



# Information Security Policy Tilburg University



Version: 1.02  
Date: August 2021  
Status: Final



This Information Security Policy is based on the SCIPR Information Security Policy Model, which is part of the SCIPR Information Security Framework.

For information on SCIPR see <https://www.scipr.nl>

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



## Version management

| Version | Date       | Author                      | Notes   |
|---------|------------|-----------------------------|---|
| 0.1     | 12/03/2020 | Ko Groen                    | First version of IS policy based on the SCIPR model                             |
| 0.2     | 20/05/2020 | Ko Groen                    | Revised following review by Jeffeny Hoogervorst and Miranda van der Ploeg-Cools |
| 0.3     | 06/08/2020 | Ko Groen                    | Revised following additions by Miranda van der Ploeg-Cools                      |
| 0.4     | 21/09/2020 | Miranda van der Ploeg-Cools | Revised following review by Corno Vromans and Jolanda Peters-van Nieuwenhoven   |
| 0.5     | 10/11/2020 | Miranda van der Ploeg-Cools | Revised following review by Paul Geerts   |
| 0.6     | 11/11/2020 | Miranda van der Ploeg-Cools | Revised following review by Ton Aben  |
| 0.7     | 23/11/2020 | Miranda van der Ploeg-Cools | Revised following review by Paul Geerts   |
| 0.8     | 19/01/2021 | Miranda van der Ploeg-Cools | Review by Jolanda Peters-van Nieuwenhoven                                       |
| 0.9     | 08/02/2021 | Miranda van der Ploeg-Cools | Review by Jolanda Peters-van Nieuwenhoven discussed and processed               |
| 1.0     | 02/03/2021 | Miranda van der Ploeg-Cools | IS policy finalized   |
| 1.01    | 25/06/2021 | Paul Geerts                 | Revised following review by LIS MT  |
| 1.02    | 28/06/2021 | Tessel Stoppelenburg        | Textual revisions   |

## Table of Contents

|   |    |
|---|----|
| Foreword .....  | 4  |
| Summary .....   | 5  |
| 1. Introduction.....                                    | 7  |
| 1.1 Background.....                                     | 7  |
| 1.2 Target group .....                                  | 7  |
| 1.3 Scope of the policy .....                           | 7  |
| 2. Definition and aim .....                             | 8  |
| 2.1 Information safety and information security .....   | 8  |
| 2.2 Aim.....  | 8  |
| 3. Information security policy principles.....          | 9  |
| 3.1 Introduction.....                                   | 9  |
| 3.2 Policy principles .....                             | 10 |
| 4. Legislation and regulations.....                     | 12 |
| 5. Organization of information security .....           | 12 |
| 5.1 Aim.....  | 12 |
| 5.2 Three Lines of Defense Model.....                   | 12 |
| 5.3 Roles and responsibilities .....                    | 13 |
| 5.4 Strategic, tactical and operational .....           | 18 |
| 5.5 Information security documents .....                | 19 |
| 6. Awareness-raising and training .....                 | 20 |
| 7. Checks, practice, compliance and sanctions .....     | 21 |
| 8. Funding .....  | 21 |
| 9. Reporting and handling of incidents .....            | 22 |
| 10. Determination and amendment .....                   | 22 |
| Appendix A – Schematic Overview of the ISMS Setup ..... | 24 |
| Appendix B – Information Security Principles .....      | 26 |
| Appendix C – The AIC Classification .....               | 31 |
| Appendix D – Legislation and Regulations .....          | 32 |
| Appendix E – The RASCI Matrix .....                     | 34 |
| Appendix F – Information Security Roles .....           | 38 |
| Appendix H – The CERT Setup .....                       | 39 |



## Foreword

In order to do our work, it is increasingly important for us to secure our information and information systems properly. Tilburg University's work processes cannot be carried out without collecting, recording and sharing information with both internal and external partners, colleagues and students, and information security is vital here.

This information security policy (IS policy) sets out how Tilburg University provides satisfactory information security, thus complying not only with the relevant legislation and regulations but also with the internal security standards. With its IS policy, Tilburg University aims to help improve the quality of information provision and ensure the right balance between functionality, security and privacy.

Tilburg, ... August 2021

The Executive Board

## Summary

Information security is the totality of measures, processes and procedures that guarantee the availability, integrity and confidentiality of information and information provision. This information security policy (IS policy) lays down how we at Tilburg University shape these processes and procedures and who is responsible for what.

Information security permeates every level of the organization. The IS policy sets out the scope: to whom, to what units and to what devices and applications the policy applies, and the responsibilities of the officials concerned. Ultimate responsibility rests with the Executive Board (EB). This responsibility for processes (including security measures) is assigned to the deans and directors under the mandate and power of attorney rules. The Information Security Department (part of Library and IT Services) advises on the required security measures and monitors the processes associated with information security.

The required security measures comprise a set of basic measures, known as the 'Security Baseline', that apply to all information systems and processes, and may also include a set of additional security measures. How an information system or process rates in terms of Availability, Integrity and Confidentiality is shown by an AIC classification. If that classification is higher than the Security Baseline classification, additional measures will be needed to mitigate risks. Both the measures in the Security Baseline and the additional measures are explained in a separate document; they are not included in this IS policy.

### **The policy is based on five principles:**

1. Risk-based  
We base the required measures on the potential security risks of our information, processes and IT facilities (in the broadest sense).
2. Everyone (all staff, students, guests, visitors and external partners of Tilburg University)  
Everyone is and feels responsible for the correct, safe use of resources and powers.
3. At all times  
Information security is in the DNA of all the work we do.
4. Security by Design  
From the outset, information security is an integral part of every project or change in information, processes or IT facilities.
5. Security by Default  
Users only have access to the information and IT facilities that they need for their work. Making information available is a conscious choice.

Policies and measures are not sufficient to rule out information security risks completely. People themselves create the greatest risks. At Tilburg University we therefore make constant endeavors to increase security awareness in the organization, with the aim of increasing knowledge of risks and encouraging safe, responsible behavior.

Information security is an ongoing process, and we are constantly looking for ways of improving it, for example by drawing up and implementing annual plans, checks and adjustments. In addition to the Chief Information Security Officer (CISO, second line) and the Risk Consultant (second line), the Data Protection Officer (DPO, third line) and the Internal Auditor (IA, third line) may be asked to give advice on these on request or on their own initiative.



The management cycle for periodic revision is discussed in the Appendices. The five information security policy principles are set out in full there, along with an overview of the most important legislation and regulations on information security and further information on the roles of the officials concerned.

## 1. Introduction

### 1.1 Background

Digital and physical reality are in constant flux, resulting in ever new and different information safety risks.<sup>1</sup> These are a threat to the quality and continuity of processes and to the achievement of the strategic goals. The threats can affect the availability, integrity and confidentiality of information.

1. Availability: the information is available when required.
2. Integrity: the information is correct and complete.
3. Confidentiality: the information is only available to authorized persons.

The privacy<sup>2</sup> of students, staff and guests and Tilburg University's reputation can also be harmed, hence information security is vital. It needs to be constantly revised so as to maintain an appropriate security level, due to such things as ongoing technological developments, developments in cyber crime, the tougher requirements that need to be met in order to comply with the legislation and regulations on data protection and privacy (the GDPR), and the agreements with research and education partners.

Risk reduction and control requires endeavors in the areas of organization, processes and technology. In addition, all staff, students, guests, visitors and external partners of Tilburg University need to become and remain aware of the risks and act accordingly.

With the world constantly changing, implementing measures and creating awareness is a dynamic process. The five main principles on which information security at Tilburg University is based are therefore set out in this document. The measures, procedures and guidelines to be laid down can be checked against the five main principles set out in Chapter 3.

### 1.2 Target group

Tilburg University's IS policy is primarily the responsibility of the Executive Board, deans and directors, the security organization and managers. It applies to all staff, students, guests, visitors and external partners, and to all the organizational units: in short, to everyone – internal or external – who is in any way involved in any aspect of Tilburg University's business process.

