NORWEGIAN MINISTRIES

Strategy

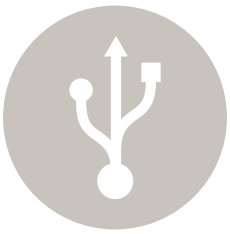
Cyber Security Strategy for Norway

NORWEGIAN MINISTRIES

Strategy

Cyber Security Strategy for Norway

Contents



Foreword

Information and communications technology (ICT) has caused major changes to society over the past decades. There have been significant improvements for individuals, businesses and society as a whole. ICT systems have become increasingly integrated into all aspects of society. People have access to better and more diverse services. Technology is now the foundation for all interaction across sectors, making ICT a strategic security challenge. The infrastructure for these services has become critical for society to function normally.

An increased use of ICT has made society more vulnerable. Threats to ICT systems are on the rise, and attacks are increasingly more sophisticated. Therefore, good preventive information security is increasingly important for national security. By *information security*, we mean that information is protected against unauthorised access, that it is available when needed, and that it is protected against unauthorised changes.

Our networks and systems must be secure and stable at all times. Industry, government and the general public must all feel confident that the digital services our society relies on work. By publishing a national cyber security strategy, the Government is setting the direction and priorities on which public authorities should base their information security efforts. The strategy describes current and future security challenges and points to where we should focus our efforts in order to meet those challenges.

Information security requires transboundary initiatives and encompasses technology, policies, attitudes and culture. This strategy has been developed jointly by the Ministry of Defence, the Ministry of Justice and Public Security, the Ministry of Transport and Communications and the Ministry of Government Administration, Reform and Church Affairs. An advisory group with representatives from the public and private sectors has assisted the ministries in formulating this strategy.

To achieve a comprehensive approach to current challenges, the National Security Authority's 2009 Cyber Security Strategy and related hearings, were used as important background material for this cyber security strategy and accompanying action plan.

ICT is a very dynamic field, and security challenges are constantly changing. Therefore, this cyber security strategy will be revised accordingly.

17 December 2012

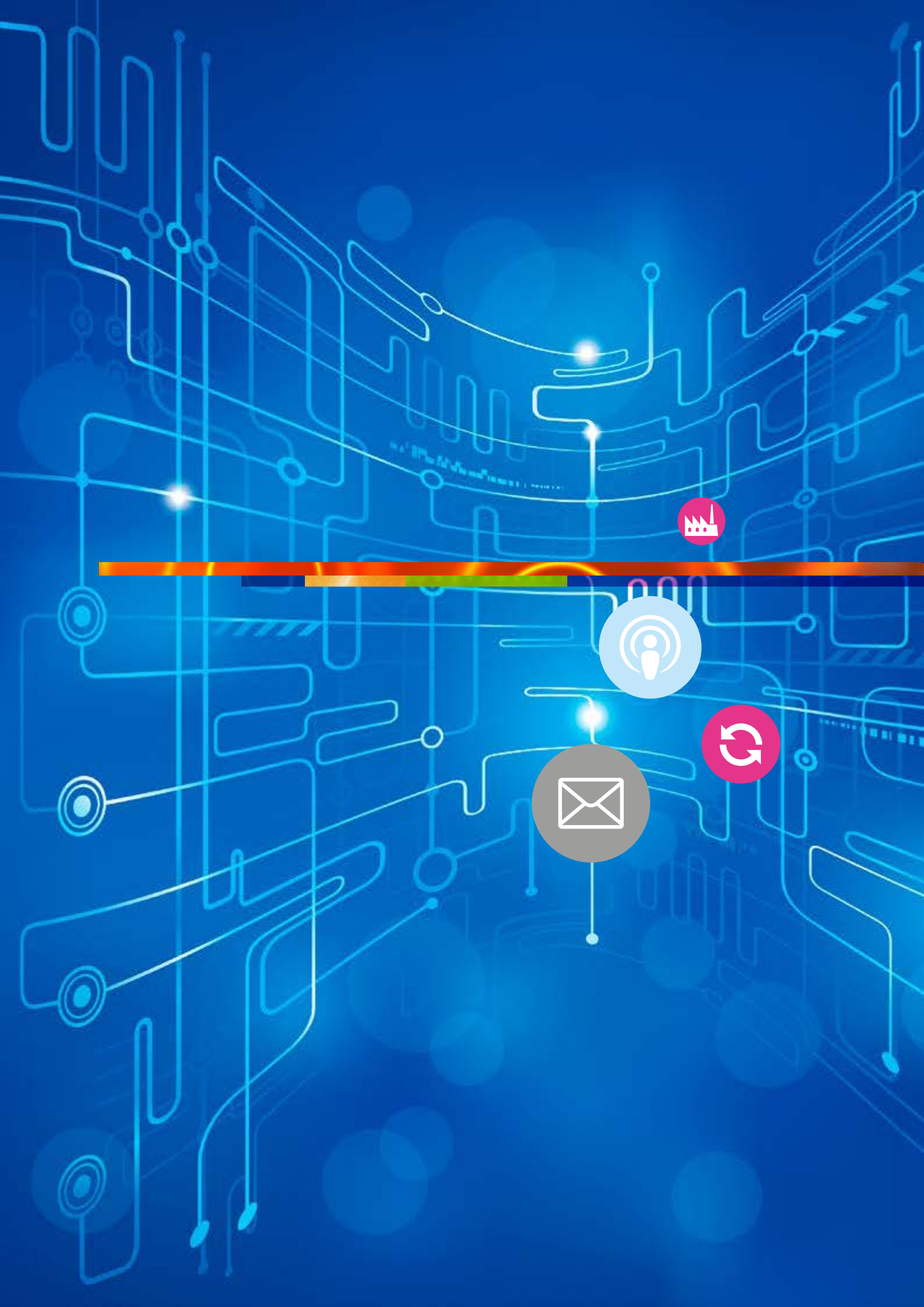
Minister of Justice and Public Security, Grete Faremo
Minister of Defence, Anne-Grete Strøm-Erichsen
Minister of Transport and Communications, Marit Arnstad
Minister of Government Administration, Reform and Church Affairs, Rigmor Aasrud

