Strategic Policy on Information Security

2023-2027

Universiteit Leiden

Established: Executive Board 10.06.2023

CONTENTS

SUMMARY 3
1. INTRODUCTION 4
1.1 The importance of information security *4*
1.2 Objective of the policy *4*
1.3 Scope of the policy *5*
1.4 Structure of the policy – 'layerd' model *5*
1.5 Validity & responsibility *6*
1.6 Structure of the policy *6*
2. INFORMATION SECURITY 7
2.1 What is information security *7*
2.2 How it relates to privacy and data protection *7*
2.3 Digital threats *7*
2.4 Vision *8*
2.5 Strategy and objectives relating to digital resilience *8*
2.6 Risk-driven approach *9*
2.7 Laws and regulations *9*
3. PRINCIPLES AND POLICY RULES 10
3.1 Strategic principles *10*
3.2 Policy rules *11*
4. HOW INFORMATION SECURITY IS ORGANISED 13
4.1 Three Lines Model *13*
4.2 Consultation and reporting structures *15*
5. FRAMEWORK CONDITIONS 16
6. COMPLIANCE AND EVALUATION 17

Summary

The success of Leiden University depends increasingly on information, new technologies and computer systems. Information must be properly secured, particularly when personal data is stored. This document sets out the way in which Leiden University ensures adequate information security and thus complies with the relevant laws and regulations.

One of Leiden University's aims with this strategic policy on information security is also to contribute to improving the quality of information provision and to ensuring the right balance between functionality, security and privacy.

This document describes to whom, to which parts of the organisation and to which devices and applications the policy applies. Information security applies at all levels of the organisation. In addition to the scope of the policy, the responsibilities of the officials involved are also described. Final responsibility rests with the Executive Board.

The policy has five key principles, namely:

1. *Information security is risk-driven*
   We base the measures on the potential security risks to our information processes and IT facilities.

2. *Information security is the responsibility of everyone*
   Everyone is and feels responsible for the proper and secure use of resources and authorities. Policies and technical measures are not sufficient to exclude risks in the context of information security. People themselves create the greatest risks. We therefore work constantly to promote awareness of security in order to achieve a greater understanding of the risks and to encourage safe and responsible conduct.

3. *Information security is a continuous process*
   Information security is in the DNA of all our activities. It is a continuous process, where we are always looking for possible improvements. This is visible in, for example, our annual planning, the testing we do and the adjustments we make to our policies and processes.

4. *Security by Design*
   Information security is from the outset an integral part of every project or every modification made to information, processes and IT facilities.

5. *Security by Default*
   Users have access only to information and IT facilities that they need for their work. Making information accessible is a conscious choice.

Checks are carried out to monitor and evaluate compliance with the policy, and reports on this are submitted to the Executive Board. Improvement measures are taken based on these findings to continuously optimise the effectiveness and functionality of information security.

1. Introduction

The quality and reliability of information are a precondition for Leiden University with its leading education and research in society (see the Leiden University Strategic Plan 2022-2027). More far-reaching digitalisation, computerisation and chain integration within the domains of education, research and operational management demand the reliable provision of information, where adequate information security is in place that is compliant with the relevant legislation.

We can no longer function without the digital collection, recording and sharing of information with both internal and external partners, colleagues and students. At the same time, Leiden University is aware of the growing threat from cybercriminals and state players. The Executive Board therefore considers information security to be of essential importance in a time of digitalisation and chain dependence. The Executive Board's intention with this strategic policy is to define the parameters for adequately safeguarding information security.

1.1 The importance of information security

Information is one of Leiden University's most important operational resources for the domains of research, education and operational management. Accessible and reliable information are essential for a university. Students, researchers, staff (including lecturers) and partners (including chain partners) must at all times be able to count on the reliable provision of information and on careful management of their data, including personal data.

Information security should be a standard element of all processes within the domains of research, education and operational management. Besides an overview of potential information risks for the domains mentioned, it is essential to have insight into the consequences (impact) should these risks manifest themselves. Information risks constitute a threat to the quality and continuity of processes and to our strategic objectives.