### 1.3 Scope of the policy

Tilburg University places a broad interpretation on information safety. It relates to all types of formally recorded information, including personal data that is processed, that the university or its partners generate and manage, in digital form or otherwise. We also do our best to promote information safety in matters for which we are not formally responsible but that could be laid at the door of Tilburg University.<sup>3</sup>

There is an important relationship and a partial overlap with risks such as safety, physical security and business continuity. These overlaps are considered at strategic level, and we seek to coordinate them, in terms of both planning and substance. Information security is one of the elements of overall security, but it

---

<sup>1</sup>For the difference between the definitions of 'information safety' and 'information security' see the note to section 2.1.

<sup>2</sup> For Tilburg University's specific Privacy and Personal Data Protection Policy see the [intranet](#).

<sup>3</sup> See Tilburg University's [Social Media Guidelines](#), which lay down the rules on social media content posted by staff of the university.



is still dealt with separately, as a rule. This IS policy can be seamlessly integrated into an across-the-board policy on integral security, as soon as one is developed at Tilburg University.

The IS policy applies to Tilburg University's organization: the five schools, the seven support divisions and the partners that use Tilburg University's infrastructure and IT facilities. In principle, it covers all devices (both managed and unmanaged) that provide authorized<sup>4</sup> access to the Tilburg University network and its services and/or with which information at Tilburg University is processed.

The policy is not location-dependent: it also applies when using Tilburg University's information or information facilities outside its premises, for example at home, on a train or at another educational institution.

## 2. Definition and aim

### 2.1 Information safety and information security

The terms 'information safety' and 'information security' are often used interchangeably, but they have different meanings. Information safety is concerned with the availability, integrity and confidentiality of information. This involves protecting information and information systems against potential threats, which is done by taking, maintaining and checking security measures, referred to as 'information security'.

### 2.2 Aim

The aim of IS policy is to increase the university's resilience. This is achieved by detecting potential security and privacy risks at an early stage, by limiting their consequences and by taking the right management measures to guarantee the availability, integrity and confidentiality of the business process (teaching, research and management).

The IS policy thus directly supports the mission of the organization as a whole.

The IS policy, and its follow-up, are designed to enable Tilburg University to be in control and compliant. The implementation of the policy also provides the basis for complying with legal requirements.

Specifically, the aims of the IS policy are as follows:

- Framework  
The policy provides a framework for checking current and future information security measures against the security principles laid down (section 3.2), best practices and standards. It also provides a framework for assigning duties, powers and responsibilities within the university.
- Standards  
The information security management setup is based on an international standard, ISO 27001. Formal certification in line with ISO 27001 is not considered necessary in the case of Tilburg University. What is necessary is to set up a good information security management system (ISMS,<sup>5</sup> see Appendix A). The ISMS is based on ISO 27001. Tilburg University aims to achieve at least Maturity Level 3 in the Capability Maturity Model (CMM).

---

<sup>4</sup> Unauthorized access is by definition a security incident.

<sup>5</sup> Information Security Management System.

The Security Technical IT Checklist (STITCH) is used for software and services provided by outside organizations.

- Measures  
The measures taken are based on the *Information Security Baseline*, in turn based on ISO 27002, and the *SURF Framework of Standards for Information Security in Higher Education*.
- Security organization  
The responsibilities, duties and powers relating to information security are explicitly laid down and borne by the EB and, following on from this, by the entire University.
- Process approach  
Information security is an ongoing process that follows a PDCA cycle. Risk analyses and audits are carried out periodically, and the results are incorporated in annual plans setting out clear choices regarding security measures. The implementation of these security measures is checked periodically.

### 3. Information security policy principles

#### 3.1 Introduction

Tilburg University is an open institution. From the point of view of teaching and research, the approach is '*Open where possible, closed where necessary*'. Satisfactory information security is always a prerequisite, and making information available must be a conscious choice.


This IS policy sets out five information security policy principles, which help with the implementation of the policy, in the sense that they determine what security measures are needed to protect Tilburg University's processes. A policy principle has a name and comprises a core, a brief explanation and background, and a description of the main implications.


The measures laid down by Tilburg University cannot always be applied one-on-one in every situation. Sometimes, for example, there may be processes that are unusual or technical or organizational limitations. In those cases alternative measures will need to be taken that do justice to the underlying principle and adequately cover the risks, based on the 'comply or explain' principle.<sup>6</sup>

---


<sup>6</sup> 'Comply' relates to the specific measures; the principles serve as a reference for 'explain'.

### 3.2 Policy principles


|                     |  |
|---------------------|--|
| <h1>1</h1>          | <p><b>Risk-based</b><br/>Information security is risk-based.</p>    |
| <p>Core</p>         | <p>We base the measures on the potential security risks of our information, processes and IT facilities (in the broadest sense).</p>   |
| <p>Background</p>   | <p>Sharing knowledge (openness) is an important core value of Tilburg University's teaching and research process. If we are to make a good risk assessment as regards protecting information and taking the right measures, we need to establish the value of information. Once that value is known, the right degree of security can be selected, i.e. one that is appropriate to the risks and our 'risk appetite'. It also needs to be proportionate (fit for purpose), so as to make efficient use of the financial resources available.</p> |
| <p>Implications</p> | <p>Tilburg University has a risk management process in place in which 'risk acceptances' (including reasons) are logged in a central risk register. Risks are additionally assured in contracts, and the information security measures are checked based on the STITCH and the SURF Framework of Legal Standards. Tilburg University has also laid down the responsibilities explicitly in this policy document. For an overview of the various implications see Appendix B.</p>   |

|                     |  |
|---------------------|--|
| <h1>2</h1>          | <p><b>Everyone</b><br/>Information security is the responsibility of everyone (all staff, students, guests, visitors and external partners of Tilburg University).</p>    |
| <p>Core</p>         | <p>Everyone is and feels responsible for the correct, safe use of resources and powers.</p>  |
| <p>Background</p>   | <p>Everyone is aware of the value of information and acts accordingly. The value is determined by the potential harm that could be caused by loss of availability, integrity or confidentiality. Staff (in the broadest sense), students and third parties are all expected to handle information – in any form – consciously, and to contribute actively to the safety of the computerized systems and the information stored in them. The success of security stands or falls with good communication. Good communication is therefore actively promoted, at and between all levels of the university.</p> |
| <p>Implications</p> | <p>Tilburg University's terms of employment state that every new staff member is required to take the Safe Working training course. Everyone's responsibility for</p>  |

|  |  |
|--|--|
|  | <p>information security is also laid down in its codes of conduct and house rules. In addition, every year Tilburg University organizes various awareness-raising activities, based on the security awareness program. For an overview of the various implications see Appendix B.</p> |
|--|--|

|              |   |
|--------------|---|
| <h1>3</h1>   | <p><b>At all times</b><br/>Information security is an ongoing process.</p>   |
| Core         | Information security is in the DNA of all the work we do.   |
| Background   | The environment is constantly changing: cyber threats increase and decrease, processes change, there are changes in staff and students, and so on. It is not sufficient, therefore, to decide on and implement measures only once if we are to keep the climate safe. Information security is only worthwhile if it is an ongoing process of taking measures, creating awareness and carrying out checks. |
| Implications | Tilburg University has an audit process in place based on a PDCA cycle. Various awareness campaigns are also organized, based on the security awareness program. For an overview of the various implications see Appendix B.  |

|              |   |
|--------------|---|
| <h1>4</h1>   | <p><b>Security by Design</b><br/>Integrated approach to information security</p>   |
| Core         | From the outset, information security is an integral part of every project or change in information, processes or IT facilities.  |
| Background   | Security by Design means that, right from the start of a project, data security and process continuity are taken into account in the design of any new application or ICT environment and when any technical or functional changes are made. This avoids remedial work after the event, which can often be expensive.   |
| Implications | Tilburg University has adopted Security by Design as an architectural principle. The processes are organized in such a way that any new infrastructure or system or change in an infrastructure or system is first classified, and the information security measures are determined based on that classification. For an overview of the various implications see Appendix B. |

|              |   |
|--------------|---|
| <h1>5</h1>   | <p><b>Security by Default</b><br/>                 Limited access by default and safe settings</p>   |
| Core         | Users only have access to the information and IT facilities that they need for their work. Making information available is a conscious choice.  |
| Background   | Security by Default means that the security options available are enabled by default in any configuration that is implemented. This prevents undesirable and uncontrolled access to personal and other data. Making information available and configuring the settings is thus always a conscious choice, following careful consideration.  |
| Implications | Tilburg University has an Identity Access Management process in place, which means that HR determines each user’s rights in consultation with the manager concerned, based on the post that the user holds and the associated rights. In addition, logging and audit processes are organized in such a way that access to information and IT systems can be traced back to individuals. For an overview of the various implications see Appendix B. |

## 4. Legislation and regulations

The principle is that Tilburg University complies with all the applicable legislation and regulations in its processes and procedures and makes preparations to comply with any forthcoming legislation. How Tilburg University deals with relevant legislation and regulations is set out in more detail in Appendix D – Legislation and Regulations.