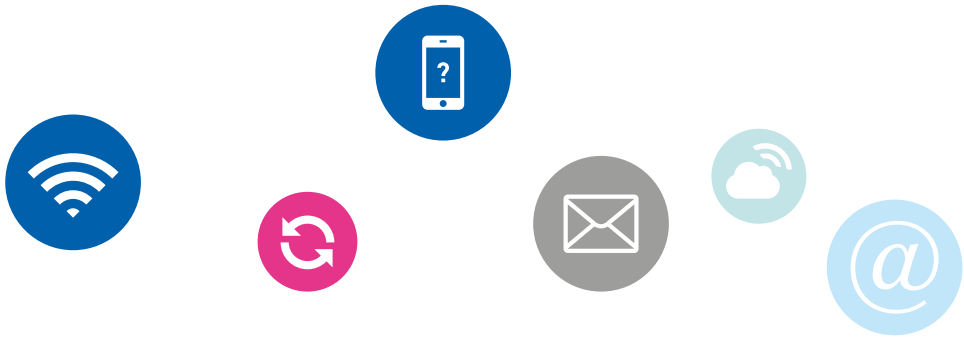
Photo: Torgeir Haugaard

Photo: Torgeir Haugaard

Photo: Olav Heggø

Photo: Johnny Syversen





1 Introduction

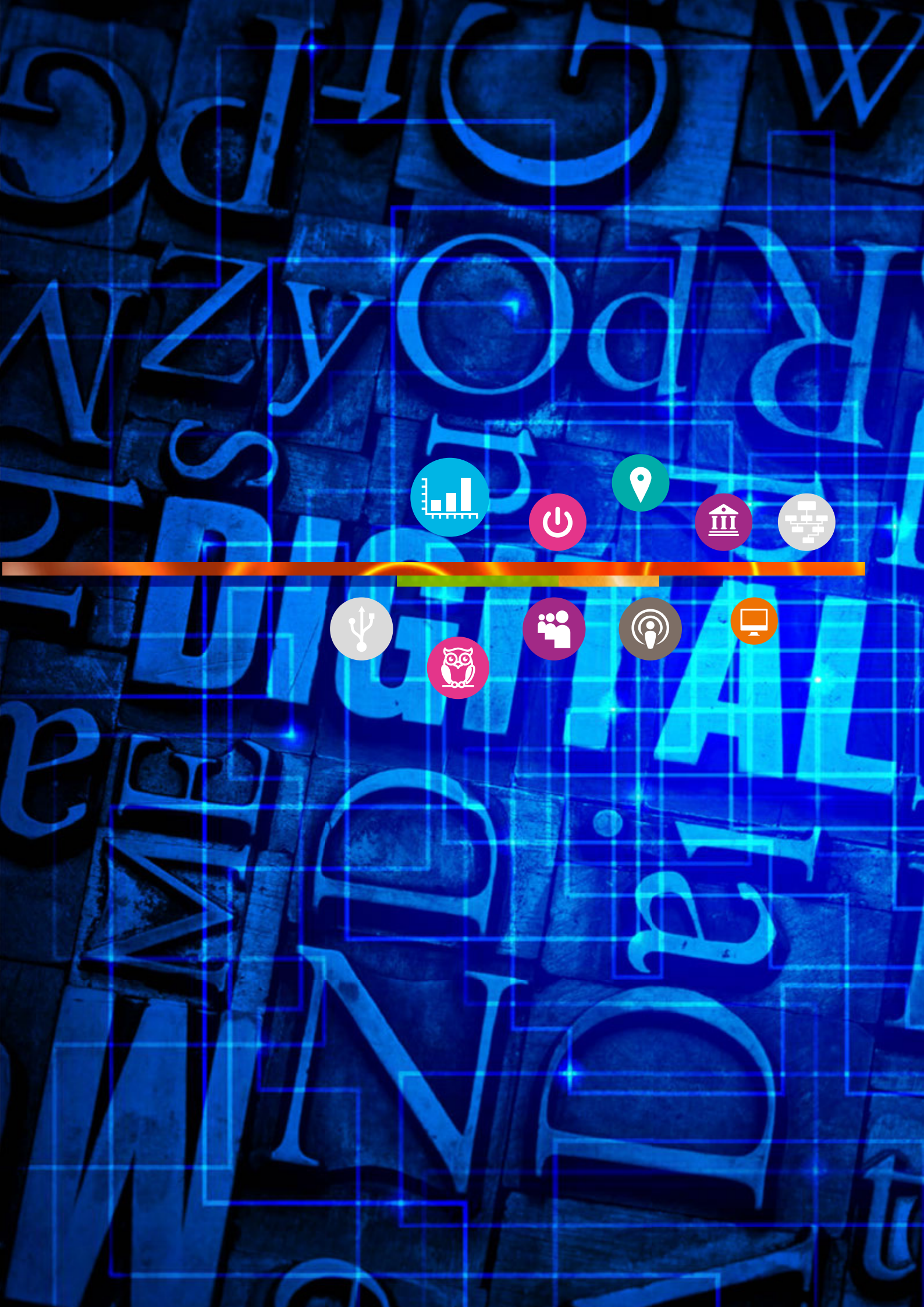
In recent decades, developments in information and communications technology (ICT) have caused significant changes to society. The Internet has brought great social gains to Norway. These gains have been significant for individuals, businesses and society as a whole. ICT systems are increasingly important, integrated into all aspects of society, and critical for society to function normally. Technology is an integral part of our work and everyday life. In many cases, the population is dependent on ICT in order to receive a service. ICT has become the foundation for all interaction across sectors, and can be considered a fundamental social infrastructure.

The increased dissemination of ICT is a natural consequence of these social gains. However, this has also made ICT a strategic security challenge.

Society will continue to develop through more extensive use of ICT. This means that we need to protect information and ensure that our networks and systems are secure and stable at all times. The general public, industry and public administration must all feel confident that digital services are reliable.

The object of ICT security efforts is that Norway should be characterised by:

- All stakeholders are familiar with risks and secure their systems and networks accordingly.
- Public authorities work actively to ensure that national ICT infrastructure is secure, through proper organisation, resource allocation, good general conditions, and effective measures.
- Private and public organisations integrate security and robustness into their information infrastructure to protect their operations and safeguard their customers and users.
- Individuals take the initiative to protect their identity, their privacy and their economic assets online.



Information security is about how to maintain the confidentiality, integrity and availability of information.

Integrity – Ensuring that information and information processing is comprehensive, accurate and valid, and the result of authorised and controlled activities.

Confidentiality – Ensuring that information is not disclosed to unauthorised persons, and that only authorised persons have access.

Availability – Ensuring that a service meets specific stability requirements, so that the information is available when needed.

Integrity, confidentiality, and availability are all important factors when it comes to safeguarding ICT security in society. Individual organisations will weigh these factors differently depending on the scope of their business and the risks they face.

Information security is an ongoing process. What was considered good security yesterday is not necessarily good enough today or tomorrow. To realise the full benefits of information security measures, we must maintain and update technical knowledge and be security conscious. New security challenges emerge as we see developments in technology, the introduction of new products and changing usage patterns.