These threats have a detrimental effect on the availability, integrity and confidentiality of information. Examples of threats are digital hacks, theft of information or knowledge, undesirable manipulation of information or hijacking information through the use of ransomware. A potential consequence is that the value of a Leiden University diploma, grades obtained or the legitimacy of research conclusions are undermined. This can also lead to discontinuity of certain processes, reputational damage or financial harm. But the privacy of students, staff, researchers and other persons can also be damaged. It is therefore of crucial importance that the security of information is guaranteed.

1.2 Objective of the policy

With this policy, the Executive Board directs the way in which the organisation must be resilient in the face of the risks inherent in current trends and developments in information security. This policy enables the organisation to ensure the reliability of its information provision and to be resilient against these threats.

1.3 Scope of the policy

- The policy is applicable to all units within Leiden University, as well as to the processes (including data processing) for which we are responsible, and for which we bear shared responsibility, that are outsourced or procured or organised in any other way.

- The policy is applicable to all processes of Leiden University and thus safeguards the provision of information throughout the whole lifecycle, irrespective of the technology used and the nature of the information. It is not limited to IT but also encompasses physical security, personnel processes and the awareness of information security of users.

- The policy is applicable to the whole data lifecycle: from generating or collecting data, the daily use of data and data storage (both digital and analogue) up to and including the eventual archiving and destruction of data.

1.4 Structure of the policy – 'layered' model

The policy is based on the 'layered' model The Executive Board aims to use this policy to set the required direction for information security by establishing a number of basic principles. This strategic policy translates into tactical policy for information security. The strategic policy and tactical policy together constitute the information security policy on the basis of which operational documents are drawn up under the responsibility of the relevant process owner. Figure 1 visualises the 'layered' model.
A deliberate choice was made in favour of this 'layered' model, because it makes it easier to maintain the policy, and to implement modifications to the policy or parts of the policy. Products listed are in line with the responsibilities in the organisation.

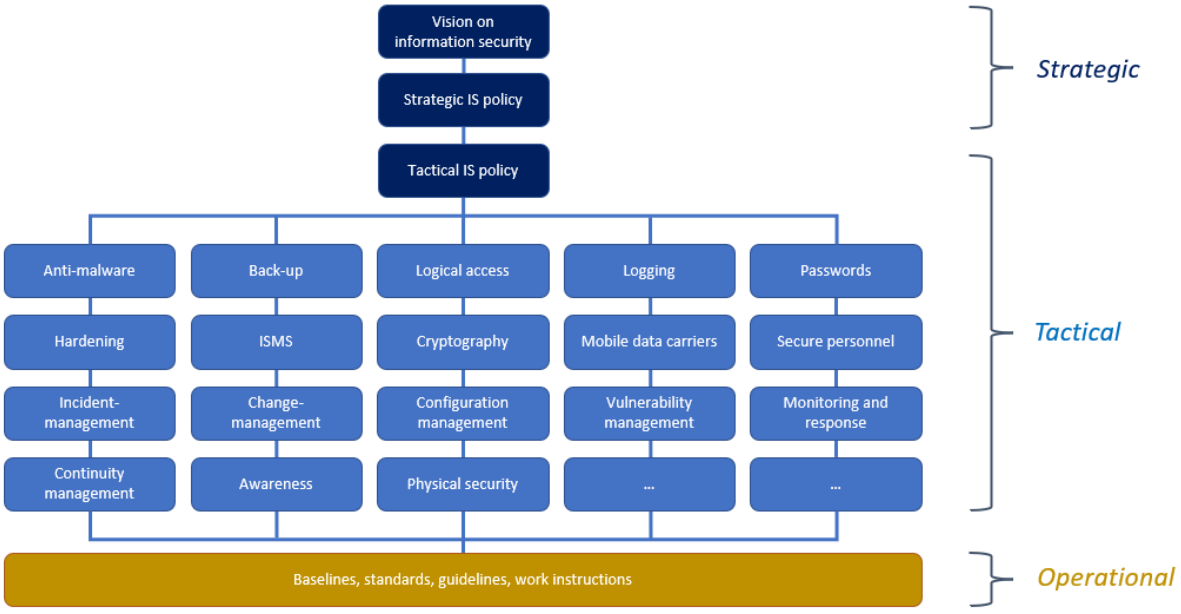

Figure 1. 'Layered' model of the information security policy

1.5 Validity & responsibility

The Executive Board is the owner of this policy document. Managing, drafting and updating the policy document are the responsibility of the Chief Information Security Officer (CISO) on behalf of the management/Executive Board.

