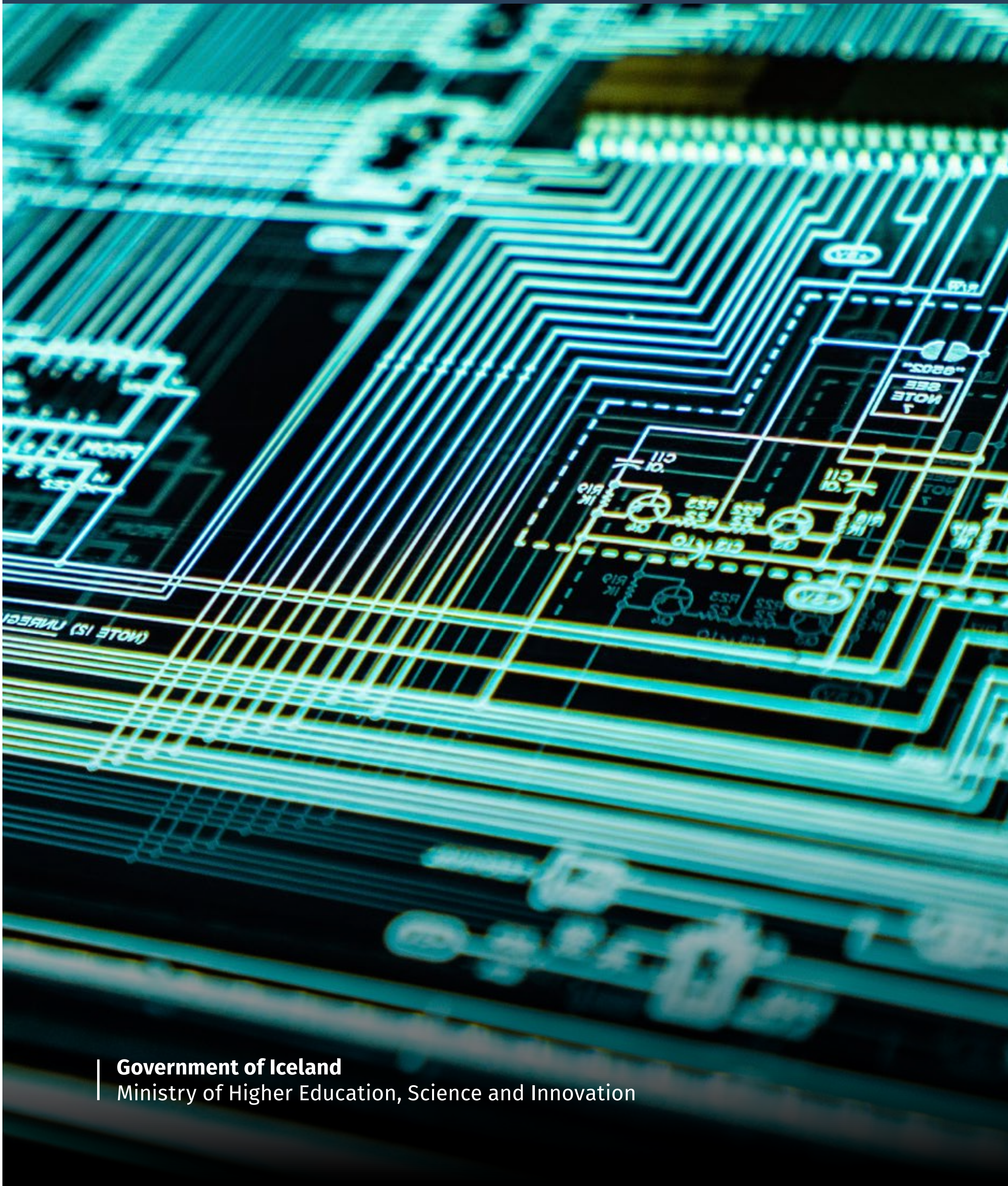
February 2022

Icelandic National Cybersecurity Strategy
2022–2037



Government of Iceland
Ministry of Higher Education, Science and Innovation

Ministry of Higher Education, Science and Innovation
Lindargata 1 – 101 Reykjavík
545 9600 | hvin@hvin.is

February 2022

stjornarradid.is

Table of Contents

1. Introduction

In this National Cybersecurity Strategy, one can find the government's vision and objectives regarding the state of cybersecurity in Icelandic society, along with indicators and emphases related to achieving defined objectives.