The Government's primary objective in publishing a national strategy for information security is to set the direction and priorities that will form the basis for the government's information security efforts in the coming years. For each strategic priority, there is a description of objectives for the initiative, a status update and a list of specific areas of focus. How the Government aims to follow up specific aspects of this strategy will be described in a detailed action plan, which will be published separately and revised as necessary. In addition, follow-up of the strategy will aid decision makers in the public and private sectors in particular, and the population in general, in increasing their awareness of the security challenges we face.

1.1 Target Audience

Public authorities play a central role in facilitating and influencing how ICT is developed and applied in society. This is also true for information security. This is achieved in part through the formulation and enforcement of laws and regulations, inspections, sharing information, and through advice and guidance. This national Cyber Security Strategy, with the accompanying action plan, complements and points the direction for further development of existing regulations and measures. The strategy is an expression of the Government's overarching priorities in this area.

The Government has the primary responsibility for public information security efforts. To fulfil this responsibility, authorities must work closely with all relevant stakeholders in the public and private sectors. There are also a number of public bodies with ICT security as a particular responsibility, see Appendix B.

The *ministries* are responsible for ensuring that all relevant stakeholders in the sectors are included in the implementation of measures within the strategy's strategic priorities.

Leaders of counties, municipalities and businesses have a responsibility, in line with their different roles, to follow up information security efforts in their own sector or business. They must, on their own responsibility and initiative, implement measures necessary to support the strategy's strategic priorities.

Beyond this *everyone* has a personal responsibility to help safeguard and strengthen information security in society. Well-functioning everyday security is a basic prerequisite for being able to handle more serious incidents effectively.

1.2 Background

The challenges related to information security are not new. They have been discussed and dealt with by changing governments for decades and include the administration of personal information, as well as the protection of state secrets and critical infrastructure. A lot of work has been done both in the public and private sectors to follow up various reports and recommendations.

The Vulnerability Committee's report, NOU 2000:24 *The Vulnerable Society,* determined that ICT systems had become one of the pillars of society, and that society had become more vulnerable to their failure. In this context, the committee emphasised conveying the significance of ICT vulnerability as part of society's overall vulnerability. The committee suggested a number of measures to mitigate security challenges, including the development of a national strategy to reduce ICT vulnerability.

The Vulnerability Committee's work laid important groundwork for St.meld. no. 17 (2001–2002) *Security for Society. The Road to a Less Vulnerable Society.* This white paper included an overview of a number of recommended measures to reduce ICT vulnerability.

In 2004, the Infrastructure Committee initiated a study of the need for securing critical national infrastructure. The committee's recommendations were presented in NOU 2006:6 *When Security is Crucial*. The Infrastructure Committee's recommendations were reviewed and followed up in St.meld. no. 22 (2007–2008) *Security for Society*. This white paper supports and describes the national CERT function (Computer Emergency Response Team).

St.meld. no. 29 (2011–2012) *Security for Society* determined that new developments, including the Internet, more mobile services, new service platforms and a greater use of offshoring, have made ICT a strategic security challenge. These developments place high demands on awareness and competence, and reinforce the need for cooperation and coordination across different sectors of society.

The first national strategy for information security was issued in June 2003 and was a joint publication by the Ministry of Trade and Industry, the Ministry of Defence and the Ministry of Justice and Public Security. During the strategy period of 2003–2006, several concrete measures and activities were executed. Protection of critical ICT infrastructure was prioritised. During that period, organisation of security efforts was also improved. This strategy was followed by the release of *National Guidelines for Improving Information Security 2007–2010*.

2 Security Challenges and Trends

ICT security challenges encompass all levels of society, from protecting individual mobile phones to safeguarding essential systems for critical societal functions.

Some of the challenges and trends that characterise the current situation include:

Internet and mobile devices. The increased use of the Internet and new computer systems, industrial control systems, mobile phones, memory sticks, social media, and tablets has made us more efficient, but also more vulnerable.

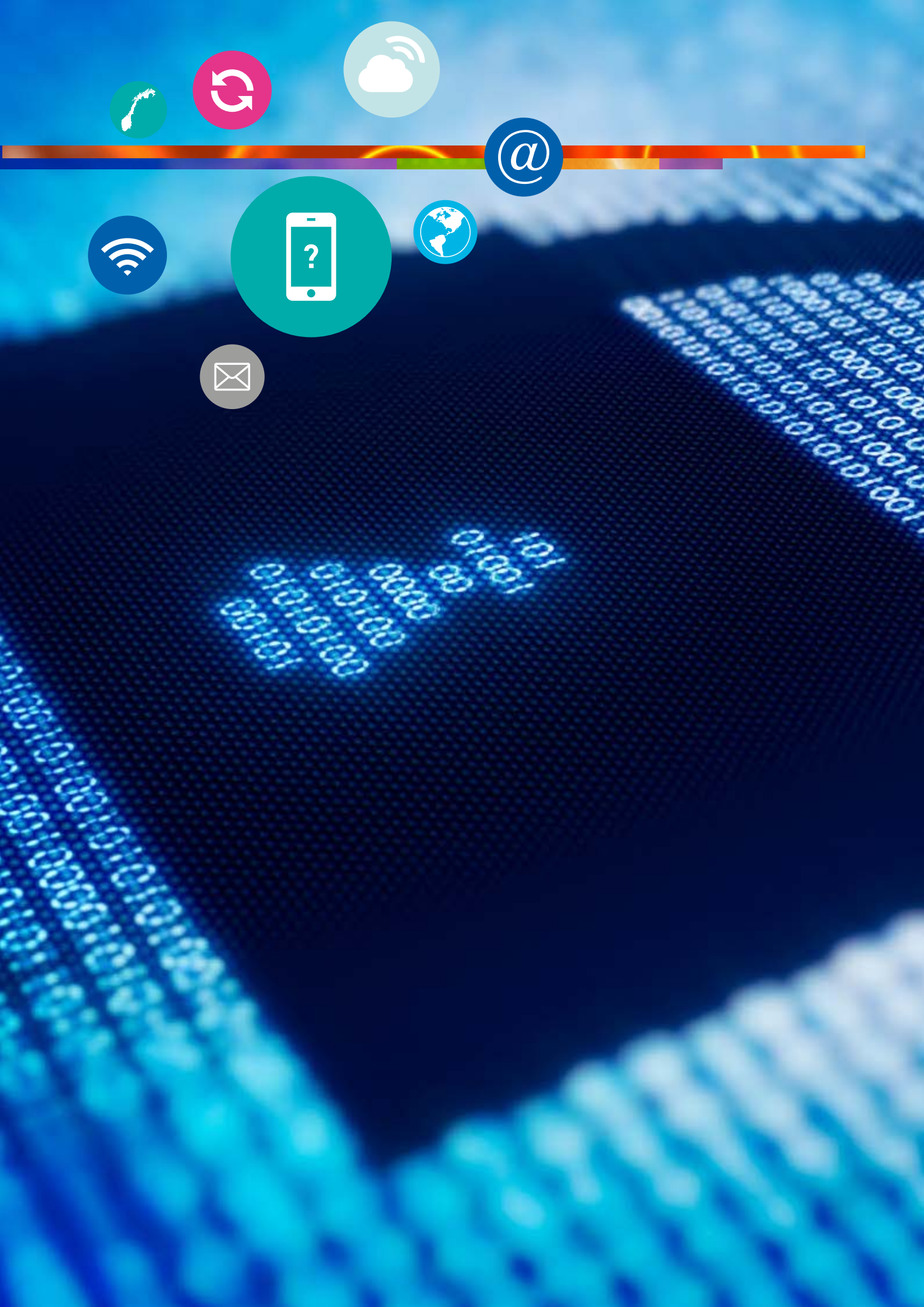
Downtime is increasingly critical. Society has become more vulnerable to even short interruptions to systems and networks, increasing the importance of having a secure and robust ICT infrastructure.