This policy comes into force on the date it is adopted by the Board. It replaces the 'Framework Strategic Information Security Policy' (2020; version 1.0).

This policy is valid until 2027 (in line with the Leiden University Strategic Plan 2022-2027) and is reviewed at least once a year under the guidance of the CISO. Interim adjustment is possible if warranted. The policy may be amended on the basis of evolving insights, such as:

- Changes to organisational objectives;
- Feedback and experience relating to feasibility, effectiveness and efficiency based on the implementation of the policy;
- The status of the technology (new security technologies);
- New threats or methods of attack;
- Legal or regulatory changes, or changes within the organisation.

1.6 Structure of the policy

- Chapter 2 describes the information security domain. This chapter sets out the goals and vision.
- Chapter 3 formulates the principles and assumptions that determine the policy to achieve the information security goals.
- Roles, responsibilities and tasks are described in Chapter 4. This chapter also explains the consultation and reporting structures.
- Chapter 5 contains the preconditions that apply to successfully embedding information security in the organisation and achieving the goals set.
- Finally, Chapter 6 describes how compliance with this policy will be monitored.

2. Information security

This chapter outlines the importance of information security, and the vision and objectives of Leiden University in this respect.

2.1 What is information security

Information security refers to devising and maintaining a comprehensive package of management measures to safeguard the required level of security of information in terms of:

- **Availability:** Information must be available at the point in time when it is needed, which places demands on the availability of information systems and databases.

- **Integrity:** The user must be able to trust that information is correct, complete and legitimate. This is anchored in process agreements, as well as in measures that prevent illegitimate or undesirable mutations (whether deliberate or accidental).

- **Confidentiality:** Information is protected at the appropriate level.

2.2 How it relates to privacy and data protection

In a digital environment, the protection of personal data is essential. Privacy and the protection of personal data are a fundamental right. Privacy is a precondition for the freedom to be who you are, do what you do and further your personal development. Every individual must be able to have control over their own data. This means that everyone has the right to know what data is collected on them, what is done with that data and how the data is protected, for example.

Every individual concerned (the persons whose personal data we process) can be confident that we process personal data carefully, legally, transparently and securely. When processing this data we take their interests into account. Additional attention is paid to the protection of data of vulnerable persons concerned, such as minors.

The safeguarding of privacy depends on adequate information security. In order to safeguard privacy, technical and organisational control measures must be in place to ensure the effectiveness of information security. Privacy cannot be guaranteed if information security is not properly safeguarded.

2.3 Digital threats

Data as well as digital security are becoming increasingly important, as an effect of the information society in which we live. We are online more than ever before; we work digitally, shop digitally, follow education digitally and meet one another increasingly in some digital form. The rapid digitalisation that makes this possible gives us many opportunities, but it also entails risks. The National Cyber Security Centre and SURF conclude from their studies that digital attacks are increasing every year and are becoming ever more complex.

The Security Office at Leiden University compiles a threat overview every year detailing the main information security threats. On the basis of this overview, the Executive Board is advised of these threats and the control measures to be taken.

2.4 Vision

Our aim is to ensure that students, lecturers, researchers, staff and partners , including chain partners, are able to count on Leiden University. We are reliable and we provide high-quality education and research. We manage information security risks and apply appropriate control measures to counter these risks. We work continuously on improving our resilience.[1]

We also have information security measures in place to ensure that personal data is properly protected. This is where privacy and information security converge and where our digital resilience plays the greatest role. Cyber incidents where personal data is at stake are one of the greatest risks for the rights and freedoms of our students, lecturers, researchers, staff and other individuals.

2.5 Strategy and objectives relating to digital resilience

Digital resilience is achieved by ensuring that the reliability of the information and the information systems and processes with which we work is guaranteed.

