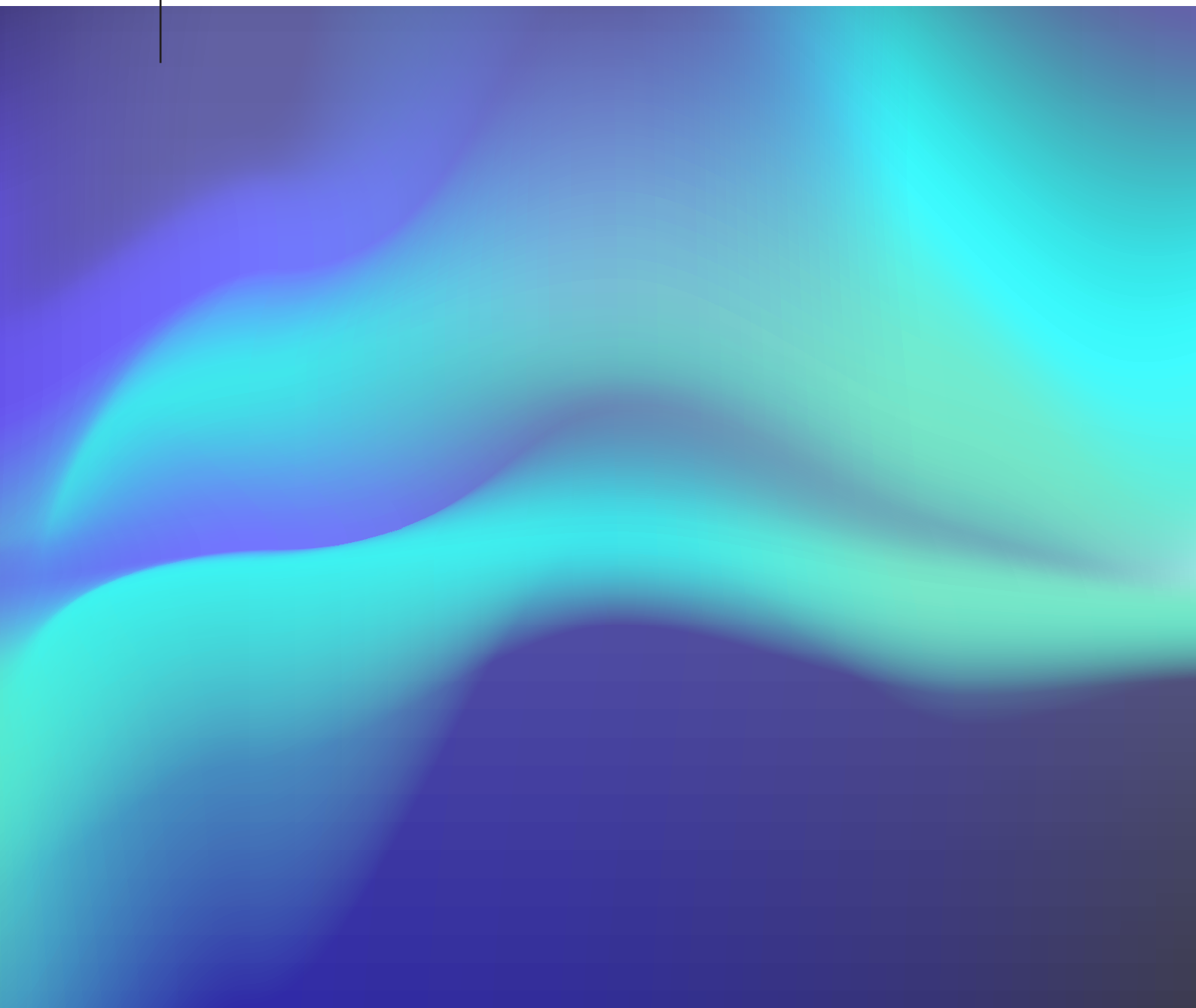
List of measures – National Cyber Security Strategy for Norway



Contents

1. Introduction

The National Cyber Security Strategy was launched by the Norwegian government in January 2019. The strategy sets out goals for five prioritised areas. The strategy is backed by this two-part list of measures, where part 1 describes key measures that support the strategy, and part 2 lists ten basic measures that both public and private companies are recommended to implement. The measures listed in part 2 of this document are provided to increase companies' own ability to protect themselves against and handle cyber incidents.

1.1. Report and follow-up on the list of measures

The Norwegian Ministry of Justice and Public Security (JD) and the Norwegian Ministry of Defence (FD) have overall responsibility for following up on the strategy. Each ministry must ensure that the strategy's priorities and the list of measures are followed up in their own sector. In this regard, ministries must work closely with government agencies and sector stakeholders so that planned cyber security measures are coordinated with other ministries as necessary.

Each ministry should actively involve affected stakeholders in the private sector in the preparation of measures. Ministries must establish whether measures initiated in their own sector sufficiently contribute to achieving the goals from the strategy.

In connection with follow-up by the ministries, it is expected that the importance of cyber security is communicated to the government agencies. It would be beneficial to make this an integral part of the governing of subordinate agencies.

This list of measures is published separately and is to be revised as necessary. It is presumed that measures which affect the business community will be implemented in close collaboration with the business community's own bodies. It is presumed that measures which affect consumers will be implemented in collaboration with consumer organisations. Prior to implementing new measures, an evaluation of how the measure in question will affect privacy should always be conducted and, if necessary, privacy protection authorities should be involved in the planning and implementation.

To track the status in following up the strategy's priorities, JD and FD will monitor the development in the area of cyber security by requesting status updates from ministries concerning their work to follow up on the strategy. Status reports will be collected approximately two years after the launch of the strategy.

Follow-up on the strategy will also be carried out by the use of an interministerial group, and through a public-private partnership forum. These groups will, for example, track development regarding security challenges and trends, and continuously determine whether this triggers a need to revise (fully or in part) the contents of the national strategy and, correspondingly, the list of measures.

2. PART 1 – Key measures for improved cyber security

2.1. Selected measures that support several of the strategic priorities

Measure 1: National technical security measures – a major national security package

Cyber attacks are becoming increasingly sophisticated. New technologies, increased use of encryption and complex infrastructures all mean that we have to think in new directions in order to maintain our national detection ability. The use of artificial intelligence, machine learning and a high degree of automated processes are becoming critical factors that must be utilised. The "P2950" project is to run over the coming years and has been accorded a considerable budget. As a part of the project, new sensor technology is to be developed for use in measures such as the Early warning system for digital infrastructure (*Varslingssystem for digital infrastruktur* – VDI). The project is to establish increased technical capacity for introducing artificial intelligence and machine learning. The project is also to establish both classified and unclassified automatic sharing platforms, mobile capacities and dynamic data collection and analysis.

Measure 1.1: New sensor for the early warning system for digital infrastructure (VDI)
For a period of almost 20 years, the current VDI solution has maintained our capacity to identify targeted cyber attacks without compromising privacy. A larger distribution of VDI sensors among owners of infrastructure and functions critical to society will significantly boost the national detection capacity. It is necessary to develop new sensor technology that is to build on and replace the current VDI sensors. The next generation VDI sensors are to allow the support of classified signatures and indicators.

Responsibility: FD and the Norwegian National Security Authority (NSM)
Implementation: 2018-2021

Measure 1.2: Next generation detection capacity
New national detection capacity is to be developed, which will apply artificial intelligence and machine learning to collected data. The platform that is to be developed will allow automatic malware analysis and automatic sharing of findings.