This strategy replaces an older strategy from 2015. Open consultation on the draft strategy (White Book) and an evaluation of the state of play in cybersecurity issues (Green Book) took place in the process of developing this strategy. This strategy is endorsed by the Minister pursuant to Act no. 78/2019 on the Cyber and Data Security of Critical Infrastructure. The strategy is also part of the government's Electronic Communications Plan.[1]

With the emphases in mind, the strategy forms a basis for actions in the field of cybersecurity that are presented in a separate action plan. The various ministries and institutions handle the elaboration of actions based on the strategy and their implementation as appropriate. The strategy presents indicators for assessing the success of actions.

The strategy shall be reviewed at intervals of no more than three years, taking into account the level of success based on the strategy's defined indicators.

[1] The cybersecurity strategy was endorsed by the Minister for Transport and Local Government in November 2021. Subsequent to the transfer of cybersecurity issues to the Ministry of Higher Education, Science and Innovation in February 2022, the strategy was reissued. The strategy now covers the years 2022-2037 and has been endorsed by the Minister.

1.1 The Cyberspace

Information technology and a range of digital solutions exist in almost all sectors of society. Widely, in our daily activities, information technology has come to play a crucial role, and a wide range of services depend on its use. However, while society relies increasingly on digital solutions, weaknesses can still be found in the underlying technology. This situation has arisen, not least because of the Internet.

These developments generally bring about better living standards and prosperity, but they can also have negative effects. New opportunities emerge, but so do threats. One could even maintain that it is impossible to achieve the objectives of economic and social gains through the use of digital solutions if actions to respond to cybersecurity threats are excluded from the equation.

The Internet offers great opportunities for Icelandic society. Emphasis on cybersecurity is a fundamental prerequisite for utilising these opportunities. This emphasis demands active participation and cooperation among the public administration, industry and the public. Cybersecurity issues encompass the whole of society, which makes it important to harness the power of all concerned. When dealing with cybersecurity, one must adopt cross-discipline values and consider diversity and inclusion for those concerned, e.g., regarding education, gender, age and cultural background.

Cybersecurity has developed from being a technological issue to a cross-discipline issue requiring extensive cooperation. International cooperation is a prerequisite for progress in this field, and many opportunities for advancements demand the use of foreign experts in Iceland to keep abreast of international trends. Emphasis on cybersecurity not only returns less likelihood of damage but also provides opportunities for advancement, such as in cybersecurity technology and cybersecurity service, which is a fast-growing sector abroad.

Successful implementation of cybersecurity actions by the authorities will lead to improved cybersecurity status in the country and increased public cybersecurity awareness and opportunities to participate in offering services in this field.

1.2 Key Dimensions

1. COMPETENCE AND CAPABILITIES

Competence and capabilities must be augmented by strengthening awareness, education, research and development. The capabilities of the authorities and industry to combat cyber-attacks and to minimise damage must be strengthened. Both national and international knowledge and opportunities must be used.

2. LAW ENFORCEMENT, SECURITY AND DEFENCE

The legal and regulatory environment must be strengthened at a national level and cross-border level in accordance with international requirements and indicators. Particular attention must be paid to protecting children on the Internet. The manner in which cybersecurity and information security challenges related to security and defence are to be handled must be better defined.

3. ORGANISATION AND COOPERATION

Cooperation within public administration and with industry must be strengthened and formalised so that division of tasks and responsibility is clear. Effective cooperation between official parties in the field of cybersecurity response must be ensured.

