber risks. Everyone will share responsibility and protect themselves and therefore also Liechtenstein from the dangers that can be associated with digitalisation. The strategy is aimed at the following stakeholders:

- **the population**
  residents and all persons working or residing in Liechtenstein;
- **the economy and the financial centre**
  national and international companies and organisations, regardless of their size (small, medium and large companies) and sector;
  banking and financial market infrastructures, in particular as part of the critical infrastructure, but not exclusively;
- **critical infrastructures**
  all essential and important entities, buildings and installations, supply systems and services, whose disruption could have a serious impact on public order, public safety, public health or could lead to a significant systemic risk for Liechtenstein, such as energy and telecommunications systems or the drinking water supply.
- **government bodies**
  Princely House, State Parliament, government, courts, National Administration of Liechtenstein and the municipalities.

4. Goals

The stakeholders know their cyber risks

The stakeholders know their specific cyber risks. They know that these risks can change and develop quickly. They are able to react promptly and appropriately to changes.

The stakeholders are resilient

The stakeholders act competently and have taken the necessary measures for protecting against current cyber threats (prevention). In the event of an incident, they react quickly and appropriately. The extent of damage caused by a security incident remains manageable and any damage is kept to a minimum.

The stakeholders are organised in a network

Individuals, companies and organisations inside and outside the country that can contribute to protecting against cyber risks work together. Liechtenstein has an international network and utilises its expertise and support. Stakeholders and the parties responsible for cybersecurity regularly discuss threats and protecting against cyber risks.

The stakeholders make their contribution

Stakeholders know that cyber risks affect everyone. They are sensitised and implement appropriate measures to protect against cyber risks. The government encourages people to take personal responsibility. Provisions are adopted where necessary.

5. Principles

Stakeholders follow the following principles when dealing with issues relating to protection against cyber risks. The government promotes cooperation and creates the necessary framework conditions.

Informing, raising awareness and educating

Stakeholders are empowered to deal with cyber risks in a responsible and competent manner by being informed and made aware of current developments and events relating to cybersecurity. The public sector promotes education and training in dealing with cyber risks at all levels and for all stakeholders, thereby strengthening digital expertise (prevention).

Pooling and strengthening resources

Liechtenstein develops its strength in protecting against cyber risks by the public sector bringing together stakeholders, creating networks between them, identifying their needs and utilising their strengths. It creates a framework where stakeholders can exchange information and work together confidentially and openly. The public sector fosters dialogue and cooperation with key partners and works with them to develop solutions and offerings for stakeholders (public-private partnership).

Cross-border cooperation

Liechtenstein maintains close cooperation and exchanges information with states and international organisations in a targeted manner, gets actively involved, makes its contribution to the international community, and cultivates and utilises its relationships to minimise cyber risks (international networking).

Working efficiently and effectively

Where possible, existing organisations and processes are used to protect against cyber risks. These are to be adapted systematically as required. Efficient action ensures that the resources deployed have the maximum impact and decisions are made on a risk basis. Liechtenstein also uses its short, unbureaucratic channels when it comes to cybersecurity.

Measurable and effective implementation

The implementation of the strategy in the fields of activity and the measures will be tangible and measurable. Both the measures and their impact will be reviewed and conclusions drawn for further measures.

6. Implementing the strategy

The first National Strategy (2020 to 2024) was characterised in particular by the development of legal, organisational and technical structures in the area of cybersecurity and comprised nine fields of activity in total.[5]

On the other hand, certain fields of activity will be removed, adapted or added to the present strategy due to the development work carried out so far by the National Cyber Security Unit and the Cyber Security Act (CSG) that came into force on 1 February 2025.

Following the consolidations, five fields of activity were identified, defined and subsequently described in more detail in order to achieve the strategic goals:

- Field of activity 1: Knowing risks and important developments;
- Field of activity 2: Informing, raising awareness and networking;
- Field of activity 3: Protecting essential and important entities;
- Field of activity 4: Protecting the financial centre;
- Field of activity 5: Overcoming crises.

