

Decision maker: Vice-chancellor Document Type: Guideline Validity period: Until further notice	Decision date: 2025-06-02 Effective date: 2025-06-02
Documents that are cancelled:	

## Guidelines for handling security incidents

### Table of contents

<b>1. Introduction</b> .....	2
1.1 Purpose of the Document .....	2
<b>2. Security Incidents</b> .....	3
2.1 Information Security Incident .....	3
2.2 Personal Data Breach .....	3
2.3 IT Security Incident .....	3
2.4 Physical Security Incident .....	4
2.5 Personnel Security Incident .....	4
<b>3. Responsibilities and Roles in Management</b> .....	4
3.1 Other Roles .....	5
3.2 Security Functions .....	5
3.3 Other Involved Functions .....	6
<b>4. Incident Management Process</b> .....	7
4.1 Identify Security Incidents .....	7
4.2 Limit Incident Consequences .....	7
4.3 Coordinate Incident Management .....	8
4.4 Analyze Risks and Take Action .....	8
4.5 Restore Operations or Function .....	8
4.6 Post-Incident Evaluation .....	8
4.7 Reporting Obligations .....	8
<b>5. Security Incident Management Group</b> .....	9
<b>6. Communication and Escalation</b> .....	9
<b>7. Reporting Security Incidents</b> .....	10
7.1 Reporting IT Security Incidents .....	10
7.2 Reporting Personal Data Breaches .....	10
7.3 Reporting in Case of Outsourcing .....	10
7.4 Reporting Security Protection Incidents .....	11

## 1. Introduction

Security incidents are events that affect, or may affect, the security of the university's information assets or personnel in a negative way. To handle incidents effectively, appropriately, and securely, clear distribution of responsibilities, predetermined action plans, and a structured approach are required. The university must have clearly established procedures for incident reporting and handling within each area of security: information security, physical security, and personnel security. See the Guidelines for Security Work at Luleå University of Technology.

According to MSBFS 2020:6, the university must have systematic incident handling within the area of information security as part of its overall information security management. Since the university aims to prevent and counter all types of incidents, Luleå University of Technology has chosen to adopt a unified guideline covering all security incidents.

This guideline applies to everyone active at the university. The first person to become aware of an incident is often an individual employee, student, or affiliate, which makes it essential that everyone knows what constitutes an incident and whom to contact.

### 1.1 Purpose of the document

The purpose of this guideline is to protect the university's information assets and personnel from relevant threats and risks, to enable continued operations and security despite disruptions or incidents, and to fulfill statutory reporting obligations. Effective incident management allows timely resolution, preventive actions, and avoidance of future incidents. The guideline also outlines what a security incident is, who is responsible, and how incidents should be managed, documented, and reported.

---

## 2. Security incidents

A security incident is an unwanted and unplanned event that may negatively affect the university's security or disrupt its ability to carry out its operations.

### 2.1 Information security incident

Information security incidents are events that impact, or may impact, the security of the university's information assets. This also includes events involving personal data where an individual's privacy is at risk.

Common traits of such incidents include:

- Unauthorized access to or disclosure of information
- Illegal access to or processing of business information
- Incorrect information
- Lack of or blocked access to information

Examples: attempted computer intrusions, receiving offensive or suspicious emails (e.g., phishing), data leaks through theft or burglary, technical failures affecting information access, or unintended sharing of protected data.

Information security incidents can also constitute IT security incidents, personal data breaches, or physical incidents.

### 2.2 Personal data incidents

A personal data breach is a security incident that results in accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data (Article 4.12 GDPR).

### 2.3 IT Security incident

An IT security incident typically requires immediate action and may disrupt business operations or compromise the security of information management.

Examples: leaked login credentials, hijacked accounts, malware attacks, data breaches, email fraud attempts, or vulnerabilities in IT systems/products.

## 2.4 Physical security incident

Physical security includes multiple measures to prevent unauthorized access and harm in areas where sensitive operations are conducted. It also protects against unauthorized surveillance.

