Policy for Digital Incident Management and Disaster Recovery

Document type	Topic specific policy
Managed by	Head of IT Division
Approved by	Director of Organization and Infrastructure
Valid from	12.06.2023
Next revision within	12.06.2025
Classification	No
Reference ISO	ISO/IEC 27002:2022 5.5-5.7, 5.24, 5.25, 5.27, 5.29, 5.30, 6.4, 6.8, ISO/IEC 27035-2:2016 4.3b, 4.6e
Reference NSM's principles for ICT-security	1.3.3b,3.3.1-3.3.7, 3.4.1-3.4.6, 4.1.1-4.1.6, 4.2.1-4.2.3, 4.3, 4.4
Reference Law/Rule	
Reference internal documents	Policy for Information Security, Policy for Security and Incident Management, Policy for Classification of Information.

1. Purpose

The purpose of this policy is to establish quality requirements within digital preparedness, digital crisis management, and the handling of security and operational incidents. The policy defines roles and responsibilities for the work related to incident management at NTNU.

2. Applies to

The Policy for Digital Incident Management and Disaster Recovery apply to all individuals who use, manage, and operate ICT systems at NTNU, with particular emphasis on:

a. Employees at the IT Division at NTNU
b. System owners
c. Line managers

3. General Principals

a. Security incidents must be reported to, handled, and coordinated by NTNU SOC at the Digital Security Section.
b. The Digital Security Section must be able to conduct its work without hindrance.
c. NTNU must adhere to the principles of responsibility, equality, proximity, and collaboration in incident management and digital preparedness work.
d. The framework for digital incident management plans must be based on ITIL, ISO27035, and NSM's Framework for ICT Incident Management.
e. NTNU must have procedures for securing and handling data and evidence material
f. NTNU must have procedures for sharing information and data about incidents.
g. NTNU must have procedures for training, evaluation, and improvement of preparedness plans.

4. Incident Management

A security incident is an event resulting from an intentional breach or an imminent threat of an intentional breach of confidentiality, integrity, or availability in a system, service, application, or information/data, or a violation of the ICT regulations, information security policies with procedures, or current security practices.

a. An incident management plan must consist of routines and procedures to be performed before, during, and after an incident occurs. An incident is an unplanned disruption or degradation of the quality of a service in production or an event that may lead to a future reduction in quality or a breach of service.
b. The incident management plan must define procedures for identifying, classifying, handling, and restoring normal operations during incidents.
c. The incident management plan, including procedures, processes, and tools, is subject to confidentiality to protect the operational security of the incident and crisis management function.

4.1 Organization of Incident Management

a. NTNU Security Operations Centre (SOC) has the operational responsibility to detect threats and coordinate, handle, and analyse security incidents in NTNU's digital infrastructure.
b. IT Incident Manager (IM) has the operational responsibility to handle and coordinate incidents related to the quality of ICT services at NTNU. The IM is the process owner for the ITIL process "Incident Management," which aims to restore normal service delivery as quickly as possible to reduce negative impacts on the organization and users when a service is unavailable or reduced.
c. NTNU CSIRT (Computer Security Incident Response Team) is an extended technical security group and a support resource for NTNU SOC, working on preventive digital security within their domain and incident management.

4.2 Reporting of Incidents and Vulnerabilities

a. Incidents that involve a security breach or a suspected security breach, must be reported to NTNU SOC[1] at the Digital Security Section without undue delay.
b. Vulnerabilities, or a suspected vulnerability, should be reported to NTNU SOC at the Digital Security Section for assessment.
c. An operational incident at NTNU is an incident that can be categorised according to the table in 4.3.4.
d. Operational incidents should be reported to the Incident Manager.

