

2024/2025

# Information Security Policy Tilburg University

## Table of contents

Version Management .....	3
Model information security policy .....	3
Foreword .....	4
Summary .....	5
Readers' Guide .....	6
1. Introduction .....	7
1.1 Rationale .....	7
1.2 Target group .....	7
1.3 Scope of the policy .....	7
2. Definition, Objective, and Principles .....	8
2.1 Information safety and information security .....	8
2.2 Objective and guiding principles .....	8
3. Information Security Policy Principles .....	9
4. Legislation and Regulations .....	11
5. Organization of Information Security Positions .....	11
5.1 Three Lines Model .....	11
5.2 Roles and responsibilities .....	11
5.3 Strategic, tactical, and operational .....	15
5.4 Information security documents .....	16
6. Awareness and training .....	17
7. Monitoring, practice, compliance, and sanctions .....	17
8. Funding .....	18
8.1 Central .....	18
8.2 Decentral .....	18
9. Reporting and Handling of Incidents .....	18
10. Adoption & amendment .....	19
Appendix A - Schematic Overview of ISMS setup .....	20
Appendix B - Information Security Principles .....	21
Appendix C - The AIC classification .....	25
Appendix D - Legislation and Regulations .....	26
Appendix E - Roles in Information Security .....	28
Appendix F - Establishment of CERT .....	29

## Version Management

Version	Date	Preparer	Explanation
1.0	March 2, 2021	LIS: Information Security	IB policy final
1.02	June 28, 2021	LIS: Information Security	Text Amendments. Version 1.02 adopted by the Executive Board on September 7, 2021.
1.1	March 25, 2024	ES: CISO Office	New version IB Policy, with changes in formatting and textual changes in: <ul style="list-style-type: none"> <li>- Section 2.2 (principles of IS Policy)</li> <li>- Chapter 3 (information security principles)</li> <li>- Section 5.2 (roles and responsibilities)</li> <li>- Section 5.3 (table governance structure)</li> <li>- Chapter 6 (awareness)</li> <li>- Chapter 9 (incident reporting and handling)</li> <li>- Appendix B (information security principles)</li> <li>- Appendix C (AIC classification)</li> <li>- Appendix D (legislation and regulations)</li> <li>- Appendix E (information security roles)</li> <li>- Appendix F (establishment CERT).</li> <li>- the RASCI matrix (old Appendix E) has been removed.</li> </ul>

## Model information security policy

This Information Security Policy is based on the Model Information Security Policy SCIPR. Part of the SCIPR Information Security Framework.

This Model Information Security Policy was prepared by SCIPR and is published under the Creative Commons Attribution, NonCommercial, ShareAlike ([CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/)) license.



More information about SCIPR is at [SCIPR community: working on better information security | SURF.nl](https://www.scipr.nl/)

## Foreword

To carry out our tasks, it is crucial that we properly secure our information systems. Tilburg University's work processes cannot be carried out without collecting, recording, and sharing information with both internal and external partners, colleagues, and students.

This Information Security Policy (hereinafter referred to as the IS Policy) sets out the way in which Tilburg University provides adequate information security and thus complies with the relevant legislation and regulations, but also with the security standards applied internally. With the IS Policy, Tilburg University aims to contribute to an improved quality of information provision and to ensure the right balance between functionality, security, and privacy.

Tilburg, March 2024

Executive Board

## Summary

Information security is the set of measures, processes, and procedures that ensure the availability, integrity, confidentiality, and the provision of information. Tilburg University uses five policy principles for information security, namely:

### 1. Risk-based

We base measures on the potential security risks to our information, processes, and IT facilities (in the broadest sense).

### 2. Everyone

All Tilburg University's employees, students, guests, visitors, and external relations feel responsible for the proper and safe use of resources and authorities.

### 3. At all times

Information security is in the DNA of all our work.

### 4. Security by Design

Information security is an integral part of any project or change related to information, processes and IT facilities from the outset.

### 5. Security by Default

In every configuration that is implemented, the available security options are on by default. Opening up information and setting up configurations are, therefore, always a conscious choice after careful consideration.

The responsibility for information security is designed in accordance with the Three Lines Model. In the first line, the business is responsible for its own processes, including risk management. The Executive Board has final responsibility. In the second line, the CISO has an advisory and supporting responsibility. Independent monitoring of the first and second lines takes place from the third line. The SURF Standards and Information Security Assessment Framework for in Higher Education, which is based on ISO 27001/27002 and the NBA/NOREA Maturity Model, are used as a starting point.

The security measures to be taken always consist of an established mandatory set of basic measures (the Tilburg University Information Security Baseline). By classifying information (systems), it is made clear which security level is required for the components availability, integrity, and confidentiality. Policy and measures alone are not sufficient to completely eliminate information security risks. People themselves create the greatest risks. At Tilburg University, we therefore continuously work to increase security awareness within our organization through the awareness annual plan.

Information security is a continuous process in which we are always looking at possible improvements. This is done in part through annual plans, audits, and adjustments, which are reported to the Executive Board. Based on these findings, improvement measures are taken to continuously optimize the effectiveness and efficiency of information security. The CISO must have an adequate budget for this.

Information security incidents are handled according to the established Incident Management Process, which includes reports of data breaches. The Data Protection Officer (DPO) handles reported data breaches.

## Readers' Guide

In Chapter 1, the IS Policy describes to whom the policy applies, to which components, and to which devices and information systems. The purpose of the IS Policy is included in Chapter 2. Tilburg University applies five security principles, which are described in Chapter 3. How Tilburg University deals with relevant legislation and regulations is touched on in Chapter 4, and the responsibilities including descriptions of the roles of the officials involved are set out in Chapter 5. Chapter 5 also includes an overview of important documents in the area of information security. Awareness is discussed in Chapter 6, and Chapter 7 elaborates on independent monitoring. Finally, Chapter 8 describes funding, and Chapter 9 discusses the handling of reports and incidents.

The appendices focus on the management cycle for periodic updating. The five policy principles for information security are fully detailed in appendix B. In addition, an overview of the most important legislation and regulations regarding information security and the roles of involved officials are listed.

# 1. Introduction

## 1.1 Rationale

Digital and physical reality is constantly changing. Consider the continuous technological developments, the developments within cybercrime, the stricter requirements to comply with the legislation and regulations concerning privacy<sup>1</sup> (GDPR) and the agreements with research and education partners. These developments constantly bring new and different risks with regard to information security and require adjustment for an appropriate level of security. The risks can threaten the quality and continuity of processes and the achievement of strategic goals. They can also potentially compromise the privacy of employees, students, and guests. The threats can affect the availability, integrity, and confidentiality of information:

1. **Availability:** information is available at desired times.
2. **Integrity:** information is accurate and complete.
3. **Confidentiality:** information is accessible only to those authorized to do so.

