Policy for Discrepancy Reporting and Discrepancy Processing in Information Security and Privacy

Type of document	Topic specific policy
Managed by	Head of IT Division
Approved by	Director of Organization and Infrastructure
Applies from	12.06.2023
Next revision by	12.06.2025
Classification	Open
Reference ISO	27002: 5.27,6.4,6.8
Reference NSMs core principles for ICT-safety	4.4
Reference LOV/Rule	eGovernment regulations (eForvaltningsforskriften) § 15, § 25, Personal data Act
Reference intern documents	Superior Policy for Information Security

1. Purpose

The purpose of discrepancy reporting and discrepancy processing in information security and privacy is to handle violations of applicable laws, regulations, as well as internal guidelines and procedures.

A specific purpose is to ensure effective reporting to the Norwegian Data Protection Authority (Datatilsynet) in case of breaches concerning the handling of personal data. It is also a purpose to ensure that affected data subjects are promptly notified so they can safeguard their interest.

2. Applies to

This policy for incident reporting and incident management applies to all individuals who have access to, process, and manage information through NTNU's digital and analogue information systems.

2.1. Scope

This policy is separate from the Guideline for Incident Management and Crisis Management in IT.

3. General Principles

a. Discrepancy management should contribute to continuous learning and improvement of NTNU's procedures, processes, and systems.
b. Reports of discrepancy and discrepancy management constitute a significant part of the systematic work on information security and are an important aspect of NTNU's internal control.

c. Reporting discrepancy is necessary and desirable at NTNU, and everyone with access to NTNU's information system is responsible for reporting incidents at NTNU
d. Reporting discrepancy and handling them should lead to positive consequences for individuals work and for NTNU as a whole, by improving and streamlining NTNU's work processes and systems
e. Reacting to discrepancy is not associated with negative sanctions. This means that both the person who discovers the discrepancy and the person who reports it are protected against negative reactions.
f. When the outcome of is related to non-conformance processing of personal data, the processing should be documented and reviewed by the management.

4. Discrepancy Management

A discrepancy, as defined in this guideline, refers to a violation of laws and regulations, as well as breaches of NTNU's internal rules, policies and guidelines that directly or indirectly regulate the use of NTNU's information systems, including the processing of personal data. Discrepancy management is the collective process of identifying, reporting, processing, reporting the status of, and closing the discrepancy. The handling should make it possible to restore the condition, remove the cause of the discrepancy, reduce negative consequences for both NTNU and the third parties, and facilitate the prevention of future information security breaches and violations of privacy. In this way, discrepancy management contributes to continuous learning and improvement of NTNU's procedures, process systems.

4.1. Reporting Discrepancy

a. The person or persons who discover a discrepancy should report it in NTNU's digital discrepancy reporting system without undue delay.
b. Examples of categories to be reported as discrepancies:
    i. Violations of laws, regulations, and instructions
    ii. Violations of policies, procedures, or processes for secure handling of information
    iii. Breaches of personal data security
    iv. Lack of policies and procedures for proper information handling and safeguarding information security
    v. Lack of procedures for safeguarding personal data security
    vi. Lack of security controls according to policies
    vii. Lack of access control to information assets or equipment used for information processing

4.2. Contents of the Report

a. The content of the discrepancy report should describe, using open and internal information, that a breach or incident has occurred, where the breach/incident occurred, and potentially describe the consequences of the breach/incident
b. The discrepancy report should not contain personal information related to names or any other type of information where confidentiality may be required.
c. Discrepancies should never be directed at individuals but at the element or action in the work process that caused the security breach or incident. The action is the "subject" of the discrepancy, not the person.
d. Discrepancies concerning the notification of reprehensible conditions in information security work should be recorded and handled in accordance with NTNU's procedures for notification under the Working Environment Act.

4.3. Follow-up of Discrepancies

a. The discrepancy is received by the Digital Security Section, which assesses the criticality of the incident (*low* (1), *moderate* (2), *high* (3), *very high* (4)).
b. The Digital Security Section ensures that necessary immediate measures are taken and that those responsible are notified.
c. For violation of privacy, see section 4.4.
d. In consultation with the discrepancy processor, the discrepancy owner should, to the best of their ability, identify and analyse the cause of the discrepancy in order to identify the root cause. The discrepancy owner is the line manager who is responsible for the work to which the discrepancy relates. The analysis allows for the development of targeted and effective measures related to competence, resources, leadership, and procedures. For all discrepancies where the criticality is considered low (1) or moderate (2), the discrepancy owner in the line should be responsible for handling and closing the discrepancy. If the criticality is considered high (3) or very high (4), the discrepancy owner should be the Director of Organization and Infrastructure or at an equivalent level.
e. For discrepancies assessed as serious/critical, the line manager in the unit where the discrepancy occurred will be the responsible person for the measures and must ensure that the necessary and immediate required measures are implemented.
f. Based on causal factors, the discrepancy owner should assess how the discrepancy should be handled and propose measures. In consultation with the discrepancy owner, the Digital Security Section must document the proposed measures in the discrepancy reporting system with a specific deadline and a responsible person for implementing the measures, a measure owner. Measure owners can be one or more system owners, process owners, managers at a different level or unit, or in some cases, the measure owner and discrepancy owner can be the same person. The measures should specify the desired effect.
g. The measure owner should assess the proposed measures. For measures that involve extensive change or resources, the measure owner must propose a solution with a rough estimate of resource requirements. This is approved by the incident owner before the measures are implemented.
h. The measure owner reports the progress of the measure implementation to the discrepancy owner in the discrepancy report system, as well as when the measures are implemented.
i. Leaders at NTNU must address incidents classified as serious or critical in their management meetings and use discrepancy processing as a significant factor in the improvement work in their part of the organization. All discrepancy related to the handling of personal data should be addressed in management meetings.

