Information Security Policy

November 2021- version 1.2

Adopted by the Executive Board of SURF on 8 November 2021

Table of contents

Foreword

Information is an important asset for SURF and its members. Information must not only be collected, stored, and accessed in an easy manner: it must also be secure. Not only for SURF but also for all those who work and study at institutions and, together with SURF employees, make daily use of our shared ICT infrastructure. Information security is also an important motivator and facilitator of innovation.

Security can be at odds with other wishes, such as efficiency and user-friendliness. By using best practices and principles, we create a clear framework within which information security can be appropriately safeguarded on the basis of five principles. There is no one-size-fits-all solution: it's about making the right choices for each situation. These principles are applied to our internal operations, but also to our SURF services.

We are proud of the quality of the services provided by SURF to the institutions and want to make that more tangible. By stating our ambition to maintain and expand our ISO 27001 certification for a large part of our services, we are setting the bar high. We are doing this consciously, because being transparant about our quality standard is important for us and our members.

At SURF, security is in our DNA, but we must not forget that dealing safely with information requires a continuous effort from all our employees and users. Behaviour and awareness are extremely important because small actions such as clicking on a link can lead to a large-scale ransomware attack. Although awareness at SURF is high, SURF is also vulnerable to cyber attacks and incidents. That is why we pay a lot of attention to the human side in our security principles. Together, we are building a safe education and research environment for the Netherlands.

Jet de Ranitz
Chairman Board of Directors

1. Introduction

SURF is the cooperative for innovative IT services to Education and Research. SURF's success is closely linked to the quality of the processing of information, the inclusion of security in the development of new technologies, and the security of our computer systems. We can no longer do without the digital collection, recording, and sharing of information with both internal and external partners and colleagues. SURF also develops and provides innovative IT services for its institutions and acts as a knowledge institute for education. Our mission: "SURF makes reliable and innovative ICT facilities possible, enabling Dutch education and research to excel." SURF's services must comply with a high quality standard for information security in order to make this possible for institutions.

The digital reality is constantly changing, which means that there are always new and different risks to information security. The risks pose a threat to the quality and continuity of processes and to the achievement of the strategic objectives of SURF and its member institutions. The threats may affect the availability, integrity, and confidentiality of information. Examples of threats are vulnerabilities in systems or unauthorised access to information. This can affect the quality of the services provided to our institutions and, in the case of incidents, can lead to damage to our reputation. The privacy of employees and guests can also be damaged. Information security is therefore of crucial importance.

Information security requires constant adjustment in order to maintain an appropriate level of security. This is partly due to new threats and vulnerabilities, the stricter requirements to comply with laws and regulations concerning data protection and privacy (AVG), and the agreements with research and educational partners.

Reducing and managing the risks requires efforts at the organisational, process and technological levels. In addition, managers, employees and guests of SURF must also become aware of the risks and adjust their actions accordingly.

Information security cannot be achieved by simply establishing a set of technical and organisational measures. It is a dynamic process because of the constantly changing circumstances. Five information security principles guide information security within SURF. Measures, procedures, and guidelines, and any interpretations, are tested against these.

There are important relationships between information risks and risks in other, partly overlapping, security themes such as international security and crisis management. This policy is part of integral security at SURF. When drawing up the policy, use was made of the SURF SCIPR Model Information Security Policy.

This policy brings together and harmonises the best practices of the former SURF subsidiaries. It has also been updated to reflect new threats and developments in security. It thus replaces all previous policies on this subject.

2. Frameworks and ambition

2.1 Information security and information protection

The terms information security and information safety are often used interchangeably, but they do not mean the same thing. Information security focuses on maintaining the availability, integrity and confidentiality of information. To do this, information and information systems must be protected against possible threats. This is achieved by implementing, maintaining and monitoring protection measures, also referred to as information protection. Final responsibility for information security rests with SURF's Executive Board (RvB).

