

# Information Security Policy

UM

2020



Version 3.0, November 2020

## Colophon

### *Information Security Policy UM Version 3.0 (2020)*

Replaces Information Security Policy UM version 2.1

Author: Bart van den Heuvel, CISO, CIOffice

Adopted by the Executive Board of Maastricht University on: 17 November 2020

Approved by the University Council on: 22 September 2021

Approved by Local Consultative Body on: 30 June 2021

Maastricht University's information security policy is based on the Model Information Security Policy created by the SURF Community for Information Security and Privacy (SCIPR), version 3.0, March 2020.

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



## Table of Contents

<b>Summary .....</b>	<b>3</b>
<b>1. Introduction .....</b>	<b>4</b>
<b>2. Legislation and regulations .....</b>	<b>4</b>
<b>3. Definition, objective, target group and scope.....</b>	<b>5</b>
3.1. Information Safety and Information Security .....	5
3.2. Objective, conditions and starting points.....	5
3.3. Target group .....	6
3.4. Policy scope .....	6
<b>4. Information security policy principles .....</b>	<b>7</b>
4.1. Introduction .....	7
4.2. Policy principles.....	8
<b>5. Information security policy governance .....</b>	<b>10</b>
5.1. Alignment with associated risks .....	10
5.2. Roles and their integration into IS governance .....	11
5.2.1 First and second line.....	11
5.2.2 Third line.....	11
5.2.3 Final responsibility.....	12
5.2.4 Duties, powers, responsibilities .....	12
5.3. Awareness and training .....	14
5.4. Monitoring, practice, compliance and sanctions .....	14
5.5. Financing.....	15
<b>6. Incident reporting and handling .....</b>	<b>16</b>
<b>7. Adoption &amp; Amendment .....</b>	<b>16</b>
<b>Annexe A – Designing an ISMS .....</b>	<b>17</b>
<b>Annexe B – Information security principles .....</b>	<b>18</b>
<b>Annexe C – Risk appetite and Classification .....</b>	<b>22</b>
<b>Annexe D – Legislation and regulations .....</b>	<b>25</b>
<b>Annexe E – Roles in IS governance .....</b>	<b>27</b>
<b>Annexe F – Information security documents .....</b>	<b>30</b>

## Summary

The success of an organisation such as UM increasingly depends on information, new technologies and computer systems. Such information must be properly secured, especially if personal data is stored. This document describes how UM provides adequate information security to comply with the relevant legislation and regulations.

With the information security policy (IS policy), UM also aims to contribute to a better quality of information provision and ensure a good balance between functionality, security and privacy.

The policy describes to whom, to which parts of the institution, and which devices and applications it applies. Information security affects all layers of the organisation. In addition to the scope of the policy, the responsibilities of the officers involved are described. Line management is responsible for its own processes, while the directors ensure that security measures are implemented. The final responsibility lies with the Executive Board.

There are five guiding policy principles:

1. *Risk based*  
The measures are based on the potential security risks of our information, processes and IT facilities.
2. *Everyone*  
Everyone is and feels responsible for the correct and safe use of resources and powers.
3. *Always*  
Information security is at the core of all our work.
4. *Security by Design*  
From the start, information security is an integral part of every project or any change regarding information, processes and IT facilities.
5. *Security by Default*  
Users only have access to the information and IT facilities they need for their work. Providing information is a conscious choice.

Policies and measures are insufficient to rule out information security risks. The human element is the greatest risk. At UM, we are constantly working to increase our employees' security awareness to increase knowledge of risks and encourage safe and responsible behaviour.

Information security is a continuous process, in which we are always looking for ways to improve. We do this using annual plans (CISO<sup>1</sup>), audits (UM-SOC<sup>2</sup> and the IT auditor) and adjustments: Plan, Do, Check, Act. In addition to Security Officers, the Data Protection Officer, Internal Audit and the Quality & Risk Board offer advice, particularly with regard to achieving a good cost-benefit balance (risk appetite).

The annexes discuss the management cycle for periodic adjustment, including the relevant information security documents. The five information security policy principles are fully elaborated in the annexe. There is also an overview of the most important laws and regulations concerning information security, and a clarification of the roles of the officials involved.

## 1. Introduction

UM's success increasingly depends on information, new technologies and computer systems. We have

---

<sup>1</sup> CISO: Corporate (Chief) Information Security Officer

<sup>2</sup> UM-SOC stands for UM "Security Operations Center", located within ICTS and coordinated by the CISO

become dependent on digitally collecting, capturing and sharing information with internal and external partners, colleagues and students.

The digital reality is constantly changing, bringing with it new and different Information Security risks<sup>3</sup>. The risks pose a threat to the quality and continuity of processes and the achievement of strategic objectives. Threats can impact the availability, integrity and confidentiality of information. Examples of threats are system vulnerabilities or unauthorised access to information, which can undermine the value of a UM degree, marks obtained or the legitimacy of research conclusions.

Students, staff and guests' privacy<sup>4</sup> and UM's reputation may also be harmed. As such, information security is crucial.

"Protect and Comply" is one of the three pillars of UM's I-Strategy adopted in 2018.

Information security always requires adjustment to maintain an appropriate level of security. This is partly due to technological developments, stricter requirements for compliance with data protection and privacy legislation and regulations (GDPR), and agreements with research and educational partners.

Reducing and managing risks requires efforts on an organisational, process and technological level. UM directors, students and guests must also become aware of the risks and adapt their actions accordingly.

Information security cannot be achieved by simply adopting a number of technical and organisational measures. The ever-changing world makes it a dynamic process. For that reason, this document sets out five main principles for information security within UM. The measures, procedures, and guidelines to be adopted can be benchmarked against the five main principles described in Chapter 4.

There is an important relationship between information security risks and risks in other areas, such as privacy, safety<sup>5</sup> (occupational health and safety legislation), security in education and research, physical security and business continuity. There may be a partial overlap in some cases.

## 2. Legislation and regulations

UM endeavours to comply with the relevant legislation and regulations in all its processes and procedures, adhering to the 'Comply or Explain' principle in doing so, which enables it to always justify why it does or does not comply. Annex D provides an overview of the relevant legislation and regulations

---

<sup>3</sup> See the explanation in section 3.1 on differences in the definitions of 'information safety' and 'information security'

<sup>4</sup> For UM's specific privacy policy, see <https://www.maastrichtuniversity.nl/privacy>

<sup>5</sup> *Safety* is used as a collective term for the various aspects of personal safety: Occupational health and safety and the environment, social safety, company emergency services, etc.

## 3. Definition, objective, target group and scope

### 3.1. Information Safety and Information Security

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. To this end, information and information systems must be protected against potential threats by taking, maintaining and monitoring security measures, also known as information security.

Everyone is responsible for information safety at UM. The final responsibility lies with the UM Executive Board.

### 3.2. Objective, conditions and starting points

Information security has the following objectives:

- ensuring the availability of information within education, research and business operations;
- ensuring that information is correct, complete and up to date (integrity), and only accessible to those whose role or position gives them access (availability, integrity and confidentiality);
- preventing security and privacy incidents and reducing their possible consequences.

With the information security policy (IS policy), UM aims to contribute to a better quality of information provision and ensure a good balance between functionality, security and privacy, and the associated costs. As such, the IS policy is in line with the institution's mission.

UM's ambition is to achieve and maintain a high level of information security systemically. It does so by describing responsibilities, duties and powers and laws and regulations. The IS policy—and adhering to it—must enable UM to achieve its ambition and remain in control and compliant. Based on that, the deans and directors involved, together with the Executive Board, can report to the Supervisory Board. The implementation of the policy is also the foundation for compliance with legal requirements.

#### **preconditions**

The following preconditions are important for UM to achieve its objectives:

- *Organisation of security*  
The responsibilities, duties and powers of the information security position are explicitly laid down and supported by the Board, and in turn, by the entire institution.
- *Process approach*  
Information security is a continuous process. 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 the security measures will be reviewed periodically.