Leiden University's aim with this strategic information security policy is to contribute to the quality of the information it provides and to ensure the right balance between functionality, security and privacy and, obviously, the associated costs. This policy is in line with the mission and strategic goals of the institution.

We work continuously on improving our resilience in order by pursuing the following aims:

- We guarantee the quality and continuity of the educational, research and operational management processes;
- We offer a secure and future-proof education, research and work environment;
- We have insight into information security risks, and apply a cohesive package of appropriate measures to properly manage these risks.

We do this by ensuring that:

- The correct level of availability, integrity and confidentiality of the information and information systems is safeguarded;
- We meet an average maturity level 3 of the SURF audit Assessment Framework.

This makes it possible to:

- Guarantee the quality and continuity of our processes within the domains of education, research and operational management;
- Adequately ensure digital security;

[1] Resilience: the ability to reduce (relevant) risks to an acceptable level by means of a package of control measures to prevent damage and, if information security incidents occur, to detect them in time, limit the damage they cause and facilitate recovery. What constitutes an acceptable level of resilience is the outcome of a risk assessment. This can help in selecting the appropriate technical, procedural or organisational measures (Definition based on the Cyber security vision 2022, NCTV).

- Manage risks and be resilient against digital threats;
- Comply with laws and regulations, including information security requirements arising from privacy legislation.

This means in concrete terms:

- A system of risk management is in place to safeguard information security, and is working effectively;
- The reliability of the provision of information is ensured in accordance with applicable standards, frameworks and best practices;
- A process of self-regulation is in place based on a plan-do-check-act cycle, whereby the effectiveness of this risk management process, the control measures implemented and the security level are evaluated and lessons are learned. This is reported on as part of the P&C cycle;
- Governance is in place, ensuring that information security is embedded in policies and processes, and responsibilities and roles are assigned accordingly;
- Adequate and pro-active action is taken if information security incidents and/or data leaks occur;
- Structural efforts are made to promote awareness.

2.6 Risk-driven approach

100% information security does not exist. It would make the University a closed environment, it is not realistic and it would also be unaffordable. Being sufficiently resilient to threats, including digital threats, keeps Leiden University open and connected to the changing needs and wishes of society. This means that choices are made at management level about which risks are acceptable and which are not. For those risks that are not accepted, appropriate control measures are taken that focus on preventing risks or adequately recovering from an incident that has occurred. The risk management process is therefore central to this policy

2.7 Laws and regulations

In addition to our goals on digital resilience, we also aim to comply with applicable laws and regulations. The most important information security-related laws and regulations concern:

- Higher Education and Research Act (WHW)
- General Data Protection Regulation Implementation Act
- General Data Protection Regulation
- Telecommunications Act
- Computer Crime Act
- NIS2 guideline
- Archives Act (and retention periods)
- Copyright Law
- Applicable standards frameworks, such as the NEN-ISO 27001 and 27002 (best practice)

3. Principles and policy rules

3.1 Strategic principles

Leiden University applies the following three principles:

1 Information security is risk-driven

Control measures are based on the potential risks of our information, processes and IT facilities.

Sharing knowledge (openness) is an important core value of the education and research process. For proper risk assessment when protecting information and taking appropriate measures, it is important to establish the value of information. Once the value of information is known, the right level of security can also be determined that matches the risks. Proportionality is desirable here, as is the efficient use the available financial resources ('Fit for purpose').

2 Information security is the responsibility of everyone

Everyone is and feels responsible for the correct and secure use of resources and authorities.

Everyone is aware of the value of information and acts accordingly. This value is determined by the potential damage resulting from the loss of availability, integrity or confidentiality. Staff, students, researchers and third parties alike are expected to handle information in whatever form consciously and to actively contribute to the security of automated systems and the information stored in them. The success of security is dependent on good communication. Good communication is therefore actively promoted, at and between all levels in the institution.

3 Information security is a continuous process

Information security is part of the DNA of all our activities.

The environment is constantly changing; cyber threats are increasing, and processes change, as do staff and students, etc. Simply identifying and implementing measures once is insufficient to maintain a secure environment. Information security is only meaningful if it is a continuous process of taking measures, maintaining awareness and carrying out checks.