This Information Security Policy helps ensure that SURF complies with the applicable legislation and regulations, including the AVG, statutory retention periods, the Copyright Act, the Network and Information Security Act (Wbni), and the Computer Crime Act III.

The scope of this Information Security Policy includes internal operations, the services developed by SURF, and the services offered by SURF to the institutions.

2.2 Ambition and objectives

Ambitions

- SURF aims to be an example to its institutions in the field of security for both security knowledge and information system security;
- Internal users of services and facilities are aware of information security risks and adjust their actions and use of (digital) tools accordingly;
- SURF wants to improve the quality of the service provided to users, striking a good balance between information security and other aspects such as functionality, user-friendliness, cost and privacy;

Objectives

- SURF aims to achieve a demonstrable level of maturity as an organisation and for its services, as described in the Normative Framework for Information Security for Higher Education;
- SURF will have part of the services in which SURF fulfils a supplier role (and for which ISO certification is conform market standards) tested by certification against ISO27001;
- SURF aims to reduce the number of security incidents with a "Significant" or "Catastrophic" impact, as defined in SURF's "Business Impact Criteria and Risk Acceptance Criteria" document, to zero;
- SURF wishes to limit the downtime in SURF services that occurs as a result of a security incident to zero, where the downtime could reasonably have been prevented by SURF

2.3 Knowledge and information systems security

The information security policy deals on the one hand with knowledge security and on the other with appropriate protection of the IT resources (information system security).

Knowledge security means taking an appropriate and consciously secure approach towards information and the responsible use of the relevant IT and other resources. 'Information' in this context can be interpreted in a wide variety of ways and encompasses all forms of information (i.e. not only digital information) generated and managed by SURF.

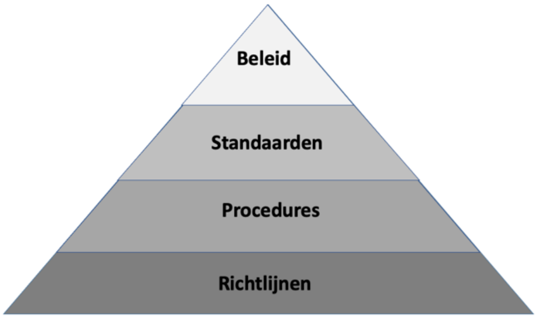
Information system security is about providing appropriate services and IT tools to support knowledge security. This process is independent of geographical location and includes all IT services (both managed by SURF itself and externally) and digital or other tools and resources, both business and privately owned, on which SURF information is processed or stored.

The information security policy is therefore aimed at the following two target groups:

1. In the context of knowledge security: all users of SURF information (employees, guests and external relations).
2. In the context of information systems security: all IT systems and services providers

2.4 Security documentation

The information security documentation consists of four layers. The top three layers are mandatory documents.



On a strategic level, there are policy documents. Policy answers the question why we consider information security important and what we focus on. An example of policy is the Information Security Policy.

At the tactical level, standards are described that SURF complies with. These documents answer the question of what we are going to do and indicate how we set things up. Examples of standards are the Baseline Information Security SURF and the ISMS manual.

At the operational level, procedures are described. These documents describe how we deal with information security and how we perform our tasks. An example of a procedure is the incident procedure.

The fourth layer contains guidelines. Guidelines help us to translate standards into pragmatic solutions. Often, there are several ways to translate a standard into a concrete measure. Examples are guidelines for cryptography or setting security headers. Guidelines are intended to give the organisation something to hold on to and are not compulsory.

2.5 Security control framework

In addition to this policy document, risk-based control frameworks have been established for both knowledge security and information system security, including baselines that specify the required control measures in greater detail and contain operational guidelines. These frameworks are in line with the SURF Framework of Legal Standards for Information Security in Higher Education (*Normenkader Informatie Beveiliging Hoger Onderwijs*, IBHO), which has been developed specifically for education and research institutions. The IBHO is based on the best practices set out in the ISO-27000 series. The IBHO outlines a standard for the maturity of information protection according to the Capability Maturity Model (CMM).