#### **Starting points**

The objective and conditions result in the following starting points:

- *Framework*  
The policy provides a framework for benchmarking current and future information security measures against the established security principles (chapter 4), best practices and standards. It also provides a framework with which the duties, powers and responsibilities within the institution can be assigned.

- *Standards*

The “SURF Standards Framework for Information Security in Higher Education” (IBHO) has been drafted specifically for the SURF community<sup>6</sup>. The IBHO is based on the standards laid down in the ISO 27000 series. Together with this policy document, the IBHO forms the basis for UM’s information security management system (ISMS<sup>7</sup>, see annexe A). The ISMS has been designed according to the international ISO 27001 standard. UM does not consider formal certification (e.g., according to the ISO 27001 standard) to be necessary. Nevertheless, UM endeavours to obtain formal certification for specific parts of the information provision process to demonstrate the quality of those parts<sup>8</sup>.

- *Maturity*

IBHO defines a standard for the maturity of information security according to the Capability Maturity Model (CMM)<sup>9</sup>. UM aims for a level of maturity in accordance with the SURF guidelines.

- *Measures*

UM’s measures are based on the international ISO 27002 standard. The “SURF Baseline Information Security Higher Education” and other best practices in the SURF community are used as a starting point. UM-specific measures are outlined at <https://www.maastrichtuniversity.nl/informationsecurity>.

### 3.3. Target group

The IS policy is intended for all internal or external parties involved with UM’s business processes. It focuses primarily on the board and senior management (process owners), the security organisation and the executives. They convey the policy to all employees, lecturers, students, administrators, guests, visitors and external relations.

### 3.4. Policy scope

Information security is interpreted broadly at UM. It is about dealing with all forms of formally recorded information (i.e., not just digital information), which the institution or its business relations generate and manage, either in UM systems or in externally managed systems (outsourcing). The policy also relates to non-formally recorded information—such as statements made by students and employees in discussions, on web pages and personal websites—which UM can be held accountable for.

The IS policy applies to all institution departments and services. It concerns all UM-managed devices and applications that provide authorised access to the UM network and its services, or are used to process data from the institution.

Devices and applications include:

- all devices physically connected to the network such as servers, workstations, laptops, building management systems and communication systems;
- all wirelessly connected mobile devices such as notebooks, tablets, smartphones and smart-watches;
- IoT<sup>10</sup> devices such as surveillance cameras and sensors.
- All web/cloud services and applications (“apps”) available on these devices.

---

<sup>6</sup> The current documents can be found at <https://www.surf.nl/informatiebeveiliging> and <https://www.surf.nl/surfaudit-inzicht-in-je-informatiebeveiliging-en-privacy>. Supporting wikis are available for members of the SCIPR community: <https://wiki.surfnet.nl/display/SCIPR/SCIPR+Home> and <https://wiki.surfnet.nl/display/SA/SURFaudit+Home>

<sup>7</sup> ISMS: Information Security Management System.

<sup>8</sup> This could be an ISO 27001 certificate for storage facilities for research purposes, for example.

<sup>9</sup> [https://nl.wikipedia.org/wiki/Capability\\_Maturity\\_Model](https://nl.wikipedia.org/wiki/Capability_Maturity_Model)

<sup>10</sup> Internet of Things

UM facilitates the use of personal devices (BYOD<sup>11</sup>) by students, guests and, to a limited extent, employees. This IS policy covers the use of BYOD on the UM network to access the institution's applications or information.

The policy is location and equipment independent: it remains applicable if people work with UM information or information facilities at a location other than on UM's premises (e.g., at home, on the train or at another educational institution) or with non UM-managed equipment (such as a home-computer or BYOD).

## 4. Information security policy principles

### 4.1. Introduction

UM is an institution with an open nature. From an educational and research perspective, our approach is *"Open where possible, closed where necessary"*. This also fits in with the FAIR<sup>12</sup> objectives in the research domain. Adequate security of information is always a prerequisite, and making information available must be a conscious choice.

UM has established five policy principles for information security, which help to determine the security measures needed. A policy principle consists of:

- a title (often explanatory);
- a brief explanation (background);
- the implications resulting from the policy principle as a basis for the measures to be taken.

Section 4.2 offers a brief introduction to the five policy principles, while Annexe B provides a detailed elaboration.

The measures ultimately adopted by the institution are not always directly applicable practicable in all situations. For example, there may be deviating processes or technical or organisational limitations. In such cases, replacement measures must be taken that achieve the intention of the underlying principle and sufficiently cover the risks, in accordance with the "Comply or Explain" principle<sup>13</sup>.

Replacement measures must be benchmarked against UM's IS policy to properly assess whether they lead to an acceptable residual risk. This assessment can take place with the policy principles and their implications for information security from this chapter, even if replacement measures are not exhaustively laid down in the policy or baselines.

### 4.2. Policy principles

The five policy principles listed below help with the implementation of the IS policy. Based on these principles, measures can be formulated that are relevant to the protection of UM processes. The policy principles form the basis for communication regarding UM's IS policy.

Many components derived from the IS policy can be benchmarked against the policy principles, including:

- the ISMS (Annexe A);

---

<sup>11</sup> Bring Your Own Device

<sup>12</sup> Findable- Accessible- Interoperable- Reusable (see <https://nl.wikipedia.org/wiki/FAIR-principes>)

<sup>13</sup> "Comply" is about the specific measures; the principles serve as a reference for "explain".





- guidelines for project-based work, work instructions and awareness programmes;
- classification (Annexe C) according to which a risk analysis can be conducted to determine technical and organisational measures.

The policy principles are also intended to serve as a basis for evaluating exceptions or options in unforeseen circumstances.


The five policy principles adopted by UM are:


1. Risk-based;
2. Everyone;
3. Always;
4. Security by Design;
5. Security by Default.

<h1>1</h1>	<p><b>Risk-based</b> Information security is risk-based</p> 
Core	The measures are based on the potential security risks of our information, processes and IT facilities.
Background	Sharing knowledge (openness) is an important core value of UM's teaching and research process. It is important to determine the value of information to properly assess risks when protecting information and taking appropriate measures. If the value of information is known, the right security level can also be determined, which matches the risks. Proportionality is desirable to use the available financial resources efficiently, among other things ("Fit for purpose").
Implications	Examples include setting up a risk management process (classification), establishing responsibilities, safeguarding risks in contracts. See Annexe B for an overview of all implications.

<h1>2</h1>	<p><b>Everyone</b> Information security is everyone's responsibility</p> 
Core	Everyone is and feels responsible for the correct and safe use of resources and powers.
Background	Everyone is aware of the value of information and acts accordingly. The value is determined by the possible damage resulting from loss of availability, integrity or confidentiality. Employees, students and third parties are expected to handle information in any form with care and actively contribute to the security of

	the automated systems and the information stored therein. The success of security depends on good communication. Good communication is actively promoted at and between all levels in the institution.
Implications	Examples include recording agreements in terms and conditions of employment, codes of conduct, house rules, etc. See Annexe B for an overview of all implications.

<h1>3</h1>	<p><b>Always</b> Information security is a continuous process</p> 
Core	Information security is at the core of all our work.
Background	The environment is ever-changing; cyber threats increase and decrease, processes change, employees and students change, etc. Defining and implementing the measures once is not enough to maintain a safe climate; information security only works if it is a continuous process of measures, awareness and checks.
Implications	Examples include holding awareness campaigns, setting up an audit process. See Annexe B for an overview of all implications.

<h1>4</h1>	<p><b>Security by Design</b> An integral approach to information security</p> 
Core	From the start, information security is an integral part of every project or any change regarding information, processes and IT facilities.
Background	Security by design means that at the start of a project, data security and the continuity of processes are considered in the design of a new application or ICT environment and in the event of technical or functional changes, preventing often-expensive repairs later.
Implications	Examples include establishing and testing security requirements in projects and setting up permission schemes. See Annexe B for an overview of all implications.


