Icelandic National Cyber Security Strategy 2015–2026

Plan of action 2015–2018

Summary in English
of the Icelandic National Cyber Security Strategy
approved by the Minister of the Interior
in April 2015

Ministry of the Interior
June 2015

Contents

Future vision and strategy regarding cyber security

This is a summary of Iceland's ***Future Vision 2026 on National Cyber Security*** and ***Main Strategy Aims.*** The Introduction describes the work of the task force which prepared the strategy and action plan; subsequently presenting a survey of various cyber security threats and stressing the importance of tackling them. This is followed by a discussion of how well Iceland is prepared to deal with these threats and what can be done to take the initiative and use cyber security as a means of promoting progress and welfare.

Future Vision 2026

> Iceland should have an Internet culture that is sound, promotes human rights, protects the individual and respects freedom of action to support economic prosperity and development. Security in cyber space should be one of the main cornerstones of economic prosperity in Iceland, resting on a foundation of sophisticated awareness of security issues and adequate legislation.
> At the same time, Iceland must be prepared to tackle cybercrime, respond to cyber-threats and take measures to prevent espionage and the abuse of personal and commercial data.

Main strategy aims

1. **Capacity building**. The public, enterprises and government should have the knowledge, skills and equipment needed to cope with cyber security threats.
2. **Increased resilience**. Key factors in enhanced resilience are greater capacity in the fields of assessment, preparedness and response. The aim is to raise the resilience of Iceland's information systems and their preparedness to a level comparable with that of the other Nordic countries. This should be done through, amongst other things, improving capacity in threat assessment, enhanced cooperation and making security concerns an integral part of the maintenance of cyber systems.
3. **Strengthened legislation**. Icelandic legislation should reflect the international demands and obligations the country undertakes regarding cyber security and the protection of personal data. Furthermore, legislation must also support innovation and the development of security-related services, e.g. hosting.
4. **Tackling cybercrime**. The police should have, or have access to, the professional knowledge, skills and equipment needed to resolve issues concerning cyber security.

Introduction

A task force to address strategy on cyber security in Iceland was appointed by the Ministry of the Interior in June 2013. Its main task is to formulate government strategy on cyber security and the protection of IT infrastructure elements that are relevant to national security, i.e. the IT systems of key institutions in Icelandic society. Most of these systems are in turn linked to other IT systems in one way or another via the Internet.

Demarcation of the strategy

The strategy is intended to address the protection of important elements of the infrastructure in Iceland and the responses called for in view of the growing cyber-threats which pose a hazard to the government, the economy and the ordinary citizen. The Internet has already become an integral part of the daily life of almost all people in Iceland and will continue to do so to an ever-greater degree. In this environment, security is of paramount importance; hence, **the strategy covers all use of the Internet and Information Technology.**

The social aims of the strategy are as follows:

- To enhance the security of individuals and groups in society by increasing cyber security.
- To promote the integrated functioning of important elements of the infrastructure of society by increasing the resilience of cyber systems to cope with hazards.
- To establish closer collaboration and coordination on cyber security between Icelandic and international authorities.

Efficient collaboration must be established between Icelandic and international authorities, with a demarcation of the division of responsibilities and tasks between them in the field of cyber security. In drawing up the strategy, attention was given to various other strategies in this field, both in Iceland and in the other Nordic countries and also those of international organisations of which Iceland is a member.

The task force consists of: Sigurður Emil Pálsson, a specialist at the Ministry of the Interior (Chairman); Guðbjörg Sigurðardóttir, Head of Department in charge of the Information Society Project at the Ministry of the Interior; Páll Heiðar Halldórsson and Ottó V. Winther, specialists at the Ministry of the Interior, Jón F. Bjartmarz, Detective Chief Superintendent and Ágúst Finnsson (from January 2014), specialist, at the Office of the National Commissioner of the Icelandic Police, Hrafnkell V. Gíslason, Director of the Post and Telecom Administration, Stefán Snorri Stefánsson, Head of the National CERT - CERT-ÍS at the Post and Telecom Administration, Jónas Haraldsson, specialist at the Ministry of Foreign Affairs and Þorsteinn Arnalds (from May 2014), specialist at the Data Protection Authority (Persónuvernd).

