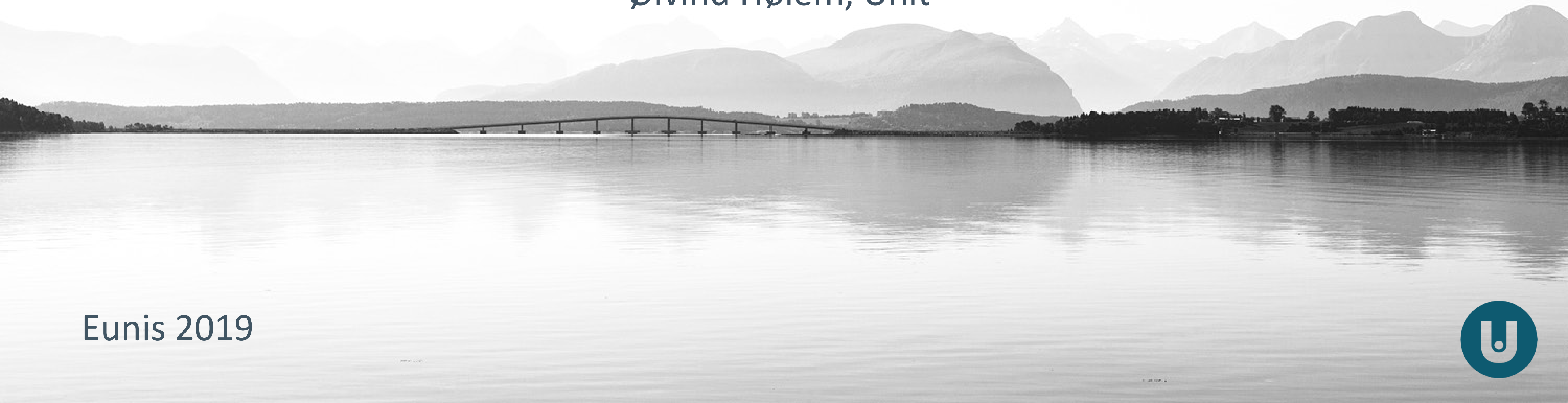
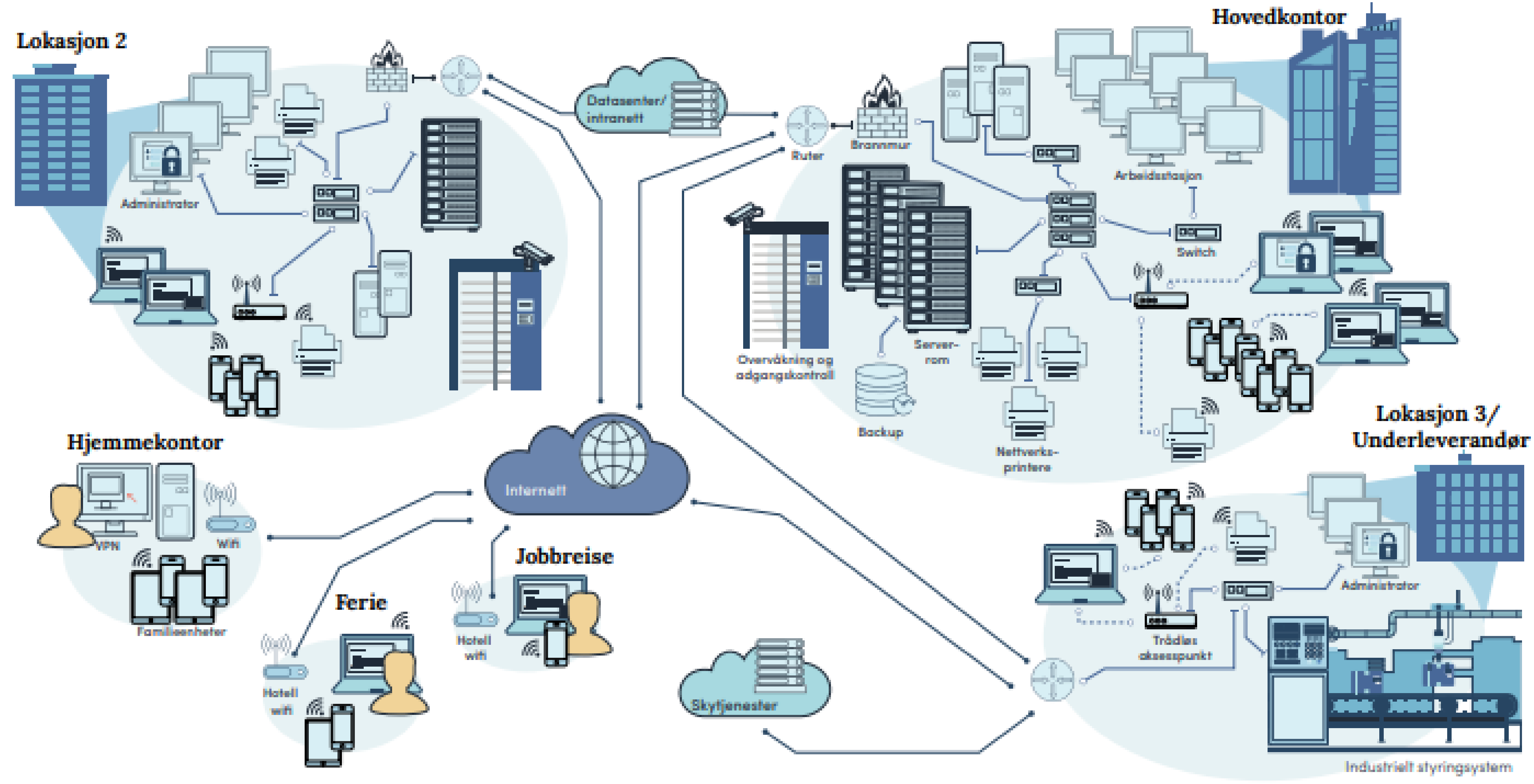
Framework for handling ICT security incidents in higher education and research in Norway