The descriptions (see chapters 6.1 to 6.5) each contain the starting point and intention and the desired target status. The resources required to achieve the goals and any necessary policy and regulatory measures will be defined in detail in a second step in an Implementation and Action Plan and are not the subject of the present strategy.

[5] 1. Establishing National Cyber Security Unit, 2. Knowing risks, 3. Informing and sensitising the population, 4. Protecting critical infrastructures, 5. Networking the economy, 6. Supporting and networking government bodies, 7. Developing recommendations, 8. Ensuring cyber defence with partnerships, 9. Taking coordinated action in case of an incident.

6.1 Knowing risks and important developments

Starting point and intention

Between February 2023 and February 2024, the National Cyber Security Unit prepared a cyber risk analysis for Liechtenstein. The results of this analysis were incorporated in the "Hazard and Risk Analysis for Civil Protection 2024" in the form of twelve specific cyber threats[6].

However, individual stakeholders may be exposed to different specific cyber hazards or cyber threats and therefore risks. Knowledge of the specific cyber risks in each case is, however, a prerequisite for taking effective measures and being able to deploy the available resources in a targeted manner. In this respect, not only the essential and important entities are called upon to do this.

Liechtenstein will make its contribution by intending:

- to prepare and periodically update an overview of current cyber threats to the country;
- to prepare a continuously updated status report - situational overview of current cyber threats;
- to create an overview of new technical and regulatory developments that may have a positive or negative effect on cybersecurity in Liechtenstein;
- to inform stakeholders about the findings on cyber threats, current vulnerabilities and security-related developments in a manner appropriate to the target audience;
- to support essential and important entities, financial institutions and the economy in carrying out their own risk assessments;
- to motivate essential and important entities and other organisations and companies to share their findings and experiences with each other;
- to promote research and education in the field of cybersecurity and the handling of cyber threats and security-related developments in the information and communication technology sector.

Target status

The following is to be achieved in the coming strategy period:

- Overview of cyber threats relevant to civil protection is up to date and publicly available.
- Liechtenstein has an up-to-date overview of the current situation regarding relevant cyber threats.
- All stakeholders are regularly informed about current cyber threats and security-relevant developments.
- An overview of current technical and regulatory developments in the field of cybersecurity is available and is communicated in a manner appropriate to the target audience.
- Regular dialogue (networking) takes places between the stakeholders on issues relating to current cyber threats and security-relevant developments.
- Dialogue with experts on cyber risks, cyber threats and security-related developments is established and takes place regularly.
- The exchange of specialist knowledge and cooperation between public bodies and research and educational institutions is established. Research and teaching takes place in connection with current cyber threats and risk management measures.

[6] Hazard and Risk Analysis for Civil Protection, Relevant Threats and Risk Assessment from April 2024, https://www.llv.li//serviceportal2/amtsstellen/stabstelle-cyber-sicherheit/nis-strategie/2024-04-30_bericht_update_gefaehrdungsanalyse_fl-kombiniert.pdf.

6.2 Informing, raising awareness and networking

Starting point and intention

With increasing digitalisation, not only can individual companies and organisations be harmed by cyber threats. The maintenance of critical, social or economic activity as a whole is exposed to a growing cyber risk.

Especially the "population" stakeholder group and the small and medium-sized companies in the economy are often not fully aware of what threats they are exposed to. In many cases, they only have limited resources and knowledge to adequately protect themselves against cyber threats and existing cyber risks. However, small and medium-sized companies in particular are an important economic factor in Liechtenstein.

Liechtenstein will make its contribution by intending:

- to inform all stakeholders about cybersecurity issues via suitable channels and formats, such as media appearances, events, newsletters, etc. In particular about current cyber threats, vulnerabilities, appropriate protective measures and suitable behaviour;
- to create a framework where the stakeholders can safely exchange information, work together and support each other;
- to focus on the population and small and medium-sized companies when providing information and raising awareness, for example by providing recommendations on cyber hygiene and the use of resource-saving protective measures;
- to promote education and training in dealing with cyber risks at all levels and for all stakeholders;
- to promote networking between all stakeholders, particularly between small and medium-sized companies, as well as public-private cooperation;
- to offer help for self-help or to provide support in preparing for incidents or dealing with security incidents.