The task force focused on reviewing the general foundations and recommendations on which strategies in this area have been based. The strategies of some of the other Nordic countries were examined and discussions were held with domestic and foreign parties, consultants and government officials on various aspects of information security. The task force also discussed the threats and opportunities that have been defined and the experience gained from the plans of action already been put into practice in other Nordic countries.

A well-attended consultative meeting with stakeholders was held on 2 June 2014. Those present included about 80 representatives of some 60 institutions and enterprises. Another similar meeting,

held on 15 January 2015, was attended by about 60 people. The views voiced at these meetings were taken into consideration in drawing up the strategy.

Connection with other strategies and parliamentary resolutions
Direct and indirect links exist between the strategy on cyber security and many other official strategies and resolutions, e.g. the national strategy on civil protection and public security, law enforcement, telecommunications, the planned strategy on national security and the Icelandic State and Municipal Policy on the Information Society 2013-2016: "e-Power Expansion: - create, connect, participate"

Strategy and action in Iceland: Taking the initiative on security

The threats and challenges outlined above call for responses. As a whole, the situation presents an important opportunity to forge ahead and make Iceland's IT environment more secure and more competitive in the international context. Generally, prioritising security straight away at the initial planning stage means that expensive situations can be avoided later on. Integrating security considerations in the initial plan makes it possible to design reliable computer systems, just as sound foundations make it possible to build a skyscraper: without them, the project remains a 'castle in the air'. Priority must be given to *security by design* and *privacy by design*, i.e. the inclusion of security and privacy considerations from the outset in the design process. Cyber security must form a part of computer-related studies at all levels of the educational system. Moreover, such studies at university level must be upgraded, with closer collaboration with universities abroad to enable students graduating from Icelandic universities to undertake postgraduate studies in cyber security.

It is likely that ever more stringent security requirements will be made on the market for software and software-related services. Many states intend to make use of this opportunity to create for themselves a competitive advantage over others and offer an IT environment supporting the needs of commerce, industry and private individuals. This could involve both a more secure environment for e-commerce and also being in the forefront of cyber security and making it into a valuable export product. Defence against industrial espionage is also an important aspect of this, since such espionage constitutes a large part of the economic damage caused by cyber security threats. Consultancies are starting to use nations' cyber security status as a factor in their advice on choice of location for enterprises which intend to set up data centres or other computer-related services.

The legal environment in Iceland must also support software-related development and provide protection against cybercrime in order to deter criminal organisations from seeing the country as a suitable venue for their activities because of low level of cyber security. At any given time, steps must be taken to evaluate how Iceland's legislation stands in comparison with that of the other Nordic countries. Furthermore, the police must have the powers to enforce this legislation. Particular attention must be given to the protection of personal data: technical developments and standards can change very rapidly and it is important that the level of protection in Iceland is not lower than in other Nordic countries.

Considerable results can also be achieved through simple awareness-raising. By employing relatively simple precautionary measures, it is believed that hazards both to private individuals and enterprises can be reduced significantly. A great deal is at stake when it comes to combating cybercrime.

Defences must be raised around important elements in the infrastructure in Iceland. This is a many-faceted task. It is important to have a high-capacity cyber security team capable of analysing and evaluating cyber-attacks of various types and providing assistance in the case of attacks.

Telecommunications systems and the primary data transmission networks must be reliable. IT and IT security in public administration must be enhanced, for example regarding coordination, education and awareness-raising.