<h1>5</h1>	<p><b>Security by Default</b> Restricted access and secure settings by default</p> 
Core	Users only have access to the information and IT facilities they need for their work. Providing information is a conscious choice.
Background	Security by default means that every implemented configuration has the available security options turned on by default, preventing unauthorised and uncontrolled access to data. As a result, making information available is always a conscious choice after careful consideration.
Implications	Examples include defining standard roles, limiting permissions by default and protecting all external communications with SSL technology by default. See Annexe B for an overview of all implications.

Table 1: Policy principles

## 5. Information security policy governance

### 5.1. Alignment with associated risks

Governance must take all types of risks and their interrelationships into account. UM focuses heavily on the alignment of information security, occupational safety, physical security, business continuity and privacy protection on a strategic level. Where possible and necessary, that alignment also translates to the tactical and operational levels.

This chapter discusses the governance of information security and information security (hereinafter: IS governance) as part of UM's I governance.

### 5.2. Roles and their integration into IS governance

This section describes how IS governance is organised, who is responsible for what, and who reports to whom. A distinction has been made in the various roles between directing (strategic), steering (tactical) and executive (operational). The responsibilities associated with the various roles are set out in the RASCI table in Annexe E and are safeguarded in the UM's mandate agreement.

The designation of the specific roles for information security is as close to the Platform for Information Security (PvIB) guidelines as possible<sup>14</sup>:

	Information safety (risk management)	Information security (ICT security)
	CISO	CISM

<sup>14</sup> Information security occupational profiles <https://www.pvib.nl/kenniscentrum/documenten/beroepsprofielen-in-formatiebeveiliging-2-0>

Strategic/tactical		(ICT security manager)
Tactical/operational	(L)ISO	(L)ISM (ICT security specialist)

Table 2: Role designation according to PvlB

CISO Corporate (or Chief) Information Security Officer

CISM: Corporate (or Chief) Information Security Officer

Parallel to the IS roles, there are also privacy roles: a Central Privacy Officer (CPO) similar to the CISO and Local Privacy Officers (LPO) at the administrative units. Locally, these roles are usually combined as Information Manager (IM) roles in the administrative units.

UM's IS governance is structured according to the so-called Three Lines of Defence model<sup>15</sup> (3LoD), which is generally applied as a model to safeguard Governance, Risk and Compliance (GRC) in an operational organisation. It describes not only the roles within the organisational structure but also their mutual collaboration.

### 5.2.1 First and second line

The 3LoD model is based on the principle that line management (the business) is responsible for its own processes<sup>16</sup>. The deans and directors ensure that security measures are implemented, awareness programmes are carried out, personnel is trained, etc. This is the first line. In their role as LISO, the information managers in the administrative units serve as the information security contact person within the administrative unit.

There also needs to be a role that supports, advises, coordinates and monitors whether the management fulfils its responsibilities. This is the second line. Second-line tasks include certain policy preparation tasks, organising the PDCA cycle, integral risk analyses and self-assessments, and drawing up annual plans and reports.

### 5.2.2 Third line

There should be a role within the organisation to check whether the interaction between the first and second lines functions smoothly and make an objective, independent judgment about this and identify areas of improvement. This role should also check for overlap and blind spots. This is the third line.

The GDPR-mandated Data Protection Officer (DPO) and the internal IT auditor typically belong to the third line. Both operate completely independently from all other organisational units and report to the Executive Board and the Supervisory Board.

<sup>15</sup> <https://www.icas.com/ca-today-news/internal-audit-three-lines-of-defence-model-explained>

<sup>16</sup> This is in line with UM's integral management model

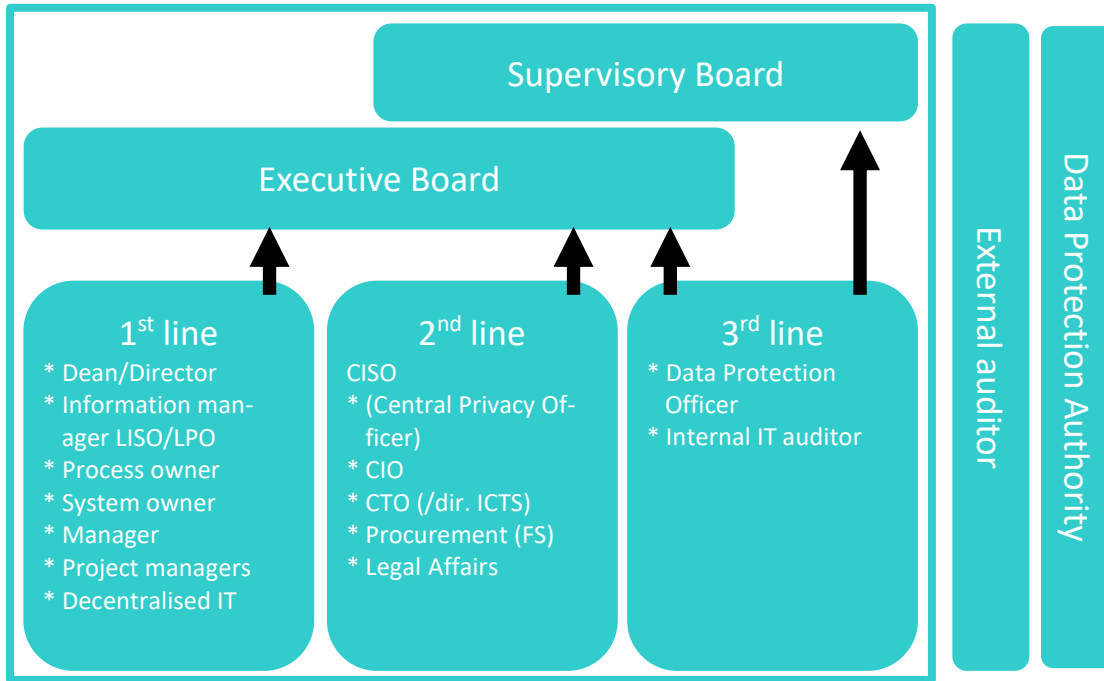


Diagram: Three Lines of Defence translated into Education

Annexe E further describes the various IS governance roles and the 3LoD model. The Supervisory Board, the external auditor and the external supervisors (Data Protection Authority, but also Inspectorate of Education) are not taken into further consideration.

### 5.2.3 Final responsibility

From a legal perspective, the Executive Board is ultimately responsible for information safety and, by extension, the institution's information security. Specific parts of this responsibility are mandated to the deans or directors in the mandate agreement and are more deeply vested within the organisation.

### 5.2.4 Duties, powers, responsibilities

The various duties, powers and responsibilities are subdivided into Strategic, Tactical and Operational levels, characterised by their consultation structure.

Strategic level	Tactical level	Operational level
The Corporate Information Security Officer (CISO) is both a strategic and tactical role. The CISO is responsible for the policy and the ISMS process. The decentralised LISOs translate that policy to their departments.	The role of the Corporate Information Security Manager or CISM is both tactical and operational. The CISM is responsible for translating the strategy and policy into tactical and operational plans together with the CISO and in consultation with the LISOs (for uniformity), the system and process owners and the CPO and LPO.	The operational level is responsible for implementing information security measures and handling incidents in consultation with the functional managers and relevant IT officers and, where necessary, with the tactical layer (the LISOs).

The following table summarises each level's duties, powers, and responsibilities, supplemented by the underlying documents<sup>17</sup>.

<sup>17</sup> Some documents have not yet been produced or administratively adopted at the time of establishing this policy. Because they depend, for example, on the administrative adoption of this policy.