New service platforms and lack of clarity. The increased use of new types of service platforms, such as online and cloud computing means less transparent solutions and can make it more difficult for users to assess risk and vulnerability, and document their own security.

Increased use of offshoring. Norwegian companies are increasingly outsourcing operational and systems development tasks to suppliers located in other countries and on other continents, resulting in a number of security and emergency challenges. For example, local operating conditions and other national regulations and practices may differ from Norwegian ICT security requirements or regulations for privacy and personal information. The lack of transparancy also makes it difficult for Norwegian authorities to carry out inspections and control activities

A market for crime. The Internet and mobile devices have led to a greater risk of being exposed to cyber crime. Today, there is an underground market, easily accessible over the Internet, for buying and selling information and trading tools for cyber crime. Criminals are exploiting this opportunity more and more.

Espionage and sabotage – a growing threat. The trend toward targeted and professional hacking of critical ICT systems is increasing. Targeted espionage attacks against vital national security interests now constitute a significant challenge. Civil services, military units and private companies are all vulnerable to espionage and sabotage. Many countries are developing capabilies for espionage and warfare against critical infrastructure. We must assume that sophisticated sabotage and attacks will be directed against critical information resources, including the computer systems that control industrial processes and critical infrastructure.
Major requirements for awareness and competence.



New services and devices place great demands on the competence of ordinary users. It is difficult for owners of critical infrastructure to have sufficient awareness and knowledge of vulnerabilities, interdependencies between infrastructure components, and what individual businesses must do to protect their infrastructure.

Increased complexity. Most companies currently have a system portfolio that is far more complex than just a few years ago. ICT is now part of almost all new products and systems, and it is taken for granted that they will interact seamlessly with other systems and across organisations and sectors. It is a challenge to keep track of all the interdependencies and potential vulnerabilities. The increasing complexity of systems and networks has also made it more difficult for procurers of ICT systems to set clear and precise security requirements.

Disloyal employees. Internal vandalism, theft or misuse of the organisation's ICT resources by its own employees can be difficult to detect. This is partly because many businesses have bad or poor operating and administrative procedures, or that management is not entirely aware of what system privileges their employees actually have. Internal attacks against a computer network can also be harder to detect than external attacks.

Privacy and identity abuse. Personal privacy is also threatened by new methods of communication and ways to use information systems and the Internet. Identity abuse is a growing challenge for individuals, businesses and public authorities.

International attention. Information security is an area that many countries and international organisations emphasise as increasingly important for economic growth, societal security and national and international security policies. Many countries have developed their own cyber security strategies and guidelines. Each country's reciprocal commitment to the community and to political alliances is a significant focus in this context.

Information security weaknesses. The Office of the Auditor General has revealed major weaknesses in cyber security in public administration in Document 1 (2010–2011). In the *Report on Security 2011*, The Norwegian National Security Authority asserts that crucial national ICT systems in many cases are insufficiently protected, and that threats to the organisations are on the rise.

The Computer Crime Study of 2012 indicates that the gap between threats and security measures taken by both public an private organisations is increasing in parallel with an increase in their dependency on ICT.

Security challenges and trends are described in more detail in the Government's information security action plan.

3 Roles and Responsibilities of Ministries for Information Security

Company Responsibility

ICT security is primarily a responsibility at the company level. This follows the Principle of Responsibility, in that whoever is responsible for an organisation under normal conditions is also responsible in a crisis situation. In practice, this means that responsibility lies with the owner of the organisation, be it in the private or public sector.

More comprehensive national ICT security measures are planned and implemented in a close collaboration between the authorities and the individual business. The state of national security is the sum of all security initiatives taking place in businesses, in each sector and at a national level. A good culture of security in the organisation will reduce the chance that employees are the weakest link in our security barriers.

Responsibilities of Sectoral Ministries

The primary responsibility for safeguarding security in each sector's ICT infrastructure, and for ensuring adequate preventive measures for information security, lies with the sectoral ministries. This means that each sectoral ministry has a responsibility to:

- Identifying critical infrastructure in their sector, and ensuring adequate security
- Assess, determine and implement preventive measures in their sector
- Plan emergency measures with respect to various crisis situations
- Plan for and, if necessary, initiate crisis management in their sector
- Supervise and monitor information security efforts in their suborinate departments.

In practice, most of these tasks will be executed by the departments or their subordinate departments because they are the ones most familiar with their dependence on key information systems and infrastructure.

Ministries with Special Responsibility for ICT Security

Based on the above allocation of responsibility, most of the ICT security work is done in the individual sectors, and primarily in the individual organisations. Beyond this, some ministries have a specific role related to ICT security.

The Ministry of Justice and Public Security is responsible for coordinating civilian security. Besides initiating, developing and implementing measures through its own channels, the ministry is a driver and coordinator for other sectorial authorities. The Ministry of Justice and Public Security shall assume and develop responsibility for society's information security.

The Ministry of Government Administration, Reform and Church Affairs is responsible for coordinating the Government's ICT policy. The ministry is also responsible for promoting a stronger and more comprehensive approach to information security in public administration.

The Ministry of Defence is responsible for cyber security in the military sector. The Ministry of Defence has ministerial responsibility for the National Security Authority, and administrative responsibility for the Security Act.

The Ministry of Defence is responsible for cyber security in the military sector. The Ministry of Defence has ministerial responsibility for the National Security Authority, and administrative responsibility for the Security Act.

The Ministry of Transport and Communications is responsible for ICT security in electronic communications networks and services, including Internet. The electronic communications sector is regulated by the Electronic Communications Act and its regulations. The Post and Telecommunications Authority, a government agency under the Ministry of Transport and Communications, has a special responsibility for security and emergency preparedness for electronic communication networks and services.