2. Cybersecurity

Cybersecurity relates to the security of digital services and solutions and their secure application in cyberspace. Solutions and methodologies in cybersecurity are used to combat *cybersecurity threats*[2] which can become cybersecurity incidents if they are realised.

Cybercrimes are either committed by using the Internet or are directed at the Internet and in a *cyber-attack*, the Internet is used to damage the functionality of computer systems or to enable unauthorised access to them. It must be kept in mind that normal use of digital solutions and the Internet to commit crimes, such as selling illegal products or services, or abuse or bullying, are also considered cybercrimes.

[2] Other threats related to information systems can entail social or economic factors such as discrimination or loss of income through automation of jobs, which is a manifestation of the Fourth Industrial Revolution.

Cybersecurity incidents can also be attributed to people or systems without being a cybercrime, such as through breakdowns, maintenance or mistakes, negligence or misconduct. Cybersecurity incidents can also result from natural events. Cybersecurity incidents can lead to irretrievable damage and considerably weaken trust in digital solutions and the Internet, thus inhibiting positive development and the progress it brings.

To ensure security in the use of digital solutions, measures should be in place to protect the confidentiality of data as appropriate in each instance, to ensure the integrity of data and systems, and the availability of data and systems in the manner intended by owners or responsible parties. Persistent and increased cyber threats are directed at these fundamental factors in the cybersecurity of digital solutions. However, the security of using these solutions can be increased with the appropriate defences, knowledge and behaviour.

When assessing the security of digital solutions, one considers whether the risk inherent in their use is acceptable. On the other hand, one considers resilience, such as whether response time to combat negative consequences of a cybersecurity incident is adequate. The assessment also relates to how quickly a service can be restored, even if the service is provided in a different manner.

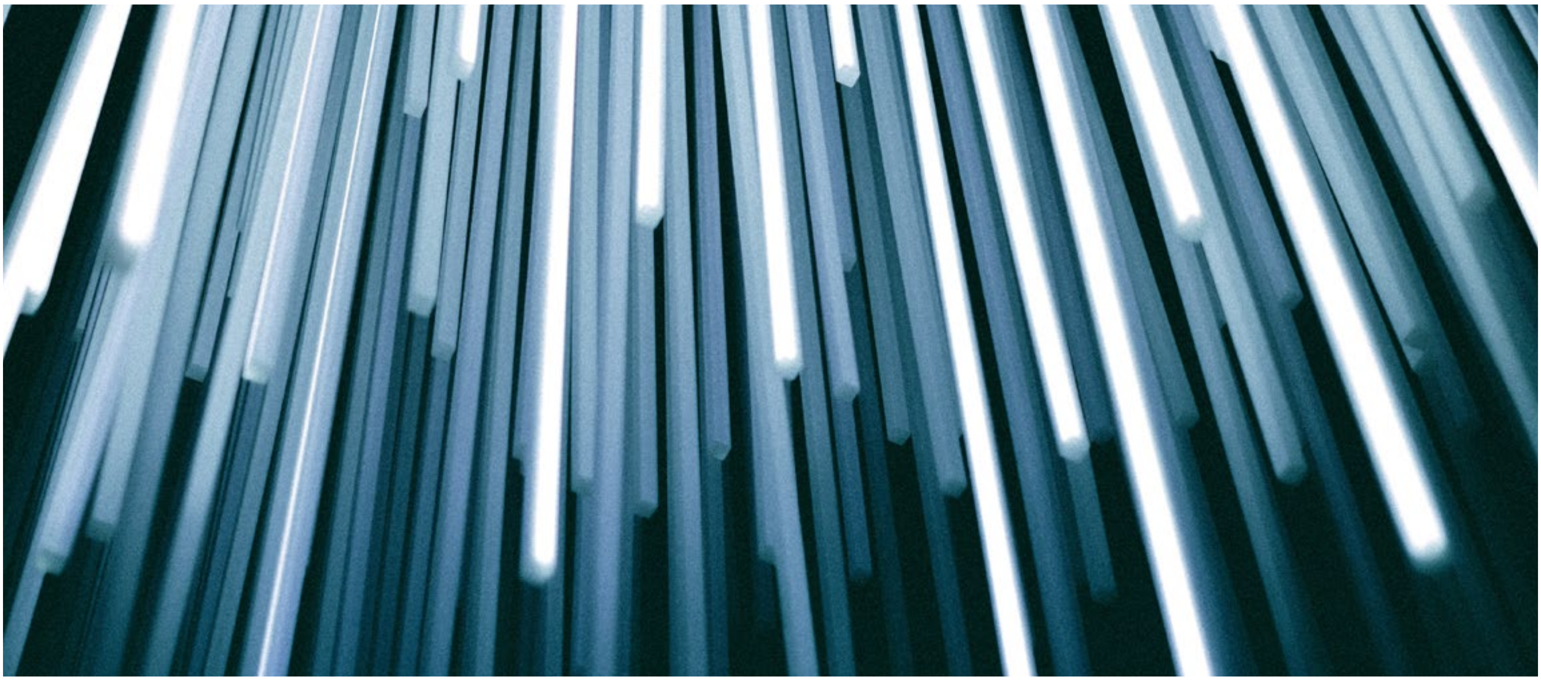
Cybercrime has become a part of organised crime. In this respect, attempts are increasingly made to find and use legal and jurisdictional uncertainty or to create an ethical quandary. Continued technical development will create previously unknown threats that render obsolete and useless those solutions and methods currently in use. In this way, the European Union Agency for Cybersecurity ENISA has defined artificial intelligence and the use of quantum computers as the main cybersecurity challenges for the coming years. Furthermore, increased use of digital solutions for abuse and violence calls for a focus on protecting vulnerable groups, particularly children.