Responsibility: FD and NSM
Implementation: 2018-2021

Measure 1.3: Allvis NOR, mapping and vulnerability analysis
"Allvis NOR" is a service NSM provides to improve cyber security among public sector companies and owners of critical infrastructure. The service primarily consists of regular mapping and vulnerability analysis of selected IP addresses that are exposed to the internet. Information about vulnerable services is then shared with system owners. The service is to be developed and upscaled so that it can detect more vulnerabilities at more companies.

Responsibility: NSM
Implementation: 2018-2021

Measure 1.4: DNS service for the public sector
NSM currently provides a DNS service for selected companies. Using this service makes it possible to stop traffic to specific websites. The DNS service is to be developed, upscaled and made available to the public sector.

Responsibility: NSM
Implementation: 2018-2021

Measure 1.5: Secure email service for the ministries
Email is the preferred means of digital communication among Norwegian companies in the public and private sectors, even though new technology opens up other methods for communicating electronically. The vast majority of cyber incidents targeted at nationally critical digital infrastructure start with a fraudulent email. A number of improvements to the email standard exist today. Several of these improvements are intended to limit the scope for receiving fraudulent email. A shared service for receiving emails and analysis of unwanted emails is to be established for the ministries.

Responsibility: FD
Implementation: 2019

Measure 2: National strategy for cyber security competence

The national strategy for cyber security competence (2019) is to influence direction and content, as well as highlighting responsibility for measures in the fields of education and research. Moreover, the strategy encompasses measures intended to raise awareness among the general public, local authorities and the business community. The strategy is part of an ongoing process to develop measures for improved cyber security competence in partnership with the authorities, public and private companies, the education sector and research institutions.

The current long-term plan for research and higher education sets out guidelines for stronger research input in the field of cyber security. Conditions will be established to reinforce cooperation to place more emphasis on cyber security as a part of study programmes in the fields of technology and engineering.

In the national strategy for cyber security competence, particular emphasis is placed on having an adequate knowledge basis for sufficient cyber security competence. JD will ensure access to updated statistics and analyses to keep track of the cyber security competence gap. Furthermore, conditions will be established for an improved knowledge basis as regards to security culture for the general public and for companies. Priority areas in this field are planned to be accorded more than 800 million NOK. This budget does

not include the places on technology related study programmes that have been assigned over the past three years, and which have included strong elements of cyber security. The investments that derive from the revised Long-term plan for research and higher education are not included in this budget either.

Responsibility: JD and the Norwegian Ministry of Education and Research (KD)
Implementation: 2019

Measure 3: National cyber security centre

NSM is planning to establish a National cyber security centre. The centre will build on previously decided and established measures, basing its framework on a structure similar to those used in other influential countries with equivalent centres. The centre represents a reinforcement of the work NSM is already doing. The intention is for the centre to underpin cooperation between the various cyber security communities, such that the different governmental agencies operate in a common threat landscape and have a common situational awareness. The establishment is a key measure to increase private-public partnership in the area of cyber security. In order to ensure clear division of roles and responsibilities, it is important to establish good cooperation between the National cyber security centre and the NC3 centre (see Measure 4) for the best possible utilization of cyber security resources. The cyber security committee's recommendations (see Measure 6) may be of relevance for the future development of the centre.

Responsibility: FD, JD and NSM
Implementation: Start-up 2018

Measure 4: NC3 (The police national cyber crime centre)

In 2018, the National Police Directorate (POD) started establishing a national cyber crime centre (NC3) under the National Criminal Investigation Service (Kripos), following the example of many other countries. NC3 will serve as an expert body designed to improve the ability of the police to prevent and combat cyber crime.

JD will ensure that POD takes a comprehensive approach, where the competence and capacity at NC3 are incorporated into POD's consolidated management and oversight of police competence and capacity.

Responsibility: POD and JD
Implementation: Start-up in 2018

Measure 5: Secure digitalisation in the public sector

In 2018, the Agency for Public Management and eGovernment (Difi) evaluated the work with information security in public administration. The findings revealed a need to continue strengthening the work on management and control of information security in these organisations. In addition, it was revealed that in their governing of subordinate agencies, all ministries need to improve their following up on the security work in subordinate governmental agencies.

- Difi's work with the management and control of information security is to be expanded to include both the public administration and the local authorities, because the challenges that exist at public administration level also apply to the local authorities.
- Public sector companies are to establish a better coordinated and more encompassing range of measures regarding guidance in cyber security.
- Difi is to continue developing its role in the context of recommendations and guidance in this area.
- The approach government agencies take to managing cyber security is to be adapted to match significance and risk. Working with the Norwegian Government Agency for Financial Management (DFØ), Difi is to provide guidance to the ministries to help them follow up appropriately on the area of cyber security.
- Difi's work in this area is also to be aligned with the authorities affected, with particular emphasis on NSM and the Norwegian Data Protection Authority.
- The Norwegian Directorate for Civil Protection (DSB) will prepare and teach courses in planning and conducting exercises for public sector companies. Difi contribute to this work by developing exercises in cyber security.
- The recommendations from the evaluation in 2018 will be followed up in a collaboration between Difi, DFØ, DSB, NorSIS and NSM.

Responsibility: The Ministry of Local Government and Modernisation (KMD) and Difi
Implementation: 2019-2024

2.2. Preventive cyber security

The following section presents key measures designed to support the goal of helping Norwegian companies to digitalise in a secure and trustworthy manner, and to improve their ability to protect themselves against cyber incidents.

Measure 6: Cyber security committee

The cyber security committee was appointed in council on September 15th 2017. The committee was to assess whether the current cyber security regulations are appropriate and whether an appropriate division and organisation of cross-sectoral responsibility is applied at government agency level. The committee also had a mandate to suggest specific legal and organisational changes. The committee delivered its report to JD on December 3rd 2018. The committee's NOU was sent for public consultation in December 2018 and JD will then consider further follow-up.

Responsibility: JD
Implementation: 2019

Measure 7: Follow-up of the white paper on cyber security and the committee on digital vulnerability

The Committee on Digital Vulnerabilities in Society presented several recommendations for reducing digital vulnerabilities in society. White Paper No. 38 (2016-2017) "*Cyber security – a joint responsibility*" provides a status report on the follow-up on the committee's recommendations. JD will continue to use this status report to follow up on the ministries regarding their ongoing work with cyber security. A new report on the status of the follow-up will be prepared in 2019.

Responsibility: JD
Implementation: 2019

Measure 8: National recommendations and consultancy

Measure 8.1: National recommendations and consultancy activities under the auspices of NSM

NSM is to continue development of national recommendations and make these available through websites, courses and other consultancy activities. The recommendations are to be prepared on the basis of experience from operative units, actual incidents, the threat landscape, research and development in the field of technology, as well as the exchange of experience with national and international actors in the public and private sector.

Responsibility: NSM
Implementation: Ongoing

Measure 8.2: NSM Cyber Security Principles

NSM's Cyber Security Principles define a set of principles and underlying measures to protect ICT systems (hardware, software and associated infrastructure), data and services they offer against unauthorized access, harm or abuse. The product will be updated regularly based on input from users and relevant stakeholders from the public and private sectors.

Responsibility: NSM
Implementation: Ongoing

Measure 8.3: National cyber security risk assessment

The report entitled *Comprehensive Cyber Security Risk Assessment*, which is published annually by NSM, is to help generate a common snapshot that allows companies and authorities to adopt appropriate risk mitigation measures. The report is also to serve as a tool for companies to use in their risk assessment work. The report is to be evaluated and developed further.

Responsibility: NSM
Implementation: Annually

Measure 8.4: Research and development activities under the auspices of NSM
The rapid development of technology, changed usage pattern and a modified threat landscape translate into increased risk of unwanted cyber incidents, and result in a greater need for research and development to produce effective preventive security measures. Cyber security is one of the prioritised areas in NSM's R&D activities. NSM is to carry out research and contribute to the development of preventive measures, including cryptography and security in virtual systems.