Øivind Høiem, Unit



Eunis 2019


Lokasjon 2
Administrator
Datasenter/ intranett
Hovedkontor
Ruter
Brannmur
Arbeidsstasjon
Switch
Overvåkning og adgangskontroll
Server-rom
Backup
Nettverks-printere
Hjemmekontor
VPN
Wifi
Familieenheter
Internett
Jobbreise
Hotell wifi
Ferie
Hotell wifi
Skytjenester
Lokasjon 3/ Underleverandør
Administrator
Trådløs aksesspunkt
Industrielt styringsystem

Kilde: NSM

«Complexity is the greatest vulnerability in the Norwegian digital society today»

Norwegian National Security Authority: «A secure digital Norway - ICT Threat Landscape 2018»

«In 2019, more countries' intelligence services will try to recruit sources and map people and businesses in Norway.

They will also try to gain unauthorized access to Norwegian companies' computer networks. The purpose will be to obtain sensitive information and to influence decisions.

The operations of these services will be directed towards individuals and businesses within Norwegian government administration, critical infrastructure, defense and emergency preparedness, as well as against research and development ”

The Norwegian Police Security Services
Threat assessment 2019

"Threats against Norwegian values is dynamic, and together with the societal and technological developments, changes occur so quickly that the countermeasures do not follow.

At the Norwegian National Security Authoritys NorCERT, the alarm goes many times daily, and we are seeing increasingly complex and extensive attacks. "

Background

- In 2016, the Norwegian government decided that a national framework should be established to handle digital events. A first version of the framework was completed in 2017.