Level	What?	Who?	Consultation	Documents
Directing (strategic)	<ul style="list-style-type: none"> <li>• Determining IS strategy</li> <li>• Establishing IS organisation</li> <li>• Determining IS planning and control</li> <li>• Business continuity management</li> <li>• Communication to management and organisation</li> </ul>	Executive Board (the Information Security portfolio holder) based on advice by CISO, CIO and CTO	Executive Board determines; I Board, Q&R board <sup>18</sup> and CBB advise	<ul style="list-style-type: none"> <li>• IS policy</li> <li>• Privacy policy</li> <li>• Code of Conduct and Integrity</li> <li>• ISMS</li> <li>• Classification guideline</li> </ul>
Steering (tactical)	<p>IS Planning &amp; Control:</p> <ul style="list-style-type: none"> <li>• Preparing testing standards and method</li> <li>• Evaluating policies and measures, including those of contracted external parties</li> <li>• Supervising internal assessments and external audits</li> <li>• Communication to process and system owners and IT support</li> </ul>	<ul style="list-style-type: none"> <li>• Process owners</li> <li>• System owners</li> <li>• CISO</li> <li>• LISO (= Information Manager role)</li> <li>• Central Privacy Officer</li> </ul>	Information Managers Consultation (I4MU)	<ul style="list-style-type: none"> <li>• Classifications/Risk analyses and audits, including DPIAs and SURFaudit</li> <li>• IS baselines (basic measures and elaboration according to CIS-20 framework)</li> <li>• Annual plan and report</li> <li>• Cyber Crisis annexe to Crisis Protocol</li> <li>• Business continuity plan</li> <li>• Responsible Disclosure Procedure</li> </ul>
Executive (operational)	<ul style="list-style-type: none"> <li>• Implementing IS measures.</li> <li>• Registering and evaluating incidents, including data leaks</li> <li>• Communication to end-users</li> <li>• Conducting audits and penetration testing</li> </ul>	<ul style="list-style-type: none"> <li>• IT in collaboration with process and system owners</li> <li>• Functional management</li> <li>• CISM</li> <li>• UM-SOC<sup>19</sup></li> <li>• UM-CERT<sup>20</sup></li> <li>• Local Privacy Officer</li> </ul>	DO-ICT UM-SOC/UM-CERT consultation	<ul style="list-style-type: none"> <li>• SLAs (security paragraph)</li> <li>• Incident registration, including evaluation</li> <li>• UM-CERT Operational Model</li> <li>• UM-SOC Operational Model</li> </ul>

### Consultation

To achieve proper coherence in the organisation of the information security role and coordinate the information security initiatives and activities within the various components, UM holds regular information security consultations at various levels.

Strategic	Tactical	Operational
At the strategic level, governance, risk and compliance, and information security goals, scope and ambition are discussed in con-	At the tactical level, the strategy is translated into plans, measures, standards to be applied, evaluation methods, etc., which guide the execution.	At the operational level, matters are discussed concerning day-to-day operations in the sense of execution and implementation.

<sup>18</sup> Quality & Risk Board

<sup>19</sup> UM-SOC stands for UM "Security Operations Center", located within ICTS and coordinates by the CISO.

<sup>20</sup> UM-CERT stands for UM "Computer Emergency Response Team"

<p>junction with privacy. These discussions are held by the directors, advised by the I Board, the Q&amp;R board and the CISO and aligned with UM's I strategy and risk appetite.</p>	<p>These tactical consultations are held between the CISO, the LISOs, (C)POs and (C)ISMs, in consultation with other relevant officials such as the UM-SOC/UM-CERT coordinator and processor or system owners where necessary.</p>	
---	--	--

All three types of consultation are integrated into existing forms of consultation of the same nature as much as possible. For example, at the strategic level, not only information security and privacy are discussed, but also other risks UM may face, such as financial, personnel and commercial risks. At UM, this means that information security is on the agenda of the Executive Board, CBB, I Board and Q&R board. At the tactical level, consultations with the information managers (I4MU) will also cover the choice of IT functionality and services. The information managers will also serve as the contact point for the decentralised privacy role (LPO). At the operational level, information security is discussed by IT support (DO-ICT), functional administrators and IT managers, as well as in consultations with key users and project teams, and in SCRUM sessions (Agile-Sprints).

#### Documents

UM follows the same PDCA management cycle for information security as for other topics: vision/idea, policy, analysis, plan implementation, execution, checks and evaluation. A number of formally adopted documents support the cycle at various levels. Annex F provides a more detailed overview of the documents UM uses for information security as listed in the table above.

### 5.3. Awareness and training

Policies and measures are insufficient to rule out information security risks. The human element is the greatest risk. At UM, we are constantly working to increase our employees' security awareness to increase knowledge of risks and encourage safe and responsible behaviour. The policy includes frequent awareness campaigns for all employees, students, third parties and, in particular, operational managers. The managers, CISO and LISOs are responsible for raising security awareness, and it is included in the induction programme for new employees and students.

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

At UM, the Internal IT Auditor and CISO are responsible for planning internal IT audits<sup>21</sup> in accordance with the IS policy. The CISO is also responsible for monitoring the implementation of the annual information security plans. The LISOs and (C)ISMs support this. UM-SOC and the Internal IT Auditor are responsible for conducting the audits

Internal checks are conducted annually and, in addition to the regular formal audits, are supplemented by various incidental activities, such as random security checks, conducting penetration tests, and checking the adopted security measures' actual performance. Skills and operational procedures are regularly tested in brainstorming sessions or exercises, such as information security/UM-CERT fire drills<sup>22</sup>.

<sup>21</sup>in consultation with the Data Protection Officer, preferably in combination with privacy audits.

<sup>22</sup>One example is the annual (N)OZON exercise coordinated by SURF.

UM's information systems or processes are audited internally. The audit focuses on (1) classification of data recorded in the information system, (2) identification of risks, (3) security measures taken and (4) consistency between 1, 2 and 3. Audit frequency is determined per information system according to risk classification. If an information system is replaced or undergoes significant security changes, an audit is conducted based on a new business impact and risk analysis. The external audit is carried out by an independent party in a four-year cycle. In terms of planning, it is linked to the financial audit<sup>23</sup> and combined with the normal planning & control cycle as much as possible.

The IBHO standards framework (see chapter 3) is used as a starting point for internal and external audits. Additional, more detailed standards may be adopted for audits of specific components or information systems.

UM participates in the SURFaudit self-assessment cycle and the associated two-year benchmark. A SURF peer review is requested at least once every four years.

The findings of the internal and external audits and any external security requirements serve as input for UM's new annual plans. These can also lead to changes in the IS policy.

Compliance is reviewed by monitoring how information security is handled in daily practice. Managers (including those responsible for education) must hold staff and students accountable for shortcomings. The 'Data Protection Officer' (DPO) is responsible for monitoring compliance with the GDPR.

If the checks reveal serious shortcomings in compliance, UM may impose sanctions on the employees or students responsible. The sanctions will be imposed within the framework of the CAO-NU and employment contracts, the Acceptable Use Policy (AUP) and other formally adopted integrity or behavioural codes, and the legal options such as those in the Higher Education and Scientific Research Act (WHW). Sanctions are primarily the Board's responsibility but can be mandated to the responsible managers (dean or director) in some cases.

## 5.5. Financing

Financial resources for information security are systemically incorporated in the various budgets. Information security financing is both centrally and decentrally implemented at UM.

### Central

General matters, such as drawing up an information security plan for the institution or an external audit, are paid for from general resources. Institution-wide awareness campaigns and training courses are also paid for from these funds.

### Decentralised

The security of information systems and processes, including their costs, is an integral part of responsible management of the information system or process concerned. Workplace security costs are an integral part of workplace costs. Information and training for specific applications or target groups are paid for from decentralised funds.

---

<sup>23</sup> (limited to so-called general IT controls related to the presentation of the financial statements)



## 6. Incident reporting and handling.

An incident is an event or threat that can negatively affect business operations. Incident management and registration involve detecting, recording and handling incidents. Employees, students and third parties must recognise and report any incidents or breaches of information security.

Lessons can be learned from incidents. A mature information security environment includes incident registration and periodic reporting on incidents that have occurred.

Incidents can be reported to the UM-CERT hotline: [Servicedesk-ICTS@maastrichtuniversity.nl](mailto:Servicedesk-ICTS@maastrichtuniversity.nl) (+31 43 388 55 55). UM has clearly communicated the contact details of 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, including data leaks. Incidents and infringements must be reported to the UM-CERT hotline immediately.