## 5. Organization of information security

### 5.1 Aim

The IS policy needs to be rolled out and observed throughout the organization. To ensure this, it is not only necessary to lay down the various roles and responsibilities in the organization as regards information security but also how they relate to each other. This chapter discusses the roles and responsibilities and how they interrelate in more detail.

### 5.2 Three Lines of Defense Model

Information safety at Tilburg University is organized in line with the Three Lines of Defense Model. Each of the three lines in the model has specific responsibilities. The model describes not only the roles within the organizational structure but also how they work together.



### Three Lines of Defense Model

- **Executive Board/Deans:**  
The Executive Board and the Deans ensure that the organization has sufficient resources to achieve objectives and mitigate risks and to encourage a culture of ethical, responsible behavior. The Executive Board lays down the university's frameworks for risk appetite and reports to stakeholders.
- **First line: management responsibility**  
Management (the vice deans, directors and managers) is the first line, which bears overall responsibility for the business activities. The first line provides leadership and guidance and is in a constant dialog with the Executive Board and the Deans on achieving the objectives and risk control.
- **Second line: advisory and supporting responsibilities**  
Management is supported by control posts (including risk management) in the second line, which report on progress and monitor risks with the aid of internal control systems. The coordination and monitoring of risk management is the responsibility of the independent Internal Audit and Compliance Department.
- **Third line: independent checks**  
Internal Audit, the independent third line, assesses the reliability of information and systems and advises on how to improve risk management and internal control.

### 5.3 Roles and responsibilities

Information security is not a standalone operation but an integral part of the organization, relating to disciplines such as privacy, risk management and contract management. Privacy protection, for instance, focuses on handling personal data (e.g. of students and staff) with care, whereas information security focuses on protecting all data, including personal data. Each discipline has its own roles and responsibilities, which are discussed below in more detail in line with the Three Lines of Defense Model.

### Executive Board

The Executive Board (EB) bears ultimate responsibility for information safety at the university, lays down policy and provides the resources needed to implement information safety at the university in line with the principles. The EB's responsibility is assigned to the deans and directors under the mandate and power of attorney rules.<sup>7</sup> One of the members of the EB holds the post of Information Security Portfolio Manager.

### Deans and directors

The Three Lines of Defense Model is based on the principle that line management (the 'business') is responsible for its own processes. The Director of LIS, for instance, bears ultimate responsibility for the central IT infrastructure and the operating system software purchased centrally, with the managers of the various IT departments responsible for technical implementation. The Director of LIS thus also bears ultimate responsibility for information safety in those units. LIS can also create conditions (e.g. information safety and architecture) for local systems.

- *Process owners*: the owner of the primary or support process is responsible for local IT infrastructure.  
*System owners*: a system owner is responsible for an important system platform or application that supports one or more processes. A system owner will often be the owner of the particular process and thus bear ultimate responsibility.

The process and/or system owner will generally be a dean or director, who is thus responsible for embedding and applying information security measures in his/her process and/or system. He/she will therefore:

1. carry out a risk analysis based on an AIC classification;<sup>8</sup>
2. decide whether that risk analysis complies with Tilburg University's Information Security Baseline or whether additional measures are needed to achieve the right degree of security.<sup>9</sup>

There may be valid reasons for opting to deliberately deviate from the information security measures laid down and possibly take mitigating measures to limit the residual risk. Such residual risks should always be taken consciously by the process or system owner and recorded in the risk register by signing a Risk Acceptance Agreement. This agreement informs the responsible party (the risk owner) of the risk concerned, so that arrangements can be made for any temporary measures and whether, and if so when, the risk will be mitigated. Signing the Risk Acceptance Agreement means that responsibility for the risk is recorded and risks can be controlled and managed. The risk acceptance matrix below shows the levels at which risks can be accepted. The risks are estimated by calculating probability x impact.

| Estimate | Authorized to accept          |
|----------|-------------------------------|
| Critical | EB                            |
| High     | EB                            |
| Medium   | Process/system owner          |
| Low      | No formal acceptance required |

*Risk acceptance matrix*

<sup>7</sup> The mandate and power of attorney rules have been published on the intranet: <https://www.tilburguniversity.edu/nl/intranet/organisatie-beleid/mandaatregeling>.

<sup>8</sup> Classification of Availability, Integrity and Confidentiality (AIC).

<sup>9</sup> The Information Security Team provides support and advice. The process owner signs the results of the risk analysis and shares them with the CISO. The CISO stores the risk analysis in digital form. The information manager of the division or school concerned has a lead role to ensure that all the disciplines concerned, e.g. architecture, privacy and security, are involved.



The CISO has an advisory role in the drawing-up of the risk register and Risk Acceptance Agreement and consults with the EB to reach a final decision. The residual risks taken are evaluated annually, and the Information Security Portfolio Manager and the Audit Committee are periodically updated on critical and high risks.

### Managers (including Program Directors)

Compliance with the IS policy is part of the overall business process. Each manager is required to:

- ensure that his/her staff/students are aware of the aspects of the IS policy that are relevant to them;
- oversee compliance with the IS policy by staff and students;
- periodically draw attention to the issue of information security at staff meetings;
- be available as the point of contact for any personnel-related information security matters.

## Second line

### Information Security

Information safety is the responsibility of the Information Security Department. The roles within that department are set out below.

#### Chief Information Security Officer

The CISO maintains the IS policy on the instructions of the EB and has an independent role vis-à-vis the Board. He/she carries out this role by advising the Board on request or on his/her own initiative. The CISO defines the information security strategy and policy, helps to translate it into terms appropriate to organizational units, oversees uniform compliance with it and reports on any gaps, inconsistencies and imperfections (and hence risks). On that basis he/she lays down policy and priorities based on risk and compliance. The CISO oversees compliance and assurance in the ISMS.

The role of CISO is performed by a single person. The CISO has various powers: for instance, he/she can carry out research, commission investigations (audits), request information, give advice on his/her own initiative or on request, and oversee the handling of information security incidents. The CISO (or a member of his/her team) needs to be involved in any projects, purchases and partnerships that have an information technology component.

The process owner (first line) is responsible for assuring a safe process (digital or otherwise), overseen by the CISO. If the process owner does not act on the advice (when there is a clear risk indication) and accepts the risk, the CISO may escalate the matter to the EB if he/she considers this unacceptable.

The Director of LIS is the CISO's functional manager, and the CISO has a direct reporting line to the Information Security Portfolio Manager on the EB. The CISO heads the Information Security Department and runs the CERT.

#### Information Security Officer

The ISO provides direct support to the CISO and implements information security in line with the organization's information security strategy. He/she provides support with carrying out AIC classifications and advises on specific information security measures, e.g. in projects and when purchasing software or hardware, working together closely with the Architects and Information Managers. The ISO is also concerned with setting up and initiating (periodic) awareness-raising programs and advises on information security education and training.



Tilburg University has appointed two ISOs. They are members of the Information Security Department and have the CISO as their hierarchical manager.

#### Safe Working Officer

The Safe Working Officer (SWO) at Tilburg University is concerned with arranging training courses and awareness campaigns on safe working centrally, particularly for new staff, in consultation with the CISO, ISOs and ITSOs and the Central Privacy Officer.