The 'Baseline information security SURF' describes how internally supplied and externally purchased IT services are appropriately protected to support the processing of sensitive information. See the attached frameworks for a list of the different key areas of the control framework. The Chief Information Security Officer (CISO) adopts, regularly updates and adjusts the control framework to ensure adequate protection against threats.

Knowledge security	Security of information systems
• Appripriate Use of IT resources • Information Security Awareness • Clear Desk, Clear Screen • Individual Background Checks • Threat Management and Anti-Spy Protection • Authorisations • Intake-Transfer-Exit • Procedures for working from home • Sanctions • Confidentiality Agreements and Obligations • Capacity Monitoring and Personnel Managem • Secrecy and Obligations • Portable Media and Data Transfer Procedures • Supplier management • Data Archiving and Data Retention • Crisis and Incident Management • Project and Change Management	• Management of IT Equipment and Services • Sensitive Access Control • Vulnerability Management • Network security • Logging and Monitoring • Uptime and Availability Monitoring • Security Monitoring • Workstation Security • Identity and Access Control • Physical Security • Back-up and Restore • Secure Software Development • Data Breach Prevention • Application security • System hardening and Patch Management • Data Retention and Deletion • System Communication • Incident Processes • Conditions of Use and Guides • Certificate and key management

2.6 Adoption and amendments

The Executive Board adopts this information security policy. The policy is reviewed and readopted at least once every three years, or in response to a substantial change in the institution's policy or major developments in cyber security.

3. Policy principles

3.1 Information Security Principles

SURF has identified five policy principles for information security that help to determine the necessary protection measures. Each policy principle has a name and is made up of an essence, brief explanation with background, and the key implications.

Baseline measures cannot always be applied to all situations. In those cases, alternative measures need to be implemented that adhere to the underlying policy principle and that sufficiently cover the risks, in accordance with the ‘Comply or explain’ principle. The specific measures relate to ‘comply’, while the principles serve as a reference for ‘explain’. The alternative measures are evaluated against the policy principles to determine whether they lead to an acceptable residual risk.

The five policy principles described below help to support communication about, and the implementation of, the information security policy. Based on these five policy principles, control measures are formulated that are relevant for the protection of SURF’s information and processes.

3.2 Principle: Risk-based

	Risk-based Information security is risk-based
Core	Measures are based on the potential security risks affecting information, processes and IT facilities.
Background	Knowledge sharing (openness) is an important core value of SURF. In order to carry out a proper information security risk assessment and implement the appropriate measures, it is important to determine the value of information by means of information classification. Once the value of information is known, an appropriate level of protection can be determined in keeping with the risks. Security measures need to be proportional, for instance to ensure efficient use of the available financial resources.
Implications	• In the case of all information processing activities, the data controller determines the information classification, which includes a limited business impact assessment. A suitability level is specified for IT services and resources. • Where personal data is involved, the risk analysis includes a data protection impact assessment (DPIA) in the context of the GDPR (General Data Protection Regulation). • Measures are taken to bring the identified risk to availability, integrity and confidentiality to an acceptable level. • Information sets have a single data controller and a defined source. • The data controller, system manager and process owner are responsible for the implementation and operational enforcement of control measures based on the 'Comply or explain' principle. • Deviations can be accepted within SURF's risk appetite. • The risk acceptance process must be followed in the case of deviations. Acceptance takes place at an appropriate level of management depending on the potential impact. • Measures are designed in such a way that their impact is measurable and therefore verifiable and demonstrable. • The greatest risks in relative terms (taking into account required effort) are mitigated first. • Measures are in line with risk reduction in terms of costs (principle of proportionality). • SURF remains responsible for the adequate protection of information when using external information processing services. Where applicable, contracts include security requirements and/or requirements with regard to external assessment/certification that demonstrate compliance.