3. Icelandic National Cybersecurity Strategy

3.1 Vision

The vision for Iceland’s cybersecurity is as follows:

Icelanders enjoy security on the Internet based on strong security culture, reliable cybersecurity and law enforcement, active cooperation, national and international, and comprehensive legislation that supports innovation and progress in Internet service.



This means, among other things, that Icelanders should enjoy the most secure environment on the Internet as possible, which they can trust and where human rights and personal data protection are respected, along with freedom of action, economic gains and progress. Secure information technology and secure Internet service shall be essential pillars of prosperity in Iceland, based on robust cooperation and supported by a strong culture of security, active international collaboration and robust legislation. Society is furthermore well prepared to deal with cybercrimes, cyber-attacks, espionage and abuse of personal and business information, both with its capabilities and with international cooperation of cybersecurity teams, the police and security and defence cooperation.

3.2 Objectives

There are two cybersecurity objectives:

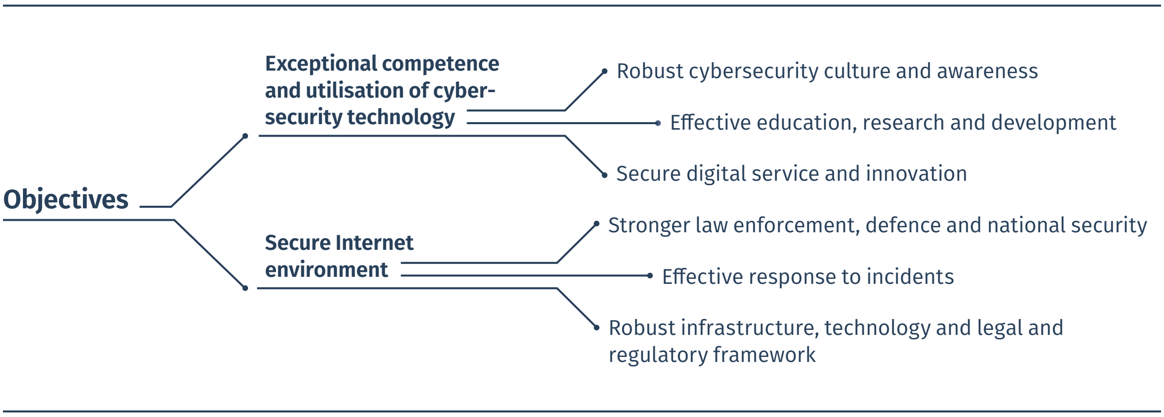
1. EXCEPTIONAL COMPETENCE AND UTILISATION OF CYBERSECURITY TECHNOLOGY

Knowledge and competence will be enhanced with increased emphasis on information to the public, education, research, development and international cooperation. The ability to avoid, respond to and minimise damage from cyber-attacks will be increased with the use of technology, international remedies, and the best available solutions.

2. SECURE INTERNET ENVIRONMENT

Stronger law enforcement on the Internet and a legal and regulatory framework in line with international standards will create trust in responding to inappropriate Internet behaviour. Emphasis will be placed on protecting children on the Internet. Security infrastructure, risk assessment and resilience of critical infrastructures will be strengthened and response capability to threats in the fields of security and defence will be increased.

Each objective is divided into two factors, as shown in the following figure:



Objectives

Exceptional competence and utilisation of cybersecurity technology

- Robust cybersecurity culture and awareness
- Effective education, research and development
- Secure digital service and innovation

Secure Internet environment

- Stronger law enforcement, defence and national security
- Effective response to incidents
- Robust infrastructure, technology and legal and regulatory framework

Results of actions will be measured and assessed against the indicators specified for each objective.

3.2.1 Exceptional Competence and Utilisation of Cybersecurity Technology

Robust cybersecurity culture is based on awareness of risks inherent in the use of the Internet, on risk assessment and prioritisation of actions according to these factors. To build the appropriate competence and utilisation of cybersecurity technology, a key requirement is an access to effective and varied education, which targets differing needs, and there should be active participation in research. This is the basis for innovation and secure utilisation in the future.

Indicators

	Status 2021	Status 2026
Status according to the ITU[3] index on capacity development	60%	>90%
Status assessment according to Oxford Model[4] with respect to basic aspects of the objective	9 of 32 aspects reach at least the stage “Established”	32 of 32 aspects reach at least the stage “Established”

[3] See: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[4] According to the Oxford University model (https://gcscc.ox.ac.uk/the-cmm#/) each aspect of cybersecurity capacity is categorised into five distinct and defined stages of maturity. The medium stage of “Established“ is used here as a reference.

Main Emphases

a Factors that can erode trust in the Internet and the services provided should be combatted.

b Awareness-raising and cybersecurity education programmes will be increased with the emphasis on appropriate education for the most vulnerable groups. News media and social media shall be used in a targeted manner.

c Understanding of the importance of protecting personal data in digital service shall be enhanced.

d Accessible reporting mechanisms shall be available to report cybersecurity crimes.

e Increase the supply and accessibility of appropriate cybersecurity education and training for various groups nationally and in international cooperation.

f Particular attention shall be paid to the needs of small and medium-sized enterprises in both rural and urban areas, among other things keeping in mind ENISA guidelines in this respect.