Reducing and controlling the risks requires efforts at an organizational and technical level. Tilburg University must become and remain aware of the risks and adjust its actions accordingly.

Tilburg University is an institution with an open character. From the education and research perspective, the approach is "Open where possible, closed where necessary." Adequate security of information is always a precondition and opening up information must be a conscious choice. The measures, procedures, and guidelines to be adopted can be tested against the five main principles described in Chapter 3.

## 1.2 Target group

Tilburg University's IS Policy applies to Tilburg University's organization: the five Schools, the seven supporting Divisions, and the collaborative partners who use Tilburg University's infrastructure and IT facilities and (cloud) services provided by third parties. In short, to everyone who—internally or externally—is involved, in any way, with (aspects of) Tilburg University's business process. The Executive Board, Deans, and Managing Directors are primarily responsible for complying with and propagating the Policy and by showing exemplary behavior.

## 1.3 Scope of the policy

Tilburg University interprets information safety broadly. There is a close relationship and partial overlap with adjacent policy areas, such as privacy, knowledge security, physical security, social security, emergency response, and business continuity. Within the framework of integral security<sup>2</sup>, attention is paid to these interfaces at the strategic level, and alignment is sought both in terms of planning and content.

In principle, the IS Policy covers all devices and information systems (both managed and unmanaged) that allow authorized<sup>3</sup> access to (services of) the Tilburg University network and/or that process Tilburg University information.

The Policy is location independent: it applies even if one works with Tilburg University information or information facilities at a location other than Tilburg University premises, such as at home, on the train, or at another educational institution.

---

<sup>1</sup> For Tilburg University's specific Privacy and Personal Data Protection Policy, see the [Intranet](#).

<sup>2</sup> Integral security is designed to address security problems within an organization in a cohesive manner, with the goal of achieving the highest possible security level.

<sup>3</sup> By definition, unauthorized access is a security incident.

## 2. Definition, Objective, and Principles

### 2.1 Information safety and information security

The terms “information safety” and “information security” are often used interchangeably, but they do not have the same meaning. Information safety focuses on the availability, integrity, and confidentiality of information. This requires protecting information and information systems from potential threats. This is done by determining, taking, maintaining, and verifying security measures, also called “information security.”

### 2.2 Objective and guiding principles

The IS Policy aims to provide direction on how Tilburg University should be resilient regarding the risks posed by current developments in information safety. This Policy enables the organization to guarantee the availability, integrity, and confidentiality of education, research, and business operations.

The following principles are used in this regard:

- **Three Lines organization**

The internal organization of risk control, risk management, and information security are shaped according to the Three Lines Model<sup>4</sup>. This Model is commonly used as a model to secure Governance, Risk, and Compliance in an operational organization. It describes not only the roles within the organizational structure but also their mutual collaboration.
- **Framework**

The IS Policy provides a framework for testing (future) measures in information security against the established security principles (Section 3.2), best practices, and standards. It also provides a framework for assigning duties, powers, and responsibilities within the institution.
- **Process approach**

Information security is a continuous process and follows a PDCA cycle. Risk analyses and audits are carried out periodically. The results are included in established annual plans with clear choices of security measures. The implementation of these security measures is verified periodically.
- **Standards**

The basis for setting up information security management is the international standard ISO 27001. Specifically for the SURF community, the "SURF Framework of Standards for Information Security in Higher Education" (*IBHO*) has been established. The *IBHO* is based on the standards set forth in the ISO-27000 series.
- **Measures**

Measures are taken on the basis of best practices in higher education and on the basis of the Tilburg University Information Security Baseline (hereafter referred to as: Baseline), based on ISO 27002. The use of the Baseline ensures that the basic information security measures can be implemented and demonstrated. By classifying information (systems), it is clarified which security level is required for availability, integrity, and confidentiality. If this classification scores higher than the Baseline, additional measures are needed to mitigate risks.
- **Maturity**

Tilburg University aims to achieve at least a maturity level 3 in design, existence, and operation according to the Capability Maturity Model (CMM).


---


<sup>4</sup> [three-lines-model-updated-english.pdf \(theiia.org\)](https://theiia.org/three-lines-model-updated-english.pdf)





### 3. Information Security Policy Principles


Tilburg University has five policy principles for information security:

<b>1</b>	<p><b>Risk-based</b> Information security measures are taken on a risk-based basis</p> 
Core	We base the measures on potential security risks to our information, processes and IT facilities.
Background	Sharing knowledge (openness) is an important core value of Tilburg University's education and research process. For proper risk assessment in protecting information and taking appropriate measures, it is important to determine the value of information. If the value of information is known, the right level of security can also be determined: one that is in line with the risks and our so-called risk appetite. Proportionality in this is desirable, also to use the available financial resources efficiently (fit for purpose).
Implications	Consider establishing a risk management process (classification), establishing responsibilities, and securing risks in contracts. See Appendix B for an overview of all implications.

<b>2</b>	<p><b>Everyone is responsible</b> Information security is everyone's responsibility</p> 
Core	The responsibility for information security and privacy protection lies with everyone (all Tilburg University employees, students, guests, visitors, and external relations) and management directs this.
Background	Everyone is aware of the value of information and acts accordingly. This value is determined by the potential harm resulting by loss of availability, integrity, or confidentiality. Employees, students, and third parties are all expected to handle information consciously and to actively contribute to the security of automated systems and the information stored therein. The success of security hinges on good communication. Good communication is therefore actively promoted, at and between all levels within Tilburg University.
Implications	Examples include establishing agreements in terms and conditions of employment (such as mandatory participation in the Digital Safety Training course), etiquette, codes of conduct, and house rules, etc. See Appendix B for an overview of all implications.