Examples: hate crimes, threats, violence, unlawful entry, burglary, theft, vandalism, sabotage, fires, or intrusions into secure facilities.

## 2.5 Personnel security incident

A personnel security incident involves an individual who, based on vulnerability, reliability, or loyalty, may pose a risk—primarily concerning sensitive information or materials (according to the Swedish Security Service guidance).

Severity depends on the person's role, responsibilities, and access to sensitive data. Each case must be individually assessed.

Such incidents often coincide with others, such as policy breaches, either intentional or accidental.

---

## 3. Responsibilities and roles in management

Responsibilities for handling security incidents follow the Vice-Chancellor's decision-making and delegation procedure, which states that:

### **Heads of department and head of VSS**

Responsible for handling security incidents at each activity with the support of the Head of Security at the university. Responsible for following up on the implementation and compliance with decided security measures caused by security incidents.

### **Division heads**

Responsible for implementing and following up on security measures decided upon due to security incidents.

### **Unit heads / Subject coordinators**

Ensure that decided measures are implemented in response to incidents.

## 3.1 Other roles

### **Security manager**

The Security Manager leads and coordinates security incident management and convenes the Security Incident Management Group when necessary. Informs and escalates when necessary to other parts of the university. Informs the Security Group and management groups involved at the university about ongoing security incident management. The Security Manager also decides whether to file a police report if a report has not been made previously.

### **Security group**

The security group is led by the head of security and is responsible for overall coordination, joint planning and follow-up of security issues, and makes decisions on major security-enhancing measures that affect the university's operations. The group is also responsible for decisions on restrictive security measures that significantly affect an individual.

### **Security incident management group**

The security incident management group analyzes and coordinates the management of major security incidents and forwards the need for security measures to the affected function or operation. The group analyzes the operational impact/consequences, informs the affected operation and prepares reports. For more information about the group's tasks, see point 5.

## 3.2 Security functions

- **Information security:**

The information security function analyzes and handles incoming information security incidents and forwards them to the relevant function if necessary.

- **Data protection:**

The Data Protection Officer defines, analyzes, handles or supports the handling of incidents and reports them when necessary. Other types of incidents are forwarded to the relevant function. The Data Protection Officer is also responsible for reporting personal data incidents to the supervisory authority in accordance with applicable regulations.

- **IT security:**

Analyzes and handles IT security incidents and, if necessary, forwards these to the relevant function. Assesses the severity and if necessary, reports IT security incidents to the regulatory authority.

- **Physical security:**  
Security coordinators for physical security analyze and handle physical security incidents and, if necessary, forward these to the relevant function.
- **Personnel security:**  
HR specialists analyze and handle personnel security incidents and, if necessary, forward them to the relevant function.

### 3.3 Other involved functions

- **Archives and registry:**  
Coordinates and handles requests for the release of public documents/information, including in the event of security incidents. Archives and Registry are one of the contact points for the university and the function may be the first to learn of security incidents and they forward this information to the relevant security function.
  - **Service point:**  
The Service Point receives and, if necessary, assists in registering security incidents that they become aware of and forwards this information to the relevant security function.
  - **Communications:**  
Assists in internal and external communication when necessary.
-

## 4. Incident management process

To ensure that any incidents have minimal impact on the university's operations, there is an incident management process that describes the flow for reporting, analysis and handling.



### 4.1 Identify security incidents

There are several ways to identify security incidents. Available warning and reporting systems are used to raise alarms, collect information and analyze information and data. Another important part is that anyone who discovers a deviation in normal operations that could lead to a security incident reports this as soon as possible. Instructions for reporting incidents can be found under "When something has happened" on LTU's website.

The respective security function that receives an incident shall initially conduct an analysis to determine the potential impact on information, individuals and the university's operations and how it should be escalated to the head of security.

Security incidents of great importance or that may have serious consequences for the operations shall, in addition to the incident notification as above, be reported to the head of security as soon as possible.