Responsibility: NSM
Implementation: Ongoing

Measure 8.5: Difi's centre of expertise and guidance material – security in ICT procurement
Difi is to further develop its centre of expertise and guidance resources linked to the acquisition of unclassified ICT procurement. Guidance related to the acquisition of cloud services and outsourcing of ICT targeted at the public administration will be given priority. This includes security and risk assessments. NSM and Difi are to work together on how best to ensure a comprehensive approach to guidance on cyber security, including on procurement and outsourcing of ICT.

Responsibility: Difi and NSM
Implementation: Ongoing

Measure 8.6: NorSIS (Norwegian Center for Information Security)
NorSIS receives an annual operating grant from JD, and is part of the government's initiative on cyber security. NorSIS contributes to the strategic goals for the work on cyber security, though improving both companies' and private individuals' knowledge on cyber security, as well as activities intended to reinforce this. The goal of the grant to NorSIS is to make society more robust in its defence against cyber incidents. The grant is to be used to reach the target group of Norwegian companies in the private and public sectors, including the municipal sector. Priority is to be given to small and medium-sized companies. NorSIS is also to contribute with advice and guidance to the general public.

Responsibility: JD and NorSIS
Implementation: Ongoing

Measure 8.7: Nettvett.no
The nettvett.no service was launched in 2005, and its purpose is to help build up a security culture among consumers, key stakeholders and companies by functioning as a portal that provides information to consumers and small and medium-sized companies regarding safe use of the internet. Since 2017, a cooperation centred around the service has existed: NorSIS holds editorial responsibility and runs the site on behalf of NSM and the Norwegian Communications Authority (Nkom), and is to contribute to a better, more coordinated information sharing to the target group.

Responsibility: NorSIS, with support from NSM and Nkom
Implementation: Ongoing

Measure 8.8: Slettmeg.no
The slettmeg.no service is a free service for advice and guidance for those who experience violations online. The service is run by NorSIS. To ensure guidance to the population about risk related to online activity and behavior, the Slettmeg.no service should be further developed.

Responsibility: NorSIS
Implementation: Ongoing

Measure 9: Public-private partnership forum

In 2018, the Norwegian government set up a partnership forum (the "National Cyber Security Forum"), which comprises representatives from the authorities, the business community, stakeholder and sector organisations, and academia. The parties represent companies that either own or manage critical digital infrastructure or critical societal functions, or which play key roles in research and education.

The purpose of the forum is to ensure that strategic issues linked to cyber security challenges and international collaboration are discussed between private companies and public authorities. The forum is to promote openness, trust and interaction between public and private operators with regard to sharing information and discussing problem issues related to cyber security. The forum establishes a new cooperation among the authorities at ministerial level and between selected companies, and it is to be assessed following a start-up period, to ensure the arena functions as intended.

Responsibility: JD
Implementation: 3-4 meetings annually, to be evaluated before 2020

Measure 10: Interministerial network

The "National Cyber Security Network" is to ensure that strategic issues linked to cyber security challenges are discussed and coordinated between the ministries. For 2018, the network has been further developed to reinforce public-private, civilian-military and international cooperation related to cyber security. The network is to be assessed before 2020 to ensure the arena functions as intended.

Responsibility: JD
Implementation: Meets 3-4 times annually, to be evaluated before 2020

Measure 11: Interaction arena for key supervisory authorities

NSM has been tasked with establishing and leading an arena for the key supervisory authorities in the different sectors. The intention is to secure exchange of information and transfer of competence, thus improving the quality of the sector's cyber security supervision.

In 2017, NSM invited DSB and Nkom to join in a cooperation centred on establishing the arena. The report was delivered in 2017, and the first meeting was held in March 2018. DSB, Nkom, the Petroleum Safety Authority Norway (PSA), the Supervisory Authority of Norway and the Norwegian Water Resources and Energy Directorate (NVE) were invited.

There is appreciable interest in the arena, and numerous supervisory bodies want to participate. The arena will be expanded to include more supervisory bodies, and work is continuing with the following main issues forming the basis for cooperation:

- Exchange of experience between supervisory authorities both before and after the new Security Act came into effect on 1 January 2019
- Uniform supervision with a shared supervision methodology as far as possible
- Knowledge transfer and competence development
- Collaboration agreements between NSM and the sector supervisory bodies

Responsibility: NSM
Implementation: Ongoing

Measure 12: Scheme for recognition of security providers

In 2017, NSM launched the first scheme for recognition of security providers for suppliers who provide services for detecting and handling cyber attacks. The purpose of this scheme is to allow companies to choose suppliers that, in the assessment of NSM, present satisfactory service quality, and which contribute to raising the general level of cyber security skills in Norway. The scheme is a pilot that was evaluated in 2018. Provisional experience with the scheme is positive. An expansion of the scheme to other types of services is to be considered on the basis of the evaluation. Other services that will be considered as a part of the scheme include vulnerability testing and consultancy.

Responsibility: NSM
Implementation: 2019

Measure 13: Penetration tests

Penetration testing is a highly effective resource for exposing vulnerabilities and establishing conditions for measures designed to reduce risk. Penetration testing as a tool is becoming increasingly important in ensuring that the critical digital infrastructure is sufficiently secure and robust. The new Security Act allows for the use of private providers for running penetration tests on critical systems that require protection. It may also be relevant to demand such tests before systems that require security approval are granted it. If the business community is to be able to provide such services for critical and/or classified systems, it would be relevant to prepare a scheme for the approval of providers. For 2019, NSM's capacity for penetration testing increased by 10 million NOK to improve cyber security and make critical societal cyber infrastructure more robust.

Responsibility: NSM
Implementation: 2019

Measure 14: ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security. ENISA develops recommendations, contributes to the development of regulations and guidelines, and works closely with operative units in Europe. Norway participates in ENISA through the EEA relationship.

Implementation of the NIS directive (see Measure 30) will reinforce ENISA by allocating the agency the role of professional hub for the network of national professional authorities that the NIS directive establishes. Proposals have also been put forward (cf. COM/2017 477 "Cybersecurity Act") that would reinforce the ENISA mandate and introduce a European framework for the security certification of ICT products and services.

International collaboration is crucial to the development of global guidelines for reducing and combating cyber threats. Norway plays an active role in the work of ENISA, although without entitlement to vote. With the reinforcement of the role of ENISA and its increased capacity, Norway will prioritise working with ENISA, and will increase the use of ENISA deliveries at national level.

Responsibility: JD and the Ministry of Transport and Communications (SD)
Implementation: Ongoing

Measure 15: Information sharing and situational picture regarding cyber incident management

Information sharing is essential in exposing and countering cyber attacks. It is necessary to expand the cooperation and the flow of information in general – and especially in relation to those companies that are not currently covered by the framework for handling cyber security incidents (see Measure 40). In this context, two key measures should be mentioned:

- Establishment of tools for sharing sets of technical indicators. Private and public companies that participate in the solution are to be able to share their own sets of indicators with others, and to receive sets of indicators from NSM NorCERT.

- Development of an unclassified national situational picture, which is to be available via a portal with login options for sector-specific response communities and national decision-makers.

Responsibility: NSM
Implementation: Ongoing

Measure 16: Standardisation

Difi is continuing to examine the use of security standards in public administration. All IT standards in the public sector are categorised as "recommended" or "mandatory", depending on area of application, Norwegian and European laws, regulations and directives. Mandatory standards are included in the regulation on IT standards in public administration. The standards are collected in a reference catalogue administered by Difi. The reference catalogue presents an overview of recommended and mandatory IT standards for the public sector.