<p><b>3</b></p>	<p><b>At all times</b> Information security is a continuous process</p> 
<p>Core</p>	<p>Information security is in the DNA of all our work.</p>
<p>Background</p>	<p>The environment is constantly changing; cyber threats increase and decrease; processes change, employees and students change, etc. Defining and implementing measures once is insufficient to maintain a secure environment. Information security only makes sense if it is a continuous process of taking measures, creating awareness, and carrying out checks.</p>
<p>Implications</p>	<p>Consider establishing a PDCA cycle and conducting awareness campaigns based on the awareness annual plan. See Appendix B for an overview of all implications.</p>

<p><b>4</b></p>	<p><b>Security by Design</b> Information security is an integral part of any project or change related to information, processes, and IT facilities from the outset.</p> 
<p>Background</p>	<p>Security by Design means that already during the start of a project, the design of a new information system or ICT environment and during technical or functional changes, the security of data and the continuity of processes is taken into account. This prevents (often expensive) remedial work afterwards.</p>
<p>Implications</p>	<p>Consider establishing and testing security requirements in projects and setting up authorization schemes. See Appendix B for an overview of all implications.</p>

<p><b>5</b></p>	<p><b>Security by Default</b> In any configuration that is implemented, the available security options are enabled by default.</p> 
<p>Background</p>	<p>Security by Default prevents undesirable and uncontrolled access to (personal) data. Opening up information and setting up institutions are thus always a conscious choice after careful consideration.</p>
<p>Implications</p>	<p>Consider defining standard roles and limiting authorizations by default. See Appendix B for an overview of all implications.</p>

The policy principles help implement IS policies in that the principles define the security measures required to protect processes. Appendix B elaborates on the policy principles with key implications.

## 4. Legislation and Regulations

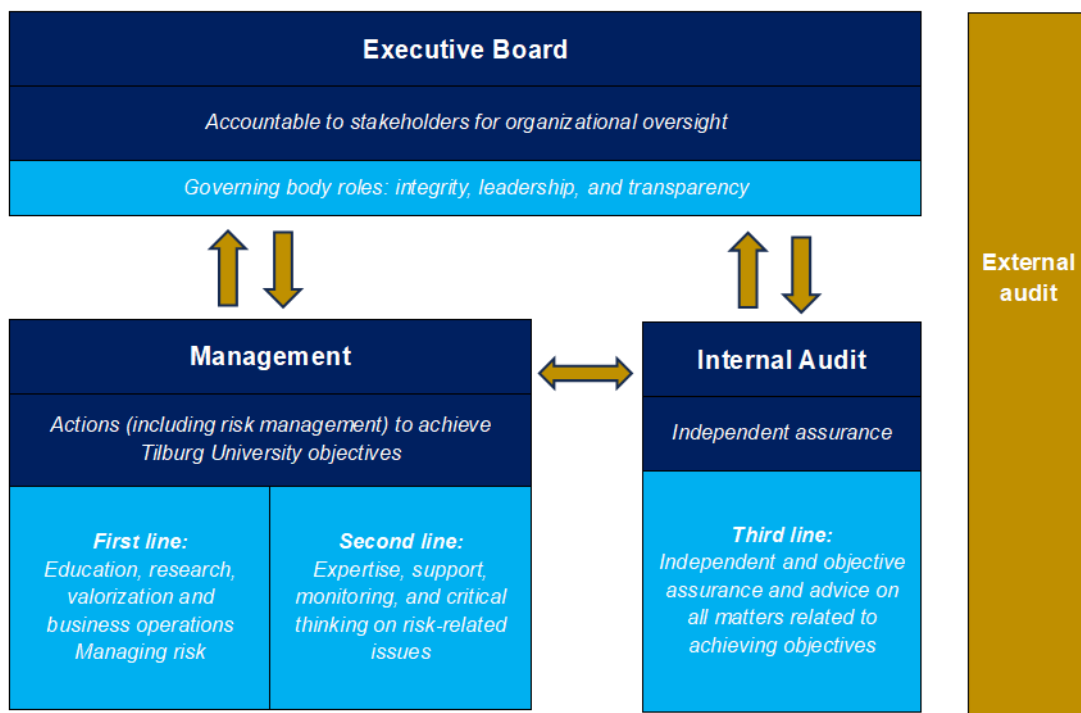
The premise is that Tilburg University complies with all applicable legislation and regulations in its processes and procedures and makes preparations to comply with upcoming legislation. How Tilburg University deals with relevant legislation and regulations is described in more detail in Appendix D - Legislation and Regulations.

## 5. Organization of Information Security Positions

The assurance of the IS Policy requires not only that the various roles and responsibilities in the organization in the area of information security are defined but also how these roles and responsibilities relate to each other. This chapter details the roles and responsibilities and their interrelationships.

### 5.1 Three Lines Model

Information safety within Tilburg University is organized according to the so-called IAA's Three Lines Model. Within this model, three lines with their own responsibilities are distinguished. It describes the roles within the organizational structure and mutual cooperation.



Three Lines Model

### 5.2 Roles and responsibilities

#### Executive Board

The Executive Board is ultimately responsible for information security and sets policy. It provides the resources necessary to implement the policy, meet goals, mitigate risks, and promotes a culture of ethical and responsible behavior. The Executive Board sets the frameworks for risk appetite and is accountable to stakeholders. The responsibility of the Executive Board is assigned to the Deans and Directors through the Mandate and Authorization Regulations<sup>5</sup>. Within the Executive Board, one of the members has been appointed as portfolio holder for information security.

<sup>5</sup> The Mandate and Authorization Regulations are published on the [Intranet](#).

## First line

The Three Lines Model is based on the premise that the first line (the business) is responsible for its own processes, including risk management. The first line provides leadership and direction and is in constant dialogue with the Executive Board regarding the achievement of objectives and risk management.

Directors and Deans are often process<sup>6</sup>, system<sup>7</sup>, or information owners<sup>8</sup> and, therefore, responsible for the implementation of and compliance with IS policies in their own processes and systems. They ensure that:

- security measures are implemented;
- the awareness program is implemented;
- employees are trained;
- risk management is carried out. The CISO Office supports this by performing an AIC classification<sup>9</sup>. The owner provides the appropriate input for this;
- meeting the Baseline and implementing additional measures to achieve the appropriate security level. The CISO Office verifies compliance with the Baseline.

For valid reasons, one may choose to deliberately deviate from the prescribed security measures and take mitigating measures to reduce the residual risk. Such residual risks are recorded in the risk register by completing a Risk Acceptance Form. With this form, the risk owner is informed, and agreements are made about possible temporary security measures and/or when the risk will be mitigated. Signing the Risk Acceptance Form establishes responsibility for the risk and allows risks to be controlled and managed. The risk acceptance matrix below shows the level at which risks can be accepted. The risks are estimated by determining probability x impact.

Estimate	Authorized to accept
Critical	EB
High	EB
Medium	Process/system/information owner
Low	No formal acceptance required <sup>10</sup>

*Risk acceptance matrix*

The CISO has an advisory role in preparing the Risk Register and Risk Acceptance Form and consults with the Executive Board to reach a final decision. The residual risks taken are evaluated annually. In addition, the information security portfolio holder and the Audit Committee (Board of Governors) are periodically informed of the critical and high risks.