3.3 Principle: Everyone

	Everyone Information security is the responsibility of everyone
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. This value is determined by the potential damage resulting from loss of availability, integrity or confidentiality. Both employees and third parties are expected to handle information in any form consciously and to contribute actively to the security of the automated systems and the information stored in them. Successful security depends on clear and understandable communication. That is why such communication is actively promoted at and between every level of the organisation.
Implications	• All users are actively informed about their responsibilities regarding the use of digital resources and information. These responsibilities are outlined in the Acceptable Use Policy (AUP), which also sets out the frameworks for user monitoring and supervision/checks. • Those who infringe information security laws, rules and regulations may face penalties. • The secure use of information and information carriers is written into the employment contract of all employees. • Information security is part of the employee induction process, annual consultations and regular discussions. • Information security is an item on the agenda of regular project meetings. • Employees call each other to account for unsafe use of information and systems. • Employees report security incidents and suspected or actual vulnerabilities to the CSIRT.

3.4 Principle: Always

	Always Information protection is an ongoing process
Core	Information protection is part of the DNA of all our activities.
Background	The environment is constantly changing, cyber threats come and go, processes evolve, employee behaviour changes and so on. Defining and implementing measures as a one-off process is not enough to maintain a secure environment. Information protection is only effective if it is an ongoing process of taking action, awareness and checks.
Implications	• An Information Security Management System (ISMS) is set up for the risk-based monitoring and improvement of the implementation of the information security system and control measures by means of an improvement cycle (plan, do, check and act). • Audits and assessments are carried out on a regular basis to check the effectiveness (verifiability) of the policy and the measures taken. • New employees and visitors coming to SURF are made aware of the risks and SURF's security procedures with regard to access to, and use of, information as well as public and private IT resources. • Accounts with high privileges are periodically validated. • SURF organises regular cybersecurity awareness activities for the various target groups. • If an individual's roles, tasks and responsibilities change, their authorisations are also updated accordingly. • A process has been put in place to determine and periodically adjust the threat assessment for SURF. New threats lead to the adjustment of measures where necessary. • An operational SOC (Security Operations Centre) has also been set up to proactively identify threats and ensure a rapid response to incidents.

3.5 Principle: Security by design

	Security by design An integrated approach to information security
Core	From the very outset, information security is an integral part of every project or every change in relation to information, processes and IT facilities.
Background	The *security by design* approach means taking data protection and process continuity into account at the start of any project, the design of a new application or IT environment and in the event of any technical or functional changes. Doing so avoids often expensive remedial work later on.
Implications	• For every new project/software purchase/innovation, the security requirements (control framework) are included from the outset. • Security is an integral part of architecture and frames of reference from the control framework are incorporated into relevant architecture products. • The application of the security requirements are verified and/or tested before going live. • The 'least privilege' and 'need-to-know' principles are applied to every IT system or structure to promote information protection. This means that no more rights are granted than those required for the proper performance of professional and business activities. • The principle of separation of duties is applied to processes and procedures (for instance a distinction between users and functional or technical administrators). • Access is person-specific and traceable to individuals. • A security guideline is adopted in projects based on the measures resulting from the information classification and any measures arising from the data protection impact assessment in the context of the GDPR.

3.6 Principle: Security by default

	Security by Default Secure and limited access by default
Core	Users only have access to the information and IT facilities they need to carry out their activities. Making information openly available is a conscious choice.
Background	‘Security by default’ means that the security options available in any configuration are implemented as standard, guaranteeing the highest possible level of built-in information security in the default configuration. This prevents undesired and unauthorised access to data, personal or otherwise. As a result, making information openly available is always a conscious choice following careful consideration.
Implications	• There is a defined protection baseline setting out the default configuration for information systems. • The principle on initial setup of an information system or infrastructure is ‘closed, unless’. • Any deviations from the initial setup must adhere to the ‘Comply or explain’ principle. • Security is built into the change and architecture management process. • Access to information is role-based, which means that users only have access to the information they need to do their jobs (specified in an authorisation schedule) or the information owner themselves determine who has access. • Logging and audit processes are set up in such a way that access to information and IT systems is traceable to individuals.