Responsibility: KMD and Difi
Implementation: Ongoing

Measure 17: Standards Norway

Norway is to be represented in international arenas where standards for cyber security are developed. In 2016, 2017 and 2018, Standards Norway has been assured subsidy for the programme entitled "Standardisation in cyber security". A Norwegian mirror committee 1/SC 27, under the leadership of NSM, has been set up to clarify needs for standards in the area of cyber security. Moreover, priority is to be given to participation in a newly established committee – 1 SC/41, "Internet of Things". Experts are to be taken on, and the project also includes working closely with research communities.

Responsibility: JD and NSM
Implementation: Ongoing

Measure 18: Standard Agreements (SSA)

Standard Agreements are used to a wide extent, not only for public procurements, but also between business owners. The Ministry of Trade, Industry and Fisheries has an overall responsibility for the standard agreements. More explanatory security clauses, initially in the agreements used for ICT operation and cloud services, may potentially have a significant positive effect on many agreements concerning the outsourcing of ICT services. JD and KMD will, in partnership with subordinate agencies, assess the need for revising the security clauses relevant to outsourcing.

Responsibility: JD and KMD, in partnership with Difi and NSM
Implementation: 2019

Measure 19: Classified communication between the ministries, government agencies and other key emergency response operators in the sectors

FD holds responsibility for operating and administering the *Nasjonalt BEGRENSET nett* (National RESTRICTED Network – NBN). NBN is an ICT platform for the exchange of classified information. NBN has been rolled out to all ministries, and relevant public and private companies are being connected to NBN on an ongoing basis.

FD has been commissioned to develop a *Nasjonalt HEMMELIG nett* (National SECRET Network – NHN) for classified communication graded SECRET in the public administration. NHN is currently under development, with roll-out to the ministries scheduled for 2019. NHN is built using the same architecture as NBN.

Responsibility: FD
Implementation: 2019

Measure 20: Secured Public Network (SON)

The Secured Public Network (*Sikret Offentlig Nett* – SON) is a high-speed computer network between participating stakeholders. The primary purpose is to ensure that participants receive a higher level of protection against intentional, unwanted incidents from the internet. Should internet service be lost, participants can communicate with one another via SON. In the event of an ongoing cyber attack against one participant, the company can disconnect from the internet and use the internet connection of one of the other participants. SON can also be used to stop traffic to internet addresses that are being used in the attack, or which are delivering viruses and malware.

On establishment of SON as the carrier network, it is possible to set up shared services between all or some participants. Examples of such services include SharePoint solutions, shared security solutions, telephony and email. SON has also been considered as a possible carrier for a national classified network for the Armed Forces and the police ICT systems and for the police force's alarm and warning system. In addition, participants in SON can use security-classified sensors (see Measure 1), an option that will improve national detection capacity.

SON is a pilot currently being developed jointly by JD, FD, the police and NSM. NSM is to head up the further development work, where SON is intended to function as a key component in NSM's new, centralised VDI solution (see Measure 1) and as an important emergency response measure for all participating companies. Proposals for mandate and ownership are also to be examined, with an operating and management model that includes all the necessary conditions that derive from a national measure of this kind – including finance.

Responsibility: NSM
Implementation: 2018-2021

Measure 21: National Cyber Security Awareness Month

One of the larger stand-alone measures implemented with the aim to increase knowledge and competence in cyber security is "National Cyber Security Awareness Month". This is a public-private initiative to raise awareness about cyber security. National Cyber Security Awareness Month takes place annually in October and was organised for the eighth time in 2018. In 2018, training lessons were provided for 250 000 employees in 330 companies. NorSIS coordinates the National Cyber Security Month on commission from JD.

Responsibility: NorSIS and JD
Implementation: Annual

Measure 22: National Crypto Policy

The "Norwegian Crypto Policy" was published in 2001 by what was then the Ministry of Trade and Industry, and is based on the OECD Crypto Policy Guidelines published in 1997. Encryption as a security measure helps protect the confidentiality, integrity and authenticity of the information, and forms the very foundations of secure electronic data processing and communication. There is appreciable potential for improving the security of services that are to process sensitive data through the use of commercial solutions. The need to maintain the necessary national crypto-competence and to promote both innovation and product development are other reasons why it is necessary to revise the National Crypto Policy.

A working group is set up under the leadership of FD, tasked with revising the crypto policy. Key topics include technological development, crypto competence, national security, commercial interests, the eIDAS regulations, and regulation of the use of crypto.

Responsibility: FD and JD
Implementation: 2018-2019

Measure 23: NATO Cooperative Cyber Defence Centre of Excellence

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in Tallinn, Estonia, was formally established as a multinational NATO-accredited professional cyber centre in 2008. NATO CCD COE employs more than 40 people, works with legal, political and operational cyber issues, and publishes work that enjoys global recognition. Norway has applied for membership of the centre. It is expected that formal inclusion will be granted in 2019.

Responsibility: FD, JD and the Norwegian Ministry of Foreign Affairs (UD)
Implementation: Establishment in 2019 (subsequently ongoing)

Measure 24: European Centre of Excellence for Countering Hybrid Threats

The security-policy landscape is characterized by increasingly complex challenges and an increasing number of actors. The use of hybrid methods and activities is becoming more widespread. An increasing number of countries are experiencing disinformation, attempts to influence elections, and cyber attacks on critical infrastructure. The effect of these and other hybrid methods and activities is being amplified by our increasing dependence on cyberspace.

It is essential to meet these challenges through a comprehensive approach and appropriate coordination at both a national and international level. The Norwegian Government is therefore strengthening its efforts towards hybrid threats, and as part of this effort Norway in 2017 joined the European Centre of Excellence for Countering Hybrid Threats in Helsinki. Here, Norway will work with allies and other partners to improve its capacity to understand and counter hybrid threats.

Responsibility: UD, FD and JD
Implementation: Ongoing

Measure 25: Capacity building at international level

Norway is currently supporting projects designed to chart the need to reinforce cyber security in developing countries. As a part of this work, Norway is to continue its participation in the Global Conference on Cyberspace (GCCS). GCCS was organised for the first time in London in 2011, and is referred to as “the London process”. GCCS is a discussion forum where both state and non-state actors from the business community, academia and civilian society meet to discuss different aspects of the challenges in cyberspace, with particular emphasis on capacity building and on exchanging experiences.

Focus on capacity building has developed from the establishment of principles to the implementation of the these. In 2014, the Global Forum on Cyber Expertise (GFCE) was established as follow-up to the London process and constitutes a practical measure for working together on capacity building and sharing best practice. Norway is a member of GFCE and participates in the work in different expert groups. Other authorities and academia are encouraged to make professional experts available to participate in expert groups at international level, to assist with the transfer of competence and the expansion of capacity. Participation in such groups must be funded within the budgets of each participating organisation.

Responsibility: UD and JD – other companies are encouraged to contribute
Implementation: Ongoing

Measure 26: Measures to build capacity in cyber security in developing countries

UD supports various actors in order to contribute to capacity building in developing countries. Capacity building in cyber security will strengthen the ability to protect critical infrastructure and combat digital threats, as part of the sustainable development agenda.

Responsibility: UD
Implementation: Ongoing

Measure 27: Norwegian Cyber Range (NCR)

The Norwegian Cyber Range (NCR) is the first national test arena for cyber security that covers all sectors of society. NCR is to be both an academic and a commercial arena, and in the long term it will also provide commercial services for different market segments in the private and public sectors.