### Information manager of Divisions and Schools

The information managers, with the Director's mandate, monitor the IS Policy within their own Division or School. In this, they are supported by managers. Within Tilburg University, information managers are appointed from the Divisions and information managers from the Schools. The information manager is involved in information provision projects and developments in education, research, and business operations and stimulates compliance with the IS Policy in these projects and developments. The information manager works closely with the CISO Office.

<sup>6</sup> For decentralized IT infrastructure, the owner of the primary or support process is responsible.

<sup>7</sup> A system owner is responsible for an information system, which supports one or more processes. A system owner is often also the process owner of the process in question and thus ultimately responsible.

<sup>8</sup> An information owner is responsible for the information in the process and/or system.

<sup>9</sup> Classification on Availability, Integrity, and Confidentiality (BIV).

<sup>10</sup> Low risks do get recorded in the risk register and assigned to the appropriate owner.

## Second line

The second line supports and advises the first line and monitors whether management fulfills its responsibilities. Certain policy preparation tasks, organizing the PDCA cycle, integral risk analyses, self-assessments, and the preparation of an annual plan are also tasks of the second line. The second line reports directly to the Executive Board.

### CISO Office and IT Security Office

Information security is vested in the CISO Office and IT Security Office. The CISO Office is positioned within the Executive Services (ES) Division and, thus, falls under the responsibility of the ES Director. The IT Security Office is part of the CIO Office. The different roles within both units are detailed below.

### Chief Information Security Officer (CISO)

The CISO maintains the IS Policy and has an independent role towards the Executive Board. He/she performs this role by providing solicited and unsolicited advice to the Executive Board. The CISO defines the information security strategy and policy, assists in its correct translation to institutional Divisions, monitors its (uniform) compliance, and reports on gaps, inconsistencies, and deficiencies (and therefore risks). On this basis, he/she prescribes policy and risk and compliance-based priorities. The CISO monitors compliance and assurance in the Information Security Management System (ISMS).

The CISO has various powers. For example, he/she can conduct research, commission research (audits), request information, and issue unsolicited and solicited advice. If the owner does nothing with the advice (in case there is a clear risk identification) and accepts the risk, the CISO can escalate to the Executive Board if he/she does not consider this to be acceptable.

The CISO has a direct reporting line to the Executive Board's information security portfolio holder. The CISO heads the CISO Office.

### Information Security Officer (ISO)

The ISO is the direct support for the CISO and implements the information security strategy in the organization. The ISO supports in performing an AIC classification and performs risk analyses and security checks and advises on specific information security measures, for example, in projects and in acquisitions of software or hardware. In doing so, the ISO works closely with the architects and information managers.

The position of the ISO is invested in several people. The ISO is part of the CISO Office.

### Privacy & Security Awareness Officer

The awareness officer directly supports the CISO in defining and implementing awareness activities in the organization. The awareness officer initiates and sets up (periodic) awareness programs. In addition, the awareness officer facilitates education and training to employees and students on information safety and privacy.

The role of awareness officer is vested in one person. The awareness officer is part of the CISO Office.

### IT Security Officer (ITSO).

The ITSO defines the IT security guidelines for the organization in accordance with the information security strategy and architecture and identifies and monitors the security of IT systems and developments in this area, constantly establishing the relationship with business and organizational goals. The ITSO advises on specific technical information security measures. He/she also evaluates the results of penetration tests, vulnerability scans, and assessments submitted by delivering parties.

The ITSO is part of the Computer Emergency Response Team (CERT team) and directs services regarding the Security Operations Center (SOC), which is outsourced to SURF. The role of ITSO is invested in several individuals. The ITSO is part of the CIO Office.

### Computer Emergency Response Team (CERT).

The CERT is the team of IT professionals within the organization capable of acting quickly if there is an IT security incident involving one or more computers or the network. The goal is to reduce damage and quickly restore services. The CERT consists of on-call specialists within the organization in addition to the ITSOs.

## Architecture

The information architect ensures the implementation of the Information Security Baseline and any additional measures resulting from the classification. He/she also monitors the consistency of the measures by means of a project start architecture.

## Link with privacy

### Central Privacy Officer

The central privacy officer (CPO) is centrally concerned with the application of and compliance with the GDPR within Tilburg University and is an advisor in this area.

### Data Representative

The Data Representative is the first point of contact and advisor for questions about how to deal with privacy and personal data, such as, when a new information provision or a change to an existing one. Each Division and School has a locally appointed Data Representative.

## Link with risk management

### Governance, Risk, Safety & Compliance Officer (GRSCO).

The GRSCO focuses on developing, implementing and maintaining policies, processes and procedures to ensure the overall governance, risk management, and compliance of the organization. The emphasis is on creating a structured approach to managing risk and complying with legislation and regulations. The GRSCO is independent and reports directly to the Executive Board. The coordination and monitoring of risk management is housed in the independently positioned Governance, Risk, Safety & Compliance unit within ES.

## Link with contract management

### Contract Manager

The contract manager is always involved in the procurement of central systems and pays explicit attention to information security. This is done by making the information security measures from the risk analysis part of the procurement process and of the procurement terms and conditions and by laying down security requirements in contracts.

### Third line

The independent third line assesses the reliability of information and systems and recommends improvements in risk management and internal controls.

### Internal Audit

Internal Audit provides added value from its independent position by testing the design, existence, and operation of the internal control concerning information security. It performs checks or advises the first and second line on improvement opportunities, also checking for overlap or blind spots. Internal Audit reports directly to the Chairman of the Executive Board and to the Audit Committee (Board of Governors). Internal Audit is part of the PDCA cycle (especially the Check and Act components).

### Link with privacy

#### Data Protection Officer (DPO)

The DPO oversees the application of and compliance with the AVG and has an independent position. The DPO reports directly to the President of the Executive Board and is functionally managed by the Head of Governance, Risk, Safety & Compliance.

## 5.3 Strategic, tactical, and operational

The above roles and responsibilities are translated to strategic, tactical, and operational levels:

- **Strategic level:** at the strategic level, policy discussions are held about governance, risk, safety, and compliance, as well as goals, scope, and ambition in the area of information security, in conjunction with privacy.
- **Tactical level:** at the tactical level, the strategy is translated into plans, measures, standards to be used, evaluation methods, etc. These plans and instruments guide the implementation.
- **Operational level:** the operational level is responsible for implementing information security measures and handling incidents. This is done in consultation with the functional administrators, relevant IT officers and, where necessary, with the tactical layer.

The following table summarizes the governance structure by level.