Although information security is primarily an organisation and sector responsibility, our increasingly networked society demands a comprehensive approach. ICT infrastructure and security challenges cut across established businesses and sectors. Effective protection of ICT infrastructure will require good coordination between public authorities, business and individual users.

4 Overarching Goals and Strategic Priorities

This strategy mainly addresses the challenges that we as a society must work together to solve. Based on the security challenges and trends discussed in Chapter 2 of this strategy, the Government has identified four overarching goals for information security:

1. Better coordination and common situational understanding
2. Robust and secure ICT infrastructure for everyone
3. Good ability to handle adverse ICT events
4. High level of competence and security awareness

None of these overarching information security goals is more important than another, and are mutually dependent success factors.

These overarching goals will be operationalised through seven strategic priorities:

- Ensure a more comprehensive and systematic approach to information security
- Improve ICT infrastructure
- Ensure a common approach to information security in public administration
- Safeguard society's ability to detect, alert and handle serious ICT incidents
- Safeguard society's ability to prevent, detect and investigate cyber crime
- Continuous efforts to raise awareness and competence
- High quality national research and development in the field of information security

This strategy also contains a brief status report and indicates specific areas that should be emphasised in the future. Processes for further clarification of strategic priorities and the implementation of specific measures are described in chapter 5 of this strategy. How the Government will follow up this strategy through specific measures will be described in an action plan, which will be published separately and revised as necessary.

4.1 A More Comprehensive and Systematic Approach to Information Security

Private and public organisations shall safeguard information security *comprehensively and systematically*. This entails a conscious use of information security management systems (ISMS) as a part of corporate governance. Recognised standards must be applied. Requirements must be tailored to the risk facing the individual organisation. The nature, size and social significance of the organisation will dictate its level of ambition and allocation of resources to security efforts.

Several regulations require organisations to have an information security management system, e.g. Electronic Public Administration Regulations, which apply to the entire public sector. Regulations relating to the Personal Data Act apply to both the private and public sector. In addition, the Security Act applies to the entire public sector and parts of the private sector. Several regulations state that security efforts must be tailored to the risk. Thus, it is crucial that public administration conduct good risk and vulnerability assessments. The Data Protection Authority, National Security Authority and Office of the Auditor General have revealed weaknesses in risk assessments conducted by public administration. They point out that existing security measures are often unsystematic, fragmented, and that information security efforts neither have enough support from management nor are they well integrated into business management. An increased use of international security standards in public administration could contribute to more comprehensive and systematic security efforts.

Increased use of certified ICT products and systems may also help boost confidence in and improve the security of public sector systems and services in Norway.

The following must be an area of focus:

- All departments and state-owned companies must have an information security management system. This management system must be based on recognised security standards. The system's scope and level of detail must be tailored to the scope and nature of each organisation and the risk it faces. Local governments and private companies should be encouraged to establish similar management systems.

4.2 Improving ICT Infrastructure

ICT infrastructure that supports critical societal functions must be robust and reliable so that adverse events and actions are avoided to the greatest extent possible. The power grid and electronic communications networks need particular attention. One primary objective is to require all stakeholders in the public and private sector to adhere to clear requirements and provide them with appropriate advice and guidance to enable them to procure and administrate electronic communications services with an adequate level of security based on the risk facing the individual organisation. The same requirements should apply to owners of businesses with important societal functions.

Technological developments entail that ICT infrastructure is constantly changing. Parts of it will be renewed continuously. The traditional telephone network for voice communications is being replaced by electronic communications networks used for all kinds of services. It is therefore difficult to label certain parts of ICT infrastructure as critical and other parts as less critical for national security.

It is important to emphasise that there are many electronic communications networks. Users who are dependent on electronic communication must be able to use alternative communication solutions if necessary. Users must have sufficient expertise to choose appropriate solutions and ensure that they receive the level of quality and reliability that they require from their service providers. This means that organisations need to have good user guidelines.

To ensure increased redundancy and a more robust infrastructure, security must be weighed against environmental and economic considerations when planning and developing infrastructure. Environmental and economic considerations are often important when establishing an infrastructure, for example, several companies using the same route for installing cables, many companies sharing a communications mast, and the co-location of technical equipment for several companies. Experience shows that this can be at the expense of security. On the other hand, security measures for one type of infrastructure can help safeguard other infrastructure along the same route. For example, securing a road against landslides can also help protect cables that run along the same route.

The implementation of changes to the the Security Act's asset security regulations is an important tool for identifying critical societal functions and revealing mutual dependencies. This will strengthen national ICT and societal security.

Selected areas of focus include:

- Sectoral authorities must set requirements for the operational continuity of systems that are crucial for society.
- Security measures for physical infrastructure must be coordinated across sectors so that different measures work together and do not conflict with each other.
- There should be regular drills for situations where infrastructure has partially reduced capacity or drops out.
- Sectoral ministries must verify that the sector's organisations identify and propose ICT functions and systems that can be classified as critical societal functions, in line with asset security regulations.

4.3 A Common Approach to Information Security in Public Administration

Digital communication should be the norm for communication with and within public administration. Our citizens, industry and public administration must be confident that electronic services in the public sector, as well as sectoral systems and online services, are secure and reliable. Therefore, we must establish comprehensive national solutions for secure communication and access to services. These kinds of national solutions include ID-porten and government issued electronic IDs (eID) at a high level. In addition to security benefits, a centralised approach will also entail financial savings in the form of more unified development and operation of these systems. The public authorities must clarify which general legal, organisational and technical security requirements apply to ministries and their subordinate organisations, key infrastructure owners and owners of classified ICT systems for use in public administration. A common approach to information security will also put more pressure on arriving at a common way to express risk, potential harm, and security level for public administration. Risk and vulnerability analyses should form the basis for all implementation of ICT security in public administration.

There are many regulations for information security, and various departments have regulatory responsibilities. Currently, there is not one set of common minimum standards for the public sector with regard to security procedures and technical measures for individual organisations, or for owners of critical infrastructure. This may contribute to business systems not being compatible, or that organisations do not have confidence in each other's security levels, such that they cannot communicate and share information securely. Since there is such a large number of networks serving the public sector, it is difficult to establish secure, comprehensive solutions for the flow of information between ministries and between ministries and directorates. In addition, such fragmented solutions do not facilitate a satisfactory level of security.

Ministries and directorates need to communicate highly classified information with each other, both in daily work and in various crisis situations. Practical experience has revealed challenges related to the ability of ministries to both administrate and communicate such information. Evaluations of various drills also indicate that there is a lack of joint systems in public administration for communicating sensitive, confidential and classified information.