Testing, training and practice are resources used to expose companies and individuals to incidents in realistic but secure surroundings. NCR assures efficient and realistic reinforcement of competence, and links together societal models, digital value chains and cyber infrastructure in one or more defined environments. In addition, an arena of this kind will allow preparations to be made for targeted pre- and post-training programmes in the field of national cyber security.

NTNU has received financial support from Oppland County Council in the amount of 20 million NOK over three years to build up NCR. The build-up is carried out as part of a cooperation with the Norwegian Armed Forces Cyber Defence, Norwegian Civil Defence Force, Telenor Norge, EVRY, NorSIS, NSM and mnemonic through NTNU's Centre for Cyber and Information Security (NTNU CCIS).

The cooperation also include a joint project with Estonia. This part of the project is called "Open Cyber Range". Estonia and Norway have been awarded 32 million NOK in EEA funds to improve their capacity to combat cyber crime. The project is led by the Estonian Ministry of Defence, with participation from the Technological University of Tallinn, and NTNU's Department of Information Security and Communication Technology.

Responsibility: NTNU
Implementation: Launched in 2018

Measure 28: The Norwegian Ministry of Defence guidelines for cyber security and cyber operations for the defence sector

The FD guidelines for cyber security and cyber operations in the defence sector were published in 2014. Since then, changes have been made to the structure of the ministry's subordinate agencies, the use of concepts, legal bases and so on. It is therefore necessary to revise the guidelines.

Responsibility: FD
Implementation: 2018-2019

2.3. Cyber security in critical societal functions

Our society depends on a range of functions crucial to its operation, such as energy supply, financial services and satellite-based services. These are functions that must be maintained at all times in order to safeguard the fundamental needs of society. Several societal functions require a digital infrastructure that operates more or less everywhere and all the time. The following section presents key measures designed to support the goal of ensuring that critical societal functions are backed by a robust and reliable digital infrastructure.

Measure 29: New Security Act

In June 2017, FD put before the Norwegian parliament proposition for a new Security Act. The new act came into effect on 1 January 2019.

The area of application of the Security Act has been expanded because of the increasing dependencies across civilian-military and public-private boundaries – and between sectors of society. The act lays down requirements to secure all information systems that contain information that require protection, not just those used to process classified information. Regulations regarding ownership control also make it possible to regulate and even block procurement made by strategically important companies that are subject to the Security Act. The act sets out more closely adapted rules on classified procurements.

The ministries are directed to identify services, production and other types of activities that, should they become partially or completely unavailable, will affect Norway's ability to safeguard national security interests (fundamental national functions). The ministries shall further decide on the activities to which the law applies.

NSM will be strengthened by 38 million NOK in 2019, to enable the agency to implement and exercise the new and expanded responsibilities it is tasked with under new the Security Act, including also to improve the capacity to conduct penetration tests

Responsibility: FD
Implementation: 2019

Measure 30: The NIS Directive

The NIS Directive obliges EU Member States to ensure they maintain a minimum level of national cyber security by undertaking a national cyber security strategy, establish a national response environment for cyber incidents (a Computer Security Incident Response Team – CSIRT), appoint a competent national authority, and oblige suppliers of services crucial to society and some digital services to comply with cyber security requirements and to undertake to provide notification in the event of serious cyber security incidents. The Member States also undertake to participate in the collaboration groups that have been established under the NIS Directive, i.e. the NIS collaboration group for strategic management and CSIRT networks.

As of now, Norway is not obliged to implement the NIS Directive since the directive is not encompassed by the EEA Agreement. In December 2016, however, the Norwegian government considered the directive to be EEA relevant and acceptable, and Iceland has adopted the same position. Liechtenstein has not yet adopted a final position. The EEA process has therefore not yet been concluded.

However, the Norwegian government does presume that the directive will become binding for Norway. The work on a potential implementation of the directive in Norwegian law has therefore already begun. A consultation paper on the implementation of a law proposal implementing the directive was submitted for public review in December 2018.

In several areas, the directive allows national latitude to make more comprehensive security demands on the companies that will be affected by the directive, and on more than directly stipulated in the directive. The government's current position is that the Norwegian regulations are to be as closely tied as possible to the scope and requirements laid out in the directive. The intention is provisionally to use the existing authority structure as far as possible. However, this could be changed as a result of the recommendations from the cyber security committee (see Measure 6).

Responsibility: JD
Implementation: 2019

Measure 31: National core infrastructure

For the ecom sector, it is particularly important to continue the work to increase the diversity and robustness of the ecom networks both within national borders and to key points abroad. The "National Transport Plan 2018-2029" includes an initiative for a pilot designed to stimulate the market to increase redundancy in the transport section of the domestic ecom networks. The sum of 40 million NOK was set aside for this work in 2018. This grant was continued in 2019. In 2018, on commission from and in consultation with SD, Nkom has worked to specify and launch the pilot programmes.

Responsibility: SD and Nkom
Implementation: 2018-2020

Measure 32: International fibre connections

International fibre infrastructure constitutes a critical part of the modern national infrastructure. Unilateral routing of Norwegian internet traffic through Sweden is a significant national vulnerability. New international connections and alternative routing of traffic will contribute to increasing total national capacity, redundancy and security in the ecom networks.

A total of 40 million NOK was set aside in 2018 to prepare conditions for establishing international fibre connections to and from Norway. This grant was continued in 2019, along with a commitment authorisation of 20 million NOK, bringing the total financial framework for the initiative to 100 million NOK. In 2018, on commission from and in consultation with SD, Nkom has prepared an announcement of the funds.

Responsibility: SD and Nkom
Implementation: 2018-2020

Measure 33: Increased security in ecom

An interruption in ecom can have serious consequences on the vast majority of our society and for critical social functions. SD has initiated efforts to investigate various measures to increase safety in Norwegian ecom. Among other things, consideration should be given to

clarifying requirements for the owners of the networks, including whether more stringent requirements should be made for security related to e-communications equipment providers that carry critical social functions.

Responsibility: SD and Nkom
Implementation: Start-up 2018

Measure 34: Proposal for a new act on the Intelligence Service and access to cross-border electronic communication

In 2016, FD assembled a committee (the "Lysne II Committee") to examine the principle aspects of possibly providing the Norwegian Intelligence Service with access to cross-border electronic communication. The committee delivered its report on 26 August 2016, and recommended the introduction of a digital border defence, with a clear frame of reference and strong control mechanisms to safeguard privacy. The report was submitted for public review and gave rise to broad public debate.

In 2017, the government decided that FD should investigate how a digital border defence system could be legislated and established in Norway. The investigation has been performed on the basis of developments in the threat landscape, the reinforcement of the position of human rights in Norwegian law, and the ongoing digitalisation of society. Technological development has resulted in almost all communication having been transferred from radio and satellite connections to digital signals carried by cables. The Norwegian Intelligence Service does not have its own access to information that is carried by cross-border communication cables. The need for such access is made relevant by prominent trends in society, including the rise of cross-border threats and the increased occurrence of cyber threats targeted at state bodies and private operators.

An examination of possible access to cable communication for the Norwegian Intelligence Service was made in parallel with a review of the prevailing law on the Norwegian Intelligence Service. FD's assessments and proposals for legislative regulation linked to both these examinations was sent on public review on 12 November 2018 with consultation deadline February 12, 2019.

Responsibility: FD
Implementation: 2018-2019

Measure 35: National framework for comprehensive assessment of value chains

The Lysne Committee recommended establishing a national framework to handle a comprehensive assessment of value chains. The committee bases its recommendation on the fact that long and complex value chains - which encompass multiple sectors, levels and national borders - constitute a core challenge in the evaluation of digital vulnerability. The Committee has identified that this is a common challenge in all sectors covered by the report. As follow-up to the recommendation, a working group was set up in 2018 to propose a national framework for assessing digital value chains.