The main basis of Iceland's security and defence lies in the country's collaboration with NATO, active collaboration with other Nordic countries and the Defence Agreement with the United States. It also includes the IT infrastructures mentioned above. The protection of the infrastructures on which these activities rely in Iceland is therefore one of the most important aspects of Iceland's national defence. In view of this, the agreement signed recently with NATO's *Cyber Defence Management Board* will lead to increased collaboration in this field. As an indication of the importance attached by NATO to cyber security, it was decided that cyber-attacks could be classified under Article 5 of the NATO Treaty.

Increased collaboration with other international organisations such as the United Nations, the Council of Europe, the European Union and the Organisation for Security and Cooperation in Europe can also promote cyber security in Iceland.

A great deal can be gained from taking the initiative and forging ahead in this area. Building up cyber security is a challenge that no single entity in our society can undertake. To ensure optimum results it is necessary to approach the task in a comprehensive manner, involving as many IT users as possible. Both government institutions and private companies in addition to individuals should be included in this process.. It is important to begin this work immediately and create a common forum for development and collaboration, e.g. regarding security standards, coordination, identification of cyber security threats and the organisation of responses. Last but not least it is important to be aware of the fact that this will be an on-going process subject to continual review as it progresses, with new challenges calling for new solutions.

The strategy envisages the development of cyber security along the same lines as other aspects of civil protection and security.In the event of a catastrophe or cyber-threat, the emphasis will be on the rapid exchange of information between the parties concerned in order to minimise and mitigate damage, after which work will proceed on the next steps to be taken; assessment and recovery measures will follow the same pattern as is described in the civil defence programme. Furthermore, the event will be analysed in order to learn as much as possible from it. If the event is caused by human agents, then it must also be guaranteed that an efficient police investigation can go ahead.

Review of the strategy and action plan

This strategy shall be examined and reviewed as necessary, at minimum every four years. Measures based on the strategy shall be designed to cover shorter periods and shall be reviewed at least once a year. Procedure in implementing the strategy shall be in the spirit of public administration.