The SWO is a member of the Information Security Department and has the CISO as his/her hierarchical manager.

#### IT Security Officer

The ITSO provides support to the CISO in defining the IT security guidelines for the organization in line with the information security strategy and architecture. He/she draws attention to and monitors the cohesion of IT systems security and developments in that area, in each case looking at the relationship with the business and organizational goals. The ITSO advises on specific technical information security measures, e.g. in projects and when purchasing software or hardware, and assesses the results of penetration tests, vulnerability scans and assessments submitted by suppliers.

Tilburg University has appointed two ITSOs. They are both members of the Information Security Department and have the CISO as their hierarchical manager. One of the ITSOs chairs the CERT and participates in the 24x7 services run by the CERT.

#### Incident Response Handler

The Incident Response Handler (IRH) at Tilburg University is the first point of contact for IT security-related issues, both internal to the organization and external. He/she provides support with resolving cyber security incidents and answers questions about cyber security from staff and students. The IRH contributes to the university's resilience by identifying and analyzing threats in the network and technical security risks. He/she is a member of Tilburg University's CERT and provides the bridge between technology and end-users.

The IRH is a member of the Information Security Department and has the CISO as his/her hierarchical manager.

#### Computer Emergency Response Team (CERT)

The CERT is a hands-on, specialist team of IT security professionals who are able to act quickly in the event of a security incident involving computers and/or networks. The CERT's aim is to prevent, detect and correct problems by applying measures. It is also concerned with supporting security awareness. The CERT currently comprises two IT Security Officers (who also act as backup Incident Response Handlers), a full-time Incident Response Handler and specialists in the organization who can be called in.

The CERT is part of the Information Security Department. Its duties, powers and responsibilities are set out in a CERT Charter.

From the point of view of information security, the information managers are regarded as the CISO's antennas in the organization. Tilburg University appoints divisional information managers (who are members of their divisions) and schools information managers (who are members of the Project and Information Management Department of LIS). An information manager is involved in information projects and developments in teaching, research and management and encourages compliance with the IS policy in those projects and developments. Information managers work together closely with the Information Security Department.

### **Information architects**

The information architects assure the implementation of the Information Security Baseline and any additional measures resulting from the classification. They also monitor the consistency of measures by means of a project start architecture. Two Business Architects and an IT Architect have been appointed to LIS.

### *The link with privacy*

#### **Data Protection Officer**

The DPO at Tilburg University oversees the application of and compliance with the GDPR and is independent, as laid down in the university's Privacy and Personal Data Protection Policy. The DPO reports directly to the President of the EB and has the head of Internal Audit and Compliance as his/her functional manager. The DPO also plays a role in the third line.

#### **Central Privacy Officer**

The Central Privacy Officer (CPO) at Tilburg University is concerned with the application of and compliance with the GDPR centrally and is an adviser on the subject, in some cases in collaboration with the CISO, ISO, ITS0 and SWO, e.g. when analyzing actual or potential data leaks and setting up and initiating awareness-raising programs. Other examples are assessing risks and measures in the case of a DPIA or when signing processor agreements under the GDPR.

#### **Data Representative**

The Data Representative is the first point of contact for and adviser on questions that a division or school has about how to deal with privacy and personal data, e.g. in the case of a new information service or a change to an existing one. He/she will usually be brought in by the information manager. Each division and school has appointed a local Data Representative.

### *The link with risk management*

#### **Governance Risk and Compliance Officer**

The Governance Risk and Compliance Officer (GRCO) reports directly to the EB. He/she coordinates, facilitates and monitors governance, compliance with legislation and regulations and risk management at Tilburg University. The GRCO is also the head of the Internal Audit Department.

### *The link with contract management*

#### **Contract manager**

The contract manager is always involved in purchasing central systems, where he/she pays explicit attention to information security: this is done by making the information security measures based on the risk analysis part of the procurement process, by including security as a standard feature of the procurement terms, and by making security requirements compulsory in contracts.

**Third line**

**Internal Audit**

Given its independent position, Internal Audit provides added value by scrutinizing the design, existence and, if appropriate, operation of internal control relating to information security. It carries out checks or advises the first and second lines on areas for improvement, also checking whether that are no overlaps or blind spots. Internal Audit reports directly to the President of the EB and the Audit Committee (Board of Governors). Internal Audit is part of the PDCA cycle (in particular the Check and Act components).

**Data Protection Officer**

See the description of the DPO on p. 16 of this IS policy.

**5.4 Strategic, tactical and operational**

The above roles and responsibilities are translated into goals at strategic, tactical and operational level:

- Strategic level  
At strategic level there are policy discussions about governance, risk and compliance, and about aims, scope and aspirations in the area of information security and privacy.
- Tactical level  
At tactical level the strategy is translated into plans, measures, standards to be applied, evaluation methods, etc. These plans and instruments guide implementation.
- Operational level  
The operational level is responsible for implementing the information security measures and handling incidents, in consultation with the functional managers, appropriate IT officials and, where necessary, the tactical level.

The table below summarizes the governance structure at each level. The RASCI matrix can be found in Appendix E. The current roles at Tilburg University in terms of posts/officials can be found in Appendix F – Current Information Security Roles.

| Level            | What  | Who                                      | Consultation/Persons Concerned  | When                           |
|------------------|---|--|---|--------------------------------|
| <b>Strategic</b> | <ul style="list-style-type: none"> <li>· Ultimate responsibility for information security at Tilburg University.</li> <li>· Determining, adopting and communicating IS strategy and policy.</li> <li>· Setting up organization of IS. Laying down IS Planning and Control.</li> <li>· Business continuity management.</li> <li>· Communicating to management and organization.</li> </ul> | EB (based on advice from Security Board) | Laid down by EB.<br><br>Strategic Information Provision Meetings<br><br>Security Board (including the CISO, GRCO, School Director, expert in personal capacity and Director of LIS) and geared to Tilburg University's IT strategy and risk management process. | 2x per year<br><br>2x per year |

|                    |   |   |   |   |
|--------------------|---|---|---|---|
| <b>Tactical</b>    | <ul style="list-style-type: none"> <li>· Monitoring application of and compliance with IS Policy.</li> <li>· Communicating to process owners.</li> <li>· Operational responsibility for information security.</li> </ul>  | CISO  | <p>IS Steering Committee, chaired by the CISO, (comprising the Director of LIS, GRCO, CPO, ISO, HR, Teaching Representative and Research Representative, in consultation with other officials concerned, such as process or system owners, where necessary.)</p> <p>The Information Security Steering Committee monitors the activities relating to information security and is thus responsible for supporting and monitoring the implementation of and compliance with IS policy and the associated guidelines.</p> |   |
| <b>Operational</b> | <ul style="list-style-type: none"> <li>· Implementing IS measures</li> <li>· Providing communication to end-users</li> <li>· Implementing technical security measures</li> <li>· Security monitoring and advice</li> <li>· Recording, analyzing and evaluating incidents, including data leaks</li> </ul> | <ul style="list-style-type: none"> <li>· Process owners, facilitated by LIS</li> <li>· Information manager</li> <li>· LIS</li> <li>· CERT</li> <li>· Data Protection Officer</li> </ul> | <p>Matters relating to day-to-day management (i.e. implementation) are discussed at operational level:</p> <ul style="list-style-type: none"> <li>- Information Security meeting</li> <li>- IT security meeting</li> <li>- Privacy and Security meeting</li> <li>- CERT meeting</li> </ul>  | <ul style="list-style-type: none"> <li>1x per 2 weeks</li> <li>1x per 2 weeks</li> <li>1x per month</li> <li>1x per week</li> </ul> |

*The information security governance structure summarized in a table*

## 5.5 Information security documents

Tilburg University uses the following documents in connection with information security:

### Policy/guidelines

1. IS policy

The IS policy underlies the approach to (digital) information security at Tilburg University. It is drawn up by the CISO and laid down by the EB.

