Directives on Information Security Governance at the University of Bern

The Executive Board of the University of Bern

based on Article 39 paragraph 1 section b of the Law of September 5, 1996 Governing the University (UniG)

has decided as follows:

1. The objective and purpose of the directives

The Directives on Information Security Governance define the basic objectives, principles, responsibilities and processes of information security at the University of Bern. Governance aims to manage and optimize information security. The directives also lay the foundation for fulfilling the field of action "*Meeting security-related challenges*" from the Digitalization Strategy 2030 of the University of Bern.

2. Area of application

These directives are applicable to the entire University of Bern and are binding on all employees. Students are exempt and are not affected by these directives.

3. Basic principles

- **Risk orientation**
  Information security is not an end in itself. The implementation of measures and initiatives aimed at achieving security objectives is risk-based, proportionate and takes into account costs and benefits.
- **Best practice**
  The University of Bern uses recognized standards. The following standards are used to implement cybersecurity/information security.
  - CIS (Center for Internet Security) Critical Security Controls, Version 8
  - NIST (National Institute of Standards and Technology) Cybersecurity Framework.
  - DMP (Data Management Plan of the Swiss National Science Foundation (SNSF), based on the FAIR Data Principles)
- **Security/privacy by design**
  Information security and privacy are a fundamental part of our daily activities and are

integrated into business processes and taken into account in projects from the very beginning.

- **Personal responsibility**
  All employees are responsible for implementing safety in their area of responsibility.
- **Responsibility**
  A responsible person is defined for all information, ICT systems and business processes (items to be protected).
- **ISMS**
  The University of Bern maintains an information security management system. This is used to permanently define, control, inspect, maintain and continuously improve information security.

4. Information security goals/strategy

4.1 Statement of intent

The University of Bern has developed an awareness of the management of information security risks in relation to systems, people, assets, data and skills. Appropriate organizational and technical protection measures are applied to ensure the establishment and operation of the University's critical services. In addition, as an organization, we are able to detect cyber security events early, respond to them in a timely manner, and in the event of a service outage, restore them in the predefined time.

4.2 Goals

- **Resilience**
  Information security for teaching, research, administration and services is ensured in line with a needs-based, risk-oriented and systematic approach, thus increasing the resilience to cyberattacks.
- **Awareness raising**
  The Information Security Policy at the University of Bern is actively lived by, understood as an essential aspect of its work and not perceived as a hindrance.
- **Confidentiality of information**
  Data and information are only available to authorized persons in the permitted manner.
- **Availability of information**
  Data and information required by the University to conduct its business activities are available within the specified period.
- **Integrity of Information**
  Data and information are complete, up-to-date, unaltered and processed and transmitted in the required quality

5. Organization and responsibilities

5.1 The Executive Board of the University of Bern

The University Executive Board (in the last instance the Rector) is responsible for information security. It is the senior governance body and has the following tasks. The Executive Board of the University of Bern

- adopts the information security objectives and strategy;
- issues directives on information security;
- decides on risk management according to its competence (see Chapter 6.2.1 Risk management);
- provides the necessary financial and human resources to establish and maintain an information security policy and defined information security objectives.

5.2 Managing directors (MD)

The **MD** ensure that the information security requirements (directives and guidelines) are known and integrated and implemented in the operational processes of their organizational unit. They

- ensure that the relevant requirements (such as directives, specific laws and regulations [e.g. the Human Research Act] or requirements of the SNSF for research projects) are known and implemented in their impact areas;
- are responsible for implementing basic ICT protection in their organization;
- appoint persons authorized to make decisions in the area of information security in their organizational unit, but at least information owners (IO), information security officers (ISO) and technology managers (TM) as required (see Chapters 5.3 to 5.5);
- decide on risk management according to their competence within their organizational unit (see Chapter 6.2.1 Risk management);
- provide the necessary human and financial resources to cover the defined tasks as far as possible.

The tasks can also be delegated within their own organization. Responsibility remains with the MD.

5.3 Information owners (IO)

The information owners are responsible for a collection of information. A collection of information is a collection of information that is used in a specific context, regardless of how it is stored. As a rule, a collection of information is edited using an application.

Examples include applications (incl. databases), business records, research data, archive (physical or digital).

The information owners are appointed by the Managing directors.