Several ministries and their departments have called for a common set of requirements for public sector security. There have been attempts to coordinate regulations, but they have proven difficult. Regulation administrators and other regulatory bodies, such as the Agency for Public Management and eGovernment (Difi), has done much work in this area, but the efforts have not been sufficiently coordinated. There is also a need to secure electronic communication between government agencies on the one hand and citizens and businesses on the other hand.

Selected areas of focus include:

- Public authorities must clarify the general legal, organisational and technical security requirements that apply to ministries and their departments, key infrastructure owners and owners of classified ICT systems in the public sector. These requirements must be the basis of all exchange of information in public administration. They should also include general requirements for suppliers of ICT products and systems to the public sector.

- Public organisations should be able to securely send and receive documents electronically, such that the confidentiality, integrity and authenticity can be guaranteed.

- The need for specific systems and solutions to secure existing and new sectoral systems in public administration must be reduced to a minimum.

- Ministries must have ICT solutions that make it possible to store, manage and communicate sensitive and classified electronic information across ministries. These solutions must be compatible with corresponding systems in the defence sector.

4.4 Safeguard Society's Ability to Detect, Alert and Handle Serious ICT Incidents

Norway must be in a constant state of proactive operational preparedness in order to prevent, detect and coordinate reactions to serious ICT incidents. In this context, relevant authorities and organisations must work in close collaboration, with special emphasis on working with those parts of the private sector that own or operate infrastructure. This collaboration must address both intentional and unintentional events, such as technical or human error, accidents, or natural disasters.

In this context, serious ICT incidents include: targeted attacks against critical ICT infrastructure and sensitive, confidential and classified information. Together, the large volume of minor incidents can also have serious consequences (such as leaks of sensitive business information or loss of confidential or sensitive information). Currently, not all organisations know what to do if they have a major ICT incident, or do not have the necessary routines and detection mechanisms in place to prevent, detect, alert and manage ICT incidents. There is great variation in terms of what incidents are recorded and reported to national authorities. In many cases, measures that make ICT systems more robust and reduce the impact of incidents, regardless of the cause, will be common for all organisations. It would be economically beneficial if such measures were coordinated. Organisations that are subject to the Security Act, are required to report to the National Security Authority if they detect incidents that threaten security, but this is not enough to get a comprehensive overview of the situation.

The Norwegian Computer Emergency Response Team (NorCERT) in the National Security Authority, with the help of the Early Warning System for Digital Infrastructure (VDI) and a national collaboration, have the ability to prevent, detect and analyse data related to serious incidents on the Internet. NorCERT works closely with other countries and similar services in international organisations. NorCERT also participates in a Nordic CERT collaboration. Some key sectors of society have established sectoral response teams in close contact with NorCERT and businesses in their sector, or are in the process of doing so (for example, the defence, health and welfare, and justice sectors). Their sectoral expertise improves our overall ability to handle incidents, and also ensures that the responsibility of sectoral authorities is safeguarded. More and more individual organisations are establishing internal response teams or outsourcing such services. NorCERT is jointly financed by public and private funds.

For incidents affecting electronic communications, such as software errors, loss or interruption of Internet services, mobile phone services or other electronic communication services, there are routines in place for network providers to notify the Post and Telecommunications Authority.

Selected areas of focus include:

- There must be ICT alert teams with the basic capacity to coordinate and manage ICT incidents for all sectors (such as a sectoral CSIRT), and for the most important organisations that support critical societal functions. These alert teams should be structured such that they take into consideration the use, architecture and governance of ICT infrastructure in the sector.

- The national CERT function (NorCERT) must actively collect and analyse information related to serious ICT incidents. NorCERT shall have the national responsibility for coordinating the management of such incidents and provide relevant and timely information and guidance to sectoral response teams and response teams in organisations that manage ICT infrastructure that is critical or important for societal functions.

- Cooperation with the private sector must be expanded and improved. NorCERT must analyse and communicate relevant risk information in an appropriate and responsible manner to those who are responsible for taking action, whether it be companies, sectoral authorities, the police, other public authorities or at the political level.

- Preparedness for dealing with malicious incidents (crime, espionage, sabotage, and terrorism)

should be coordinated at all levels, with adequate preparedness for handling random events caused by failures, accidents, the weather, and natural disasters.

- Notification and management procedures for faults, failures and loss of electronic communication must be improved. The Post and Telecommunications Authority and NorCERT must establish procedures for the prompt and effective exchange of information about adverse events.

- Companies and sectors must plan and conduct drills designed to improve their ability to manage incidents. Furthermore, collaboration across sectors and international boundaries must also be drilled.

4.5 Safeguard society's ability to prevent, detect and investigate cyber crime

Cyber criminals should not be able to plan or execute crimes without a significant risk of being detected and prosecuted. Society's ability to prevent, detect and investigate cyber crime must be prioritised. All stakeholders should, on their own initiative, implement crime prevention measures in their own organisations, and seek to minimise losses or damage as a result of cyber crime. Public authorities shall achieve this through increased expertise, and improving specialist expertise and the skills of police generalists. The police must make this a priority and increase their capacity to give them a greater ability to prevent, detect and investigate cyber crime. Public authorities will continue to increase their capacity in this field in order to detect cyber crime that directly or indirectly may have an impact on national security or vital national interests.

Cyber crime includes crime aimed at computer systems and networks, and crime in which key elements of the chain of events are committed using computers or computer networks. There is no clear division between the two. Hackers often have a goal of gaining access to information that could be used to commit traditional crimes at a later time. In recent years, cyber crime has evolved from "troublesome pranks" to serious organised crime. Criminals are also increasingly using new technology to commit traditional crimes.

Some crimes may have consequences that may require infrastructure providers, sectoral authorities or companies themselves to implement crisis management (e.g. with assistance from NorCERT or sectoral CSIRT).

There is a need for information retrieval over the Internet and securing electronic leads during a crisis. The police must also investigate what (and who) caused the criminal offense that triggered the crisis.

Criminals purchase tools for conducting various crimes over the Internet, such as software that can take control of other computers. Threat assessments and experience indicate that organised crime in particular employs the most modern computer tools to hide their activity from the police and impede investigations. All trend reports point to an expected increase in cyber crime as a result of technological developments in general and the increase in mobile devices such as mobile phones and computers in particular.

Police are largely dependent on tips or complaints from the public to detect cyber crime. It is a challenge that for certain types of cyber crime there is a gap between public perception of what is right and wrong and the relevant regulations. Copyright infringement and peer-to-peer file sharing is one example of this challenge.

The Norwegian Business Security Council's cyber crime survey for 2012 indicates that the gap between threats and security measures taken by both public and private organisations is increasing. At the same time, there is an increase in their dependency on ICT. Norwegian companies, especially at the executive level, lack knowledge about information security and do not have an overview of threats and incidents. In many cases, companies will not be aware that their server/network identity has been compromised. In addition, companies experience that the police don't have the capacity to prioritise cyber crime other than in very serious cases.