4.3 Assessment of Incidents and Vulnerabilities

a. Incidents must be categorised, prioritised, and assigned within 30 minutes during regular working hours (08:00-15:45 / 08:00-15:00 Summertime).
b. Incidents should be categorised according to the table in 4.3.1.
c. Incidents are prioritised based on the classification of systems and information according to the "Policy for Information Classification."
d. The triage procedure should prioritise incidents based on classification and the incidents:

[1] https://www.ntnu.no/adm/it/ntnu-soc

- Level of negative impact on the functionality of a system, application, or service (Functional Impact)
- Level of negative impact on the confidentiality and integrity of information (Information Impact)
- Level of negative impact on the ability to restore normal service or system operations within a given time (Recoverability Impact).

4.3.1 Categorisation of Security Incidents

NTNU	*NSM*	*Description / Examples*
Abusive content	Støtende innhold	Spam and unwanted emails, publication of content that violates ethical guidelines, threats and harassment through digital channels, distribution of illegal material using NTNU resources.
Information gathering	Rekognosering/ Informasjonsinnsamling	Attempts to compromise systems or services by exploiting vulnerabilities in the system/service or misconfiguration, password guessing, or attempts to bypass security mechanisms, attempts at malware infection.
Intrusion attempts	Forsøk på kompromittering	Attempts to compromise systems or services by exploiting vulnerabilities in the system/service or misconfiguration, password guessing, or attempts to bypass security mechanisms, attempts at malware infection.
Compromised asset	Kompromittering	Successful unauthorized privileged access to a system or service, loss/theft of equipment and devices, successful malware infection.
Compromised user	Kompromittering	Successful unauthorized access to a user account, leakage of user accounts with passwords.
Compromised information	Kompromittering	Successful unauthorized access to data or information, information leakage, leakage of personal information.
Vulnerability	Rekognosering/ Informasjonsinnsamling	Vulnerable, misconfigured, and exposed application, service, or system.
Availability	Tjenestenekt	Denial of service (DoS) / Distributed denial of service (DDoS) attacks against a system, service, or application, sabotage.
Fraud	Svindel	Phishing, Smishing, Telephone scams, Extortion, Unauthorized use of NTNU resources.
Other	-	Incidents that threaten the digital security of NTNU but cannot be categorised in the other categories.

4.3.2 Categorisation of Operation Incidents

a. The table shows the main categories of ICT operational incidents defined at NTNU. If it is appropriate to provide more detailed granularity, subcategories can be used. Subcategories are defined in the incident management plan.

Category	*Definition*
Hardware error	Physical failure in hardware, including firmware.
Software error	Logical error in software.
Connectivity error	Physical or logical failure in network equipment.
Operational environment error	Physical failure in the operational environment where ICT infrastructure is located.
Procedural error	Humar error, including error handling, poor configuration management, etc.
User error	Human error.

4.3.3 Response Time

a. Response time is the maximum time from when an incident occurs/is reported to when incident or crisis management activities begin during regular working hours.
b. Downtime refers to the acceptable period of system unavailability or information unavailability.

Classification	*Response time*	*Acceptable lower time*
Organisation critical	30 min	None
Functional critical	60 min	4 hours
Severe	4 t	2 days
Less severe	48 t	More than 2 days

4.4 Sharing of Security Incidents

NTNU must comply with the established Traffic Light Protocol (TLP[2]) for sharing information and data related to threats and security incidents (table below) to receive, share, coordinate, and collaborate with the higher education sector and international, national, and private response teams. TLP was developed to facilitate the sharing of information related to security incidents. TLP is a set of procedures (colour codes) used to label information to ensure that sensitive information is shared securely.