Level	What	Who	Consultation
<b>Policy (strategic)</b>	<ul style="list-style-type: none"> <li>• Ultimately responsible for information security within Tilburg University.</li> <li>• Define, establish, and communicate IS strategy and policy.</li> <li>• Set up organization for IS. Establish IS planning and control.</li> <li>• Business continuity management.</li> <li>• Communication to management and organization.</li> </ul>	<ul style="list-style-type: none"> <li>• Executive Board (the IS portfolio holder)</li> </ul>	<ul style="list-style-type: none"> <li>• Periodic consultations between CISO and IS portfolio holder</li> </ul>
<b>Steering (tactical)</b>	<ul style="list-style-type: none"> <li>• Monitor application and compliance with IS policies.</li> <li>• Communication to process owners.</li> <li>• Operational responsibility information security.</li> </ul>	<ul style="list-style-type: none"> <li>• Information, process and system owners</li> <li>• CISO</li> <li>• Information security officers</li> <li>• IT security officers</li> <li>• Central privacy officer</li> </ul>	<ul style="list-style-type: none"> <li>• Periodic interviews with Directors</li> <li>• Domain consultations research, education, and business operations</li> </ul>

<b>Implementation (operational)</b>	<ul style="list-style-type: none"> <li>• Implement IB measures</li> <li>• Provide communication to end users</li> <li>• Implement technical security measures</li> <li>• Security monitoring and consulting</li> <li>• Record, analyze, and evaluate incidents, including data breaches</li> </ul>	<ul style="list-style-type: none"> <li>• Information, process and system owners</li> <li>• Managers</li> <li>• Functional Administrators</li> <li>• Information managers</li> <li>• Information security officers</li> <li>• IT security officers</li> <li>• Awareness officer</li> <li>• CERT</li> <li>• Central privacy officer</li> <li>• Data protection officer</li> </ul>	<ul style="list-style-type: none"> <li>• The weekly CISO Office consultation</li> <li>• The four-weekly Privacy &amp; Security Consultation</li> <li>• Every 6 weeks, the operational Tilburg University CERT consultation. An ISO also participates in this.</li> </ul>
-------------------------------------	--	---	--

*Information security governance structure summarized in a table.*

## 5.4 Information security documents

In the context of information security, Tilburg University uses the following documents:

### Policies/guidelines

1. **IS Policy:** the IS Policy underlies the approach to information security within Tilburg University. The Policy is drafted by the CISO and adopted by the Executive Board.
2. **Tilburg University Information Security Baseline:** the Baseline describes the measures that ensure a minimum level of information security. These baseline measures should be implemented throughout Tilburg University.
3. **AIC classification guideline:** an AIC classification is used to determine whether a system (or process) needs more security measures than those provided in the Baseline. The owner is, therefore, required to perform an AIC classification for each Tilburg University system (or process). The classification takes place using the AIC classification guideline and in coordination with the CISO Office, which can also provide unsolicited advice. Depending on the value of the AIC classification, it is determined which additional security measures must be implemented.
4. **Codes of Conduct:** information security guidelines for employees, students, and third parties (with or without specific target groups).

### Monitoring and accountability

5. **Information Security Management System** (process and recording).
6. **Risk Register**
7. **Annual plan/annual report:** In line with the PDCA cycle, the CISO provides an annual report on the past year and an annual plan for the following year to the Executive Board. The annual report is based in part on the results of periodic checks/audits. It includes a discussion of incidents, results of risk analyses (including measures taken), and other initiatives that have taken place in the past year.

Where necessary, separate attention is paid to specific information systems. The annual plan is checked against the availability of resources (people and means) compared with the risks that need to be mitigated. The annual plan is coordinated in advance with the Privacy Annual Plan which is drawn up by the DPO. The reports are consolidated into the administrative Planning & Control cycle.



### Information security as an integral part of documents:

8. **Service agreements (SLAs), hiring and outsourcing contracts, non-disclosure agreements (NDAs) and any related processing agreements:** when hiring staff and when purchasing resources (especially hardware and software) and services, explicit attention is paid to information security. This is done by applying the IS Policy to external parties and by making security a standard part of the purchasing conditions. Agreements are recorded and monitored in a contract with the supplier. The contract contains a standard information security paragraph in which the responsibilities of the supplier are included. The basis for this is the SURF
9. Framework of Legal Standards for Cloud Services in Higher Education and the STITCH (compliance with STITCH is verified by requesting a current pentest report).
10. **Business Continuity Plan:** the Divisions and School are responsible themselves for the contingency plan and business continuity measures that ensure the continuity of education, research, and business operations.

## 6. Awareness and training

Policies and measures are not enough to eliminate information security risks. People themselves are responsible for the greatest risks. Therefore, within Tilburg University, we work continuously to increase the security awareness of the organization to increase knowledge of risks and to encourage safe and responsible behavior. Part of the policy is the security and privacy awareness annual plan, with regular awareness campaigns for employees and students. This distinguishes between different target groups and needs so that target group-specific awareness campaigns can also be implemented. Raising security awareness is a management responsibility, supported by the CISO Office. Attention to awareness is also part of the introduction program for new employees and students.

## 7. Monitoring, practice, compliance, and sanctions

The Internal Audit unit is responsible for the (planning of) operational audits. These are performed by the operational auditor. For IT audits, external auditors are usually employed for expertise. The CISO is responsible for monitoring the implementation of the information security annual plan.

The internal checks take place annually and, in addition to the periodic audits, are supplemented by various ad hoc activities, such as carrying out partial observations, performing penetration tests (or having them performed), vulnerability tests, assessments, and verifying the actual operation of the established security measures. In addition, skills and operational procedures are regularly reviewed in brainstorming sessions or exercises. An example is the OZON exercise coordinated biennially by SURF.

SURF's IBHO standards and assessment framework, which is based on ISO 27001/27002 and the NBA/NOREA Information Security Maturity Model, is used as a starting point for internal and external audits.

Tilburg University participates in the external SURF audit, which tests the design, existence, and operation of the information security policy. The external SURF audit takes place every year. In addition, Tilburg University participates in the SURF self-assessment cycle and the associated biennial benchmark (in which only design and existence are assessed). A SURF Peer Review is requested at least once every 4 years. The CISO provides input for the audits.

In response to the findings that emerge from second- and third-line activities, the process, system, or information owner must draft an improvement plan. This improvement plan should at least include: action, final responsible party, and deadline.

In addition to conducting internal and external audits, verification of compliance takes place through monitoring from the second line. For example, security incidents, vulnerabilities, and threats are actively monitored within the Security Operations Center (SOC). In addition, managers oversee the daily practice of information security and address employees and students in case of deficiencies. The DPO is responsible for monitoring compliance with the GDPR.