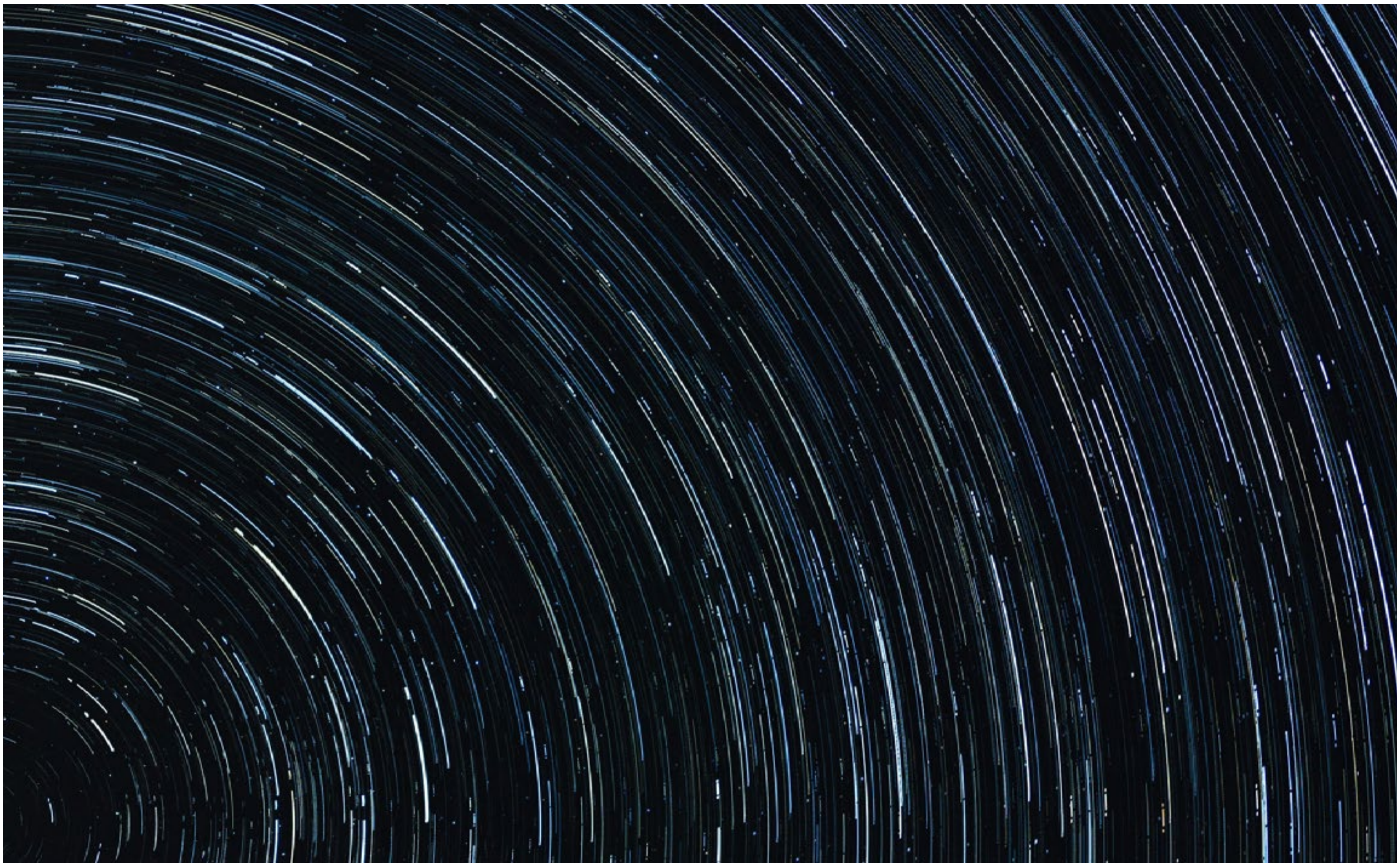
g Research and innovation built on a clear policy will be strengthened, among other things, in international cooperation and international cluster cooperation.

h Software and service shall meet increasing security demands and shall be in accordance with international security standards and criteria. More stringent security requirements shall be made in procurements and development of software and all kinds of services in the field of digital solutions. Guidelines shall be prepared to support this. Clear criteria should be defined for the public sector for procurement, development and service through digital solutions.

i Reliable and secure solutions shall be in place for eIDs and trust services.

j The cybersecurity market for service and hardware shall be strengthened nationally and for export. Cybersecurity service and equipment shall be based on clear criteria and accreditation as appropriate, including with respect to security management.

k Particular attention shall be paid to threats and security challenges inherent in outsourcing and the use of purchased services (including use of cloud services), for example, with respect to jurisdiction, supply chain and ownership.