- One key measure to contribute to such strengthening is the establishment of a framework for handling ICT security incidents

- A key point of the framework is to designate a sectoral response team

The purpose of the framework is to

- Clarify responsibilities and roles for government actors and other key players in digital incident management
- Communicate what the institutions themselves must be prepared to handle, and what kind of support and coordination can be expected from the sector CERT and the national response team, the Norwegian National Security Authority's NorCERT
- Clarify and strengthen the framework for cooperation between institutions, the response teams in the sector, the Norwegian National Security Authority, the intelligence service, the Norwegian Police Security Service and the police in general
- Further develop the ability to share relevant information and report on digital attacks
- Clarify contact points with other countries and organizations

The Ministry of Education has asked the Unit to adapt the framework to the sector for higher education and research, and to take responsibility for its implementation

When to use the framework

- The framework should be used when an institution is exposed to an ICT security incident (cyber attack) that is of such a nature that it must be escalated for national reasons,

- or when an institution is exposed to an incident that they do not have the opportunity to handle themselves.

The framework becomes mandatory for institutions that are subject to the Ministry of Education and Research's department for ownership of universities and colleges

Applicable to the following institutions

- Arkitektur- og designhøgskolen i Oslo
- Diku – Direktorat for internasjonalisering og kvalitetsutvikling i høyere utdanning
- FEK - De nasjonale forskningsetiske komiteene
- Høgskolen i Innlandet
- Høgskolen i Molde - Vitenskapelig høgskole i logistikk
- Høgskolen i Østfold
- Høgskulen i Volda
- Høgskulen på Vestlandet
- Kunsthøgskolen i Oslo
- NFR – Norges forskningsråd
- Nokut - Nasjonalt organ for kvalitet i utdanninga
- Nord Universitet
- Norges Handelshøyskole
- Norges idrettshøgskole
- Norges miljø- og biovitenskapelige universitet
- Norges musikkhøgskole
- Norges teknisk-naturvitenskapelige universitet
- NSD – Norsk senter for forskningsdata
- OsloMet - storbyuniversitetet
- Sámi allaskuvla - Samisk høgskole
- Simula Research Laboratory AS
- Uninett AS
- Unit - Direktoratet for IKT og fellestjenester i høyere utdanning og forskning
- Universitetet i Agder
- Universitetet i Bergen
- Universitetet i Oslo
- Universitetet i Stavanger
- Universitetet i Sørøst-Norge
- Universitetet i Tromsø - Norges arktiske universitet
- Universitetssenteret på Svalbard

Content in the framework

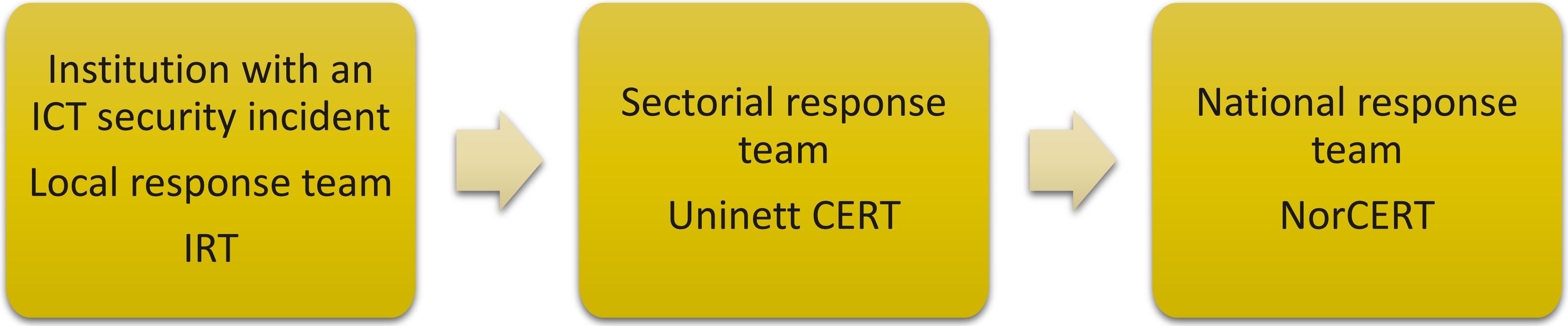
- Actor map and descriptions
- Process and routine description for handling ICT security incidents
- Liaison catalog

