Mittuniversitetet
MID SWEDEN UNIVERSITY

Order of procedure Incident management

Published: 2024-06-18

Decision makers: Universitetsdirektör Louise Beskow

Responsible department: Department of Infrastructure

Administrator: Helena Wallskog

Decision date: 2024-06-17

Period of validity: Until further notice

Last review: 2024-04-19

Summary: The document describes the framework for Mid Sweden University's internal handling of incidents. Detailed processes and working methods are described in routine documents.

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

Content

1 Introduction

The procedure for handling incidents is aimed at all employees, employees and students at Mid Sweden University. The main purpose of this procedure is to describe how incidents should be handled and how incidents should be reported at Mid Sweden University.

1.1 Definition of incidents

1.1.1 Information security incident

Information security incidents are events that affect, or may affect, the security of the University's information assets. The common denominator is that information security is threatened by, for example, unauthorised access to information, unlawful handling of data, incorrect information or lack of access to information. In the area of information security incidents, personal data incidents are also included.

Defined by the Swedish Civil Contingencies Agency (MSB) as: "An incident in which information in the system or network, rather than the system or network itself, has been affected."

Examples of information security incidents are if your computer has been compromised or if you have received offensive or offensive email. Likewise, if you suspect false emails (so-called "phishing").

1.1.2 IT-incident

An IT incident is an unwanted and unplanned disruption or a deterioration in the quality of a service that may have or has had negative consequences for the business, individual or third party. An IT incident may be due to either intentional or unintentional action.

It incidents can be interference in software or hardware, disruption in the operating environment, loss of information or information leakage. There may also be a safety deficiency in a product, an attack or an error of handling.

1.1.3 Physical and/or environmental incidents

A physical or environmental incident is an unauthorised physical influence and access to, damage to, and disruption of access to the organisation's information and information processing resources.

Examples of incidents may include fire, flood, burglary, burglary, theft, attempted theft.

1.1.4 Occupational safety and health incidents — incidents and occupational injuries

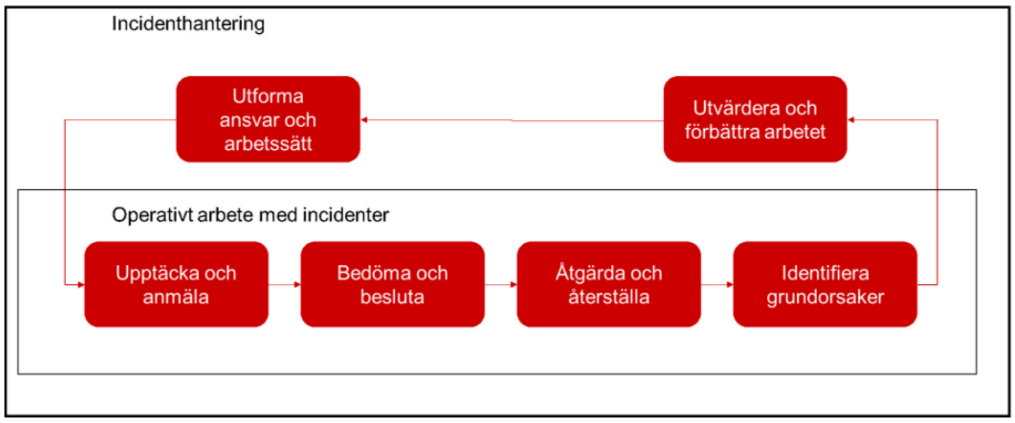
An incident is when something has occurred that could have led to illness or accident. An occupational injury is accidents at work, occupational disease and road accidents (travel to/from work).

2 Process

The purpose of incident management is to:

- Make risks visible and take action after incidents have occurred in the business through immediate handling and damage limitation. (step 1)
- Prevent recurrence of similar incidents by analysing incidents and taking proactive action. (step 2)

To ensure that any incidents have a minimal impact on the University's operations, there are processes that show how the handling, reporting and analysis of incidents should be carried out.



Figur 1: Bilden visar på incidenthanteringens olika delar.

2.1 Handling of incidents:

2.1.1 Step 1:

- limit the incident
- identify and address relevant causes
- report the incident according to specific procedures
- document information about the incident containing, timing, what happened, circumstances, etc.
- establish evidence by, for example, checking logs
- reporting of incidents to the Swedish Civil Contingencies Agency (MSB) and the Integrity Protection Authority (IMY) on the basis of the respective authority's established directives, when this is relevant.

