Procedure

2026-06-12

Registration number: MIUN 2026/1611

Mittuniversitetet
MID SWEDEN UNIVERSITY

Procedure for IT and Information Security Incident Management

Published: 2026-06-16

Decision-makers: Head of department Digitalization and services Helena Wallskog

Responsible function: Digitalization and services

Administrator: Sofie Almqvist

Date of decision: 2026-06-16

Period of validity: Until further notice

Last review: 2026-06-16

Summary: This Procedure regulates responsibilities, roles and processes for IT and information security incident management at Mid Sweden University. The Procedure forms part of the Information Security Management System and aims to describe how incidents shall be managed, as well as how reporting, follow-up and improvement shall be carried out.

Previous versions: MIUN 2024/955, MIUN 2023/651, MIUN 2020/1414.

Procedure

2026-06-12

Act number: MIUN 2026/1611

Table of contents

Procedure for Incident Management in IT and Information Security

1 Introduction

The Procedure for IT and Information Security Incident Management applies to all staff and students at Mid Sweden University. The purpose is to describe how incidents that affect or risk affecting the University's information, digital services or information processing shall be managed, as well as how reporting, follow-up and improvement shall be carried out.

The Procedure has been developed based on the Preparedness Ordinance (2022:524) and regulations issued by the Swedish Civil Contingencies Agency (MCF). When handling personal data breaches, applicable data protection legislation (GDPR) shall also be taken into account.

The document is supplemented by internal procedures and instructions.

2 Definition of Incidents

2.1 Incident

An incident is an event that affects or risks affecting the confidentiality, integrity or availability of the University's information, information processing or digital services.

Incidents may have technical, organisational or physical causes, provided that they affect or may affect information security or the University's digital services.

Example: system outages, attempted intrusion into computers or networks, unauthorised access to personal data or other sensitive information, suspected phishing, theft or loss of information carriers, unauthorised physical access to spaces where information or information systems are handled.

2.2 Serious Incident

A Serious Incident is an incident that has caused, or is assessed as being capable of causing, serious impact on the University's digital services, information

processing or information security, and therefore requires coordinated management.

In assessing whether an incident constitutes a Serious Incident, particular consideration shall be given to whether the incident results in, or risks resulting in, serious operational disruption, extensive information loss or information leakage, or significant financial, legal or reputational damage.

Example: personal data breach, ransomware attack, extensive system outages, serious data intrusion.

3 Roles and Responsibilities

3.1 Staff and Students

Staff and students at Mid Sweden University are responsible for promptly reporting incidents in accordance with this procedure.

3.2 Heads of department

Heads of department and department managers are responsible for ensuring that employees are aware of the incident management process and the importance of reporting incidents.

In the event of serious incidents, heads of department and department managers are responsible for following up the implementation of, and compliance with, decided measures within their respective areas of responsibility.

3.3 System Owners

System Owners are responsible for ensuring that decided security measures resulting from incidents are implemented and followed up for the systems for which they are responsible.

3.4 System Manager

System Managers are responsible for incidents relating to the systems they manage and shall cooperate with the Incident Manager in the handling of such incidents.

This includes:

- reporting incidents relating to their respective system and contributing necessary system expertise to the analysis and handling of the incident,
- maintaining contact with the system supplier, where necessary,
- cooperating with the Incident Manager regarding communication relating to the relevant system, and
- escalating to the System Owner in the event of serious incidents.

In the event of personal data breaches, System Managers participate in analysis and reporting to the Swedish Authority for Privacy Protection (IMY).

3.5 IT Support

IT Support is a function within Digitalization and Services that is responsible for receiving reported incidents, making an initial assessment of the nature/category and scope of the incident, and managing and resolving incidents within the scope of its assignment and mandate. Where necessary, incidents are forwarded to the responsible function according to the established process.

3.6 Incident manager

The Incident manager, located within Digitalization and Services, is responsible for coordinating the management of serious incidents. This includes:

- collecting and compiling relevant information,
- coordinating necessary resources for managing the incident,
- analysing the incident and its consequences,
- communicating with affected stakeholders,
- escalating incidents according to established escalation procedures,
- being responsible for reporting to the National Defence Radio Establishment (FRA) and the Swedish Authority for Privacy Protection (IMY) and, in specific cases, for filing a report with the Police Authority,
- acting as a contact function with the relevant authorities,
- ensuring that incident reports are drawn up and documented, and
- following up on managed incidents and, where necessary, initiate follow-up meetings with a focus on improvement.

3.7 Incident Management Team

In the event of a serious incident, the Incident Manager shall be able to convene an Incident Management Team for the coordinated management of the incident. The Incident Management Team shall consist of relevant representatives from affected functions, depending on the nature and scope of the incident.

The Incident Management Team may, for example, include representatives from:

- IT Operations and Development
- IT Support
- System Management
- Information Security
- Data Protection
- IT Security
- Property Department
- Communications Function
- Affected Operations
- Suppliers

The Incident Manager is responsible for identifying and convening relevant participants. The Incident Management Team is jointly responsible for operational coordination, maintaining situational awareness, prioritising measures and sharing information during incident management.

3.8 Contingency function

The Contingency function is a function within Digitalization and Services that handles alerts from monitored services outside regular working hours. In the event of alerts indicating an incident, the contingency function is responsible for making an initial assessment, taking necessary initial measures and escalating the matter in accordance with established procedures.