Target status

The following is to be achieved in the coming strategy period:

- Stakeholders receive low-threshold current information on the subject of cybersecurity on a regular basis and in a manner appropriate to the target audience.
- The stakeholders know the relevant points of contact for cybersecurity in Liechtenstein.
- The national authorities and public bodies work together in the areas of informing, raising awareness and networking and utilise synergies. Where appropriate and possible, existing formats are used and expanded if need be.
- Stakeholders exchange information about cybersecurity amongst each other, in particular about current cyber threats, vulnerabilities, appropriate protective measures and suitable behaviour.
- A regular (information) exchange (networking) between all stakeholders and, where appropriate, also beyond the stakeholders is established.
- Small and medium-sized companies use the existing support to implement risk management measures.

6.3 Protecting essential and important entities

Starting point and intention

The ever closer networking of society, the major and cross-border dependencies in the area of digitalisation and the constant digital development in the area of critical infrastructure also pose (cyber) risks, regardless of the numerous opportunities. Cyber incidents are more frequent, they are more complex and the scale of the damage is increasing. The strong networking and existing dependencies mean that even minor disruptions and failures can lead to considerable social and economic repercussions.

Protecting essential and important entities is of particular significance. It is essential for many (critical) sectors that network and information systems work smoothly. Disruptions or failures lead to material damage, financial losses and can weaken users' confidence in digitalisation.

Liechtenstein will protect essential and important entities by intending:

- to motivate people to be pro-active;
- to promote the exchange of information between essential and important entities about cyber threats and risk management measures;
- to inform about voluntarily reporting cybersecurity incidents and the added value of doing so;
- to promote an information exchange with other bodies and organisations;
- to provide early warnings and tips about current cyber threats to essential and important entities;
- to inform about critical vulnerabilities that are currently being exploited in the respective sectors;
- to provide assistance in monitoring network and information systems;
- to pursue a cross-risk approach that includes technical, operational and organisational measures and runs the gamut from physical protective measures and basic cybersecurity measures (cyber hygiene) to the use of new technologies (artificial intelligence, machine learning);
- to create commitment through regular supervisory activities.

Target status

The following is to be achieved in the coming strategy period:

- Essential and important entities are regularly informed about current cybersecurity issues via suitable formats and channels, such as at events or in bilateral dialogue.
- A regular exchange of information is established between essential and important entities and with other bodies and organisations.
- All stakeholders, especially critical infrastructures, are informed about the option of voluntarily reporting cyber incidents or threats and use it.
- The flow of information on vulnerabilities, early warnings and alerts is established.
- Essential and important entities are aware of the cyber threat situation and its specific risks.
- Essential and important entities have taken appropriate technical, operational and organisational measures to ensure the security of network and information systems.
- Essential and important entities fulfil the reporting obligation.
- The supervisory authorities exercise their powers vis-à-vis the essential and important entities in an appropriate manner.

6.4 Protecting the financial centre

Starting point and intention

In the digital age, the resilience of information and communication technologies to operational disruptions, i.e. digital operational resilience, is crucial for financial institutions to ensure financial stability and market integrity.

While the ubiquitous use of network and information systems and the high level of digitalisation and connectivity are already fundamental characteristics of the activities of financial institutions, their digital resilience must be further increased and integrated into the general operating framework. The financial institutions are therefore subject to a wide range of regulatory requirements in terms of the security of their network and information systems.