If the checks reveal a serious lack of compliance and culpable action, Tilburg University may impose a sanction on the responsible employee or student concerned. The sanction will be imposed within the framework of the legal possibilities (such as the Higher Education and Research Act (HERA), Collective Labour Agreement, employment contracts, and the Code of Conduct). Primarily, this is a responsibility of the EB but may in some cases be mandated to the responsible managers (Dean/Director).

## 8. Funding

### 8.1 Central

The CISO must have an adequate budget of his own to implement the strategic and tactical processes and the annual plan objectives. This budget should also be sufficient to allocate temporary staff from other parts of the organization to get information security projects realized.

### 8.2 Decentral

As indicated in Chapter 5 of this IS Policy, the CISO is not ultimately responsible for information security and is, therefore, not a risk owner. As a result, the budget for information security activities and projects is in line with the Divisions and Schools (the process and system owners respectively). This form of prioritization and budgeting must be anchored in the planning and control cycle and in project portfolio management.

## 9. Reporting and Handling of Incidents.

An incident is an event that can negatively affect business operations. Incident management and recording is about detecting, recording, analyzing, and handling incidents and improvements as a result of lessons learned. Important here is that employees, students and third parties recognize when an incident or information security breach has occurred and report it. Incident registration and periodic reporting on incidents that have occurred belong in a mature information security environment.

Incidents can be reported via the security problem form<sup>11</sup> on the intranet. Tilburg University has clearly communicated the contact information of this hotline to its employees, students, and third parties. Every employee, student, and third party is responsible for identifying and reporting incidents and information security breaches, including data breaches. Incidents are handled according to the established Incident Management Process, which includes reports of data breaches. The DPO handles reported data breaches.

Tilburg University has an established policy on Responsible Disclosure. With this, Tilburg University gives reporters of possible vulnerabilities in its information systems a guarantee that Tilburg University, subject to conditions, will not take legal action against them. A Coordinating SURF Contact (CSC)<sup>12</sup> for SURF has also been appointed within Tilburg University. The employee who has this (additional) role is a security representative on behalf of Tilburg University. This is particularly important if contact is made with Tilburg University in connection with an incident from SURF CERT or from the police. This contact is always made through the appointed CSC.

<sup>11</sup> See <https://www.tilburguniversity.edu/nl/form/report-security-problem>

<sup>12</sup> See <https://www.surf.nl/en/about/coordinating-surf-contact-special-interest-groups> for a list of the CSCs.

## 10. Adoption & amendment

The initial IS Policy was adopted by the Executive Board on September 7, 2021. The IS Policy follows the frameworks of the institutional policy, is reviewed at least once every 2 years, and adjusted if necessary. Also after a substantial change in the institutional policy or significant developments in the cybersecurity field, the Policy is reviewed by care of the CISO and adopted again.

Review of the Policy took place in March 2024. Textual and formatting changes were made.

For questions or comments regarding this Policy, please contact the CISO Office ([ciso-office@tilburguniversity.edu](mailto:ciso-office@tilburguniversity.edu)).

## Appendix A - Schematic Overview of ISMS setup.

Information security is a continuous process. First, it must be determined what is required, and subsequently, measures must be taken. These measures are recorded in an annual plan. The measures can change because threats and risks change, but also legislation and regulations are subject to change. Monitoring can then lead to adjustment of the measures. In addition, the total package of requirements, measures, and checks may also need to be reassessed and will, therefore, have to be evaluated periodically. The entire process of information security thus follows a Plan-Do-Check-Act (PDCA) cycle (see the figure).



The complete set of measures, processes, and procedures is recorded in an Information Security Management System (ISMS) and, thus, provides support in completing the PDCA cycle.

Through repetition of the PDCA cycle, the organization works continuously to improve the ISMS and, thus, becomes more in control.

### Preparation

In the preparatory phase, the following issues are addressed:


- Understanding the context of the organization: the external and internal environment;
- Understanding stakeholder needs and expectations;
- A good description of the scope of the ISMS: what is covered and what is not;
- Leadership and commitment, without which information security in an organization cannot be taken seriously.

Subsequently, the ISMS must be drafted.


### The PDCA cycle includes the following phases:


<p><b>Plan</b></p> <p>The following are defined in the plan phase:</p> <ul style="list-style-type: none"> <li>• Policy</li> <li>• Scope</li> <li>• Organizational assets</li> <li>• Risks and opportunities</li> <li>• Resources</li> <li>• Competencies</li> <li>• Awareness</li> <li>• Communications</li> <li>• Documented information</li> </ul>	<p><b>Do</b></p> <p>Implementation of the ISMS involves:</p> <ul style="list-style-type: none"> <li>• The operational planning and control</li> <li>• Risk assessment(s)</li> <li>• Risk handling</li> </ul>
<p><b>Check</b></p> <p>The check phase includes evaluating the operation of the ISMS:</p> <ul style="list-style-type: none"> <li>• Monitoring, measurement, analysis, and evaluation</li> <li>• Reporting</li> <li>• Internal audit</li> <li>• Management review</li> </ul>	<p><b>Act</b></p> <p>Based on the results of the check phase, improvements are made.</p> <p>Then a new PDCA cycle starts.</p>

## Appendix B - Information Security Principles


<b>1</b>	<p><b>Risk-based</b> Information security measures are taken on a risk-based basis.</p> 
Background	<p>Sharing knowledge (openness) is an important core value of Tilburg University's education and research process. For proper risk assessment regarding protecting information and taking appropriate measures, it is important to determine the value of information. If the value of information is known, the right level of security can also be determined: one that is in line with the risks and our so-called "risk appetite." Proportionality in this is desirable, also for efficiently use of the available financial resources (fit for purpose).</p>
Implications	<ul style="list-style-type: none"> <li>• Tilburg University conducts an AIC classification for all processes and/or information systems.</li> <li>• Risks are estimated and determined based on a risk classification (see Appendix C).</li> <li>• Risk classification is performed based on the Classification Guideline. Where necessary, additional baseline measures are taken to bring the identified risk of availability, integrity, and confidentiality to the accepted level.</li> <li>• Information within Tilburg University has a single owner.</li> <li>• Owners of information, information systems, and processes are responsible for the implementation and operational enforcement of measures under the "comply or explain" principle.</li> <li>• Deviations can be accepted within Tilburg University's risk appetite, ultimately to be determined by the Executive Board. For deviations, the risk acceptance process is followed, with acceptance by the process, system, or information owner.</li> <li>• Risk acceptances, including motivation, are logged in a central risk register.</li> <li>• The process, system, or information owner signs off the risk acceptance.</li> <li>• Measures are designed so that their effect is verifiable.</li> <li>• The highest risks are mitigated first.</li> <li>• Based on the risk analysis, user-friendliness may be chosen over and above information security.</li> <li>• Measures must be balanced (in terms of cost) with risk reduction (proportionality principle).</li> <li>• Information has a single source, making ownership and single source of truth easy to interpret. This also creates additional chain responsibility for the consequences of changes at the source.</li> <li>• Tilburg University remains responsible for adequate protection of information, including when using external information processing services.</li> <li>• Where applicable, contracts include security requirements and the requirement for delivery of external review (assurance) showing that measures are effective.</li> <li>• Software and services must meet various security requirements and standards. Tilburg University uses STITCH and the SURF Framework</li> </ul>


of Legal Standards for Cloud Services in Higher Education for this purpose.