4. Governance

4.1 ISMS manual

A number of governance components are briefly mentioned below. These components are further elaborated on in the ISMS manual. The ISMS manual describes how the governance of information security is set up and what the tasks and responsibilities are of the various management levels. Because information security is risk-based, the ISMS manual also contains a description of Risk Management and the improvement cycle. Security Incident Management is further described, as well as awareness and training. The ISMS handbook is approved by the Chief Information Security Officer (CISO) and periodically updated and calibrated.

4.2 Management levels

The responsibilities within the framework of the governance of information security are divided among the organisational management levels strategic, tactical and operational with corresponding roles, responsibilities, consultation forms and reporting lines. These roles and responsibilities are described in more detail in the ISMS manual.

Strategic	Executive Board, department managers, CISO
Tactical	Security Officers
Operational	SOC, CSIRT

4.3 Three Lines Model

The IS governance at SURF is structured according to the Three Lines Model. This model is generally applied as a model for ensuring Governance, Risk, and Compliance (GRC) in an operational organisation. This model is explained in more detail in the ISMS manual.

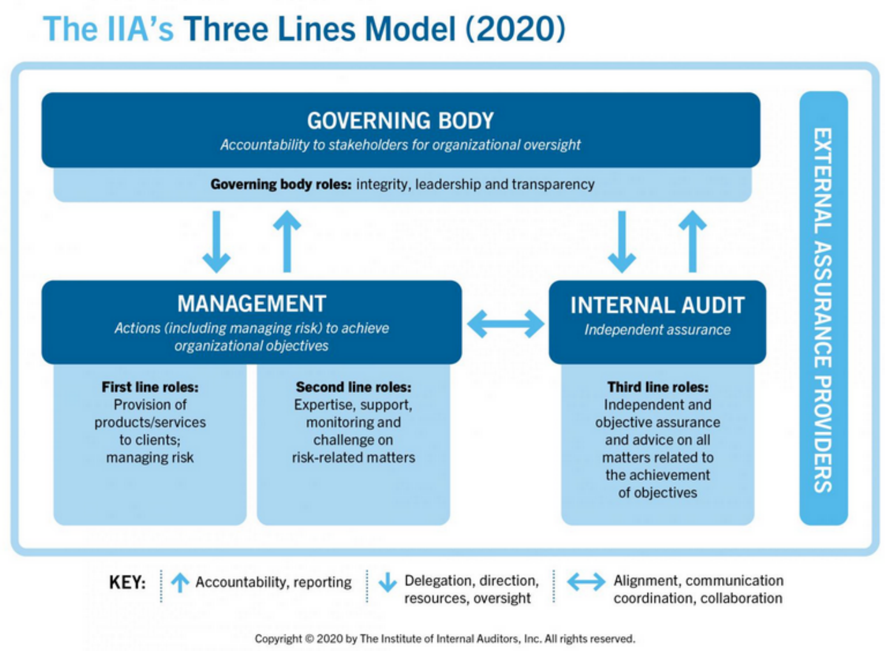

The IIA's Three Lines Model (2020)
GOVERNING BODY
Accountability to stakeholders for organizational oversight
Governing body roles: integrity, leadership and transparency
MANAGEMENT
Actions (including managing risk) to achieve organizational objectives
First line roles: Provision of products/services to clients; managing risk
Second line roles: Expertise, support, monitoring and challenge on risk-related matters
INTERNAL AUDIT
Independent assurance
Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives
EXTERNAL ASSURANCE PROVIDERS
KEY:
Accountability, reporting
Delegation, direction, resources, oversight
Alignment, communication coordination, collaboration
Copyright © 2020 by The Institute of Internal Auditors, Inc. All rights reserved.