4 Security by Design

Information security is from the outset an integral part of every project and every modification, whether to information, processes or IT facilities ('Security by Design).

Security by design means that at the very start of a project, in the design of a new application or ICT environment and technical or functional modifications account is taken of the security of data and the continuity of the processes. This avoids the need for subsequent reparation activities – which can be very expensive.

5 Security by Default

By default, we apply restricted (logical) access and secure settings.
Users only have access to the information and IT facilities they need for their work.

Security by default means that in every configuration that is implemented, the available security options are activated by default. This prevents unwanted and uncontrolled access to data, including personal data.

Making data accessible is therefore always a deliberate choice, which is made following careful evaluation.

3.2 Policy rules

The five principles lead in practice to the following policy rules (standard premises):

1. Information security is a contributing factor in achieving our **societal ambitions and objectives** in the field of education, research and operational management. In this regard, we take the applicable laws and regulations into account.

2. Organising the provision of information in line with this policy in terms of its design, existence and operating effectiveness provides an **adequate guarantee** of our digital resilience.

3. The primary principle is **risk management**. We apply a risk management system in accordance with NEN-ISO 27001, enabling us to continuously identify risks, take appropriate control measures where necessary and monitor whether these control measures continue to be effective and efficient over time. The classic approach based on restricting possibilities is giving way to safe and responsible facilitation.

4. S**ecurity standards can be upgraded at different levels**. Basically, we aim for level 3 maturity based on the SURF audit Assessment Framework. Where necessary or required, specific additional measures are taken over and above this basic level. This may be warranted on the basis of a risk analysis carried out, or as a result of updated legislation and regulations.

5. Information is **classified** to determine the control measures that are necessary and appropriate. The nature of the information in the processes is the determining factor. Classification is in line with the three reliability aspects of information: Availability, Integrity and Confidentiality (AIC). The classification determines how this information should be handled.

6. When starting **projects**, designing **processes** and **procuring** or **outsourcing** services and systems, a risk analysis is carried out at an early stage. An explicit decision is made by the risk owner on how the risks identified will be controlled and how the advice will be followed up.

7. The policy is authoritative and ensures that the reliability of our information is adequately protected when working with **suppliers** and other **partners, including chain partners**. Agreements have been made in the area of information security, and compliance is monitored

8. Efforts are made structurally and systematically to promote **awareness**.

9. The system of **self-regulation** is central, and an annual evaluation is made of the design, existence and operating effectiveness of the policy rules. An improvement plan is drawn up based on this self-regulation. The accountability of the Executive Board to the Board of Governors is effected via the **P&C cycle.** We work in accordance with the plan-do-check-act improvement cycle.

10. The **Zero-trust principle** is applied. This is a recognised security model to protect modern digital environments.

4. How information security is organised

This chapter describes how the governance of information security is organised, who is responsible for this and to whom it is reported. This is given as a broad outline.[2]

4.1 Three Lines Model

Information security governance is structured according to the so-called Three Lines Model, see Figure 3. This model is commonly used as a model to secure Governance, Risk and Compliance (GRC) in an operational organisation with regard to risk management. It describes not only the roles within the organisational structure, but also how they relate to one another.