Traffic light protocol (TLP)	**Recommended NTNU grading**	**Description**	**Sharing conditions**
TLP:RED	Level 4 *Strictly Confidential / Not for Publication* *Exempt from public*	The information is for the recipient only. If it is necessary to share the information, the recipient must have the approval	The owner will have control over named individuals who

[2] https://www.first.org/tlp/

	Cf Sec 24.3 Freedom of Information Act	of the information owner to provide it to a named individual.	have access to the information.
TLP: AMBER **TLP: AMBER+STRICT**	Level 3 *Confidential / Not for Publication* *Exempt from public Cf Sec 24.3 Freedom of Information Act*	The information is for the recipient's organization (including consultants, outsourced personnel working for the organization) who have a need-to-know and a valid non-disclosure agreement to take necessary actions. If the recipient wishes to share the information with other organizations, they must have the approval of the information owner to provide it to a named organization.	The owner will have control over named organizations that have access to the information.
TLP:GREEN	Level 2 *Internal / Not for Publication* *Exempt from public Cf Sec 24.3 Freedom of Information Act*	The information can be shared with other organizations or individuals within the information security community but should not be published or posted on websites/open mailing lists.	The owner will not have control over the dissemination but assumes that no recipient will publish the information.
TLP:CLEAR	Level 1 *Open*	The information is publicly available, published, and distributed to the public. Any contact person can publish the information.	The information owner expects the information to be publicly disclosed.

4.5 Access, Data Collection, and Evidence Handling

a. The incident management plan must have a procedure for data collection and preservation of evidence. This procedure must define when data collection should take place and the legal basis for the collection.
b. Procedures for data collection and evidence handling must ensure that:
    - Data collection starts as soon as possible and is carried out by competent personnel.
    - Data collection complies with laws and regulations.
    - Data collection follows the principles of forensic soundness.
    - Data collection follows the principle of order of volatility.
    - Data collection is handled properly and correctly.
    - Data collected is deleted/destroyed when the need for processing ceases.

- All collected data is stored and processed in a manner that ensures confidentiality, integrity, and privacy.

c. NTNU SOC must have read access to data from all systems and services to perform security analysis.
d. NTNU IRT (Incident Response Team) must have system administrator access to all systems to handle incidents.
e. Individuals responsible for data collection and handling of evidence must document competence demonstrating sufficient knowledge to perform this task. This competence must be approved by the Digital Security Section.

4.6 Exercise and Review of Incident Management Plan

a. The incident management plan must be reviewed at least once a year to ensure its relevance following the updated threat and risk landscape for NTNU. This work must be based on risk assessments, handling incidents, and trends in the threat landscape.
b. Procedures for incidents must be documented and approved for implementation in the plan as they are developed if they do not already exist in the incident management plan.
c. Procedures in the incident management plan must be continuously reviewed after being used as part of the post-incident handling routine.
d. The incident management plan shall be exercised at least annually.

5. Digital Crisis Management

A crisis is any event, expected or unexpected, that puts lives or the core operations of NTNU at risk or reduces NTNU's ability to perform normal operations[3]. A crisis is classified as either business-critical or function-critical.

a. The crisis management plan is based on procedures for managing crises to minimize consequences and restore normal operations as quickly as possible. The plan also extends the incident management plan and describes the procedures for preparing to handle a crisis. The plan must include, at a minimum:
    - Procedure for effectively mobilizing roles and functions to initiate crisis management quickly.
    - Procedure for communication and collaboration among relevant parties.
    - Procedure for escalating and activating central emergency management for the organization.
    - Procedure for activating the business continuity plan.
    - Procedure for gathering, processing, analysing, and utilizing information to build a situational picture that provides the best possible basis for decision-making.

[3] Policy for Readiness at NTNU

b. The crisis management plan should cover function-critical and business-critical services and systems. These are crises that affect teaching, research, dissemination, innovation, as well as administration and management.
c. The crisis management plan should identify resource requirements for recovering normal operations from a crisis.
d. The crisis management plan should have a risk-based approach and be based on risk and vulnerability analysis, including an analysis of business impact.