3.2.2 Secure Cyber Environment

Icelanders rely on a comprehensive cybersecurity infrastructure to be in place, which can efficiently respond to cybersecurity incidents that could threaten national security, critical infrastructures and the rights of individuals. Particular emphasis shall be placed on protecting the vulnerable, particularly children.

The rapid development of cybersecurity issues and the ever-changing landscape require legal and regulatory framework that supports the protection of individuals, the private sector and society as a whole. This is followed up with law enforcement, including appropriate societal cooperation.

Indicators

	Status 2021	Status 2026
Status according to the ITU's[5] index with respect to legal, technical and organisational measures	86%	>90%
Status assessment according to Oxford model[6] with respect to basic factors of the objective	14 of 30 aspects reach at least the stage "Established"	30 of 30 aspects reach at least the stage "Established"

[5] See https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[6] According to the Oxford University model (https://gcscc.ox.ac.uk/the-cmm#/), each aspect of cybersecurity capacity is categorised into five distinct and defined stages of maturity. The medium stage of "Established" is here used as a reference.

Main Emphases

a The legal and regulatory framework fulfils international criteria and expectations, making it possible to tackle abuse and criminal use of the Internet in a manner equivalent to that in our neighbouring countries. This includes an assessment of how well the conditions of the Budapest Convention are fulfilled and that defences against authentication and data theft are present.

b Powerful security organisation is supported based on risk assessment of the appropriate infrastructure and strengthening resilience.

c Security organisation of critical infrastructure reflects best practice with respect to guidelines of the European Union Agency for Cybersecurity, ENISA. Insider threats are also considered.

d Protection of children against abuse on the Internet will be ensured with policy, clear legislation and responsible implementation and monitoring. Other groups that may need additional protection will also be considered similarly.

e Cooperation between law enforcement, the private sector and other stakeholders against cybercrime will be strengthened, as will active participation in international cooperation in this field.

f Monitoring of reliability and resilience will be increased for critical infrastructures and systems of the public and private sectors. The development and operation of management systems for the security of information based on international standards will be encouraged.

g Cybersecurity will be made an appropriate part of civil security and of foreign affairs, security and defence.

h The police, prosecutors, courts and administrative institutions shall have the capacity to deal with offences related to the Internet and the international cooperation this may require.

i Regulatory bodies and response systems shall be capable of responding to serious cybersecurity incidents that can threaten the rights of individuals, critical infrastructures and society as a whole.

j Analysis of cybersecurity threats will be strengthened, and the dissemination of threat assessments shall be organised. Threat assessment shall be published at regular intervals.

k Efficient organisation shall be in place to facilitate responsible notifications of breaches in network and software systems and digital service. The Computer Emergency Response Team (CERT-IS) shall be the point of contact for the dissemination of reliable information on cyber vulnerabilities.

3.3 Cooperation

An important factor, and in fact the prerequisite for achieving the strategy's objectives, is to further strengthen and structure cooperation within public administration, with industry and with the public, with a clear division of roles and responsibility. Active coordination between official players must be ensured. Wide-reaching consultation, coordination and cooperation on cybersecurity creates not only the necessary security of future digital solutions but also the foundation for profitable industry and service.