Liechtenstein will support its financial centre and financial institutions in Liechtenstein in their efforts to increase resilience to cyber threats by intending:

- to create incentives to implement cybersecurity and cyber hygiene measures;
- to promote a regular and secure exchange of information about current cyber threats, procedures and tools between financial institutions;
- to promote an information exchange with national and international bodies and organisations, especially with critical infrastructures;
- to support financial institutions with obtaining information on specific cyber threats affecting the financial centre;
- to establish a regular exchange of information on current cyber threats with the competent (supervisory) authority;
- to develop the basis for inter-agency technical cooperation;
- to create commitment from financial institutions through regular supervisory activities.

Target status

The following is to be achieved in the coming strategy period:

- The financial institutions use secure channels to inform each other about current cybersecurity issues, such as current cyber threats.
- A regular exchange of information is established between financial institutions.
- The financial institutions are informed about and use the cybersecurity services offered by public bodies, such as the warning and information service of the Computer Security Incident Response Team (CSIRT.LI) set up by the National Cyber Security Unit.
- The financial institutions use the opportunity to voluntarily report security incidents or cyber threats.
- The financial institutions are aware of the cyber threat situation and its specific risks.
- The financial institutions have a solid, comprehensive and well-documented risk management framework in place to address specific cyber risks.
- The supervisory authorities exercise their powers vis-à-vis the financial institutions in an appropriate manner.
- A regular exchange of information and cooperation between the competent public bodies has been established.

6.5 Overcoming crises

Starting point and intention

Despite an established risk management system and correctly implemented technical, operational and organisational security measures, network and information systems may be affected by disruptions and failures. This may be due to physical events, technical faults, human error or a vulnerability in a hardware or software component used that has not yet been made public and has been exploited by an attacker.

Not only can security incidents significantly disrupt ongoing operations, they can also do lasting damage to the confidence of customers, partners and the public. The ability to quickly identify, manage and recover from (cyber) crises is therefore crucial for the long-term security and stability of companies, organisations and government bodies.

Given the existing cyber threats, stakeholders should not only take preventative security measures, but also develop a clear plan for dealing with crises. Resilience to cyber threats requires, for instance, the ability to react quickly, continuous staff training and the implementation of robust emergency strategies.

Liechtenstein supports stakeholders with crisis management by intending:

- to set up and regularly review a national crisis organisation for managing large-scale cybersecurity incidents and crises;
- to involve stakeholders, especially critical infrastructures, in the national crisis organisation;
- to inform about best practices and techniques of crisis management;
- to support stakeholders with managing incidents by providing general assistance;
- to support the affected organisation or person by providing information and general analysis in the event of an incident or crisis.
- to participate in trans-organisational exercises to promote dialogue and cooperation in the area of crisis management amongst stakeholders.

Target status

The following is to be achieved in the coming strategy period:

- The national crisis organisation for managing large-scale cybersecurity incidents and crises is established. There is consistency with the applicable framework for general national crisis management.
- The roll of the national leadership team and the cooperation with the various public bodies and, if necessary, other actors are defined in the event of a “cyber crisis”.
- The national crisis organisation at government level is regularly tested with exercises.
- The stakeholders test their respective crisis organisation in joint regular exercises.
- Cross-border cooperation and support in the event of an incident are defined and appropriate agreements have been reached.

7. Advisory Board

The National Cyber Security Unit plays a central role in implementing this strategy. It is supported by an "Advisory Board". As an advisory body, the Advisory Board contributes wide-ranging expertise from various fields and supports the implementation of the strategy with valuable input. It provides support in identifying and prioritising measures to achieve objectives as well as pointing out important issues and current developments. It serves as an interface between theory and practice.

The Advisory Board consists of representatives of stakeholders, actors and partners who, in particular, have expertise in the fields of cybersecurity, digitalisation or strategy implementation.

The Advisory Board is a flexible body that operates exclusively in an advisory capacity and has no fixed rules or bylaws. The members of the Advisory Board are convened by the National Cyber Security Unit.

The National Cyber Security Unit coordinates the regular meetings of the Advisory Board and is available to members as a point of contact.

8. Validity and adjustment

This strategy will apply as of 1 February 2025. It will be evaluated after five years at the latest based on key performance indicators and updated if necessary.