Prevention, detection, investigation and legal prosecution of cyber crime is challenging. This work is often time consuming and requires specialised expertise and tools. In addition, there are often considerable challenges in identifying the criminal/source. There are currently few police units with the necessary expertise for this type of investigation in Norway, as evidenced by the relatively low number of convictions related to cyber crime. The danger is that applicable legislation could lose its general and individual preventive effect, since the chances of being convicted are perceived as small.

Selected areas of focus include:

- All stakeholders must take initiative to help prevent and mitigate losses or damage resulting from cyber crime and identity theft and abuse.
- The police must have sufficient expertise and capacity to detect, identify and deal with cyber crime.
- Police must be present on the Internet, both openly and covertly, in order to prevent, avert and, when necessary, investigate and try to bring this type of crime to justice.
- There must be clear procedures for collaboration and sharing knowledge both within the police, and between the police, government agencies and key security environments.

4.6 Continuous Efforts to Raise Awareness and Competence

Our citizens, staff and executives in Norwegian companies must be security conscious and increase their information security skills. Everyone should have access to information about security challenges and countermeasures. Everyone should understand that measures must be taken. Companies must have the necessary procurement expertise for purchasing new ICT tools and services, employing external consultants or outsourcing services. CIO's must have adequate knowledge of ICT security, vulnerabilities and the need for redundancy in conjunction with the acquisition and operation of ICT systems. All children and young people should have basic information security skills.

Security incidents happen daily. In some cases, they have significant consequences for individuals or for society as a whole. Established activities organised by the Centre for Information Security (NorSIS), the Business Security Council, the Norwegian Data Protection Authority, the Post and Telecommunications Authority and the Media Authority an increasing need for awareness and education. Data can be lost, abused and manipulated without it being the result of a deliberate attack. There has also been an increase in targeted attacks, and attackers increasingly exploit end-users in order to achieve their ends. This suggests that the focus on education, skills and awareness must increase.

Authorities responsible for security and emergency preparedness are responsible for collecting and communicating information about threats on national and macro level. There are also many organisations in the public and private sectors striving to improve the general public's security skills. These organisations collaborate on various levels, working with various segments of the population. This work could be improved with an increased coordination of activities. The goal of this coordination is to give everyone access to the same information about threats and measures for reducing the likelihood of attacks being successful.

Selected areas of focus include:

- Public authorities and business associations should have joint or coordinated programmes for building awareness, training and developing a culture of cyber security. Government participation in relevant networks will ensure good exchange of information both nationally and internationally.

- All owners and suppliers of components for critical ICT infrastructure in the public and private sector should be invited to share information in public forums.

- Public authorities should survey the level of competence of the general population and businesses. The effect of initiatives must be measured to determine their effectiveness or if efforts can be improved.

4.7 High quality national cyber security research and development

Norwegian researchers should be at the forefront of numerous aspects of information and communication security, such as robustness and reliability, risk management, encryption technology, distributed systems and the law. This should be in close collaboration with universities and colleges, with industry and other user groups and the Research Council of Norway. Norwegian participation in international forums should be encouraged.

Research related to information and communication security is being conducted at a number of institutions in Norway. ICT security is also a key priority in the Research Council of Norway's large-scale ICT programme – VERDIKT (Core Competence and Value Creation in ICT) – which started in 2005 and will run throught 2014.

ICT security is also a priority in EU research programmes (including the Seventh Framework Programme for Research and Technological Development and Horizon 2020). The EU's research and innovation budget will trigger coordinated efforts by member states and countries participating through separate agreements, including Norway.

Selected areas of focus include:

- Information security research must maintain a high international level, and be quick to snap up changes in technology, infrastructure, and methods. Allocation of funding should be based on international cooperation and close collaboration between academia, infrastructure owners, relevant user groups, and the authorities. ICT security should also be integrated with other relevant research programmes. Information security should be a priority field in the Research Council of Norway's portfolio.

- All stakeholders should strive to facilitate productive interaction between both basic and applied research groups, and leading ICT companies and academic environments across sectors. The public and private sectors should facilitate opportunities for students of information security at the master's level or higher to work with current relevant security issues within a sector, or a single business, by proposing topics with concrete applications for master's and doctoral theses in information security.

- Public authorities should employ R & D groups actively in its role as customer of various products, development projects and services. Public authorities should facilitate information sharing with the research community.

- Norwegian cyber security researchers and affected businesses in the public and private sector should be encouraged to participate actively in projects within the various EU research programmes and other international research programmes of national interest.

5 Responsibility for Implementation

Although information security is first and foremost a company responsibility, a successful follow-up of this strategy requires effective collaboration between private sector stakeholders, central and local authorities, and individual users. ICT development is on a global level and extensive international collaboration on information security is an essential prerequisite for the success of information security efforts. At the same time, we must also address purely national interests in this area.

Each sectoral ministry must – in line with the Principle of Responsibility – ensure that the strategy's priorities are followed up in their sector. This follow-up must be in accordance with a nationally adopted action plan. In this regard, ministries must work closely with subordinate organisations and sector stakeholders so that planned security measures are coordinated with other ministries as necessary. Each ministry should actively involve stakeholders in the private sector as they develop initiatives for the action plan. Ministries must establish whether measures initiated in their sector contribute to achieving the goals formulated as strategic priorities.

The Ministry of Justice and Public Security will be primarily responsible for following up the strategy.

As old security problems are solved, new ones arise as a result of the introduction of new technology, changes in use patterns, and changes in the threats. Consequently, security measures that are appropriate today may be outdated tomorrow. The Government has therefore decided to develop an overarching strategy, and describe areas of focus rather than specific security measures. A detailed action plan describing how the strategy's priorities should be followed up will be developed and published separately and revised as necessary. Sectoral ministries should include sector stakeholders during the development and implementation of action plan initiatives.

Specific measures in various priority areas should be initiated as part of the work on the ministries' annual allocation letters to subsidiaries. These letters define goals and priorities for the coming year. Measures affecting the private sector should be implemented in close collaboration with private sector bodies. Measures affecting consumers should be implemented in collaboration with consumer organisations. Prior to implementing new measures, a privacy impact assessment should be conducted and, if necessary, the Norwegian Data Protection Authority should be involved in planning and implementation.

To assess the current status during follow-up of the strategy's priority areas, the Government will regularly request a status update for sectoral implementations of action plan initiatives, in order to monitor developments in information security. The Ministry of Justice and Public Security is responsible for this work. An inter-ministerial group will be appointed to monitor the strategy continuously over the long-term. The group's work will include following developments in security challenges and trends, and assessing whether those developments will trigger a need to revise all or part of the national strategy on an ongoing basis. The group will also be a driver for updating and developing the action plan further.