Responsibility: JD and DSB
Implementation: 2019

Measure 36: NATO Cyber Defence Pledge

NATO's heads of state and government ratified a joint cyber pledge during the NATO summit in 2016. The declaration was prepared on the basis of new security threats against NATO, as well as the need to highlight and prioritise the work to reinforce cyber security in digital networks and infrastructures across sectors in society and between countries.

Norway is to follow up on the obligations set out in the cyber pledge. Through the declaration, the countries have pledged to make improvements in a number of areas at national level, since the member countries themselves hold responsibility for their own security against cyber threats in national infrastructure. The obligations encompass areas such as resource allocation, collaboration, understanding, information sharing and developing skills.

Responsibility: FD and other relevant ministries
Implementation: Ongoing, with annual reporting to NATO

Measure 37: Future public safety communication solutions

The 700 MHz spectrum will be awarded to commercial mobile network operators. The 700 MHz frequencies have good coverage properties and will be important in ensuring wide availability of advanced mobile services throughout Norway. The 700 MHz spectrum is one of the resources pointed out for the roll-out of 5G, the next generation mobile network, which is crucial to successful digitalisation in private and public sectors and to cover the needs of both the authorities and the market.

The commercial mobile network operators must be able to deliver future communication solutions for emergency and preparedness agencies and the Armed Forces. These critical users' needs have to be covered through a combination of regulations and commercial procurements.

JD, SD, DSB and Nkom are working on examinations linked to future public safety communication solutions in commercial mobile networks. A concept evaluation of the topic will be prepared.

Responsibility: JD, SD, DSB and Nkom
Implementation: The examination work is ongoing. Quality assurance will be carried out when the concept evaluation is completed

2.4. Competence – list of measures in the national strategy for cyber security competence

Competence in cyber security is a resource in short supply at both national and international levels. In recent years, the Norwegian government has prepared the ground for improved education capacity and greater research into cyber security. A separate strategy is to set out conditions for a long-term build-up of competence in cyber security – particularly national capacity in the fields of research, development, education and measures designed to raise awareness among the business community and the general public. The table below lists measures that follow from the national strategy for cyber security competence.

MEASURES IN THE NATIONAL STRATEGY FOR CYBER SECURITY COMPETENCE
Priority: Longterm research of good quality
Cyber security is prioritized in the revised Longterm Plan for Research and higher Education
Projects supported by the IKTPLUSS programme, run by the Norwegian Research Council
Strengthen cyber security as a part of the SAMRISK-programme by the Norwegian Research Council
Lighthouse projects; cooperation between researchers and users for innovation by the Norwegian Research Council
Establish an arena (an annual conference) for dissemination of cyber security research findings
Strengthen the core research institutions by prioritizing cryptology from 2018
Priority: Sufficient national specialist expertise
Education within ICT and cyber security
Increase the amount of persons with Ph.D education within Cyber Security, including Cryptology
Encourage the use of the arrangement of the Industrial Ph.D-scheme (a doctoral project in industry) and the Public sector Ph.D.-scheme by the Norwegian Research Council
Measures to motivate more girls to enter studies within cyber security
Priority: Cyber security as part of ICT related educations and adjacent/related studies
Map the needs and offers of courses in cyber security as a part of ICT and adjacent studies
Strengthen the capacity of cyber security within educations of engineers and technologists
Priority: Further education within ICT and cyber security
The government's Competence Reform – learning through life / learn your whole life
The Markussen Committee – a public committee – on unmet/uncovered needs for continuing and further education
Funds for the development of flexible further education programs in digital competence
Priority: Cyber security in vocational educations and (higher) professional studies
Reviews of relevant subject curriculums (teaching plans) in the vocational education
Police training (education) – courses within cyber crime/cyber security, as a part of bachelor and master education
Enhanced cyber security in health education (cyber security within different health educations)

Priority: Good primary education
The first phase of the renewing of primary education subjects is development of core elements
Continuing education for strengthening the teachers competence
The technological school bag contains several measures for technology competence and cyber security learning materials
Priority: Awareness raising and improved digital security culture
Survey of cyber security culture
Measuring cyber skills of the pupils within primary and secondary education
Skills campaign directed towards selected groups of the population
Participating in the European Security Challenge by ENISA
A pilot of teaching techniques of children and youth on behalf of different institutions in Norway, relevant for Cyber Security (NSM, NVE, NorSIS, NTNU, UiO and Abelia) in the two municipalities Oppegård, Ski and the county of Rogaland

2.5. Detect and handle cyber attacks

Cyber attacks can be difficult to detect and, in a worst-case scenario, may constitute a threat to national interests or even violation of Norwegian sovereignty. It is therefore imperative to improve our national capacity to detect and handle cyber attacks. The following section presents key measures designed to underpin the goal of ensuring that society has improved ability to detect and handle cyber attacks.

Measure 38: Sector-specific response communities

One national initiative in the field of cyber security is the establishment of sector-specific response communities, combined with reinforcement of the national model for incident management. The ambition behind sector-specific response communities is for these to have the capacity to support their respective sectors with competence, and to serve as hubs for information and the flow of data between companies within the sector, between sectors, and between sectoral and national level (NorCERT). NorCERT's coordination and support in management entails, for instance, sharing information with the sector-specific response communities, the police force, companies crucial to society, and other relevant operators. NSM also supports the establishment and follow-up of the sector-specific response communities. As a minimum solution, a single point of contact must be set up within the sector for cyber incidents, as well as for procedures for issuing warnings internally within the sector and to NSM NorCERT. In addition to this, the sectors themselves must determine what type of needs they have for dealing with unwanted cyber incidents, and how they may need to upscale their response communities accordingly.

Work is to continue on implementation of a national structure for dealing with incidents in accordance with the framework for handling cyber security incidents. The sector-specific response communities are to have an affiliation with the sectorial ministry.

Responsibility: JD, with follow-up by all ministries
Implementation: Ongoing

Measure 39: JustisCERT

In step with the national guidelines, JD previously established a minimum-level response community for issuing warnings within the sector and to NSM NorCERT. In consultation with the sector, JD has assessed the additional needs and has decided to establish JustisCERT as a replacement for the previous minimum solution. This establishment will be in line with the framework for handling cyber security incidents. JustisCERT will have the capability to detect, analyse, alert, coordinate and handle cyber incidents in the justice sector, and to contribute actively through a variety of measures to reducing vulnerability in this sector. JustisCERT will serve more than 19 units in the justice sector, as well as many large sub-units of these. Irrespective of size, all units in the justice sector will be able to benefit from the JustisCERT capability, and the initiative is financed by all participating organisations.

Responsibility: JD, the National Police Directorate (POD) and associated companies
Implementation: 2018–2019

Measure 40: Framework for handling cyber security incidents

Better and more effective cooperation is required when dealing with incidents that affect multiple companies and sectors. Work will continue on implementing a national structure for handling incidents in line with the framework adopted in 2017. The framework will be further developed through, among other things:

- Formalisation and deployment of sector-specific response communities at ministerial level in all sectors to ensure protection of fundamental national functions.
- Formalisation of the role of sector-specific response communities in planning and exercises for crisis management.
- Establishment of tools and processes for effectively sharing information about incidents.
- Inclusion of private stakeholders.
- Establish a structure for the role of the county and municipal authorities in the response communities and in the framework for handling cyber security incidents.