Rammeverk for håndtering av IKT-sikkerhetshendelser i høyere utdanning og forskning

Sektortilpasning av rammeverk for håndtering av IKT-sikkerhetshendelser utarbeidet av Nasjonal sikkerhetsmyndighet

Versjon 1.0

Basic process for handling ICT security incidents



Institution with an ICT security incident

Local response team

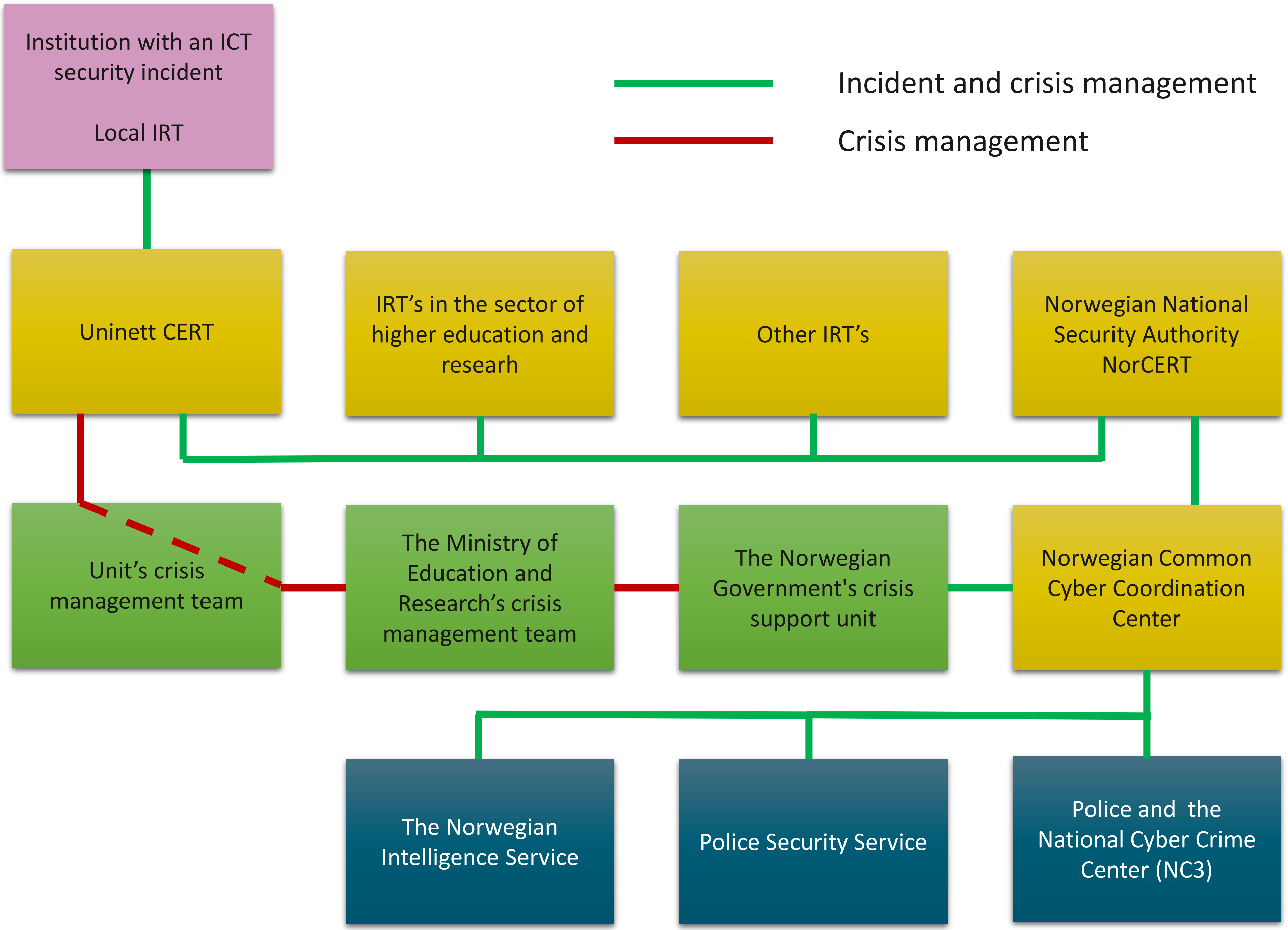
IRT

Sectorial response team

Uninett CERT

National response team

NorCERT



🟩 Incident and crisis management

🟥 Crisis management

Institution with an ICT security incident

Local IRT

Uninett CERT

IRT's in the sector of higher education and researh

Other IRT's

Norwegian National Security Authority NorCERT

Unit's crisis management team

The Ministry of Education and Research's crisis management team

The Norwegian Government's crisis support unit

Norwegian Common Cyber Coordination Center

The Norwegian Intelligence Service

Police Security Service

Police and the National Cyber Crime Center (NC3)

Process and procedures for event handling

ICT security events that fall under the scope of the framework are handled through one systematic process consisting of

1. Planning and preparation
2. Detection and assessment of extent and severity of an event
3. Notification of relevant parties
4. Processes and security controls to deal with the incident
5. Situation reporting
6. Reversal and learning of the incident

Prosess and prosedure levels

The process is divided into the three levels on which the framework is based:

a. Institutions in the sector for higher education and research
b. Uninett CERT as the sectorial response team
c. The Norwegian National Security Authority at national cross-sectoral level

Example of sub-process 2, Detection and assessment of the extent and severity of an event:

Institutions should:

- Have a necessary organization as an incident response team for timely disclosure of incidents
- Have expertise in relevant systems within the institution and be able to assess the severity, extent and consequences at the overall level
- Be able to assess whether critical infrastructure and or critical public functions are or are in danger of being affected by the incident
- Use the Norwegian National Security Authority’s system for classifying of events, or a system that is compatible with this
- Consider the need for assistance

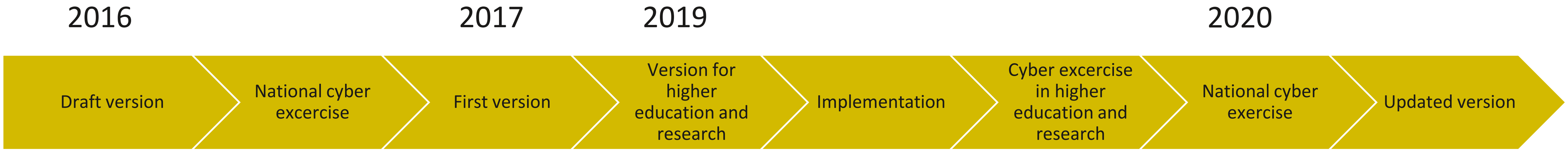
Uninett CERT should:

- Have expertise on relevant systems in the sector and be able to assess the severity, extent and consequences at the overall level
- Be able to decide whether critical infrastructure and or critical public functions in the sector are or are in danger of being affected by the incident
- Be able to advise on further handling and who is to be involved in the incident management
- Use the Norwegian National Security Authority’s system for classifying events, or a system that is compatible with this.

The Norwegian National Security Authority should:

- Monitor the Norwegian digital infrastructure alert system
- Be able to assess whether critical infrastructure and or critical public functions are or are in danger of being affected by the incident
- Be able to recommend further handling and who is to be involved in the incident management

Timeline for the framework



2016 2017 2019 2020

Draft version

National cyber excercise

First version

Version for higher education and research

Implementation

Cyber excercise in higher education and research

National cyber exercise

Updated version

www.unit.no