Incidents or threats of incidents may also be discovered during regular or incidental checks/audits or by alerts from UM-SOC's 24/7 monitoring system.

Incidents are handled in accordance with UM's Incident Management Process, which includes data leaks. The UM-SOC and UM-CERT Operational Models<sup>24</sup> describes the process for handling serious incidents and incidents outside regular business hours. Part of that process is the UM-SOC or UM-CERT's mandate to immediately shut down or order the shutdown of IT facilities for which an excessive risk has been identified.

The Executive Board has adopted a Responsible Disclosure policy<sup>25</sup>. With this policy, UM guarantees that subject to certain conditions, no legal action will be taken against those who report vulnerabilities in the information systems.

## 7. Adoption & Amendment

With the employee participation body's consent, the Executive Board will adopt the IS policy proposed by the Corporate Information Security Officer (CISO). The IS policy follows the frameworks of institutional policies, such as the I strategy. The policy is evaluated once a year and adjusted if necessary. The policy is reviewed and redefined at least every four years or following a substantial change in institutional policy or major cybersecurity developments.

This policy, version 3.0, was adopted by UM's Executive Board on 17 November 2020 and can be cited as "UM Information Security Policy 2020".

---

<sup>24</sup> Yet to be determined for UM-SOC; for UM-CERT, see

<https://www.maastrichtuniversity.nl/nl/over-de-um/service-centra/ict-servicecentrum/um-cert>

<sup>25</sup> Reference to be added in due course: This policy still has to be formally approved. It will be drafted in accordance with Responsible Disclosure guidelines issued by the Public Prosecution Office (OM) and NCSC.

## Annexe A – Designing an ISMS

Information security is a continuous process. In short, the requirements must be determined, after which measures are taken. The measures are laid down in an annual plan. The measures may change (because threats and risks change, and laws and regulations are also subject to change). Checks can give rise to adjustments to the measures. The total package of requirements, measures and controls may also need to be adjusted over time and must be evaluated periodically. The entire process of information security follows a Plan-Do-Check-Act (PDCA) cycle (see figure). The complete set of measures, processes and procedures is recorded in an Information Security Management System (ISMS) and supports the completion of the PDCA cycle. By repeating the PDCA cycle, UM continuously works to improve the ISMS and, in turn, retain more control. The annual plans can be found in the CISO’s plan and—in more detail—in the administrative units' annual IT plans.



### Standards

UM maintains an ISMS based on the international ISO27001 standard and uses the CIS-20<sup>26</sup> framework as a supporting tool to implement the ISMS


### Elaboration

After determining the organisation’s context (IS policy in relation to the external and internal environment), the needs and expectations of stakeholders and the scope, the ISMS is drawn up based on a PDCA cycle with the following phases:


<p><b>Plan</b></p> <p>The following matters are defined in the plan phase:</p> <ul style="list-style-type: none"> <li>• Context and scope</li> <li>• risks and opportunities</li> <li>• operating assets</li> <li>• resources and competencies</li> <li>• awareness and communication</li> <li>• documented information</li> </ul>	<p><b>Do</b></p> <p>The implementation of the ISMS involves:</p> <ul style="list-style-type: none"> <li>• operational planning and control</li> <li>• risk assessment</li> <li>• risk management</li> </ul>
<p><b>Check</b></p> <p>The check phase includes the evaluation of the performance of the ISMS:</p> <ul style="list-style-type: none"> <li>• monitoring, measurement, analysis and evaluation</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>


<sup>26</sup> <https://www.cisecurity.org/controls/cis-controls-list/>

## Annexe B - Information security principles


<h1>1</h1>	<p><b>Risk-based</b> Information security is risk-based</p> 
<p>Core</p>	<p>The measures are based on the potential security risks of our information, processes and IT facilities.</p>
<p>Background</p>	<p>Sharing knowledge (openness) is an important core value of UM's teaching and research process. It is important to determine the value of information to properly assess risks when protecting information and taking appropriate measures. If the value of information is known, the right security level can also be determined, which matches the risks. Proportionality is desirable to use the available financial resources efficiently, among other things ("Fit for purpose").</p>
<p>Implications</p>	<ul style="list-style-type: none"> <li>• The risks are assessed and defined according to a risk classification (Annexe C).</li> <li>• UM will adopt a Classification Directive<sup>27</sup> (see also Annexe C).</li> <li>• The risk analysis includes a Data Protection Impact Assessment (DPIA) in the context of the GDPR where appropriate.</li> <li>• Measures are taken to bring the identified risk regarding Availability, Integrity and Confidentiality to the accepted level.</li> <li>• Information has one 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 may be accepted within UM's risk appetite, ultimately determined by the Executive Board.</li> <li>• Deviations require the risk acceptance process to be followed, with acceptance by the information, process or application owner.</li> <li>• The information owner (and potentially also the process or application owner, depending on the necessary mandate) must sign for acceptance of the risks.</li> <li>• Measures must be designed in such a way that their impact is verifiable.</li> <li>• The highest risks must be mitigated first.</li> <li>• Based on the risk analysis, information security can be weighed against ease of use.</li> <li>• Measures must be in balance (in terms of costs) with the reduction of risks (proportionality principle).</li> <li>• Information has a single source, which makes ownership and "single point of truth" easy to interpret. This also creates an additional chain of responsibility for the consequences of changes at the source.</li> <li>• UM remains responsible for adequate protection of information when using external data processing services.</li> <li>• Where applicable, contracts must include security requirements and the provision of external review (assurance) to demonstrate the efficacy of measures.</li> </ul>


<sup>27</sup> <https://www.maastrichtuniversity.nl/informationsecurity>

<h1>2</h1>	<p><b>Everyone</b> Information security is everyone's responsibility</p> 
<p>Core</p>	<p>Everyone is and feels responsible for the correct and 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 possible damage resulting from loss of availability, integrity or confidentiality. Employees, students and third parties are expected to handle information in any form with care and actively contribute to the security of the automated systems and the information stored therein. The success of security depends on good communication. Good communication is actively promoted at and between all levels in the institution.</p>
<p>Implications</p>	<ul style="list-style-type: none"> <li>• An Acceptable Use Policy (AUP) is available to all users of UM's digital information services and is published on UM's website. The AUP applies to students, staff and third parties.</li> <li>• The safe handling of information and information carriers is part of all employees' employment contracts.</li> <li>• Information security is considered when hiring employees and during performance reviews and periodic meetings.</li> <li>• Information security is discussed in regular meetings in departments and projects.</li> <li>• Employees and students call each other to account for unsafe use of information and systems.</li> <li>• Employees and students report vulnerabilities and suspected vulnerabilities to UM-CERT.</li> <li>• The Executive Board has adopted a Responsible Disclosure policy.</li> <li>• Violation of information security legislation, rules and regulations may lead to sanctions by or on behalf of the Executive Board.</li> </ul>

<h1>3</h1>	<p><b>Always</b> Information security is a continuous process</p> 
<p>Core</p>	<p>Information security is at the core of all our work.</p>
<p>Background</p>	<p>The environment is ever-changing; cyber threats increase and decrease, processes change, employees and students change, etc. Defining and implementing the measures once is not enough to maintain a safe climate. Information security only makes sense if it is a continuous process of measures, awareness and checks.</p>

Implications	<ul style="list-style-type: none"> <li>• An Information Security Management System (ISMS, appendix A) will be set up and used to adequately monitor all IS policy aspects through a PDCA cycle.</li> <li>• Audits and assessments will be carried out periodically, making it possible to evaluate the efficacy of the policy and measures taken (verifiability).</li> <li>• Upon arrival of new employees and students, attention is paid to raising awareness of the risks and UM’s security procedures for access to and use of IT resources.</li> <li>• High-privilege accounts must be validated periodically (at least annually).</li> <li>• UM regularly organises cyber-awareness activities for the various target groups: students, employees, managers and partners of UM.</li> <li>• If a person’s roles, duties and responsibilities change, their permissions will be adjusted accordingly.</li> <li>• A process will be established to determine and periodically adjust the threat level for UM. New threats will result in the adjustment of measures where necessary.</li> </ul>
--------------	--