2.1.2 Step 2:

- after the incident has been handled and addressed, an analysis shall be carried out and documented:
    - ◊ summery incident
    - ◊ experience gained
    - ◊ short-term solution
    - ◊ long-term solution

- ◊ updating routines, processes, etc. to minimise the risk of repeated incidents.

3 Report incidents

Anyone who detects an incident at Mid Sweden University should report it immediately.

Information security incidents, IT incidents, and physical and environmental incidents may be reported in any of the following ways;

- Via service portal
- E-mail: itsupport@miun.se
- Phone: 010-142 80 00, select IT Support

In case of more serious information security incidents, IT incidents or physical and environmental incidents, IT Support is always contacted via the above phone number.

Occupational Safety Incidents: Reporting is done by employees/students via Mid Sweden University's incident reporting system (IA). Events can also be reported by phone by downloading IA as an app.

3.1 Incident reporting to the Swedish Civil Contingencies Agency

3.1.1 What incidents should be reported to the MSB

An IT incident that

- affected the accuracy, availability or confidentiality of the information deemed to be in need of enhanced protection; or
- means that information systems that process information deemed to be in need of enhanced protection have not been able to maintain the intended functionality; or
- affected the Authority's ability to carry out its tasks; or

- otherwise, it may seriously affect the security of the information management for which the authority is responsible, or in services provided by the authority to another organisation.

The assessment of whether the information is in need of increased protection shall be carried out by means of information classification in accordance with Section 6 p. 1 The Swedish Civil Contingencies Agency's regulations on information security for state authorities (MSBFS 2020:6)[1].

The Authority shall promptly, but no later than six hours after the Authority has identified that an IT incident is subject to reporting obligations, provide an overall description of what has occurred (notification).

Within four weeks of the Authority's identification that an IT incident is subject to reporting obligations, the Authority shall provide the following information (final reporting).

1. The name of the authority.
2. A description of the IT incident occurring, from the outside
   a) the time when the IT incident occurred and when it was detected;
   b) the time when affected information systems returned to normal operation;
   c) the course of events,
   d) the management of the IT incident; and
   e) type, cause and consequences.
3. Actions taken and planned in response to the IT incident.

If, within one year of final reporting, the Authority finds that the information provided is incorrect, the data shall be corrected without undue delay.

According to the Government, the purpose of mandatory IT incident reporting is to support society's information security; it enables an

[1] The Swedish Civil Contingencies Agency's Regulations on Information Security for Government Authorities (MSBFS 2020:6)

improved situational picture of information security, creates the conditions for taking the right security measures and develops the ability to prevent, detect and manage IT incidents.

By promptly reporting to the Swedish Civil Contingencies Agency (MSB) in order to obtain a comprehensive and comprehensive picture, it is also possible to take coordinated measures to avert or limit the consequences of serious IT incidents. If there is a suspicion that a crime has been committed, contact will be made with law enforcement authorities after dialogue with the management.

When reporting to the Swedish Civil Contingencies Agency (MSB), a notification must be made to the MSB within 6 hours, after which a final report must be submitted within 4 weeks. The documentation for the final report can be found on the MSB website.

3.1.2 Who reports to the Swedish Civil Contingencies Agency, MSB?

The Incident Coordinator at the Department of Infrastructure is responsible for reporting IT security incidents to the Swedish Civil Contingencies Agency (MSB) in accordance with applicable regulations.

3.1.3 Registration and archiving

The reports and other documents on the file, such as correspondence with the MSB, are kept and registered and given a confidentiality mark in the register.

3.2 Incident reporting to the Swedish Authority for Privacy Protection

3.2.1 What is a Personal Data Incident?

A personal data breach is an information security incident that can pose risks to people’s freedoms and rights. The risks may mean that someone loses control of their data or that rights are restricted.

Example:

- discrimination
- identity theft
- fraud
- harmful reputation spread
- financial loss
- breach of confidentiality or confidentiality.

For example, a personal data breach has occurred when data relating to one or more data subjects have:

- been destroyed
- lost in another way
- come into the wrong hands.

It does not matter whether it has been done unintentionally or intentionally. In both cases, there are personal data breaches.