<p><b>2</b></p>	<p><b>Everyone</b> Information security is everyone's responsibility</p> 
<p>Background</p>	<p>Everyone is aware of the value of information and acts accordingly. This value is determined by the potential harm resulting from loss of availability, integrity, or confidentiality. Employees, students, and third parties are all expected to handle information consciously in any form and to actively contribute to the security of automated systems and the information stored therein. The success of security hinges on good communication. Good communication is therefore actively promoted, at and between all levels within Tilburg University.</p>
<p>Implications</p>	<ul style="list-style-type: none"> <li>• Board and management steers for information safety and privacy protection and ensures the right "tone-at-the-top."</li> <li>• A Code of Conduct is available for all users of Tilburg University's digital information facilities and is published on the Tilburg University website.</li> <li>• The secure handling of information and information carriers is part of the appointment/employment contract of all employees.</li> <li>• Tilburg University conducts an annual security awareness program.</li> <li>• There is mandatory participation in Digital Safe Working training for all employees.</li> <li>• Information security receives attention when employees are hired and at annual appraisals.</li> <li>• Information security receives attention in regular organizational unit and project consultations.</li> <li>• Staff and students speak to each other about unsafe handling of information and systems.</li> <li>• Employees and students report (suspected) vulnerabilities to the CERT (possibly with the intervention of IT support).</li> <li>• An established Responsible Disclosure policy is in place.</li> <li>• Violation of information security legislation, regulations, and rules may lead to sanctioning measures, by or on behalf of the EB, as established in the Codes of Conduct.</li> </ul>

<p><b>3</b></p>	<p><b>At all times</b> Information security is a continuous process</p> 
<p>Background</p>	<p>The environment is constantly changing; cyber threats increase and decrease; processes change, employees and students change, etc. Defining and implementing measures once is insufficient to maintain a secure environment. Information security only makes sense if it is a continuous process of taking measures, creating awareness, and implementing checks.</p>

Implications	<ul style="list-style-type: none"> <li>• An Information Security Management System (ISMS, Appendix A) has been set up to adequately monitor all aspects of the IS Policy through a PDCA cycle.</li> <li>• Audits and assessments are carried out periodically that allow the policy and measures taken to be verified for effectiveness (verifiability).</li> <li>• Upon intake of new employees and students, attention is paid to awareness of the risks and the Tilburg University security procedures regarding access and use of IT resources.</li> <li>• High privilege accounts are validated periodically.</li> <li>• Tilburg University regularly organizes privacy and (cyber)security awareness activities for its various target groups: Tilburg University students, employees, managers, and collaboration partners.</li> <li>• When changes in roles, tasks, and responsibilities of a person are made, authorizations are also aligned and adjusted accordingly.</li> <li>• A process will be established to determine and periodically update Tilburg University's threat landscape. New threats will lead to adjustment of measures where necessary.</li> </ul>
--------------	---

<b>4</b>	<p><b>Security by Design</b></p> <p>Information security is an integral part of any project or change related to information, processes, and IT facilities from the outset.</p>	
Background	<p>Security by Design means that already during the start of a project, the design of a new information system or ICT environment and, during technical or functional changes, the security of data and the continuity of processes is taken into account. This prevents (often expensive) remedial work afterwards.</p>	
Implications	<ul style="list-style-type: none"> <li>• Tilburg University has incorporated Security by Design as an architectural principle.</li> <li>• For any new project/software/service procurement/innovation, security requirements (non-functional requirements) are included from the outset.</li> <li>• Before going live, the application of the security requirements is reviewed and/or tested.</li> <li>• In any IT system or facility, to promote information security, the principle of "least rights" is used. This means that the principle is to grant no more rights than strictly necessary for adequate job and business performance.</li> <li>• Access to systems is based on authorization schemes.</li> <li>• Separation of responsibilities is applied in processes and procedures.</li> <li>• The design incorporates that the use of information and IT facilities is always traceable to a responsible user.</li> <li>• A "security in projects" guideline has been established, based on the measures resulting from the risk classification and measures that may result from the data protection impact assessment (DPIA) under the GDPR.</li> <li>• The process design includes the measures that can adequately ensure the continuity of the process.</li> </ul>	

<p><b>5</b></p>	<p><b>Security by Default</b>                  In any configuration that is implemented, the security options present are on by default.</p> 
<p>Background</p>	<p>Security by Default prevents unwanted and uncontrolled access to (personal) data. Opening up information and configuration of settings are, therefore, always a conscious choice after careful consideration.</p>
<p>Implications</p>	<ul style="list-style-type: none"> <li>• Tilburg University has set up an Identity Access Management process, which means that HR, in consultation with the relevant manager, determines the rights of the user based on the position and the corresponding rights (recorded in an authorization scheme).</li> <li>• The security baseline of the default configuration is defined (e.g., protecting all external communications with TLS technology by default).</li> <li>• The principle in initial design of an information system or infrastructure is "closed unless."</li> <li>• Deviation from the initial setup follows the principle of "comply or explain."</li> <li>• Security is secured in a change management process.</li> <li>• Some main roles are identified on the basis of which baseline authorizations are granted. For example, the main roles are student, employee, supplier, etc. By default, users are only assigned these particular roles.</li> <li>• Logging and auditing processes are set up so that access to information and IT facilities is traceable to a responsible user.</li> </ul>



## Appendix C - The AIC classification

Classification according to AIC (Availability - Integrity - Confidentiality) can be applied to data itself and to the information system in which data is processed and/or stored and to processes. Currently, the choice has been made for TiU to perform classifications on information systems.

When assessing the need for availability, integrity, and confidentiality of information systems, we need to consider what type of data is being processed in this information system.

The CISO Office (second line) advises, and Internal Audit (third line) ensures that the process proceeds as agreed upon. Classification focuses on:

1. the classification of the information system in which data is captured;
2. the inventory of risks;
3. the security requirements to be taken from the Baseline;
4. the relationship between 1, 2 and 3.

