EUNIS 2019: Framework for handling of ICT security incidents in higher education and research in Norway

Author: Øivind Høiem

Senior advisor
Section for law and information security
Unit – The Norwegian Directorate for ICT and Joint Services in Higher Education and Research
Abels gate 5A, NO-7030 Trondheim, Norway
oivind.hoiem@unit.no

Keywords
Digital security, Handling of ICT security incidents, National coordination of incidents, CERT, Computer emergency response team, IRT, Incident response team, Higher education and research, Public authorities, Roles, Responsibilities, Framework, Good practice, Norway

1. Summary

The purpose of the framework is to clarify the efforts of relevant actors to better enable public authorities in Norway to handle serious ICT security incidents that affect across sectors.

2. The purpose of the framework

The framework for handling of ICT security incidents will help to

- Clarify responsibilities and roles for government actors and other key players in digital incident management
- Communicate what public and private institutions themselves must be prepared to handle, and what kind of support and coordination can be expected from 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

3. Implementation of the framework in the sector for higher education and research

The Ministry of Education and Research has an overall responsibility for the implementation and compliance of this framework in its sector. Unit – The Norwegian Directorate for ICT and Joint Services in Higher Education and Research shall, in consultation with the ministry, ensure the implementation of a framework for handling ICT security incidents. Unit's responsibility is to ensure that all areas of responsibility and tasks that do not lie with the ministry level in the framework are taken care of.

This entails, among other things, ensuring that Uninett CERT maintains the task of being a sector-based response team as described in the framework and preparing a division of tasks and ongoing cooperation between Unit and Uninett in handling ICT security incidents. Uninett CERT has been delegated tasks within operationalization and compliance. This must be done in close cooperation with the sector's own incident response teams (IRTs). The work on the implementation of the framework is largely about coordinating and improving the sector's established routines and capacity for incident management and putting this into a larger national context.

Uninett CERT started in 2017 the work of establishing incident response teams at institutions affiliated with the Norwegian research network provided by Uninett, the Norwegian NREN. They also provide training for team members. This work will ease the work of establishing the framework in the sector. The framework is mandatory for institutions that are subject to the ministry's department for ownership of universities and university colleges.

The framework consists of four main parts; an actor map, a description of how to handle ICT security incidents, a contact directory and a description of how to classify of ICT security incidents. Figure 1 shows the actor map.

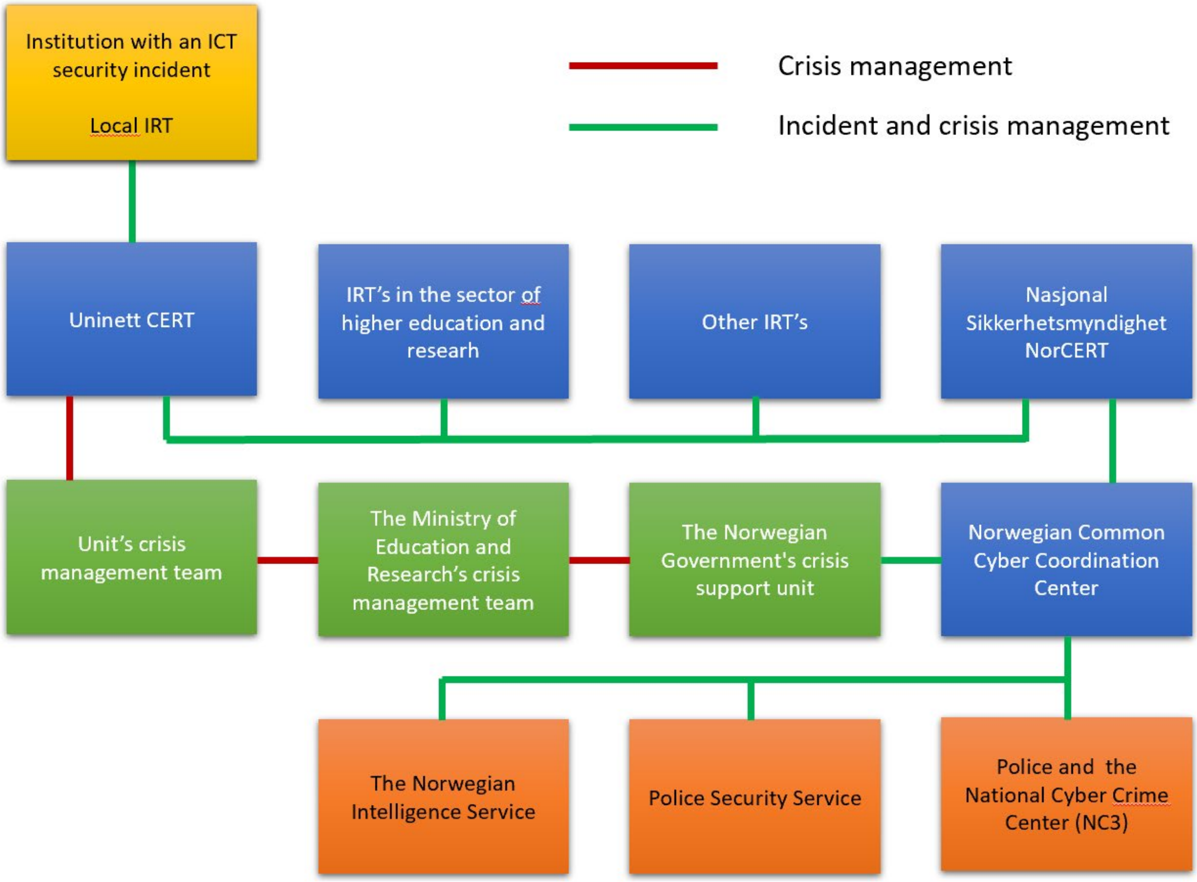
Institution with an ICT security incident
Local IRT
Crisis management
Incident and crisis management
Uninett CERT
IRT's in the sector of higher education and researh
Other IRT's
Nasjonal Sikkerhetsmyndighet NorCERT
Unit's crisis management team
The Ministry of Education and Research's crisis management 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)

Figure 1 - Actor map

4. References

Norwegian National Security Authority (2018). *Rammeverk for håndtering av IKT-hendelser (NO)*. https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/rammeverk-hendelseshandtering

5. Authors' biographies

Øivind Høiem (CISA, CRISC, ISO27001 LI) is Senior advisor at Unit - Directorate for ICT and Joint Services in Higher Education and Research in Norway. He has over 25 years' experience with information security, awareness, risk management and management systems. Previously he worked at Uninett, the Norwegian NREN, where he advised managers and information security officers at the higher educational and research sector and in Equinor (Statoil), where he among other things worked with risk, IS-audit and awareness programs. Linked in profile: https://www.linkedin.com/in/ohoiem/

6. Reviewers Comments

Q: Did you Benchmark with other NREN's to compare, or be inspired by their frameworks?

A: No, because in this case it was important to align with the common framework made by the Norwegian National Security Authority for the public sector in Norway.