4.4. Violation of Privacy

a. If the discrepancy concerns a breach of the security regarding personal data that poses a risk of negative privacy consequences for the data subject, or if the magnitude of the discrepancy is significant, the Norwegian Data Protection Authority should be notified within 72 hours.
b. The legal expert and the Data Protection Officer should be notified with the discrepancy report when it relates to a possible breach of security regarding personal data.
c. Notification to the Norwegian Data Protection Authority
    i. The Digital Security Section must, in consultation with the legal expert and/or the Data Protection Officer, assess whether the discrepancy should be reported to the Norwegian Data Protection Authority. In the absence of a legal expert, the Digital Security Section will assess whether the deviation should be reported to the Norwegian Data protection authority.

ii. The legal expert, in collaboration with the Digital Security Section and the discrepancy owner, and in consultation with the Data Protection Officer, must write the notification to the Norwegian Data Protection Authority. In the absence of a legal expert, the Digital Security Section and the Data Protection Officer must prepare the notification.
iii. The line manager at the unit where the discrepancy occurred must be the responsible party for sending a report to the Digital Security Section as a basis for the consolidated report.

d. In the event of a breach of the security regarding personal data that may pose a high risk to the rights and freedom of the data subjects, the discrepancy owner/measure owner must take immediate action to notify the data subjects so that they can safeguard their interests. The notification must include:
    i. A clear and precise description of the nature of the breach
    ii. Contact information for the Data Protection Officer
    iii. Probable consequences
    iv. Description of any damage limitation measures that have been implemented or planned for implementation
    v. The notification must be made by the measure owner without undue delay after becoming aware of the discrepancy.

4.5. Closing the Discrepancy

a. The discrepancy is closed by the discrepancy processor when the measures have been implemented/carried out by the measure owner and are functioning as intended. Discrepancy can also be closed when more extensive and long-term measures have not yet been implemented but have been accepted and planned for implementation by the measure owner.
b. The discrepancy owner accepts completed measures. The Digital Security Section closes the discrepancy in consultation with the discrepancy owner.
c. The discrepancy can also be closed when not all measures have been fully implemented, provided that short-term measures to limit the harmful effects have been implemented. It is assumed that corrective measures have been initiated, but are of such scope that it will take a long time to complete implementation.
d. The discrepancy owner reports to the discrepancy reporter that the discrepancy has been closed.
e. The discrepancy owner reports to the IT Division on the desired and achieved effects of the discrepancy handling.
f. In the case of discrepancy related to personal data that have been reported to the Norwegian Data Protection Authority, feedback from the Norwegian Data Protection Authority must be registered as a separate case in the document management system “ephorte”, case number 2018/43111. The legal expert in the Division for Governance and Management Systems or the Digital Security Section informs the Director for Organization and Infrastructure and the line manager about the outcome. The discrepancy reporter is informed of the feedback when the discrepancy is closed by the Digital Security Section.

5. Roles and Responsibilities

5.1. Rector

a. Responsible for presenting an annual report on information security and discrepancy reports to the NTNU board.

5.2. Director of Organization and Infrastructure

a. Responsible for ensuring that NTNU has a process for handling discrepancy in information security
b. Responsible for including discrepancy handling in the management's annual review of information security
c. Acts as the discrepancy owner in the case of serious or critical breaches of privacy

5.3. Line Manager (Discrepancy Owner)

a. Responsible for ensuring that employees have knowledge of when and how discrepancies should be reported
b. Responsible for including discrepancy handling in the improvement work at their own unit
c. Acts as the discrepancy owner and is responsible for appropriate handling of discrepancies at their own unit
d. Responsible for distributing measures to the measure owner for implementation
e. Is the measure owner in cases where the superior level is the discrepancy owner
f. Is responsible for seeking necessary assistance when needed
g. Must analyse the discrepancy, assess how the discrepancy should be handled, and propose measures to close the discrepancy
h. Is responsible for ensuring notification to the data subjects if personal data may be compromised.

5.4. Head of Division for Governance and Management Systems

a. Is responsible for ensuring that the discrepancy system related to information security is part of NTNU's comprehensive internal control and corporate governance.
b. Is responsible for ensuring that NTNU has a digital discrepancy system for reporting and handling discrepancy
c. Is responsible for facilitating the collection and analysis of data that demonstrate satisfactory discrepancy management at NTNU
d. Is responsible for managing discrepancies during internal/external audits
e. Must be consulted regarding changes to this policy

5.5. Head of HR and HSE Division

a. Is responsible for facilitating and providing targeted training within the discrepancy process for managers and employees to ensure compliance with this policy
b. Must be consulted regarding changes to this policy

5.6. Head of IT Division

a. Is responsible for receiving, evaluating, distributing, and reporting discrepancy notifications
b. Must assess whether the desired effects of the discrepancy management have been achieved.

5.7. Head of Digital Security Section

a. Is responsible for handling discrepancies within information security and data privacy

b. Is responsible for allocating resources to ensure the proper receipt and dissemination of discrepancies related to information security
c. Must be consulted regarding changes to this policy

5.8. Employees and Students

a. Are responsible for reporting identified discrepancies in accordance with this policy

5.9. Measure Owner

a. Is responsible for implementing the measures formulated by the discrepancy owner.
b. Must inform the discrepancy owner when measures are implemented or when there is a plan for phased implementation

5.10. Data Protection Officer

a. Must ensure compliance with NTNU's policy on discrepancy management
b. Must ensure that NTNU fulfils its obligations to notify the Norwegian Data Protection Authority and data subjects