Responsibility: JD and FD (owners) follow-up by all ministries
Implementation: Ongoing

Measure 41: National cyber security exercise

A new national cyber security exercise is to be conducted with the objective of reinforcing civilian-military, public-private and international collaboration on cyber security incident management. The exercise will, in particular, take as its starting point a more robust public-private partnership, and will therefore involve private companies in the planning, design and execution of the exercise.

Key owners of critical digital infrastructure and other selected private companies will be invited to participate at an early stage to work with the authorities on defining the objectives and framework of the exercise. The exercise is also to train civilian-military cooperation, and it will be used to develop the national framework (see Measure 40) to include private companies. JD, FD and SD hold assignment responsibility for the exercise.

DSB will head up the planning process and the actual execution of the exercise in close collaboration with partners such as NSM, Nkom and private stakeholders.

Responsibility: JD, FD and SD
Implementation: 2020

Measure 42: International exercises

Use of exercises at all levels is a key resource for improving crisis management capacity, and for identifying needs for competence. Norway participates in a series of international exercises:

- NATO's Cyber Coalition: NATO's biggest and most important Cyber Defence exercise, involving participants from a number of allies, partner countries, the EU, industry and academia. The purpose of the Cyber Coalition is to train the capacity to protect NATO's and national networks against various types of cyber attacks.

- Locked Shields: the annual exercise organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) intended for technical personnel and the technical operative communities, including CERT environments. The intention behind this exercise is to reinforce and increase proximity to skills and professional development within the NATO alliance. NSM NorCERT ensures and coordinates Norwegian participation in the exercise, using both its own resources and resources from other sectors.

- Cyber Europe: the EU's major cyber exercise that ENISA organises every two years. The exercise simulates comprehensive and serious unwanted cyber incidents, and includes both technical assignments and communication/cooperation skills. NSM participated in 2016 and 2018.

- NATO's CMX: CMX is NATO's annual crisis management exercise at political and strategic level. The intention is to train crisis management in collaboration with national and international authorities.

Responsibility: FD, JD and NSM
Implementation: Ongoing

Measure 43: Joint Cyber Coordination Centre (FCKS)

FCKS is a permanent, co-localised professional environment comprising representatives from NSM, the Norwegian Intelligence Service (E-tjenesten), the Norwegian Police Security Service (PST) and the National Criminal Investigation Service (Kripos). FCKS is to help increase the national capacity to withstand serious cyber attacks, to support strategic analysis production, and to maintain a comprehensive threat landscape for cyberspace. FCKS is not an independent body with its own decision-making authority, and the establishment entails no changes to legal basis, authorisations, roles or assignments.

After two years of operation an assessment of FCKS will be performed to ensure achievement of the purpose of establishing FCKS.

Responsibility: FD and JD
Implementation: 2019

Measure 44: Cross-sectoral cyber reserve

During the period 2018-2019, NSM is to assess a cross-sectoral personnel reserve for handling cyber incidents in the case of particularly serious crises that require input in excess of ordinary staffing. The report is to look into which requirements must be made on personnel in such a model, and which communities or persons it would be natural to link to such an initiative. Other elements that require clarification include legal issues, the need to have personnel with security clearance, and the exercises and training needed to maintain competence.

Responsibility: NSM
Implementation: 2018-2019

Measure 45: Transparency and evaluation of unwanted cyber incidents

On commission from JD, NSM has previously prepared recommendations for how public and private companies should assess transparency regarding unwanted cyber incidents. These recommendations have been prepared in partnership with Difi, NorSIS, POD and the Norwegian Business and Security Council (NSR). Public and private sector companies are encouraged to follow these recommendations.

In addition, instructions for the work of the ministries with public security imply that in the event of major incidents, the leading ministry is responsible for performing an assessment of the incident management. The purpose of such evaluation is to identify learning points, suggest measures and make sure that the measures are followed up on.

It has been decided that following the data breach in the South/East Norway Regional Health Authority in 2018, assessments are to be performed of the healthcare sector, NSM and JD. Moreover, major cyber incidents should be evaluated. The authorities recommend that private companies similarly evaluate major incidents and share experience.

Responsibility: Everyone
Implementation: Ongoing

2.6. Prevent and combat cyber crime

The government will ensure that the police have the conditions they need to prevent and combat cyber crime. Key resources are capacity and competence. In addition to the measures below, reference is made to measure 4 on the establishment of NC3.

Measure 46: White Paper on police capacity and competence

The government will publish a white paper on changes in the crime landscape and the consequences of this for police assignments and services. The report will review and discuss current and developing crime trends and their consequences for police capacity and competence.

Responsibility: JD
Implementation: 2019

Measure 47: The Norwegian Police Security Service (PST)

For 2019, PST's funding increased by 25 million NOK for work on hybrid- and cyber threats, such that PST has the personnel and technology necessary to improve capacity in cyberspace to detect, prevent, handle and investigate the most serious attempts at espionage, sabotage, influencing operations and compound (hybrid) threats. The funding will, for example, provide a basis for further development of PST's cooperation with the intelligence services, NSM and Kripos in FCKS.

Responsibility: JD
Implementation: 2019

Measure 48: Support UN efforts to combat cyber crime at global level

In 2018-2021, Norway contributes with 35 million NOK to fight cyber crime through the UNODC's Global Programme on Cybercrime to the United Nations Office on Drugs and Crime. Norway's support will focus on developing countries, in particular in West Africa, the Middle East and North Africa as well as South East Asia, to build capacities to investigate, prosecute, convict and prevent cyber crime. The objective is to make a tangible contribution to save lives and apprehend criminals, locally as well as in cases across jurisdictions. Norway is already contributing with an expert to UNODC's work on cyber crime.

Responsibility: UD
Implementation: 2018-2021

Measure 49: National electronic proof of identity (eID)

The national ID cards are scheduled to be introduced in 2020 and will contain electronic proof of identity (eID). With this, the security level for electronic identification will be the same as for passports. A person can only have one national eID. The eID will be made available to both Norwegian citizens and foreign citizens who qualify for the national ID card. With the introduction of this scheme, ICT services that require the same level of security as passport identification can start using the national eID, thus reducing the risk of fraud/misuse. It will be possible to use the national eID for both public and private sector services, and it is intended to serve as a supplement to other eID schemes available in the market. The security level for public services is defined in the "Framework and authentication and non-repudiation in public communication".

Responsibility: JD
Implementation: 2020

Measure 50: International cooperation on cyber crime

JD will promote international cooperation and participate in relevant international fora concerning Norwegian efforts to prevent and combat cyber crime. This includes cooperation within, for instance, the United Nations, the Council of Europe and the European Union.

Responsibility: JD
Implementation: Ongoing

Measure 51: The Police's citizen survey

The National Police Directorate initiates an annual citizen survey indicating the public's level of confidence in the police force. The survey provides valuable information about the public perception of safety and the impression they have concerning the capacity of the police to handle cyber crime.

Responsibility: POD
Implementation: Annually

3. PART 2 – Measures recommended to improve companies' own ability

Public authorities have presented a range of advice and recommendations in recent years with the intention of improving companies' own ability to protect themselves against – and to deal with – unwanted cyber incidents. These include NSM's "Cyber Security Principles" and Difi's "Internal control guidelines".[1] [2]

This part contains ten measures that companies in both public and private sector are recommended to implement. The measures have been drawn up through a collaboration consisting of companies from both public and private sector. The measures are based on the above-mentioned advice and recommendations, and provide Norwegian companies with a solid starting point for factors they ought to consider, irrespective of their size, maturity and competence in cyber security.

A national effort to improve basic cyber security

Good management and effective corporate processes have a significant role to play in maintaining the desired quality and development, and in delivering in accordance with stated goals. Governance and involvement from the management help ensure that the correct measures are implemented and that resources are used correctly. At the same time, cyber security cannot be achieved solely through established processes and management involvement. The security measures that are actually implemented – such as configuring the ICT systems, physical barriers in buildings, actions of individual employees – are what determine the actual level of security.