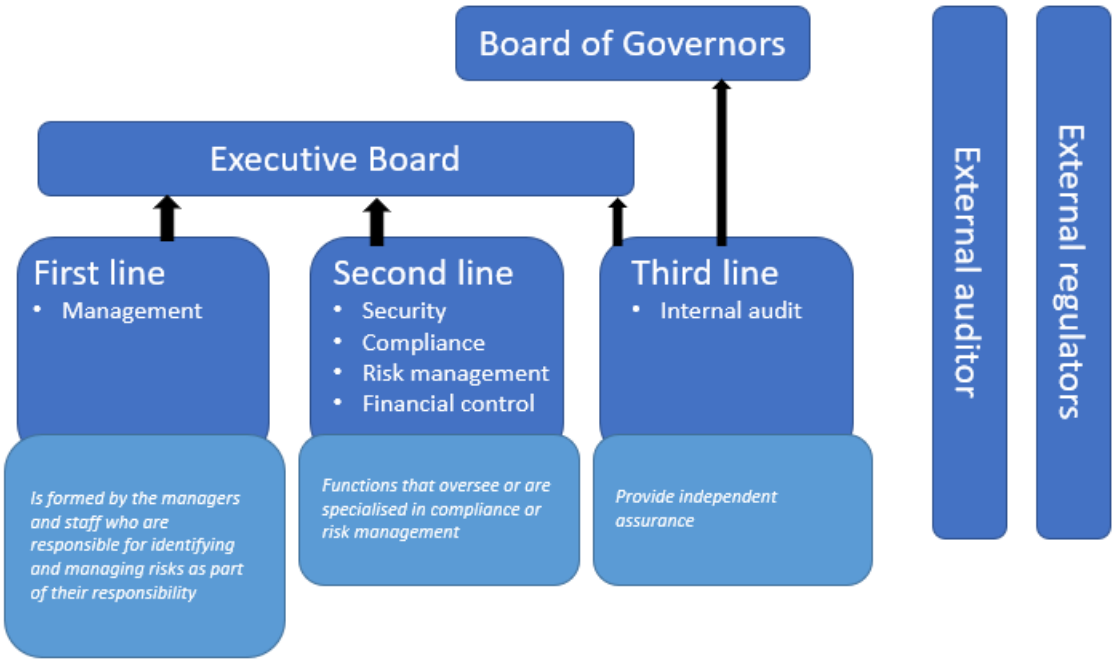

Figure 3 Three Lines Model

The Executive Board bears final responsibility for information security. The Board monitors the risk management of information security, and determines the risk appetite and the strategic information security policy. Specific responsibilities are mandated to the deans of the faculties and the directors of the expertise centres.

The key principle of the Three Lines Model is that the first line (the business) is responsible for its own processes, including risk management.

This means that the deans of the faculties and the directors of the expertise centres have final organisational responsibility for information security within their department in accordance with this policy. In doing so, they receive support in their operational activities from the second line in the person of a Local Information Security Officer (LISO)

[2] The tasks and responsibilities of the information security organisation are described in a separate document on the basis of a RACI table.

The LISO advises the first line, supports the implementation of the policy, ensures the planning and execution of risk analyses, subsequently advises on and oversees the implementation of appropriate control measures, undertakes awareness-raising interventions and collaborates with the Security Office.

The role of the second line is to support, advise, coordinate and monitor whether the first line actually fulfils its responsibilities. Drawing up policy, organising the PDCA cycle, supporting the implementation of integral risk analyses and self-assessments and drawing up annual plans and reports are tasks of the second line. The second line also includes the Security Office. The Security Office provides support, safeguards the quality of these products, and contributes to ensuring the knowledge and skills of LISOs are kept up to date.

In addition, the Security Office supports the different departments of Leiden University from the second line in the appropriate management of information security risks. The Security Office does this by means of binding guidelines, advice and professional, helpful and high-quality services. With the most up-to-date knowledge of the subject matter and local situations, the Security Office will do everything possible to remove or minimise the burden, draw up clear guidelines and communicate clearly so that the first line itself is enabled to implement appropriate information security risk management. In this process, the Security Office works closely with the LISOs. The Security Office will centrally manage the key issues in this process, and will report on and guide the progress of this risk control.

The Security Operations (/CERT) section of the ISSC is responsible for the implementation of the information security policy at configuration level with regard to the IT environment. Within the framework of the established information security policy, Security Operations (/CERT) is therefore also authorised to define the conditions necessary at this level to guarantee the security of the IT environment. This may include prescribing specific cryptographic techniques and hardening baselines and maintaining a blacklist of undesirable information systems, etc. Security Operations (/CERT) also has a monitoring and testing role in this respect. The section is responsible for detection and response, and is authorised to take appropriate remedial measures if an information security risk occurs with regard to the IT environment.