<h1>4</h1>	<p><b>Security by Design</b> An integral approach to information security</p> 
Core	From the start, information security is an integral part of every project or any change regarding information, processes and IT facilities.
Background	Security by design means that at the start of a project, data security and the continuity of processes are considered in the design of a new application or ICT environment and in the event of technical or functional changes, preventing often-expensive repairs later.
Implications	<ul style="list-style-type: none"> <li>• For each new project/software procurement/innovation, the security requirements (non-functional requirements) are considered from the start.</li> <li>• Before going live, the application of the security requirements will be evaluated and tested.</li> <li>• All IT systems and facilities use the principle of “least rights” to promote information security. The aim is to grant no more rights than are necessary for an adequate job and business performance.</li> <li>• Access to systems is based on permission schemes.</li> <li>• Separation of duties is applied in processes and procedures.</li> <li>• The design ensures that the use of information and IT facilities can be traced back to a responsible user.</li> <li>• A ‘security in projects’ directive will be adopted, based on the measures resulting from the risk classification and measures potentially resulting from the Data Protection Impact Assessment (DPIA) under the GDPR.</li> <li>• The process design includes measures that adequately guarantee the continuity of the process.</li> </ul>

<h1>5</h1>	<p><b>Security by Default</b> Restricted access and secure settings by default</p> 
<p>Core</p>	<p>Users only have access to the information and IT facilities they need for their work. Providing information is a conscious choice.</p>
<p>Background</p>	<p>Security by default means that every implemented configuration has the available security options turned on by default, preventing unauthorised and uncontrolled access to data. As a result, making information available is always a conscious choice after careful consideration.</p>
<p>Implications</p>	<ul style="list-style-type: none"> <li>• The standard configuration's security baseline must be defined for (e.g., protecting all external communications with SSL technology by default).</li> <li>• The initial design of an information system or infrastructure follows the 'closed, unless' principle.</li> <li>• Deviation from the initial design follows the "comply or explain" principle.</li> <li>• Security is safeguarded in a change management process.</li> <li>• Access to information is role-based, allowing users to access only the information and IT facilities they need for their work (defined in a permissions scheme)</li> <li>• Some key roles are identified according to which baseline permissions are granted. Key roles could include student, employee, supplier, etc. Users are given only these roles by default.</li> <li>• Logging and auditing processes are designed so that access to information and IT facilities can be traced back to a responsible user.</li> </ul>

## Annexe C – Risk appetite and classification

At UM, all data, processes, information systems and applications to which this information security policy applies are classified. The classification depends on the data to be processed and is determined according to UM’s risk appetite based on risk analyses and damage categories. The classification process is laid down in a Classification Guideline adopted by the Executive Board<sup>28</sup>.

The level of security measures depends on a defined risk class.

This annexe provides an overview of the risk appetite established, the damage categories used, and the classification process adopted.

### Risk appetite

A risk analysis can evaluate the potential damage a threat may cause to specific information (e.g., abuse through illegitimate, unauthorised access) and the likelihood of such damage occurring.

Not all risks need to be mitigated. UM is prepared to accept some risks. The risk appetite in the table below can be seen as a risk analysis based on general values rather than concrete risks.

UM’s risk appetite is displayed in the diagram below.

Table 1: Risk appetite

Risk		Damage (Impact)			
		Negligible	Low	Serious	Disruptive
Probabil- ity	Minimal	Acceptable	Acceptable	Acceptable	Acceptable
	Low	Acceptable	Acceptable	Acceptable	Unacceptable
	Likely	Acceptable	Acceptable	Unacceptable	Unacceptable
	High	Acceptable	Unacceptable	Unacceptable	Unacceptable

### Damage categories

Damage can be divided into multiple categories. The damage categories proposed below indicate the importance of the information. Measures are selected to reduce the risk of security breaches to a level deemed acceptable by the organisation in accordance with the risk appetite.

The damage categories at UM are determined as follows:

<sup>28</sup> See <https://www.maastrichtuniversity.nl/informationsecurity>.

Table 2: Indication of damage categories

INDICATION OF DAMAGE CATEGORIES				
IMPACT	Reputation	Education	Research	Financial
<b>NEGLIGIBLE</b>	A small number of negative messages in local media (including social media)	At most, disruption of a limited number of activities at an institute or department.	No or short interruptions in ongoing research, mainly already public or non-sensitive data	Direct damage between 0 and €10.000
<b>LOW</b>	Negative media coverage for a few days (including social media)	Disruption of part of the education (e.g., part of an institute or department)	Non-public research data, prolonged interruption or invalidation of research	Direct damage between €10,000 and €50.000
<b>SERIOUS</b>	Persistent negative reporting in local media (including social media). Details of socially sensitive activities (e.g., animal testing).	Prolonged disruption of a large part of education at one or more institutions.	Publication restrictions, reputational damage to researcher or institution, patents or contractual agreements	Direct damage between €50.000 and €10.000.000
<b>DISRUPTIVE</b>	Persistent negative reporting in national/international media (including social media).	Most of the education rendered impossible at one or more institutions for an extended period	Extensive contractual obligations, exclusion of future grants or life-threatening research	Direct damage is greater than €10.000.000

### Classification according to three quality aspects and three risk classes

The owner of information determines the damage category based on the maximum damage/value of the data. The value of a number of data types has already been determined for the entire organisation (Table 2).

In determining the damage category, the owner considers **three quality aspects (C, I, A)**:

<b>C = Confidentiality</b>	Are the rightsholders the only parties with access to the information or function?
<b>I = Integrity</b>	Is the information or function reliable/complete/unimpaired?
<b>A = Availability</b>	Is the information or function present/useable/readable with the correct performance at all necessary times?

The following two aspects are also important when determining measures:

#### *Verifiability*

The verifiability<sup>29</sup> of the measures taken to guarantee these quality aspects.

#### *Privacy protection*

<sup>29</sup> Verifiability: the extent to which it is possible to verify parameters relevant to availability, integrity or confidentiality after the fact. Such parameters include *downtime*, access and transactions.



The Integrity and Confidentiality aspects are also important to guarantee data subjects' privacy when processing personal data. The resulting risks are determined in a so-called Data Protection Impact Assessment (DPIA<sup>30</sup>) within the framework of the GDPR.

For the actual classification, **three risk classes** are chosen for each quality aspect: **Low, Medium and High**. The division into three classes makes it easy to determine a classification for each quality aspect and apply generic measures to them for the whole institution.

The table below provides a tool for estimating the risk class according to a generic impact indication per quality aspect, based on the assumption that the damage may occur.

Table 3: Classification of the impact in risk classes.

CLASS	AVAILABILITY	INTEGRITY	CONFIDENTIALITY
<b>LOW</b>	Total loss or unavailability of this information for longer than one week does not cause any noticeable (measurable) damage to the interests of the institution, its staff or its students or customers.	The business process allows some integrity errors.	Information which may or must be accessible to all or large groups of staff or students. Confidentiality is low. For public information, access is not an issue, but management is (for the sake of integrity).
<b>MEDIUM</b>	Total loss or unavailability of this information for longer than 48 hours causes noticeable damage to the interests of the institution, its staff or its students or clients	The business process allows very few integrity errors. Protection of integrity is absolutely necessary.	Information that should only be accessible to a limited group of users. The information is confidential.
<b>HIGH</b>	Total loss or unavailability of this information for longer than 4 hours causes noticeable damage to the interests of the institution, its staff or its students or clients	The business process does not allow any integrity errors.	This concerns highly confidential information, intended only for specifically named parties, of which inadvertent disclosure outside the specified group can cause major damage.

In special cases, such as in response to external requirements, the Board may set stricter classes for all CIA aspects. The CISO must ensure that such classes are designated and treated as exceptions.