Aspect		Low	Middle	High
<b>Availability</b>		A=1	A=2	A=3
<b>Integrity</b>		I=1	I=2	I=3
<b>Confidentiality</b>	C=0*	C=1	C=2	C=3

\* For confidentiality, there is a fourth classification, C=0. This classification is given to information that does not involve confidentiality and should be considered "public."

The AIC classification shows the extent to which an information system scores low, medium, or high on the components availability, integrity, and confidentiality. If the AIC classification scores low or medium overall, the basic security requirements must be met, in accordance with the Baseline. If risks can still be seen beyond the baseline requirements, then additional measures are needed to mitigate the risks. Those security requirements that Tilburg University considers necessary for a classification high are also described in the Baseline.

## Appendix D - Legislation and Regulations.

This appendix provides an overview of key information safety-related legislation and regulations with specific concerns for Tilburg University.

### 1. Dutch Higher Education and Research Act (HERA)

*(Wet op het Hoger onderwijs en Wetenschappelijk onderzoek)*

Tilburg University has a quality assurance system in accordance with the Institutional Audit (*Instellingstoets Kwaliteitszorg (ITK)*). This ensures (among other things) the careful handling of data in the student records system and study results. In addition, research integrity codes are observed and applied.

### 2. General Data Protection Regulation (GDPR)

Tilburg University has adopted a separate data protection policy that ensures compliance with the GDPR. Compliance with both the information security and data protection policies, including the technical and organizational measures stated therein, ensures compliance with the GDPR.

### 3. Statutory Retention Periods/Public Records Act

Tilburg University adheres to the legal requirements regarding retention periods, as laid down in specific legislation (such as the tax law and labor law) and in the Dutch Public Records Act (*Archiefwet*) and Public Records Decree (*Archiefbesluit*). Tilburg University applies the Basic Selection Document for University Education (*Basisselectiedocument Wetenschappelijk Onderwijs*) (1985)<sup>13</sup> for the universities/universities of applied sciences sector. This selection document deals with all information as recorded, for example, in (digitized) documents, information systems, websites, and e-mail. This is part of the annual external audit reports.

### 4. Copyright Act (*Auteurswet*)

Tilburg University respects copyrights and acts accordingly.

### 5. Telecommunications Act

Because Tilburg University's target group is sufficiently defined, Tilburg University's network facilities are not considered a public network within the meaning of the Telecommunications Act. Exceptions to this are some facilities for the purpose of student housing. For these, procedures in accordance with the Net Neutrality Law (*Wet Netneutraliteit*) have been established.

### 6. Computer Crime Act III

The Computer Crime Act (*Wet Computercriminaliteit*) focuses on the criminal problem areas related to computer use. This Act consists of articles added to various parts of the Criminal Code. The additional articles deal with:

- criminal damage rendering useless
- data interception
- denial of service
- computer hacking
- the use of services without payment
- malware, malicious software.

Compliance with this Information Security Policy, in particular the security measures and expected behavior, will ensure that Tilburg University has an adequate basic level of security against these threats. If attacks occur at Tilburg University that significantly breach security and are covered by the Computer Crime Act, the administration of Tilburg University will

---

<sup>13</sup> Reference VH document /reference VSNU document.

always file a report with the police.

#### **7. Network and Information Security Directive (NIS2).**

This new European cybersecurity legislation will go into effect in the Netherlands by the end of 2024. It was adopted by the European Union. With the aim of improving cybersecurity and the resilience of essential services in EU member states. This Directive has the following obligations:

- Duty of care: the organization conducts risk assessments and applies appropriate measures to secure services based on these assessments.
- Duty to report: incidents are reported to the regulator within 24 hours. A cyber incident must also be reported to the Computer Security Incident Response Team (CSIRT).
- Supervision: there is an independent (external) supervisor looking at compliance with the obligations of the Directive.

#### **8. Other codes and national agreements**

The information security policy is based on the SURF Standards Framework and Tilburg University is a participant in the Universities of the Netherlands. In this context, Tilburg University is bound by the following codes and national agreements:

- Good Governance Code for Universities
- Dutch Code of Conduct for Research Integrity.
- SURF Standards and Information Security Assessment Framework for in Higher Education.
- Basic Selection Document for Universities/UMCs.
- SURF membership requirements.
- ISTLP (Information Sharing Traffic Light Protocol).

## Appendix E - Roles in Information Security

Roles within the Information Security Policy
Awareness Officer
Central Privacy Officer
CERT chair (is part of the ITSO role).
Chief Information Officer
Chief Information Security Officer
Executive Board
Contract Manager
Data Representative
Data Protection Officer
Functional Administrators
Governance Risk, Safety & Compliance Officer
Head of Internal Audit
Information Architect
Information owner
Information Manager
Information Security Officer
IT Security Officer
Management (Deans, Managing Directors)
Staff
Information Security Portfolio Holder
Process Owner
Risk Manager
Service desk/IT support/Student Desk
Board of Governors
System Owner

## Appendix F - Establishment of CERT

The goal of the Computer Security Emergency Response Team (CERT) is to prevent information security incidents and handle them if they do occur. The objective is to ensure the continuity of Tilburg University and protecting its reputation. The CERT also deals with security incidents outside Tilburg University if its own employees are involved in any role. In such cases, whenever possible, use is made of the services of SURF-CERT, which is connected to other CERTs worldwide.

The chair of the CERT draws up a Chapter, detailing the target group, assignment, powers, escalations, working methods (including dealing with confidentiality), and composition. Among other things, this sets down that the CERT operates for Tilburg University as a whole and receives its assignment directly from the EB/CISO. Direct escalations via the chair of the CERT to the management level (via the CISO) are also laid down. Direct contacts will also be recorded with the organizational units or persons within Tilburg University responsible for legal issues and contacts with the press.

The ITSO (Head of CERT) advises in the event that Tilburg University computer systems or network segments need to be temporarily isolated. To this end, the ITSO is mandated by the Director LIS/CIO.

Incidents at Tilburg University can be reported to the CERT hotline. Tilburg University has clearly communicated the contact information for this hotline to its employees, students, and third parties.

Every employee, student, and third party is responsible for identifying and reporting information security incidents and breaches. Incidents and breaches should be reported immediately to the CERT hotline.

In order to handle incidents appropriately, they are discussed in the relevant operational consultations. In the event that Tilburg University's business process, finances, or good name are at risk, the incident is also discussed with the CISO. When discussed with the CISO, any confidentiality applicable to the incident at that time is taken into account. If disturbing trends are identified, Tilburg University's CERT proactively responds by taking additional measures or creating (additional) awareness within the organization.