2. Information Security Baseline and Risk Classification Guideline  
The Baseline describes the measures required to ensure a minimum level of information security. These basic measures need to be implemented throughout Tilburg University. Whether a system (or process) requires more security measures than those in the Baseline is determined from an AIC classification. The process owner is therefore required to carry out an AIC classification for each system (or process) at Tilburg University. The classification is based on the Risk Classification Guideline in consultation with Information Security, which can also give advice on its own initiative. What additional security measures need to be implemented will be decided based on the outcome of the AIC classification.
3. Codes of conduct and guidelines on information security for staff, students and third parties (specific target groups or otherwise).

### Monitoring and accountability

4. Information Security Management System (process and recording)
5. Risk register
6. Annual plan/annual report  
In line with the PDCA cycle, the CISO submits an annual report on the past year and an annual plan for the next year to the EB. The annual report is based inter alia on the results of the periodic checks and audits. Among other things it discusses incidents, results of risk analyses (including the measures taken) and other initiatives that took place during the past year.  
Specific systems or applications are considered separately where necessary. The annual plan is scrutinized in terms of the availability of resources (people and assets) compared with the risks that need to be mitigated. It is first coordinated with the Annual Privacy Plan drawn up by the DPO. The reports are consolidated in the administrative Planning and Control cycle.

Information security is additionally included as a regular feature of the following documents:

7. Service agreements (SLAs), temporary employment and outsourcing contracts, non-disclosure agreements (NDAs) and any associated processor agreements  
Explicit attention is paid to information security when hiring temporary staff and purchasing resources (in particular hardware, software, applications/cloud platforms and services), inter alia by applying the IS policy to third parties and making security a standard feature of procurement terms. Agreements are laid down in one or more contracts with the supplier and checked. By default, the contract includes an information security clause setting out the supplier's responsibilities. This is based on the SURF Framework of Legal Standards for Cloud Services in Higher Education, which contains an information security appendix, and the STITCH.
8. Business Continuity Plan  
The Business Continuity Plan will be drawn up at the instigation of the Business Continuity Manager in collaboration with the EB, the CISO, the ISO, the ITSO, the Head of Physical Security, the process owners, the Director of LIS and the Head of Facility Services.

## 6. Awareness-raising and training

Policies and measures are not sufficient to rule out information security risks completely. People themselves are responsible for the greatest risks. At Tilburg University we therefore make constant endeavors to increase security awareness in the organization, with the aim of increasing knowledge of risks and

encouraging safe, responsible behavior. The policy includes regular awareness campaigns for all staff, students, third parties and especially operational managers, and an annual security awareness plan. Raising security awareness is a responsibility of managers, supported by Information Security. Awareness is also an element in the induction program for new staff and students.

## 7. Checks, practice, compliance and sanctions

Tilburg University's Internal Audit Department is responsible for planning operational audits, which are carried out by the Operational Auditor. External auditors are usually brought in to carry out IT audits because of their expertise. The CISO is responsible for checking that the annual information security plans are implemented, with support from the ISOs and ITSOs. The second and third-line activities are carried out based on the frameworks of standards laid down by Tilburg University.

The internal checks take place annually, and the periodic audits are supplemented by various ad hoc activities, such as sampling, carrying out or commissioning penetration tests, vulnerability tests and assessments, and checking the actual operation of the security measures laid down. In addition, skills and operational procedures are regularly tested in brainstorming sessions or exercises, for example the OZON exercise, which is coordinated by SURF every two years.

Tilburg University takes part in the external SURF audit, which scrutinizes design, existence and operation. The external SURF audits take place every year, and are carried out by Internal Audit and/or the external auditor. Tilburg University also takes part in the SURF self-assessment cycle and the associated two-yearly benchmarking exercise (which only scrutinizes design and existence). This is carried out by the LIS management. A SURF Peer Review is requested at least once every four years. The CISO provides input to the audits.

Based on the findings of the second and third-line activities, the process owner is required to draw up an improvement plan, which should include at least the following: action, person with ultimate responsibility and deadline. The follow-up is monitored by LIS.

In addition to internal and external audits, compliance is checked mainly through second-line monitoring. There is active monitoring of security incidents, vulnerabilities and threats at the Security Operations Center, for instance. Compliance also involves specifically overseeing the day-to-day information security management process. It is important here for managers (including those responsible for teaching) to tackle staff and students in the event of shortcomings. The DPO is responsible for overseeing compliance with the GDPR.

If the checks show that compliance is seriously deficient and there is culpable behavior, Tilburg University may impose sanctions on the responsible staff or students concerned. Sanctions are imposed within the legal frameworks (e.g. the Higher Education and Research Act [Wet op het hoger onderwijs en wetenschappelijk onderzoek], the Collective Labor Agreement, employment contracts and the Code of Conduct). This is primarily a responsibility of the EB, but in some cases it may be mandated to the responsible manager (the dean/director).

## 8. Funding

### Local

As indicated in Chapter 5 of this IS policy, the CISO does not bear ultimate responsibility for information security and is therefore not a risk owner. The CISO (or a member of the Information Security Department) needs to be involved in important projects, purchases and partnerships. The budget for information security activities and projects is accordingly provided by the divisions and schools (or the process and system owners). This method of prioritization and budgeting needs to be embedded in the planning and control cycle and in project portfolio management.

### Central

The CISO needs to have an adequate budget of his/her own to carry out the strategic and tactical processes and achieve the objectives in the annual plan. It also needs to be adequate to enable temporary staff from other organizational units to be assigned to carry out information security projects.

## 9. Reporting and handling of incidents

An incident is an event that could have a negative impact on the running of the university. Incident management and recording involves detecting, recording, analyzing and dealing with incidents and making improvements based on lessons learned. It is important here for staff, students and third parties to recognize when there has been an incident or information security breach and to report it. We can learn from incidents. Incident recording and periodic reporting of incidents that have occurred are thus part and parcel of a mature information security environment.

At Tilburg University incidents can be reported to IT Support ([itsupport@tilburguniversity.edu](mailto:itsupport@tilburguniversity.edu)) or the CERT desk ([cert@tilburguniversity.edu](mailto:cert@tilburguniversity.edu)). Tilburg University has clearly communicated the contact details for these desks to its staff, students and third parties.

Every staff member, student and third party is responsible for spotting and reporting incidents and information security breaches, including data leaks. Incidents are handled in line with the Incident Management Process laid down by Tilburg University. This includes accepting reports of data leaks, which are then dealt with by the DPO.

Tilburg University has an established policy on Responsible Disclosure. It also guarantees to reporters of potential vulnerabilities in the information systems that, subject to certain conditions, Tilburg University will not take legal action against them.

Tilburg University has appointed Security Site Contacts (SSCs) for SURF. Staff who are assigned this role (in addition to their normal work) are security representatives, as it were, on behalf of Tilburg University. This is particularly important when the SURF CERT or the police contact Tilburg University in connection with an incident, as these contacts always take place via the appointed SSCs.

## 10. Determination and amendment

The EB lays down the IS policy, which follows the frameworks laid down in university policy and is evaluated, and if necessary revised, at least once every two years. It is also reviewed by the CISO and



laid down again by the EB after any substantial change in university policy or any important developments in the area of cyber security.

The present policy, version 1.02, was laid down by the Executive Board of Tilburg University on <datum> and may be cited as the 'Tilburg University Information Security Policy'.



## Appendix A – Schematic Overview of the ISMS Setup

Information security is an ongoing process. First it needs to be ascertained what is needed, then measures need to be taken. These measures are set out in an annual plan. They may change, since threats and risks change, and legislation and regulations are also subject to change. Checks may then result in a need to revise the measures. Additionally, the overall package of requirements, measures and checks may be in need of review and will therefore need to be evaluated periodically. The entire information security process thus follows a Plan-Do-Check-Act (PDCA) cycle (see the figure). The complete set of measures, processes and procedures is laid down in an Information Security Management System (ISMS), thus providing support when following the PDCA cycle.



By reiterating the PDCA cycle, the organization constantly works to improve the ISMS and thus be more in control.