This determines the risk classification. The actual risk is determined by multiplying the impact by the probability. By taking adequate measures, probability and impact can be reduced, mitigating the risk. As such, the classification outcome determines the measures to be taken to secure the information adequately.

UM has established an information security baseline<sup>31</sup> as a minimum set of measures. Based on the classification, additional measures are prescribed in accordance with the centrally established table of measures<sup>32</sup>.

<sup>30</sup> Data Protection Impact Assessment

<sup>31</sup> All "Low" measures in the UM measures database

<sup>32</sup> The "Medium" and "High" measures in the UM measures database

## Annexe D – Legislation and regulations

This appendix provides an overview of the most important legislation and regulations related to information security with specific attention points for UM.

1. **Higher Education and Scientific Research Act (Wet op het Hoger onderwijs en Wetenschappelijk onderzoek; WHW)**  
UM has a quality assurance system in accordance with the Institutional Quality Assurance Test (InstellingsToets Kwaliteitszorg; ITK). Among other things, this guarantees careful handling of data in the student administration and the study results. Integrity codes for scientific research are also observed and applied.
2. **General Data Protection Regulation (GDPR)**  
UM has adopted a separate data protection policy to ensure GDPR compliance. Compliance with the information security policy, including the technical and organisational measures therein, and the procedures and measures in the privacy policy, ensure compliance with the GDPR.
3. **Statutory Retention Periods/Archives Act**  
UM complies with the statutory regulations regarding retention periods, as laid down in specific legislation (such as the Tax Act and in employment law) and in the Archives Act and the Archives Decree. To that end, UM uses the Basic Selection Document<sup>33</sup> for Universities. The selection document covers all information recorded in digitised documents, information systems, websites, and email, and is part of the annual external financial audit reports.
4. **Copyright law**  
UM respects copyrights and acts accordingly.
5. **Telecommunications Act / Net Neutrality Act**  
Because UM's target group is sufficiently defined, UM's network facilities are not regarded as a public network within the meaning of the Telecommunications Act. Exceptions to this are a few facilities for student housing. Procedures have been established for these in accordance with the Net Neutrality Act.
6. **Computer Crime Act III**  
The Computer Crime Act focuses on criminal problem areas in relation to computer use. The law consists of clauses that have been added to various sections of the Penal Code. The extra clauses deal with:
  - destruction and rendering inoperative;
  - data tapping;
  - denial of Service, flooding attack;
  - computer intrusion;
  - purchase of services without paying.
  - malware, malicious software.Compliance with this Information Security Policy—particularly the security measures and expected behaviour—will ensure that UM has an adequate basic security level against these threats. UM will report any attacks that significantly breach UM's security and fall under the Computer Crime Act.
7. **Other codes and national agreements**  
UM's information security policy is based on the SURF Standards Framework, and the institution is a participant in the VSNU<sup>34</sup>. As such, UM is bound by the following codes and national agreements:

<sup>33</sup> <https://www.nationaalarchief.nl/archiveren/kennisbank/selectielijst-universiteiten-en-universitair-medische-centra-2020>

<sup>34</sup> Association of Cooperating Dutch Universities (Vereniging Samenwerkende Nederlandse Universiteiten)

- Code of Good Governance for Universities;
- Dutch Code of Conduct for Scientific Integrity;
- Legal Standards Framework for Higher Education;
- Basic Selection Document for Universities;
- FAIR principles.

## Annexe E – Roles in IS governance

In this appendix, the various roles in the 3LoD model are further described “top down”, and their interrelationship is summarised in a table. The Supervisory Board, External Audit and the Dutch Data Protection Authority (Dutch DPA) are not taken into further consideration.

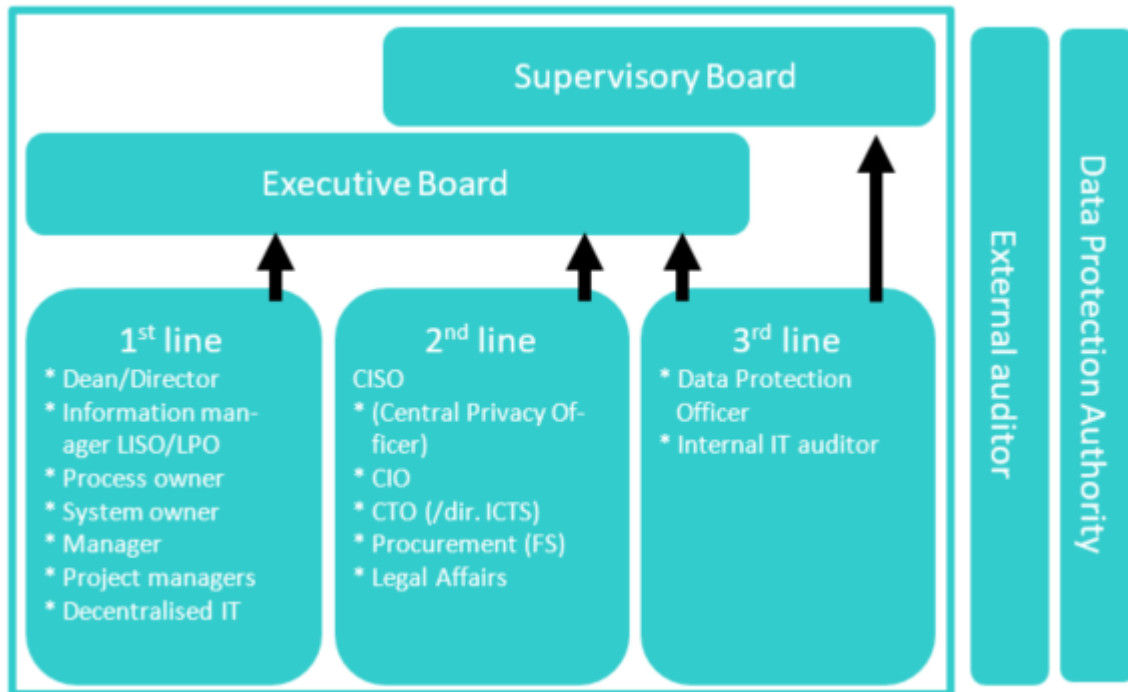


Diagram: Three Lines of Defence translated into Education

### Executive Board

The Executive Board is responsible for information security within UM and determines the information security policy and risk management process (including the classification guideline). The board discusses information security as often as necessary and at least twice a year. The board will appoint one of its members as **information security portfolio holder**.

The portfolio holder has vested the responsibility for digital information security in the CISO, who is tasked with supervising the entire institution’s digital information security. Non-digital information security is vested in the relevant process owners.

Because executive responsibility for the total digitalisation of UM and, in turn, the quality of Security (and Privacy), is vested in the CIO, the CIO is the hierarchical manager of the CISO and is operationally mandated by the Executive Board.

### Data Protection Officer (DPO or in Dutch: Functionaris Gegevensbescherming/FG)

The DPO supervises the application of and compliance with the GDPR within UM, as described in UM’s privacy policy<sup>35</sup>. The DPO’s legal duties and powers give him an independent position in the institution.

### Internal IT auditor

The internal IT auditor is part of the internal audit organisation and annually checks the proper and reliable functioning of the internal IT organisation. This includes the structure and responsibilities of the IT organisation and the hardware, software, internal and (if present) external network, and security and emergency systems. The internal IT auditor reports to the principal (usually the portfolio holder on the board)

<sup>35</sup> For UM’s privacy policy, see <https://www.maastrichtuniversity.nl/privacy>

to the Supervisory Board and the main stakeholders: CIO/CTO/CISO/DPO.

### **Corporate Information Security Officer (CISO)**

The CISO is both a strategic and tactical role, which advises and reports directly to the board. The CISO formulates the security policy, assists in its correct translation into institutional departments, ensures uniform compliance and reports on gaps, inconsistencies and imperfections. The CISO can give both solicited and unsolicited advice. The CISO's hierarchical superior is the CIO.