To maintain the desired level of security, cyber security must become an integral part of all the professional disciplines and corporate processes at a company. This relies on having control over actions, and that decisions are based on a good knowledge base. Good cyber security management is a precondition for success. To achieve this, the company board and the management must take ownership of security processes and activities. Cyber security must be included in risk and reporting processes, and the company must employ staff with sufficient professional competence. A good starting point for ensuring this comprises Difi's internal control guidelines and NSM's introduction to security management.

Companies must also implement the measures necessary to secure their ICT systems. NSM's Cyber Security Principles describe measures that all companies should implement for robust basic security. They define a set of principles and underlying measures to protect ICT systems (hardware, software and connected infrastructure), data and the services they provide against unauthorised access, damage or misuse. The list below set out ten important measures for commencing the cyber security work.

1 https://www.nsm.stat.no/grunnprinsipper-ikt
2 http://internkontroll.infosikkerhet.difi.no/

Recommendation 1: Management

Cyber security must be an integral part of the company's ICT systems and services. This, in turn, is dependent on good processes for governance and management. Cyber security management activities should be set up as a part of the corporate management system, where there are clear demands on and expectations to cyber security. This includes bringing in the necessary resources with a clear description of responsibilities and follow-up. The scope must be adapted to match the size and needs of the company. This can be set up easily, with few roles and simple implementation in a small company. Conversely, greater demands will apply to companies that have a greater need for protection.

Start-up tips: Establish sufficient systematics for security management, and make sure that an expert in the field supports the management in this work.

Recommendation 2: Risk management

Establish a process for risk management in the company that is a part of an encompassing management structure. Everyone at the company must be familiar with the risk management process. The objective is for employees to be familiar with the company's risk management setup, know how decisions are made and what risk level is acceptable.

It is important to have clear guidelines for how risk is to be understood and assessed, which criteria apply for acceptable risk, and who is to take decisions based on identified risk. This is important in ensuring that decisions about risk are made at the right level and on the right basis. Risk management for cyber security should be included as a part of the overall risk management at the company. Therefore, establish processes for the evaluation and quality assurance of security measures, where the results are reported to the management.

Start-up tips: Include cyber security in the work on risk at the company. Establish clear responsibility at the company, with effective reporting lines to the senior management and board of directors.

Recommendation 3: Map value chains, information assets, equipment and user access

Knowing your own business is essential in running it efficiently and delivering good services. Mapping goals, deliveries and services will help ensure that key value chains, information and dependencies are identified and assessed. It is important to map the company's deliveries and value chains, which units and software the business relies upon, and which users and user access rights exist. If a company does not have a sufficiently good overview, some parts of the ICT systems may be well secured, while other, vital parts are openly exposed and vulnerable to cyberattack.

Start-up tips: Prepare a list of the company's key goals, the values and value chains involved, where key data are stored, and who has access to these data.

Recommendation 4: Include cyber security in the corporate culture

The knowledge and attitudes of the employees have a significant role to play in ensuring that companies can operate securely. Companies must therefore make sure that their employees have the necessary information, knowledge and skills to maintain the desired level of security. The management of a company must communicate goals and priorities for cyber security clearly and efficiently, and present good role models. All employees – from the senior management to new appointees fresh from school – should follow adapted tracks for training, skills development and security awareness. Employees who operate and support key services must have sufficient knowledge and experience to maintain secure operation of the ICT systems.

Start-up tips: Map the companies security culture and identify what can be improved. Define the desired culture and carry out adapted annual training programmes to promote appropriate security culture.

Recommendation 5: Supplier control

When purchasing ICT products and services, it is important to make sure that security is assured at a level with which the management of the company is comfortable. The right requirements must be set for products and suppliers, such that security is maintained throughout the lifecycle of the product or service in question. Expertise in procurement is important, as are overview and control throughout the lifecycle, good risk assessments to ensure the right decisions are made, as well as good and appropriate requirements on the ICT service and on the supplier. It is also essential to ensure that the right decisions are taken at the right level.

Start-up tips: Focus on expertise in procurement and implement risk assessment that is deployed among the management.

Recommendation 6: Secure configuration

For employees to work efficiently and have confidence in their tools, the ICT systems must be thoroughly reliable. This can be done by establishing trustworthy systems and services, configuring and adapting hardware and software, and verifying that the configuration is correct. Weak points in the set-up and configuration of ICT systems can be exploited by threat agents, and increase the risk of unforeseen incidents. The configuration must be updated on an ongoing basis, in step with changes in technology, patterns of use and the threat profile.

Start-up tips: Upgrade hardware and software. Eliminate unnecessary complexity and unused functionality. Block the running of non-authorised programs.

Recommendation 7: Check networks and system components

A company's network(s) and system components will inevitably be exposed to internal and external influences. These may take the form of harmful software (malware) that may damage equipment and networks, or planned changes resulting from the introduction of a new accounts system, for example. Whatever the cause, there will be aspects the company must take into consideration such that the ICT systems maintain the desired robustness. The company must introduce measures to protect against malware, as well as to ensure monitoring and analysis of the ICT system, and management of changes. In order to check whether correct security mechanisms are in place, it will pay dividends in many cases to run tests and drills that involve attempting to gain access to data and resources to which you are not allowed access.

Start-up tips: Install security updates as soon as possible. Protect wireless networks with strong security mechanisms. Plan and document changes. Switch on logging, and review important logs regularly.

Recommendation 8: Email and web security

All companies must maintain control of their own data and services to accommodate the need for quality and security. Email and web security should be accorded particular focus given that these are commonly used for malicious activity. CEO fraud, phishing and malware such as crypto viruses are examples of such threats. Email attachments constitute one of the most common delivery systems for computer viruses, worms and other types of malware. Email attachments should therefore always be treated with care, especially if the email comes from an unfamiliar sender.

The company should maintain control of the information flows that run to and from its own network, and within its network. Data and services must be protected both when stored at the company or at a service provider, and when data are communicated through different information channels – via the internet, for instance.

Start-up tips: Use the latest version of your internet browser. Protect email with DMARC. Encrypt important information when it is stored on portable media and when it is sent via the internet.

Recommendation 9: Access control

Access to the company's data and services must be controlled to prevent misuse by non-authorised parties. This can be done by keeping track of accounts, checking use of administrative privileges, applying secure login procedures, and regularly reviewing access rights.

Physical access to networks and information systems, including computer rooms, must be controlled in the same way as logical access.

Start-up tips: Change standard passwords and do not grant administrator rights to end users. Use 2-factor authentication or, as a minimum, strong passwords.

Recommendation 10: Incident preparedness

All companies must be prepared to deal with incidents when they arise by developing and implementing effective incident management processes. This can be done by identifying incidents quickly, checking and efficiently removing the cause of the incident, and restoring confidence in the systems and networks affected. The processes include planning, defining roles, training, communication and management oversight. A key aspect of this work is the capacity to recover and restore data should this be necessary. Continuity management and emergency preparedness are key parts of the company's overall plan for business continuity.

Start-up tips: Establish an emergency response plan for different types of incidents, and run drills to test the plan.

Notes

Notes

Published by:
Norwegian Ministeries

Additional copies may be ordered from:
Norwegian Government Security and Service Organisation
www.publikasjoner.dep.no
Telephone: + 47 22 24 00 00
Publications are also available on:
www.government.no
Publication number: G-0445 E
Design and layout: Konsis Grafisk
Print: Norwegian Government Security and Service Organisation
01/2019 – Impression 500