### Preparation

The preparatory stage involves the following:


- Understanding the organizational context: the external and internal environment.
- Understanding the needs and expectations of stakeholders.
- A good description of the scope of the ISMS: what it does and does not include.
- Leadership and commitment, without which an organization's information security cannot be taken seriously.

The ISMS then needs to be drawn up.


The phases in the PDCA are as follows:

|   |   |
|---|---|
| <p><b>Plan</b></p> <p>The following are defined during the Plan phase:</p> <ul style="list-style-type: none"> <li>• Policy</li> <li>• Scope</li> <li>• Assets</li> <li>• Risks and opportunities</li> <li>• Resources</li> <li>• Competences</li> <li>• Awareness</li> <li>• Communication</li> <li>• Documented information</li> </ul> | <p><b>Do</b></p> <p>Implementing the ISMS involves the following:</p> <ul style="list-style-type: none"> <li>• Operational planning and control</li> <li>• Risk assessment(s)</li> <li>• Risk handling</li> </ul> |
| <p><b>Check</b></p> <p>The Check phase involves evaluating the operation of the ISMS:</p> <ul style="list-style-type: none"> <li>• Monitoring, measuring, analysis and evaluation</li> <li>• Reporting</li> <li>• Internal audit</li> <li>• Management review</li> </ul>  | <p><b>Act</b></p> <p>Improvements are implemented based on the results of the Check phase.</p> <p>A new PDCA cycle then begins.</p>   |


## Appendix B – Information Security Principles


|  |  |
|--|--|
| <p style="font-size: 48pt; font-weight: bold; text-align: center;">1</p> | <p><b>Risk-based</b><br/>Information security is risk-based.</p>    |
| <p>Core</p>  | <p>We base the measures on the potential security risks of our information, processes and IT facilities (in the broadest sense).</p>   |
| <p>Background</p>  | <p>Sharing knowledge (openness) is an important core value of Tilburg University's teaching and research process. If we are to make a good risk assessment as regards protecting information and taking the right measures, we need to establish the value of information. Once that value is known, the right degree of security can be determined, i.e. one that is appropriate to the risks and our 'risk appetite'. It also needs to be proportionate (fit for purpose), so as to make efficient use of the financial resources available.</p>   |
| <p>Implications</p>  | <ul style="list-style-type: none"> <li>• Tilburg University carries out an AIC classification of all processes and/or applications.</li> <li>• The risks are estimated and determined based on a risk classification (see Appendix C).</li> <li>• Tilburg University lays down a Classification Guideline.</li> <li>• The risk analysis includes a data protection impact assessment (DPIA) under the GDPR where necessary, as the supplementary questions in the Classification Guideline show.</li> <li>• Measures supplementary to the Baseline measures are taken where necessary to bring the risks identified to Availability, Integrity and Confidentiality down to the accepted level.</li> <li>• Any information at Tilburg University has a single owner.</li> <li>• Owners of information, information systems, applications and processes are responsible for the implementation and operational enforcement of measures, under the 'comply or explain' principle.</li> <li>• Deviations from this rule may be accepted within Tilburg University's risk appetite, as ultimately decided by the EB.</li> <li>• 'Risk acceptances' (including reasons) are logged in a central risk register.</li> <li>• The risk acceptance process is followed in the case of deviations, with acceptance by the information, process or application owner.</li> <li>• The information owner (or process or application owner, if appropriate) signs to confirm acceptance of the risks.</li> <li>• Measures are designed in such a way that their effects are verifiable.</li> <li>• The highest risks are mitigated first.</li> <li>• It may be decided, based on the risk analysis, to opt for convenience over information security.</li> </ul> |

|  |   |
|--|---|
|  | <ul style="list-style-type: none"> <li>• There must be a good balance between measures (in terms of cost) and risk reduction (the principle of proportionality).</li> <li>• Any information has a single source, making ownership and a single point of truth clear. This creates an additional chain of responsibility for the consequences of changes at source.</li> <li>• Tilburg University remains responsible for the proper protection of information, even when external information processing services are used.</li> <li>• Where applicable, contracts include the security requirements and the requirement of external scrutiny (assurance) to show that measures are effective.</li> <li>• Software and services must comply with a range of security requirements and standards, for which Tilburg University uses the STITCH and the SURF Framework of Legal Standards.</li> </ul> |
|--|---|

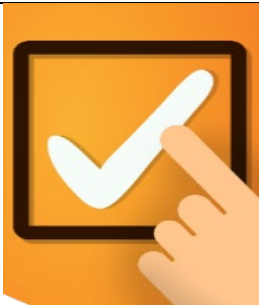
|  |  |
|--|--|
| <h1 style="font-size: 48px; margin: 0;">2</h1> | <p><b>Everyone</b><br/>         Information security is the responsibility of everyone (all staff, students, guests, visitors and external partners of Tilburg University).</p>    |
| Core   | Everyone is and feels responsible for the correct, safe use of resources and powers.   |
| Background                                     | Everyone is aware of the value of information and acts accordingly. The value is determined by the potential harm that could be caused by loss of availability, integrity or confidentiality. Staff, students and third parties are all expected to handle information – in any form – consciously, and to contribute actively to the safety of the computerized systems and the information stored in them. The success of security stands or falls with good communication. Good communication is therefore actively promoted, at and between all levels of the Tilburg University.  |
| Implications                                   | <ul style="list-style-type: none"> <li>• Handling information and data media safely is a requirement in the employment contracts of all staff when they are appointed.</li> <li>• Tilburg University organizes an annual security awareness program.</li> <li>• All staff are required to take the Safe Working training course.</li> <li>• Attention is paid to information security when staff take up their posts and in their annual performance appraisals.</li> <li>• Attention is paid to information security at regular departmental and project meetings.</li> <li>• Staff and students must tackle one another about any unsafe handling of information and systems.</li> <li>• Staff and students must report actual or suspected vulnerabilities to the CERT (involving IT Support if necessary).</li> <li>• There is an established policy on Responsible Disclosure.</li> </ul> |

|  |   |
|--|---|
|  | <ul style="list-style-type: none"> <li>Any violation of legislation, requirements or rules on information security may result in sanctions, imposed by or on behalf of the EB, as laid down in the codes of conduct.</li> </ul> |
|--|---|

|              |  |
|--------------|--|
| <h1>3</h1>   | <p><b>At all times</b><br/>Information security is an ongoing process.</p>    |
| Core         | Information security is in the DNA of all the work we do.  |
| Background   | The environment is constantly changing: cyber threats increase and decrease, processes change, there are changes in staff and students, and so on. It is not sufficient, therefore, to decide on and implement measures only once if we are to keep the climate safe. Information security is only worthwhile if it is an ongoing process of taking measures, creating awareness and carrying out checks. For example patch management.  |
| Implications | <ul style="list-style-type: none"> <li>There is an Information Security Management System (ISMS, see Appendix A) in place under which all aspects of the IS policy are properly monitored in a PDCA cycle.</li> <li>Periodic audits and assessments are carried out, enabling the effectiveness of the policy and the measures taken to be checked (verifiability).</li> <li>On the entry of new staff and students, attention is paid to awareness of risks and Tilburg University's security procedures regarding access to and use of IT resources.</li> <li>High-privilege accounts are validated periodically.</li> <li>Tilburg University regularly organizes cyber security awareness activities for the various target groups: students, staff, managers and partners of Tilburg University.</li> <li>If a person's roles, duties or responsibilities change, his/her authorizations are changed accordingly.</li> <li>A process is being set up to determine the threat to Tilburg University and revise it periodically. Any new threats will result in changes to measures.</li> <li>A patch management process is in place.</li> </ul> |

|            |  |
|------------|--|
| <h1>4</h1> | <p><b>Security by Design</b><br/>Integrated approach to information security</p>  |
| Core       | From the outset, information security is an integral part of every project or  |