There also has to be a function within the organisation that checks whether the interaction between the first and second lines runs smoothly and whether the organisational goals are being achieved through the design, existence and operational effectiveness of the required control measures in the first and second lines. It is the third line that makes an objective, independent judgement on this with opportunities for improvement. The Data Protection Officer (DPO), an obligatory officer within the AVG and the Internal Audit Department (AIC), typically belongs to the third line. The Chief Information Security Officer (CISO) is also in the third line. They operate completely separately from all other organisational units and report not only to the Executive Board, but also to the Board of Governors.

In this regard, the CISO is a strategic-level function. The CISO advises the Board and has direct access to the Board. The CISO is tasked with monitoring the effectiveness of the information security process. The CISO formulates the strategy and the strategic policy relating to information security and reports to the Executive Board on risk management. The CISO also has the authority to examine (or have an examination conducted into) the state of information security within Leiden University in order to fulfil the monitoring responsibility held by the CISO. The advice of the CISO must be sought in all matters that

have potentially significant information security implications. The CISO works closely with the Security Office in all these matters.

4.2 Consultation and reporting structures

The following consultation structure is in place for information security:

Consultation	**Frequency** (minimal)
CISO and Board of Governors	Annual
CISO and Executive Board / portfolio holder	Monthly
CISO and FG	Monthly
CISO, Security Office and ISSC representative (IB core team)	Every two weeks
CISO, Security Office, LISOs and information managers (IB team)	Monthly

The reporting on information security is in line with the format of the P&C cycle.

Reporting	**Explanation**
Annual report on information security	Annual report of the CISO to the Board
Paragraph on information security in the annual accounts	Accountability (prepared by the CISO) of the Executive Board to the Board of Governors
Quarterly reporting (on progress, risks, evaluations, etc.)	From the Security Office to the CISO, the management and the Executive Board
Monthly reporting (on incidents, threats, risks, etc.)	From Security Operations to the CISO, the Security Office and responsible management.

5. Framework conditions

The municipal Information Security Department stipulates six success factors in its threat overview (2022) that are also applicable to Higher Education. The following preconditions are taken into account in incorporating this policy.

- **Organisation**
  The information security organisation is in place. There is a culture of security awareness.

- **Management ownership**
  Information security is on the agenda of the Board and management. In addition, the Board/management organises a cyber exercise (failure of systems within the organisation) at least once every year.

- **Finances**
  A budget is in place with adequate structural funding.

- **Technology**
  Technology is not infallible. The basics are in good order and a tiered level of security is in place.

- **The human factor**
  An important building block for information security is the awareness by members of staff. Many incidents can be traced back to a lack of digital awareness, and vice versa: a higher digital awareness ensures that incidents are recognised and acknowledged rapidly. Safe handling of data is part of the primary process and thus requires permanent attention and exemplary behaviour on the part of the Board/management and continuous training of all members of staff.

- **Partnerships**
  Agreements are made with partners (IT suppliers, chain partners, third parties) and compliance with these agreements is monitored.

6. Compliance and evaluation

Control measures are taken to reduce risks. To ensure risks are kept under control, regular checks are made to determine whether these measures are still working effectively and still provide the intended level of security.

Leiden University periodically monitors the measures arising from this policy by means of checks (AIC), internal assessments and external audits with regard to effectiveness (including cost-effectiveness) and information security. This is also part of the regular reporting cycle (see section 4.2).

In addition, the CISO assesses at least annually the effectiveness of the information security management process based on data and information collected, and advises the Executive Board accordingly.

Input for this assessment is taken from:

- Incidents recorded and alerts (including vulnerability alerts);
- Tests and internal and external audits carried out;
- Supplier evaluations carried out;
- Risk analyses carried out;
- Reporting relating to the progress of the implementation of control measures and the effective functioning of the measures implemented.

Based on the findings and the advice of the CISO following an assessment of the effectiveness of the information security management process, corrective control measures are implemented where necessary with the aim of minimising the probability and/or impact of an incident, or improving the effectiveness of the management system.

Sanctions

If compliance is seriously impeded by responsible staff or students, Leiden University can impose sanctions on these persons. Sanctions are imposed within the framework of the Collective Labour Agreement, employment contracts and the legal possibilities contained in, for example, the Higher Education and Research Act (*Wet op het hoger onderwijs en wetenschappelijk onderzoek, WHW*).