## 4.2 Limit incident consequences

To reduce the spread and expansion of the incident, LTU must work urgently and actively to limit the consequences. This applies to both technical and administrative measures. To effectively limit and interrupt the incident, information and evidence need to be collected. Incidents must be handled in order of priority in relation to the level of impact that the incident may have on business.

## 4.3 Coordinate incident management

Ensure all involved functions are informed early. Coordination is led by the Security Manager when necessary.

## 4.4 Analyze, make risks visible and take action

The incident that occurred must be analyzed to highlight risks so that the correct measures can be taken before operations or functions can be restored.

## 4.5 Restore operations or function

After corrective actions and inspections, operations can return to normal.

## 4.6 Evaluation after handling a security incident

Experience from the incident should be collected from the functions and roles involved. The evaluation should highlight lessons learned and highlight whether working methods and measures have had the intended effect, but also whether support is available in existing procedures and rules. After the evaluation has been completed, the results should be communicated to those affected and any changes in procedures and rules updated to reduce the likelihood of the incident recurring.

## 4.7 Reporting obligation to other authorities, affected parties and private individuals.

The university must report incidents to external authorities, affected parties, and individuals. See section 7 for details.

---

## 5. Security incident management group

The security incident management group consists of the security manager and the relevant functions that the security manager convenes. The incident management group is therefore composed depending on the type of incident and the size of the incident.

The security incident management group is convened when coordination is required between different security functions and there are no established procedures for handling it.

If necessary, the need for security measures is forwarded to the relevant activity.

More detailed information about the workflow within each security function is described in the function's procedures for security incident management.

The incident management group raises major incidents or the need for measures that affect a large part of the university's operations to the Security Group, which has the mandate/authority to decide on measures and enforce the decisions.

---

## 6. Communication and escalation

In connection with the detection of a security incident, communication and escalation may be required.

Security incidents are categorized into 4 different levels (low, medium, high and critical). Incidents categorized as high or critical should be escalated to the Security Group.

## 7. Reporting security incidents

All suspected crimes related to security incidents, committed within the university's operations, premises or other areas, must always be reported to the police.

There are also requirements for reporting to various authorities when security incidents have occurred. These are listed below.

### 7.1 Reporting IT security incidents

By promptly reporting to the Swedish Civil Defense Agency (MCF), which is the supervisory authority, in order to thereby obtain a comprehensive and comprehensive picture, it is also possible to take coordinated measures to avert or limit the consequences of serious IT incidents.

The following IT incidents are subject to the reporting obligation if the incident has:

1. affected the accuracy, availability or confidentiality of the information that has been assessed as needing increased protection,
2. resulted in information systems that process information that has been assessed as needing increased protection not being able to maintain intended functionality,
3. affected the authority's ability to carry out its mission,
4. seriously affected the security of the information management for which the authority is responsible, or in services that the authority provides to another organization.

The assessment of whether the information needs increased protection shall be made on an ongoing basis through the organization's information classification (Section 6, paragraph 1, MSBFS 2020:6) of business information.

In cases where information deemed to require enhanced protection is affected, the university must report it to the supervisory authority within 6 hours of discovery, in accordance with applicable regulations.

### 7.2 Reporting personal data incidents

A personal data breach must be reported to the Swedish Data Protection Authority (DPIA) within 72 hours of becoming aware of the incident, unless it is unlikely that it will result in a risk to the rights and freedoms of natural persons. Even if the personal data breach is not "notifiable", it must be documented internally by the data protection officer, or the person appointed by the data protection officer.

If the personal data incidents are likely to result in a high risk to the rights and freedoms of natural persons, the controller must, as a starting point, inform the data subject about the personal data incident without undue delay (GDPR Article 34).

### 7.3 Reporting in case of outsourcing

If the university transfers part of its information management to an actor who is not subject to reporting obligations, the university must ensure that the actor undertakes to report security incidents to the university in such a way that the university can meet the reporting requirements.

### 7.4 Reporting security protection incidents

Incidents concerning security protection are reported to the Swedish Security Service and the County Administrative Board.