Action plan 2015–2018

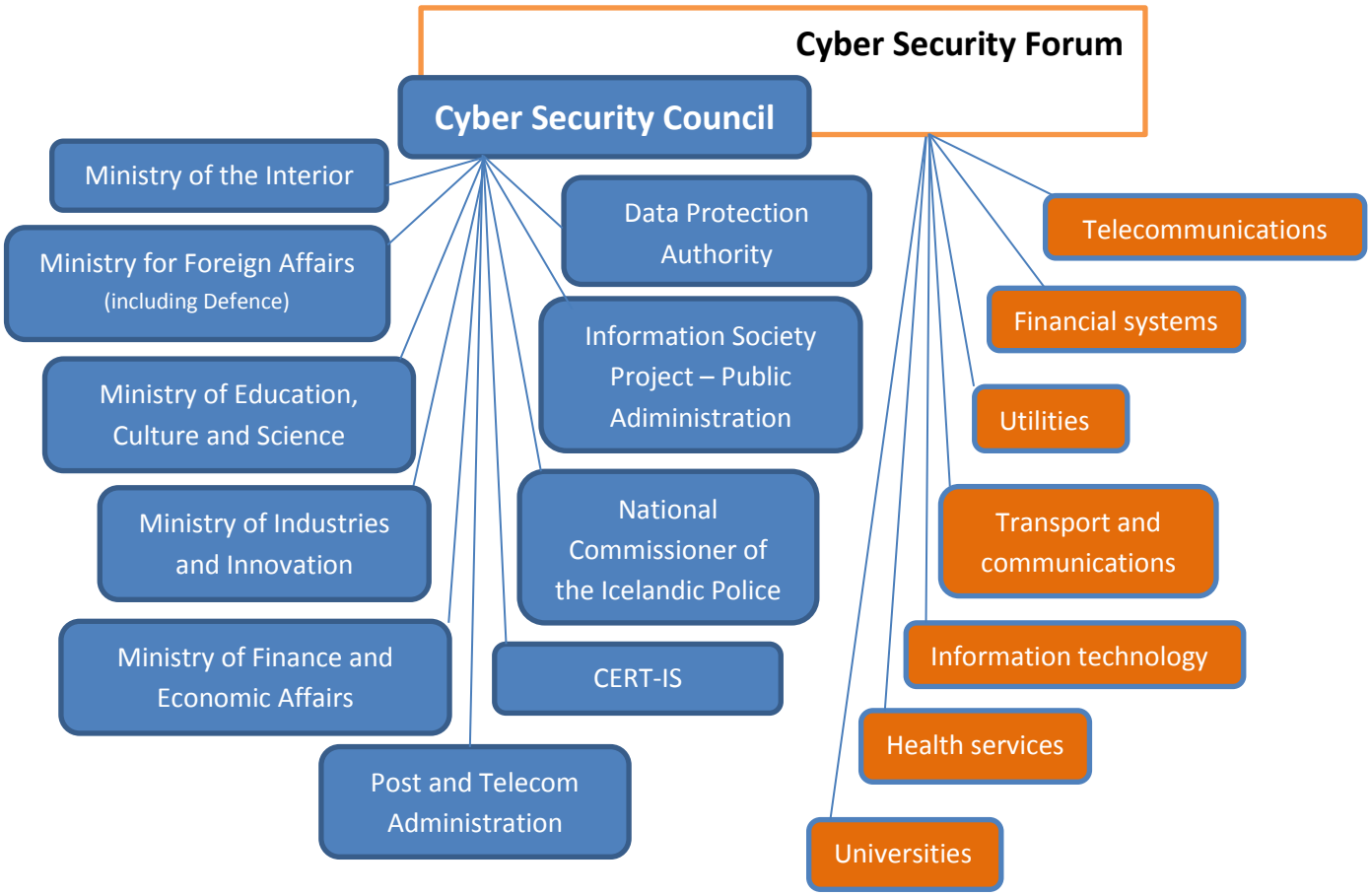
In order to put the cyber security strategy into action, it is proposed that a special **cyber security council** shall be appointed, consisting of representatives of the government bodies involved in the implementation of the strategy., Moreover, a **cyber security forum should** be set up, representing stakeholders both public and private entities.

The Cyber Security Council

Supervision of implementation of the strategy is to be the responsibility of the Cyber Security Council, which will be appointed by the Minister of the Interior. The Cyber Security Council will coordinate measures, particularly those involving government bodies. It will review the action plan at least once a year and make proposals on the prioritisation and funding of measures taken. The Cyber Security Council will submit a report to the Minister of the Interior every year on implementation of the strategy.

The Cyber Security Forum

This is a collaborative venue for representatives of public bodies who sit on the Cyber Security Council and of private entities. The forum will be able to coordinate projects involving stakeholders, in part or in their entirety, and create a basis for collaboration on specific projects, addressing cyber security in demarcated areas.



The measures planned for the first period will call for a special effort to establish the broad collaboration needed between the government and stakeholders According to the plan these measures will be reviewed annually; in subsequent periods procedure will be harmonised with normal standards of other strategy applications. The strategy is intended to form the basis of collaboration and development in cyber security. The strategy itself will not change the responsibilities and duties of those involved in cyber security even though proposals may be made for measures that may involve changes in these areas.

To implement the strategy, a collaborative forum, the 'Cyber Security Forum' will be set up in the first half of 2015. The forum is the venue for planning individual measures in detail with cost estimates. As many of these measures involve coordination in the work of various entities, special funding is not needed to begin this development. Nevertheless to ensure the effort will have sufficient capacity, about ISK 20 million will probably be needed to pay for coordination, reports and educational/training/awareness-raising work. It is envisaged that enterprises (companies) will provide the funds to meet part of the costs of some of the projects. Proposals for projects requiring public funding will be submitted to the Cyber Security Council, which will make proposals on priority ranking of projects, following consultation with stakeholders.