Main Emphases

a. Cooperation and coordination in cybersecurity-related matters will be strengthened within public administration and the industry, based on a clear division of roles, including issues related to the protection of children and revolutionary new technology, such as the IoT, artificial intelligence and quantum computers.

b. Active coordination between players in public administration shall be ensured with respect to the cybersecurity of their digital services.

c. A platform shall be developed for wide-reaching cooperation between public administration, the private sector and other stakeholders, among other things, issues related to the dissemination of information and roles of various actors. The government and the private sector shall work together, among other things, on advising on matters related to cybersecurity and information security.

d. Emphasis is placed on diversity and inclusion, as cybersecurity is for all, and everyone should be enabled to participate. Particular attention shall be paid to increased participation of women in this respect.

e. Cybersecurity knowledge and culture will be strengthened and made more varied by facilitating the involvement of immigrants with appropriate education, experience and international contact networks.

f. Defences and protective measures shall take into account fluid, international cooperation in the fields of cybersecurity and defence.

g. Coordination with civil protection infrastructure will be increased, among other things, through increased consultation across ministries and institutions, and with industry, through increased cooperation and exercises.

h. Increased participation:

   i. In international cooperation on cybersecurity, including in membership of boards and committees with such cooperation on their agendas.

   ii. In international cooperation on cybersecurity education, in cooperation between universities, such as by receiving foreign teachers to Iceland and encouraging Icelandic students to study cybersecurity abroad.

   iii. In cybersecurity awareness initiatives, including competitions for young people.

   iv. In international research and development projects, among other things, based on cluster cooperation.

3.4 Impact on Icelandic Society

3.4.1 International

Cybersecurity issues have no borders, and Iceland is an active participant in international cooperation, among other things, on education, research, projects and coordination of public administration. Such cooperation will allow Iceland to be among the leaders in securely using digital technology.

Iceland's active participation in international collaborative projects will enable the development of outstanding cybersecurity competence and knowledge. Such competence and knowledge can, among other things, be used in the field of innovation and development of digital service and cybersecurity and increase opportunities for a competitive advantage.

Certain aspects of cybersecurity are part of security and defence in Iceland and they strengthen Icelandic participation in international defence and security operations. With a robust legal and regulatory framework against cybercrime and the ability to respond to them, one can avoid Iceland being considered easy target in the digital world. Iceland's digital reputation will furthermore improve, its competitiveness will increase and make the country a more feasible investment option.

3.4.2 Regional

With increased coordination in cybersecurity between public bodies, municipalities can fully utilise the opportunities of digital technology and simultaneously provide citizens and legal entities with more efficient and improved services, e.g. remote health services, with adequate security regardless of location. With cooperation between municipalities, one can significantly improve the use of limited resources in the field of cybersecurity, which is based on increasingly broad knowledge and experience. Emphasis on small and medium-sized companies across the whole country levels the playing field for companies while simultaneously facilitating e.g. location independent jobs.

3.4.3 Private Sector

Cybersecurity issues are a joint task of the private sector and government, with an emphasis on strengthening the use of digital technology based on a robust cybersecurity foundation. Public trust in digital solutions, and thus their use, is likely to grow with increased cooperation and cybersecurity.

The requirements of the private sector for cutting-edge cybersecurity competence are on a steadily upward trajectory, as they are fundamental to being able to introduce digital solutions in any sector. Variety in education and training in cybersecurity at all levels of education and working life will enable the positive development of knowledge and competence necessary in both Iceland and international competition.

Improvements in law enforcement on the Internet will also open more accessible channels for small and medium companies in urban and rural areas to notify infringements, invoke the law and seek advice.

3.4.4 The Public

Greater cooperation allows society to strengthen cybersecurity development, thus enabling the public to utilise the wide range of opportunities in digital solutions. The role of government is in preventative action and in response in the face of danger. In this manner, public trust will grow in the country’s cybersecurity and digital service. Awareness raising and education can help the public better understand its responsibility when using the Internet. Emphasis on variety and solidarity will direct the focus on the possibility for everyone to enjoy cybersecurity for all and on active participation of all in creating this. Special attention is paid to the needs of specific groups, e.g. children and cooperation with senior citizens. Improvements in law enforcement on the Internet will also open more accessible channels for the public to notify infringements and invoke the law.

Everyone should feel in practice that law and rights are also protected on the Internet.

Government of Iceland
Ministry of Higher Education, Science and Innovation