3.9 Data Protection Officer

The Data Protection Officer is responsible for, where necessary, participating in the management and analysis of personal data breaches and supporting the Incident Manager in reporting personal data breaches to the Swedish Authority for Privacy Protection (IMY).

3.10 Property Department

The Property Department is responsible for managing physical and environmental incidents that affect IT and information security.

4 Incident process

The purpose of the incident process is to ensure that incidents are handled promptly and in a structured manner in order to limit consequences, restore operations and enable follow-up and improvement. Incident management shall be prioritised within the organisation.

4.1 Detect and report

Anyone who discovers an incident at Mid Sweden University shall immediately report it in one of the following ways:

- Via the Service Portal
- E-mail: itsupport@miun.se
- Telephone: 010-142 80 00, select IT Support

In the event of serious incidents, IT Support shall always be contacted via the above phone number.

4.2 Assess and classify

Reported incidents are assessed in terms of scope and impact on operations, information and digital services. Based on this assessment, the incident is assigned a priority according to defined priority levels.

At this stage, it is also assessed:

- whether the incident constitutes a serious incident,

- whether the incident is subject to reporting obligations to the National Defence Radio Establishment (FRA) and/or the Swedish Authority for Privacy Protection (IMY), and
- whether the incident may involve suspected criminal activity and shall therefore be reported to the police.

4.3 Contain and Resolve

Necessary measures shall be taken to limit the consequences of the incident. Measures may include technical, organisational or physical measures, such as system isolation, account closure or other mitigation measures.

4.4 Restore

After the incident has been contained, affected services and functions shall be restored to normal operation to the extent possible. Return to normal operations shall be carried out in a controlled manner, taking into account security and operational needs.

4.5 Evaluation and improvement

After an incident has been managed, it shall be followed up and analysed in order to identify causes, draw lessons learned and implement improvement measures.

Where necessary, follow-up meetings shall be conducted and procedures, processes or security measures are updated to reduce the risk of similar incidents occurring again.

The incident management process shall be exercised regularly in order to ensure its effectiveness, clear allocation of responsibilities and the capability to manage different types of incidents. Lessons learned from conducted exercises and incidents that have occurred shall be systematically incorporated into relevant governing documents, procedures and ways of working.

5 Reportable incidents

5.1 Incident Reporting to the National Defence Radio Establishment

Mid Sweden University shall report incidents that are subject to reporting obligations to the National Defence Radio Establishment (FRA) in accordance with applicable regulations. The assessment of whether an incident is subject to reporting to the National Defence Radio Establishment (FRA) is made by the Incident Manager within the framework of the incident process. Reporting shall take place promptly in accordance with the timeframes specified in applicable regulations.

5.2 Incident reporting to the Swedish Authority for Privacy Protection

Personal data breaches shall be reported to the Swedish Authority for Privacy Protection (IMY) where required under applicable data protection legislation (GDPR). The assessment of whether an incident is subject to reporting to the Swedish Authority for Privacy Protection (IMY) is made by the Incident Manager, and where necessary, in consultation with the Data Protection Officer.

5.3 Reporting to the Police in case of suspected crime

Incidents involving suspected criminal activity shall be reported to the police. Responsibility for assessing whether an incident shall be reported to the police, and for carrying out such reporting, rests with the function responsible for managing the incident.

For incidents managed by the Incident Manager, the Incident Manager is responsible for the assessment and for carrying out the police report. For incidents relating to physical security, the Property Manager is responsible for the assessment and for carrying out the police report.

The assessment shall, where necessary, be carried out in consultation between the functions concerned.

5.4 Registration and Archiving

Documents relating to reporting to the FRA, IMY and the Police Authority shall be registered, preserved and, if necessary, marked as confidential in accordance with applicable regulations.

6 Escalation procedures

Incidents are escalated based on assessed priority, scope and impact in accordance with the incident process.

Serious incidents shall be escalated to the Head of IT Operations and Development. Where necessary, the matter shall be further escalated to the Head of Digitalization and Services. Escalation shall take place as soon as the incident has been assessed as serious, or earlier if the event indicates ongoing malicious activity, extensive operational impact or a risk of information leakage.

If an incident is assessed to be of such severity that the crisis management function needs to be activated, the matter shall be handled in accordance with the applicable Procedure for Crisis Management.

7 Outsourcing

If Mid Sweden University entrusts parts of its information processing or the operation of network and information systems to an external party, this shall be governed by requirements ensuring that Mid Sweden University can continue to fulfil the requirements for incident management and incident reporting in accordance with applicable regulations.

Agreements with external parties shall include requirements for incidents that affect or may affect the University's information, information processing or digital services to be reported promptly to Mid Sweden University.

Mid Sweden University is responsible for assessment, escalation and possible reporting to the relevant authorities in accordance with this procedure.

8 Follow-up and review

Digitalization and Services is responsible for ensuring that this Procedure is kept up to date and for initiating review and updating of the document, where necessary.

Digitalization and Services is also responsible for following up and further developing the incident management process, including identifying improvement needs based on incidents that have occurred, follow-up activities that have been carried out and changes in applicable regulations.

The procedure shall be reviewed at least every three years or where necessary, for example in the event of changes in legislation, regulations or organisational structure.