At the end of each period, the Cyber Security Council will compile a report based on summaries submitted by those responsible for all the measures, give an account of the results of the work and submit proposals, following consultation with stakeholders, on a plan of action for the next three years.

The aim is that the work of the Cyber Security Council will be transparent: minutes of meetings and other materials will be published except where publication would be contrary to law, e.g. in view of personal data protection considerations.

Main aim No. 1: Capacity building

The public, enterprises and government should have the knowledge, skills and equipment needed to cope with cyber security threats.

Knowledge is the prerequisite for being able to build up capacity in cyber security. The challenge is similar to that in raising the level of traffic safety: There is a technical side, similar to having the highest possible standards of vehicle safety and well-constructed roads, etc. The ordinary person does not need to be a qualified mechanic to enjoy traffic safety, but he does need to be an active participant in traffic, with a certain knowledge of what constitutes safe vehicles and safe behaviour – this applying both to his own and to others' – for his own good and that of other road-users. An active interest in security need not be daunting or difficult; on the contrary, it makes things easier for everyone. Security issues must be a part of people's use of computers and other equipment from the outset when children are first introduced to them and so on up through the school system. Awareness-raising is a key component in the cyber security strategies of most of our neighbouring countries. It must extend to the design and use of equipment and respect for personal data.

In Iceland as elsewhere, part of this knowledge involves how we speak about the subject, i.e. the vocabulary and use of terminology. If the subject is to thrive and develop, it will be necessary to standardise and coordinate this terminology. There must also be a clear division of responsibilities, defining who is to do what, how much responsibility lies with each user and what expectations can reasonably be made of others.

Iceland has experts who have worked successfully together for many years. Nevertheless it is a major challenge to develop a reliable foundation on which to build a cyber security culture. The degree to which such a culture is established is one of the factors that investors take into account when they assess countries as potential locations for new projects.

Measures

1. **Awareness-raising**
   Enhancement of general awareness of cyber security issues.
2. **Terminology**
   Relevant international definitions of important terms in cyber security to be collected and translated into Icelandic where necessary.
3. **Education**
   Cyber security to be included in all computer-related studies at all school levels.
4. **Postgraduate studies**
   Students with first degrees from Icelandic universities to have access to postgraduate studies in cyber security meeting requirements comparable to those made in the other Nordic countries.
5. **Design values**
   Secure design and personal data protection to be included in the basic values observed in Icelandic software development.
6. **Personal data protection**
   International standards and obligations regarding personal data protection to be taken into account when developing cyber security.

Main aim No. 2: Increased resilience

An upgrading of the resilience of information systems. Greater capacity in the fields of assessment, preparedness and response as key factors in increased resilience.

Monitoring and response capacity must be increased so as to respond to abnormal situations on the Internet. Nevertheless, full regard must be given to appropriate considerations of personal data integrity.

It must be possible for key entities to exchange information about possible threats quickly. Therefore it is important to establish one or more collaborative forums on which information on cyber security threats can be shared in a clearly defined manner without infringement of competition or personal data considerations. This could require mediation through a public body to ensure that it is possible to share information on cyber-threats quickly without revealing the identity of the target.

The pace of development in the field of cyber security is very rapid. For this reason it is important that all entities involved are active in international collaboration, each in its respective area. Close collaboration between stakeholders in Iceland, with efficient exchange of information, will make it possible to respond jointly to rapid change. Active participation in international collaboration is also necessary to maintain flexibility, skills and contacts and be able to work with other national and supranational authorities when a crisis on the Internet looms. It is also vital that Iceland presents a single coordinated strategy in cyber security matters when the country takes part in international collaboration.

Increased resilience in information systems will depend on reliable design. Reliable design must be a crucial consideration in the purchase and development of software, particularly in the case of key elements in IT infrastructure. This applies at the national, corporate and individual level.