|              |   |
|--------------|---|
|              | change relating to information, processes and IT facilities.  |
| Background   | Security by Design means that, right from the start of a project, data security and process continuity are taken into account in the design of any new application or ICT environment and when any technical or functional changes are made. This avoids remedial work after the event, which can often be expensive.   |
| Implications | <ul style="list-style-type: none"> <li>• Tilburg University has adopted Security by Design as an architectural principle.</li> <li>• The security requirements and the STITCH (non-functional requirements) for each new project/software/service purchase/innovation are considered from the outset.</li> <li>• The application of the security requirements is scrutinized and/or tested before going live.</li> <li>• In order to promote information security, the principle of ‘least privilege’ is applied to every IT system or setup, i.e. no more rights are granted than strictly necessary for people to do their jobs and exercise their professions properly.</li> <li>• Access to systems is based on authorization schedules.</li> <li>• Responsibilities are separated in processes and procedures.</li> <li>• The design includes ensuring that the use of information and IT facilities can always be traced back to a responsible user.</li> <li>• A Security in Projects guideline (information safety protocol) has been laid down, based on the measures resulting from the risk classification and measures that could arise from the data protection impact assessment (DPIA) under the GDPR.</li> <li>• Measures to adequately guarantee process continuity are included in the process design.</li> </ul> |

|              |  |
|--------------|--|
| 5            | <p><b>Security by Default</b><br/>Limited access by default and safe settings</p>   |
| Core         | Users only have access to the information and IT facilities that they need for their work. Making information available is a conscious choice.   |
| Background   | Security by Default means that the security options available are enabled by default in any configuration that is implemented. This prevents undesirable and uncontrolled access to personal and other data. Making information available and configuring the settings is thus always a conscious choice, following careful consideration.   |
| Implications | <ul style="list-style-type: none"> <li>• The Security Baseline for the standard configuration is laid down (e.g. all external communication using TLS technology is protected by default).</li> <li>• The principle when initially setting up an information system or infrastructure is ‘closed unless ...’.</li> <li>• Any deviation from the initial setup must follow the ‘comply or explain’ principle.</li> <li>• Security is assured in a change management process.</li> </ul> |

- |  |  |
|--|--|
|  | <ul style="list-style-type: none"><li>• Access to information is role-based, so that users only have access to the information and IT facilities that they need for their work (as laid down in an authorization schedule).</li><li>• A small number of main roles are identified on the basis of which Baseline authorizations are granted, for example student, staff member or supplier. Users are only assigned these roles by default.</li><li>• Logging and audit processes are organized in such a way that access to information and IT facilities can be traced back to a responsible user.</li></ul> |
|--|--|

## Appendix C – The AIC Classification

### The AIC classification

The AIC classification (Availability, Integrity and Confidentiality) of information or information systems provides an estimate of the sensitivity and importance of information, enabling the right degree of security to be selected. Not all information is equally confidential or needs to be available again quickly following an incident. It would not be efficient or user-friendly, for example, to protect non-confidential information in the same way as confidential information.

Tilburg University's information systems (or processes) are classified in terms of AIC. This classification is carried out by the process and/or system owner (first line). The Information Security Team (second line) gives advice, and Internal Audit (third line) ensures that the process takes place as agreed. The classification involves:

1. Classification of the data contained in the information system;
2. Assessment of the risks;
3. The security measures required;
4. The interrelations between 1, 2 and 3.

| Aspect          | Low | Medium | High |
|-----------------|-----|--------|------|
| Availability    | A=1 | A=2    | A=3  |
| Integrity       | I=1 | I=2    | I=3  |
| Confidentiality | C=1 | C=2    | C=3  |

*AIC Classification Table*

How an information system or process rates in terms of Availability, Integrity and Confidentiality – low, medium or high – is shown by an AIC classification. If the AIC classification of an information system or process is higher than the classification in the Information Security Baseline (the standard set of security measures that are always in place), the Baseline measures will not be sufficient and additional measures will be needed to mitigate the risk. These required measures and/or recommendations are predefined in a table of additional measures.<sup>10</sup>

<sup>10</sup> The additional measures are incorporated in a separate document.



## Appendix D – Legislation and Regulations

This appendix provides an overview of the most important legislation and regulations relating to information safety, with key points specifically for Tilburg University.

1. **Higher Education and Research Act** [Wet op het Hoger onderwijs en Wetenschappelijk onderzoek]  
Tilburg University has a quality assurance system in line with the quality assurance institutional assessment (Instellingstoets Kwaliteitszorg). This guarantees inter alia the careful handling of data in the student records system and course results. Research integrity codes are also applied and complied with.
2. **General Data Protection Regulation (GDPR)**  
The University has laid down a separate data protection policy that assures compliance with the GDPR. Compliance with both information security and data protection policy, including the technical and organizational measures therein, ensures that the GDPR is complied with.
3. **Statutory retention periods/Public Records Act**  
Tilburg University observes the statutory requirements regarding retention periods as laid down in specific legislation (e.g. tax law and labor law) and in the Public Records Act [Archiefwet] and Public Records Decree [Archiefbesluit]. Tilburg University applies the Basic Selection Document for University Education [Basisselectiedocument Wetenschappelijk Onderwijs] (1985)<sup>11</sup> for the universities and universities of applied sciences sector. It relates to all information, e.g. as recorded in digitized documents, information systems, websites and email. This is included in the annual external auditor's reports.
4. **Copyright Act [Auteurswet]**  
Tilburg University respects copyrights and acts accordingly.
5. **Telecommunications Act**  
As Tilburg University's target group is adequately defined, the university's network facilities are not regarded as a public network within the meaning of the Telecommunications Act [Telecommunicatiewet], apart from a few student accommodation services, for which procedures in line with the Network Neutrality Act [Wet Netneutraliteit] are in place.
6. **Computer Crime Act III**  
The Computer Crime Act [Wet Computercriminaliteit] is concerned with the criminal problem areas in relation to computer use. It consists of sections that have been added to various parts of the Criminal Code. The additional sections are concerned with:
  - criminal damage and rendering unusable
  - data interception
  - denial of service
  - computer hacking
  - the use of services without payment
  - malware

Compliance with this Information Security Policy, in particular the security measures and the expected behavior, ensures that Tilburg University has an appropriate basic level of security against these threats.

---

<sup>11</sup> Reference VH-document/reference VSNU-document.



If attacks take place on Tilburg University that significantly breach security and are covered by the Computer Crime Act, Tilburg University will always report them to the police.

7. **Other codes and national agreements**

Tilburg University's information security policy is based on the SURF Framework of Standards, and the university is a member of the Association of Universities in the Netherlands (VSNU).<sup>12</sup> 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
- Framework of Legal Standards for Higher Education
- Basic Selection Document for universities/UMCs
- SURF membership requirements
- ISTLP (Information Sharing Traffic Light Protocol)

---

<sup>12</sup> Association of Universities in the Netherlands [Vereniging Samenwerkende Nederlandse Universiteiten]/Netherlands Association of Universities of Applied Sciences [Vereniging van Hogescholen].

## Appendix E – The RASCI Matrix

| Task                        | Deliverable   | Accountable <sup>13</sup> | Responsible <sup>14</sup> | Supportive <sup>15</sup> | Consulted <sup>16</sup>           | Informed <sup>17</sup>  |
|-----------------------------|---|---------------------------|---------------------------|--------------------------|-----------------------------------|---|
| Information Security Policy | IS Policy   | EB                        | CISO                      | Information manager(s)   | ISO<br>ITSO<br>GRCO<br>CPO<br>DPO | Director of LIS<br>IT Manager<br>PIM Manager<br>Directors' meeting<br>Process owner         |
| IS Policies                 | Misc. IS Policies<br>(e.g. data classification,<br>backups, etc.) | EB                        | Director<br>Dean          | Information manager(s)   | CISO<br>ISO<br>ITSO               | Director of LIS<br>PIM Manager<br>GRCO<br>Directors' meeting<br>DPO<br>CPO<br>Process owner |

<sup>13</sup> **Accountable:** The person who bears ultimate responsibility, is authorized and approves the results. He/she must if necessary be able to make a final judgment and have a right of veto. Only one person is Accountable.

<sup>14</sup> **Responsible:** The person who is responsible for implementation. He/she reports to the person who is Accountable.