The role of CISO is assigned to one person, but there may be additional centralised or decentralised (Local) Information Security Officers (L)ISOs.

The CISO has various powers; He can conduct investigations, have investigations carried out (audits), request information and, in general, receive it. If privacy is at stake (and in all exceptional cases), the board decides. The CISO also fulfils the role of Business Continuity Manager (BCM) within UM. This is another strategic/tactical role that aims to monitor business continuity.

### **LISO (role of the Information Manager)**

A Local Information Security Officer (LISO) role is explicitly assigned to the Information Manager within all UM's administrative units. The LISO advises and reports hierarchically to the director of the administrative unit. The LISO is consulted on the implementation of tactical/operational measures adopted in response to the IS policy and is responsible for the translation, planning and implementation of the measures in his administrative unit<sup>36</sup>, and monitoring and reporting on the measures. The LISO is also the first point of contact for UM-CERT and UM-SOC in the event of security incidents.

### **(Corporate) Information Security Manager or (C)ISM**

The CISM plays a role in translating the strategy into tactical and operational technical plans and measures, together with the CISO, the LISOs and the system and process owners. The CISM also advises on specific information security measures, e.g., in projects, for software or hardware acquisitions, etc. At UM, the UM-SOC fulfils the role of CISM. The UM-SOC's hierarchical superior is the CTO.

In addition to the CISM and the LISOs, there are several IT support employees within the administrative units who translate UM-wide measures and operational plans into their own organisation<sup>37</sup>,

### **Corporate and Local Privacy Officer**

The Privacy Officer deals with implementing and complying with the GDPR centrally within UM or the business units. The Local Privacy Officer (LPO) role is explicitly assigned within all UM's administrative units. The LPO is the first point of contact for the DPO and the central UM Privacy Team in privacy matters such as data leaks. This role is usually combined with the LISO role by the Information Manager. There is always cooperation between the LPO and the CISM and CISO/LISO, such as when analysing data leaks, assessing of risks and measures in the case of a Data Protection Impact Assessment (DPIA) or concluding processing agreements under the GDPR.

### **Process owner**

A process owner is responsible for one of the primary or supporting processes using one or multiple systems.

In many cases, the process owner of a primary process (e.g., HR or Student Administration) is also formally internally responsible for the data processed in that process and any processes derived from it (information or source owner).

### **System owner, application owner**

A system owner is someone responsible for an important system, platform or application that supports one or more processes.

---

<sup>36</sup> This is why the LISO role is often combined with the daily management of the local IT support in the administrative units.

<sup>37</sup> usually managed by the LISO

**Manager (including those responsible for education)**

Compliance with the IS policy is part of the integrated business process. Every manager is tasked with:

- ensuring that their staff or students are aware of the aspects of the security policy that are relevant to them;
- monitoring compliance with security policies by staff and students;
- periodically discussing information security in work meetings;
- serving as a point of contact for all staff-related information security matters.

**UM-CERT coordinator**

The UM-CERT<sup>38</sup> coordinator plays a specific role in the field of information security.

At UM, the CERT coordinator is appointed by the Executive Board. The CERT coordinator is responsible for information security incident management within the institution. In that context, within UM-CERT’s operational model, he is also authorised to order the temporary isolation of computer systems or network segments. To perform these tasks, the UM-CERT coordinator will cooperate with other formally appointed UM-CERT members in accordance with the UM-CERT operational model established by the Board of Directors.

**RASCI table**

- R = responsible = responsible for implementation
- A = accountable = ultimately responsible (mandated)
- S = Supportive = supports during process
- C = Consulted = consulted during process
- I = Informed = informed of results

Note 1: The Executive Board has ultimate responsibility, but the CIO is mandated in most cases.

Note 2: The Dean/Director is ultimately responsible in the MUs, but a process or system/application owner/manager is usually mandated

	Executive Board/CIO	CISO	LISO	CISM / UM-SOC	ISM / IT employee	UM-CERT	Process owner	System / application Owner	Manager	Internal IT auditor
<b>IS policy</b>	A	R	C	C	I	I	I	I	I	C
<b>Risk management</b>	A	R	C	C			C	C	I	C
<b>Classification</b>		C	R				A	A	I	
<b>Measures</b>		C	A	S	R		A	A	I	
<b>Audit (agenda, execution)</b>	A	R	S	R			S	S	I	R
<b>UM Incident Handling<sup>39</sup></b>	I	A	S	R	S	R	I	I	I	
<b>MU Incident Handling<sup>40</sup></b>	I	C	R	S	S	S	I	I	A	

<sup>38</sup> CERT: Computer Emergency Response Team (also called CSIRT: Computer/Cyber Security Incident Response Team).

<sup>39</sup> As long as there is no CMT; an S, C or I role may also be needed at Legal and M & C

<sup>40</sup> As long as there is no CMT; an S, C or I role may also be needed at Legal and M & C

## Annexe F – Information security documents

With respect to information security, UM follows the same (PDCA) management cycle which also applies to other subjects. The PDCA management cycle consists of vision/idea, policy, analysis, plan implementation, execution, checks and evaluation.

In the context of information security, UM uses the following documents:

1. *IS policy*

The IS policy forms the basis of UM's approach to digital information security. The policy is drawn up by the CISO and adopted by the board.

2. *Description of the Information Security Management System (process and record)*

3. *Classification Directive, DPIA, regulations (e.g., basic hygiene) and work instructions*

4. *Measures database*

The measures database describes the minimum measures required to guarantee the minimum level of information security defined for UM, linked to the classification guideline. The measures stem from the policy or additional decisions taken by the Executive Board and must be taken throughout the institution. The measures are drafted by the CISO and adopted in the Information Managers consultation (I4MU). Additional measures are taken if certain processes or systems require higher security requirements due to their classification or another risk analysis (e.g., a DPIA).

5. *Annual plan and annual report*

In line with the PDCA cycle, CISO provides the board with an annual report for the past year and an annual plan for the following year. The annual report is partly based on the results of the periodical checks/audits. Incidents, results of risk analyses (including measures taken) and other initiatives that have taken place in the past year are discussed. In any case, the annual plan will be coordinated with the annual privacy plan drawn up by the DPO.

The reports are consolidated in the administrative Planning & Control cycle. Particular attention will be paid to specific systems/applications where necessary.

The annual plan must be assessed in terms of the availability of resources (people and money) in relation to the risks to be mitigated.

6. *Policies*

Codes of conduct and information security guidelines for employees, students and third parties (albeit specific target groups), such as:

- Privacy Policy;
- Acceptable Use Policy, for the safe use of IT facilities, email and Internet by employees, students and third parties;
- Code of integrity/code of conduct for ICT officers;
- RFC-2350 for UM-CERT (see chapter 6. Incident Reporting and Handling (UM-CERT));
- UM-CERT Operational Model;
- UM-SOC Operational model;
- Responsible Disclosure Directive;
- Various guidelines derived from the CIS-20 Framework;
- Authentication Guideline (including password policy);
- Authorisation Directive;
- Use of cryptographic tools.

Information security is also an integral part of the following documents:

7. *Service agreements (service level specifications or service level agreements, SLAs), contracts for leasing and subcontracting and any associated data processing agreements*  
When hiring staff and purchasing resources (especially hardware, software, application/cloud platforms and services), explicit attention is paid to information security by applying the IS policy to external parties and making security a standard part of the purchasing conditions. Agreements are laid down in a contract with the supplier. The contract contains a standard information security paragraph which defines the supplier's responsibilities, based on the SURF Legal Standards Framework for Cloud Services in Higher Education<sup>41</sup>, which contains an information security annexe.
8. *Business Continuity Plan*  
The Business Continuity Plan is drawn up at the Business Continuity Manager's initiative and in cooperation with the board, CISO, process owners, CIO, CTO, and the Director of Facility Services.

---

<sup>41</sup> <https://www.surf.nl/binaries/content/assets/surf/nl/kennisbank/2013/juridisch-normenkader-cloudservices-hoger-onderwijs.pdf>