7. **A collaborative forum**
   A forum must be established where representatives of government and private enterprises can work together on cyber security issues.
8. **Security yardsticks**
   Choice of appropriate yardsticks (standards and others) for cyber security.
9. **International collaboration**
   Iceland's involvement in cyber security abroad must be increased and coordinated.
10. **Reliability of primary data systems**
    Telecommunications systems and the primary data transmission networks must offer support, with a defined degree of reliability, the Internet and IT networks of key elements in Iceland's infrastructure, both as regards connections within the country and their interface with other countries.
11. **Public administration**
    Cyber security in the field of public administration must be upgraded by means of increased training, coordination and collaboration.
12. **Analysis**
    Principal cyber security threats must be analysed and key elements in the Icelandic infrastructure identified.
13. **Protection of the infrastructure**
    The capacity of the cyber security team to raise the level of protection and assist important elements in the national infrastructure must be increased, and an active response mechanism must be in place on a round-the-clock basis every day of the year. Particular emphasis should be placed on telecoms, utilities and financial companies and the systems necessary for international aviation.

14. **Response**
    Response contingency plans to deal with cyber security threats must be developed and tested by means of exercises. The focus must be on protecting important elements in the national infrastructure.

Main aim No. 3: Strengthened legislation

Icelandic legislation should reflect the international demands and obligations the country undertakes regarding cyber security and the protection of personal data. Furthermore, legislation must also support innovation and the development of security related services, e.g. hosting.

Good legislation is a crucial factor for developing cyber security. Its importance is clear in many contexts:

- Iceland is a member of international agreements under which it is obliged to meet certain requirements in its domestic legislation. This applies to the Budapest Convention on Cybercrime of 2001.
- As the Internet is international, it is important that Iceland's legislation should be compatible with that of its neighbours as far as possible. Legislation must ensure personal data safety and serve as a basis to create an attractive environment for IT companies to operate and develop in.
- Legislation must not contain loopholes that might attract criminal organisations.
- The European Union's strategy on cyber security must be taken into account in Iceland's legislation.
- The use of cloud technology entails various legal implications and challenges. Attention must be given to what other countries, and the EU, are doing in this area and what legal interpretations they follow.
- The reporting of cyber security incidents must be made obligatory. It would be desirable to have this obligation expressed in such a way that entities see it as being in their interest, as well as being obligatory, to report these incidents. For example steps must be taken to avoid the impression that reporting might damage the image or competitive position of a company and that competitors might gain an advantage by staying silent. The arrangement already in place regarding traffic accidents could be used as a frame of reference for this, as appropriate.

15. **Strengthened legislation**
    A review of Icelandic legislation should be made to ensure that it conforms to the country's international obligations and makes it possible to tackle cyber security threats in the same way as is done in other Nordic countries. At the same time, it must be ensured that cyber security threats can be appropriately tackled in the same way as other threats.

Main aim No. 4: Tackling cybercrime

The police should have, or have access to, the professional knowledge, skills and equipment needed to resolve issues concerning cyber security

Issues of various types may arise in connection with law-enforcement and the investigation of cybercrime due to the international nature of the Internet. Questions of national jurisdiction and the increasing use of cloud solutions are relevant examples

The Icelandic police must have the capacity to investigate cybercrime. To ensure that this is the case, sufficient attention must be given to the training of specialists, but also for ordinary police officers, covering how to recognise and respond to offences in this area. The police must have access to experts in Iceland and abroad, as appropriate, not least to the resources of Europol.

Capacity to offer protection against espionage on the Internet and other abnormal data collection must be increased.

The ability to deal with cybercrime is a pre-requisite for Iceland's being able to make the full use of the social and economic opportunities offered by the Internet.

Law-enforcement capacity to tackle cybercrime is one of the factors which companies take into account when choosing a safe operating environment. Having a visible capacity in this area may therefore be of distinct advantage for Iceland.

16. **Tackling cybercrime**
    The ability of the police to tackle cybercrime should be upgraded in the form of skills based on training and awareness-raising, increased domestic and international collaboration and acquisition of the necessary equipment.