Figure 1 Three Lines Model (Source: The Institute of Internal Auditors)

4.4 Risk management and improvement cycle

The ISMS (Information Security Management System) helps to achieve the aim of progressively higher information security levels over an extended period. Having an ISMS is not a one-off activity or a project: it is a continuous risk-management process carried out within the organisation. An improvement cycle, such as the PDCA cycle/Deming circle, is used within the ISMS in order to translate information security into practical measures. Here, PDCA stands for plan, do, check and act.

Based on the ISMS, the CISO draws up an annual report for the Executive Board on the past year, and an outline annual plan for the next year. The annual report is based in part on the results of the regular inspections/audits and includes information on incidents, results of risk analyses (including measures taken) and other initiatives that have taken place in the last year.

In order to apply risk-based information security at the desired maturity level, it is important to keep risks under control using a risk-management approach. Where necessary for valid reasons, a decision can be made to consciously deviate from the prescribed information security measures and to implement, or not implement, mitigating measures to limit the residual risk. Residual risks must always be consciously taken by the person with appropriate authority, must be recorded, must have an end time, must be accompanied by mitigating measures in order to reduce the risks to acceptable levels, and must be regularly reassessed.

The CISO establishes the operational impact of risk management and the Executive Board determines the risk appetite. Depending on the residual risk for the organisation, risks can only be consciously taken at the following level:

Estimate	Authorised to accept
Criticism or "High and cross-domain"	Executive Board
High	Department Manager
Medium	Process owner
Low	No formal acceptance required

Table 1 Risk acceptance matrix

4.5 Awareness and training

Policy and measures alone are not enough to eliminate information security risks. People themselves are the greatest source of risk. That is why at SURF, we are constantly seeking to raise awareness of security among our users to improve knowledge of risks and encourage safe and responsible behaviour. The policy incorporates regular awareness campaigns for all employees, third parties and operational managers in particular. Raising security awareness is a responsibility of both managers, the CISO and ISOs. Awareness-raising is part of the indtroduction program for new employees. The design of awareness and training is further elaborated in the information security communication and awareness plan.

4.6 Security Incident Management

Security incident management is about detecting, recording and dealing with events that constitute a breach of information security and can negatively influence business operations. A key element of this process is that all parties involved recognise and report any security incidents that occur. Incidents are a learning opportunity. Incident registration and regular reporting on incidents that have occurred are therefore integral parts of a mature information security environment.

SURF has a service for the institutions called SURFcert and SURFsoc. SURFcert is the national CERT for the Education and Research sector. Incidents that affect the sector or have an impact on our institutions are reported to SURFcert. Like our members, SURF reports incidents that may have sector-wide consequences to SURFcert. Incidents that have primarily impact on SURF are reported to the CSIRT (Computer Security Information Response Team).

The purpose of the CSIRT is to combat security incidents, thus supporting the continuity of SURF and protecting our reputation. The CSIRT is authorised to take any action on the SURF IT environment to mitigate an ongoing risk/incident and to justify such action in retrospect. Any affected employees are informed and consulted in advance where possible.

SURFsoc is the SOC service developed by SURF to which institutions can connect. SURF’s SOC is based on the services of SUFsoc. The SOC actively monitors security incidents, vulnerabilities, and threats. The aim of the internal SOC is to identify security incidents at an early stage and, if possible, to prevent them or minimise their impact.

Incidents are dealt with according to the security incident process, which includes the handling of data breaches. Coordination takes place with the DPO where personal data is involved. The CSIRT Charter describes the process for dealing with serious incidents and incidents outside normal working hours.

SURF has a Coordinated Vulnerability Disclosure policy that provides anyone reporting vulnerabilities within the information systems with a guarantee that SURF, subject to conditions, will not take any legal action against them and will work with them to resolve or mitigate the vulnerabilities.