6 Economic and Administrative Implications

Primary responsibility for securing information systems and networks lies with the owner or operator, and is management's responsibility. Security work must be a daily routine and financed within the framework of the normal operations. Each sectoral ministry has a sectoral responsibility. Sectoral initiatives must be funded within current budget frameworks. The cost of measures to promote information security must be proportionate to the estimated risk to individual areas of public administration. If risk mitigation measures are not implemented, the risk of unfortunate consequences and losses must be considered.

Appendix A:
Terms and Expressions

Accessibility	Assurance that a service meets certain requirements for stability, such that the information is available when needed.
CERT	Computer Emergency Response Team. A team of experts that handles security incidents. CERT is a registered trademark of Carnegie Mellon University. Many therefore use the abbreviation C(S)IRT; Computer (Security) Incident Response Team.
Cloud computing (cloud services)	A collective term for services provided over the Internet and which are set up to work with other services. A designation for everything from data processing and storage to software on servers in remote server farms connected to the Internet.
Confidentiality	Assurance that specific information is not disclosed to unauthorised persons, and that only authorised persons have access.
Critical ICT infrastructure	Critical ICT infrastructure is defined as critical infrastructure for electronic communications. See also ICT infrastructure.
Critical infrastructure	Society's functional ability is highly dependent on a number of physical and technical infrastructures. In the event of a failure in these infrastructures, society will be unable to maintain the supply of goods and services on which the population depends (cf. critical societal functions). These infrastructures can be described as critical to society.
Critical societal functions	Functions that fulfil society's basic needs and people's sense of security, e.g. banking and financial services, health services, etc. See also critical infrastructure.
CSIRT	Computer Security Incident Response Team (CSIRT) is a group of experts who handle ICT security incidents.
Cyber security	Protection of data and systems connected to the Internet.
ECOMM network	An ECOMM network is an electronic communications network.
ICT infrastructure	Electronic systems that process data or communicate with other equipment, on which a unit or organisation is dependent to function effectively.
ICT security	How business-critical electronic networks and systems that process data or communicate with each other are protected.
ICT systems	See Information systems.
Information security	Protection of the confidentiality, integrity and availability of information.

Information security management system	A management system and guide for organisations with regard to information security. May include tools such as: • Information security handbook • Risk and vulnerability analysis • Compliance audits • Emergency plans • E-learning about information security for the entire organisation
Information systems	System for collecting, storing, processing, transmitting and presenting data.
Infrastructure	The basic structures and systems* necessary for an organisation, a collection of organisations, or a country to function effectively. *structures and systems: "Technical installations and equipment, and related administrative and organisational measures."
Integrity	Assurance that information and information processing is comprehensive, accurate and valid, and the result of authorised and controlled activities.
Sensitive information	Used in this strategy as a collective term for information that must be protected for various reasons, cf. Personal Data Act, Freedom of Information Act, Public Administration Act, Security Act, etc.
Threat	An entity that constitutes a real or potential threat to an identifiable goal or in a limited and identifiable context.
Vulnerability	The challenges a system will have to face to function when subjected to an adverse event, and challenges related to resuming normal system operation after the event has occurred. The vulnerability of a system is an expression of its weaknesses and flaws and special circumstances that would increase the likelihood that threats will materialise into a security incident (examples of special circumstances can include size, complexity, that many stakeholders are involved, geographical distribution, frequent changes, and exposed location). A system's vulnerability is reduced by increasing the system's robustness.

Appendix B:
Selected National Contacts for Information Security

The Norwegian National Security Authority (NSM)
The central directorate for the protection of information and infrastructure crucial for critical societal functions.
– Protects information, information systems and other assets against espionage, sabotage, and terrorism through inspections in accordance with the Security Act; develops security initiatives; provides advice and guidance; detects and manages countermeasures for serious cyber attacks (see NorCERT). Driving force for improving security conditions.
www.nsm.stat.no

NorCERT – the national centre for notification of and countermeasure coordination for serious cyber attacks and other ICT security incidents targeting important ICT infrastructure for critical societal functions.
www.cert.no

The Norwegian Post and Telecommunications Authority (PT)
Monitors companies providing electronic communications services, electronic communications networks and postal services, and issuers of official eSignature certificates. PT shall contribute to secure and robust networks and services.
www.npt.no

Nettvett.no – A web site run by PT providing information, advice and guidance about safe Internet use. Information is aimed at both consumers and small and medium sized companies.
www.nettvett.no

The Norwegian Centre for Information Security (NorSIS)
A resource centre created through an initiative by the Ministry of Government Administration, Reform and Church Affairs. The centre offers consultancy services for information security for all Norwegian private and public entities. All levels of society should be able to take advantage of these services. NorSIS also runs the web site *slettmeg.no* which gives advice to those who feel offended online.
www.norsis.no
www.slettmeg.no

Norwegian Directorate for Civil Protection (DSB)
Driver, advisor and coordinator for preventive and crisis measures nationally, regionally and locally. Capacity and aid supplier to support higher authorities and all other authorities in the event of major emergencies or when needed.
www.dsb.no
www.kriseinfo.no

Kripos (National Criminal Investigation Service)
The national service for combating organised and other serious crime. The main objective of Kripos is to combat organised and other serious crime.
www.politiet.no/kripos

Norwegian Intelligence Service (NIS)
Responsible for detecting and analyzing external threats and the motives, capabilities and methods of foreign actors, cf. the Norwegian Intelligence Service Act. The objective of intelligence activities is to contribute to counteract threats and to provide Norwegian authorities with a solid basis for foreign, security and defense policy decisions.

Norwegian Police Security Service (PST)
Responsible for the nation's internal security.
Prevents and investigates crimes that threaten national security, including collecting information on individuals and groups who may pose a threat, developing various analyses and threat assessments, investigations and other operational countermeasures and advice.
www.pst.politiet.no

The Norwegian Data Protection Authority (DT)
The Norwegian Data Protection Authority oversees a number of laws and regulations, where information security is an important part of the regulation. The overall regulatory framework affects much of the public and private sectors. The Norwegian Data Protection Authority has developed a number of guidelines on information security and provides guidance on compliance with legislated requirements.
www.datatilsynet.no

Published by:
The Ministry of Government Administration, Reform and Church Affairs

Public institutions can order additional copies from:
Government Administration Services
Internet: www.publikasjoner.dep.no
E-mail: publikasjonsbestilling@dss.dep.no
Tel.: +47 22 24 20 00

Publication code: P-0976
Design: Melkeveien Designkontor AS
Photo: ©Fotolia.com
Printed by: Norwegian Government Administration Services
04/2013 - impression 500