5.1 Organization of Crisis Management

a. Responsibilities and roles in the crisis management plan should include relevant functions with competent personnel and resources to handle a crisis. The organization of crisis management should be defined according to:
    1. Responsibility principle, meaning that those responsible in normal situations, also have the responsibility in case of extraordinary events.
    2. Similarity principle, meaning that the organization responsible for managing a crisis should resemble the daily organization as much as possible.
    3. Proximity principle, meaning that crises must be handled at the lowest possible level.
    4. Coordination principle, meaning that crisis management must be coordinated among the involved parties.

5.2 Exercise and Review of Crisis Management Plan

a. The crisis management plan must be periodically reviewed to ensure it is up to date and covers critical business functions.
b. The crisis management plan must be regularly tested, at least once a year. Lessons learned should be used to ensure quality, further development, and improvement of the plan and the roles included in the crisis management organization so that leadership and staff understand its implementation.
c. The crisis management plan must be based on a risk-based approach, with risk and vulnerability analysis and a business impact analysis as the foundation for the plan.

5.3 Business Continuity

Planning of business continuity involves establishing risk management processes and procedures which are aimed at preventing disruptions in business-critical services and restoring full functionality to the organization as quickly and smoothly as possible.

a. The business continuity plan is built on the crisis management plan and is an extension of it.
b. The business continuity plan should include routines and procedures for maintaining or restoring the operation of business-critical services (T4) until normal operations can be restored.
c. The business continuity plan should provide technical support to the central emergency management group to perform tasks in the event of infrastructure failure.

d. The business continuity plan should document minimum resource requirements for activation and the resource needs to remain active.
e. The business continuity plan should, at minimum, include procedures for:
    - Relocating or restoring technical infrastructure and support functions for emergency support.
    - Moving or restoring the operation of business-critical services at temporary locations.
    - Moving the IT Division to a temporary location to maintain or restore the operation of business-critical services.
    - Moving back to the original premises and restoring normal operations after a crisis.

6. Roles and Responsibilities

6.1 Director of Organization and Infrastructure

a. Delegated authority as the highest emergency preparedness official at NTNU.
b. Local emergency preparedness responsibility for the central administration.

6.2 Head of IT Division

a. Emergency preparedness responsibility for the IT Division
b. Responsible for incident and crisis management at the IT Division
c. Approves the incident management plan.
d. Approves the crisis management plan.

6.3 Head of HR and HSE Division

a. Approves the business continuity plan.
b. Ensures necessary resources are available and allocated in NTNU IRT.
c. Responsible for ensuring that managers are aware of and have sufficient competence to fulfil their responsibilities according to this policy.

6.4 Head of Communication Division

a. Ensures necessary resources are available and allocated in NTNU IRT.

6.5 Head of Division for Governance and Management Systems

a. Ensures necessary resources are available and allocated in NTNU IRT.

6.6 Head of Digital Security Section

a. Responsible for implementing the incident management plan.
b. Responsible for implementing the crisis management plan.
c. Responsible for detecting, coordinating, and handling security incidents.
d. Responsible for detecting, coordinating, and handling vulnerabilities.
e. Responsible for the triage procedure for security incidents.
f. Responsible for NTNU IRT.
g. Ensures compliance with the incident management plan at the Digital Security Section.

6.7 Head of IT Infrastructure Section

a. Emergency management leader for the IT Division
b. Responsible for detecting, coordinating, and handling operational incidents.
c. Responsible for the classification of operational incidents.
d. Responsible for the triage procedure for operational incidents.
e. Ensures necessary resources are available and allocated in NTNU IRT.
f. Consulted regarding the incident management plan.
g. Consulted regarding the crisis management plan.
h. Ensures compliance with the incident management plan in the IT Infrastructure Section.

6.8 Head of IT Development Section

a. Informed about changes in the incident and crisis management policies.
b. Ensures necessary resources are available and allocated in NTNU IRT.
c. Ensures compliance with the incident management plan at the IT Development Section.

6.9 Head of IT Support Section

a. Informed about changes in the incident and crisis management policies.
b. Ensures compliance with the incident management plan at the IT User Support Section.