Within 72 hours from the detection of a personal data breach, it shall be reported to the Swedish Authority for Privacy Protection. However, the notification does not need to be made if the incident is unlikely to result in risks to the rights and freedoms of individuals.

In some cases, the data subject shall be informed of the incident.

Where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall inform the data subject without undue delay of the personal data breach unless one of the exceptions listed in the regulation is applicable.

Information to the data subject is not required if one of the following conditions is met:

a) The controller has implemented appropriate technical and organisational safeguards and those measures have been applied to the personal data affected by the personal data breach, in particular those

which make the data unintelligible to any person who is not authorised to access the personal data, such as encryption.

b) The controller has taken further steps to ensure that the high risk to the rights and freedoms of data subjects is likely to no longer arise.

c) This would involve a disproportionate effort. In that case, the public shall be informed or a similar measure shall be taken by which data subjects are informed in an equally effective manner.

The incident shall be reported via the Swedish Authority for Privacy Protection's e-service and shall include information on:

- what kind of incident is it?
- which categories of persons may be affected
- how many people it touches
- what consequences the incident may have
- what measures have been taken to counter potential negative consequences.

3.2.2 Who reports to the Swedish Authority for Privacy Protection?

The Incident Coordinator, in consultation with system operators and the Data Protection Officer, reports personal data breaches to the Swedish Authority for Privacy Protection (IMY) in accordance with applicable rules.

3.2.3 Registration and archiving

The reports and other documents in the case, such as correspondence with the Swedish Authority for Privacy Protection, are kept and registered and given a confidentiality mark in the register.

4 Escalation routines

Incidents are categorised into 4 different priority levels (low, medium, high and critical).

IT-incidents and information security incidents categorised as high and critical are escalated to the head of IT Operation & Development. Incidents categorised as critical are escalated from the Head of Unit for IT Operation & Development to the Head of Department of Infrastructure.

Physical and/or environmental incidents categorised as high and critical are escalated to the Property Manager.

In addition, all incidents with priority high and critical must be escalated to the incident manager due to follow-up and upcoming retro meeting.

The Data Protection Officer must be contacted urgently in the event of a suspected personal data breach, regardless of priority.

5 Outsourcing

If Mid Sweden University transfers part of its information management to an actor that is not subject to reporting obligations, Mid Sweden University shall ensure that the operator undertakes to report IT incidents to Mid Sweden University in such a way that Mid Sweden University can meet the requirements of the Swedish Civil Contingencies Agency, MSB's regulation 2020:8.

6 Responsibilities in the process

6.1 Active

Working at Mid Sweden University, both students and employees, report incidents according to this processing order.

6.2 Managers

All managers are responsible for informing all employees about the incident management process and the importance of reporting incidents.

6.3 System operators

According to the system management model, the system operators are responsible for reporting incidents related to the business systems and

participating in their investigation. In the event of a personal data breach, the system operator should participate in reporting to IMY.

6.4 Roles of responsibility for information security incidents, IT incidents and physical and environmental incidents

6.4.1 IT Support

IT Support is a unit within the Department of Infrastructure and is responsible for:

- Receive and forward the incidents received to the responsible person in the respective sub-process.

6.4.2 Incident coordinator

The Incident Coordinator located in the Infrastructure Department is responsible for:

- Collect information
- Coordinate the necessary resources to deal with the incident
- Analyse the incident
- Communicate to/with different stakeholders
- Escalate incidents
- Report to MSB and IMY
- Be a contact function to MSB
- Request the necessary documents and for the incident report to be written and distributed to those concerned

6.4.3 Incident Manager

The Incident Manager located in the Infrastructure Department is responsible for:

- Monitor, analyse and develop the incident process

- Procedures for escalation, alarm and dissemination of information and other incident management processes are followed.
- The Retro Meeting is carried out
- That the procedure is updated and up-to-date

6.4.4 Data Protection Officer

The Data Protection Officer located at the University Management Staff is responsible for:

- Support incident coordinators in reporting information security incidents related to personal data to the Swedish Authority for Privacy Protection

6.4.5 Property

The Property unit located at the Department of Infrastructure is responsible for:

- Manage incidents related to physical and environmental safety.

6.5 Responsibility roles regarding occupational safety and health incidents

The HR department supports managers in dealing with reported occupational safety and health incidents.