<sup>15</sup> **Supportive:** This person supports the results. He/she helps and may (but need not) be consulted.

<sup>16</sup> **Consulted:** This person helps to guide results, he/she is required to be consulted prior to decisions or actions. This communication is bidirectional.

<sup>17</sup> **Informed:** A person who is informed of decisions, progress, results achieved, etc. This communication is unidirectional.

|                     |               |                 |      |                        |                     |   |
|---------------------|---------------|-----------------|------|------------------------|---------------------|---|
| IS Governance       | IS Governance | Director of LIS | CISO |                        | GRCO<br>ISO<br>ITSO | Directors' meeting<br>DPO<br>CPO<br>Process owner |
| Setting IS Baseline | IS Baseline   | EB              | CISO | Information manager(s) | GRCO<br>ISO<br>ITSO | Directors' meeting<br>DPO<br>CPO<br>Process owner |

| Task   | Deliverable  | Accountable <sup>15</sup> | Responsible <sup>16</sup> | Supportive <sup>17</sup>  | Consulted <sup>18</sup> | Informed <sup>19</sup>        |
|--|--|---------------------------|---------------------------|---|-------------------------|-------------------------------|
| Carrying out BIA                               | BIA for each information system  | Process owner             | Process owner             | Information manager(s)<br>Project manager(s)<br>Functional manager(s) | ISO<br>GRCO             | Director of LIS               |
| Carrying out DRA                               | In-depth risk analysis for each system that rates higher than the Baseline | Process owner             | CISO                      | Information manager(s)<br>Project manager(s)<br>Functional manager(s) | ISO<br>ITSO<br>GRCO     | Director of LIS               |
| Doing the STITCH                               | STITCH reporting   | Process owner             | ITSO                      | Information manager(s)<br>Project manager(s)<br>Functional manager(s) |                         | Director of LIS               |
| Carrying out technical security investigations | Technical advice   | CISO                      | ITSO                      |   | Technical manager(s)    | Director of LIS<br>IT Manager |

| Task   | Deliverable                   | Accountable <sup>15</sup> | Responsible <sup>16</sup> | Supportive <sup>17</sup> | Consulted <sup>18</sup> | Informed <sup>19</sup>                   |
|--|-------------------------------|---------------------------|---------------------------|--------------------------|-------------------------|--|
| Advising on information security (on request or on own initiative) | Advice                        | CISO                      | ISO<br>ITSO               | Information manager(s)   | -                       | Director of LIS<br>GRCO<br>Process owner |
| CERT incident handling   | Incident handled and recorded | ITSO                      | CERT                      | Process owner            | -                       | Director of LIS<br>GRCO<br>CISO          |

| Task   | Deliverable                        | Accountable <sup>15</sup> | Responsible <sup>16</sup> | Supportive <sup>17</sup>          | Consulted <sup>18</sup> | Informed <sup>19</sup>                           |
|--|------------------------------------|---------------------------|---------------------------|-----------------------------------|-------------------------|--|
| Reporting incidents  | Reported data leak/incident        | All staff                 | All staff                 | CERT<br>Data Representative       | DPO                     | Director of LIS<br>GRCO<br>CISO<br>Process owner |
| Reporting data leak to the Dutch Data Protection Authority | Data leak report                   | DPO                       | DPO                       | CISO<br>ISO<br>ITSO               | Data leak reporter      | Director of LIS<br>GRCO<br>CISO<br>Process owner |
| Organizing awareness training courses                      | Awareness training course/campaign | CISO<br>DPO               | ISO<br>ITSO<br>CPO<br>SWO | Marketing and Communication<br>HR |                         | Director of LIS<br>GRCO                          |

|   |                      |      |   |   |             |                                  |
|---|----------------------|------|---|---|-------------|----------------------------------|
| Monitoring- checks on compliance with IS policy | Compliance reporting | CISO | Process owner<br>IT Manager<br>Director of LIS<br>Directors | Information manager(s)<br>Project manager(s)<br>Functional manager(s) | ISO<br>ITSO | EB<br>Directors' meeting<br>GRCO |
|---|----------------------|------|---|---|-------------|----------------------------------|

## Appendix F – Information Security Roles

| Roles in information security policy  |
|---|
| The Executive Board   |
| Business Continuity Manager (BCM)   |
| Central Privacy Officer (CPO)   |
| Chair of CERT (part of the ITSO role)   |
| Chief Information Security Officer (CISO)   |
| Contract Manager  |
| Data Representative   |
| Data Protection Officer (DPO)   |
| Governance Risk and Compliance Officer (GRCO)   |
| Head of Internal Audit  |
| Incident Response Handler (IRH)   |
| Information Architect   |
| Information Manager   |
| Information Security Officer (ISO)  |
| Risk Consultant   |
| IT Security Officer (ITSO)  |
| Safe Working Officer (SWO)  |
| Information Security Portfolio Manager  |
| Most important process owners   |
| Most important system owners  |
| Deans/Directors <ul style="list-style-type: none"> <li>- Director of Academic Services</li> <li>- Director of Executive Services</li> <li>- Director of Facility Services</li> <li>- Director of Marketing and Communication</li> <li>- Director of Library and IT Services</li> <li>- Director of Finance and Control</li> <li>- Director of Human Resources</li> <br/> <li>- Director of Tilburg School of Social and Behavioral Sciences (TSB)</li> <li>- Dean of TSB</li> <br/> <li>- Director of Tilburg School of Humanities and Digital Sciences (TSHD)</li> <li>- Dean of TSHD</li> <br/> <li>- Director of Tilburg Law School (TLS)</li> <li>- Dean of TLS</li> <br/> <li>- Director of Tilburg School of Economics and Management (TiSEM)</li> <li>- Dean of TiSEM</li> <br/> <li>- Director of Tilburg School of Catholic Theology (TST)</li> <li>- Dean of TST</li> </ul> |

## Appendix H – The CERT Setup

The aim of the Computer Security Emergency Response Team (CERT) is to prevent information security incidents occurring and deal with those that do occur. The goal is to support the continuity of Tilburg University and protect its reputation. The CERT also deals with security incidents outside Tilburg University in which its staff are involved in any role. In such cases, use is made if possible of the services of the SURF CERT, which is in contact with other CERTs throughout the world.

The members of the CERT are nominated by the chair of the CERT and appointed by the CISO, on whose instructions they operate.

The chair of the CERT draws up a Charter setting out the target group, remit, powers, escalations, modus operandi (including the handling of confidentiality) and composition. This lays down inter alia that the CERT works for Tilburg University as a whole and takes its remit directly from the EB/CISO. Direct escalations via the chair of the CERT to administrative level (via the CISO) are also laid down. It also sets out the direct contacts with the departments/persons at Tilburg University responsible for handling legal issues and contacts with the press.

The ITSO (CERT) gives advice if Tilburg University computer systems or network segments need to be isolated. Here the CISO acts as the linking pin with the Director of LIS and the process/system owner.

Incident management and recording relate to how staff, students and third parties report information security breaches and how they are dealt with. We can learn from incidents. Incident recording and periodic reporting of incidents that have occurred are thus part and parcel of a mature information security environment. Incidents at Tilburg University can be reported to the CERT desk.

Tilburg University has clearly communicated the contact details for the CERT desk to its staff, students and third parties.

Every staff member, student and third party is responsible for spotting and reporting incidents and information security breaches, including data leaks. Incidents and breaches must be reported directly to the CERT desk. Data leaks must be reported to the DPO at [datalek@tilburguniversity.edu](mailto:datalek@tilburguniversity.edu).

There is an established policy on Responsible Disclosure. In this way Tilburg University guarantees to potential reporters of security gaps in the information systems that, subject to certain conditions, the university will not take legal action against them.

Incidents are discussed at the appropriate operational meeting so that they can be dealt with correctly. If Tilburg University's business process, funding or reputation is jeopardized, the incident will also be discussed with the CISO, taking into account whether it needs to be dealt with confidentially at that time. If trends are identified that are cause for concern, Tilburg University's CERT will respond proactively by taking additional measures or raising awareness in the organization.