The most important tasks of the information owners in the context of these directives include the following points: The information owners

- define the need for protection of a collection of information (confidentiality, availability and integrity) by means of classification;
- grant permissions and review them regularly;
- authorize the passing on of information;
- ensure that the retention and archiving of collections of information meet business and regulatory requirements;
- determine the purpose for which the collections of information are used;

- guarantee data quality;
- are responsible for the implementation of basic ICT protection in its impact areas;
- ensure that when outsourcing services, information security requirements and the review thereof are set forth in a contract;
- are responsible for the life cycle of research data in research projects, in particular in relation to the following areas:
    - *Data collection and documentation*
    - *Ethical, legal and security issues*
    - *Data storage and preservation*
    - *Exchange and reuse of data*

Tasks can be delegated to other offices. Responsibility remains with the information owners.

5.4 Information Security Officers (ISO)

The ISO are the extended arm of the CISO and represents its interests in the respective organizational unit. The most important tasks in the context of these directives are to:

- Close coordination with the CISO;
- First point of contact for information security issues;
- Maintain an up-to-date inventory of collections of information requiring a high level of protection;
- Identify and document information security risks and deviations from basic ICT protection;
- Development, if necessary, of supplementary security measures to basic ICT protection, in their areas of responsibility e.g. for research projects;
- Assistance with the implementation of basic ICT protection;
- Regular reporting to CISO, in particular in relation to the following areas:
    - Deviations from basic ICT protection.
    - Report identified information security risks.
    - Report relevant security incidents.
    - Report collections of information requiring a high level of protection.
- Membership in the Information Security Expert Committee.

The ISO are appointed by the managing directors.

5.5 Technology managers (TM)

The technical managers are responsible for the secure operation of the ICT infrastructure. Their most important tasks in the context of these directives are:

- Implementation and maintenance of basic ICT protection in their area of responsibility;
- Implementation of technical requirements in research projects;
- Cooperation with the ISO.

5.6 Chief Information Security Officer (CISO)

The CISO is responsible for managing information security. They create the prerequisites for adequately addressing information security risks at the University of Bern. They are the link between the University Executive Board, the faculties and institutes, the IT and the employees. Their main tasks are to:

- develop, coordinate, submit for formal consideration and maintain the Information Security Strategy of the University of Bern;

- define and coordinate information security processes;
- develop security measures (basic ICT protection);
- set up the safety organization at the University of Bern;
- initiate, implement and coordinate awareness-raising activities;
- establish and maintain the Information Security Risk Inventory of the University of Bern;
- Establish, maintain and further develop the University-wide Information Management System (ISMS);
- report to the University Executive Board – reporting on information security;
- coordinate with the Data Protection Office of the Legal Services Office and the Risk Management Office of the University of Bern.

5.7 Project Managers (PM)

Project managers are responsible for implementing basic ICT protection in projects. Deviations from basic ICT protection and any identified risks must be reported to the ISO/CISO. Project managers

- ensure that the necessary ISDP documents (protection needs analysis and, if necessary, ISDP concept and risk analysis) are available in the relevant project phases;
- ensure quality, safety and ethical standards in research projects.

5.8 Security Operation Center (SOC) / Computer Security Incident Response Team (CSIRT)

The Security Operation Center (SOC) is responsible for the discovery and defense of cyber attacks on the central ICT infrastructure of the University of Bern. The SOC and CSIRT tasks are performed by the NETSEC Group of the IT Services Office. The main tasks are:

- to identify technical vulnerabilities;
- to detect and prevent information security incidents (monitoring);
- to contain and handle information security incidents (incident response);
- to report to the CISO and the affected user groups;
- preventive detection of potential threats to the University’s ICT infrastructure (threat hunting);
- to analyze information security incidents and derive improvements.

5.9 Committees

5.9.1 Information Security Specialist Group in the Central Administration (FGIS ZB)

The Information Security Specialist Group is dedicated to the regular exchange and further development of information security in the Central Administration. The committee is made up of the Information Security Officers (ISOs) and is headed by the CISO. The committee meets at least four times a year or when necessary. The main tasks of the committee are:

- to exchange information and knowledge;
- sounding board for information security measures;
- to analyze the threat situation;
- to improve information security processes and organization (CIP).

5.9.2 Information Security Specialist Group Faculties and Institutes (FGIS F&I)

The FGIS F&I serves the regular exchange and further development of information security in the faculties, institutes and other decentralized departments of the University. The committee is made up of the decentralized Information Security Officers (ISOs) and is headed by the CISO. The committee meets at least four times a year or when necessary. The main tasks of the committee are:

- to exchange information and knowledge;
- sounding board for information security measures;
- to analyze the threat situation;
- to improve information security processes and organization (CIP).

6. ISMS and information security processes

The following sections describe the practices used to ensure the achievement of the defined information security objectives. The practices are part of the Information Security Management System (ISMS).

The ISMS serves to sustainably manage information security. External requirements, such as laws, regulations and contracts, as well as risk management, form the basis for the definition of security objectives, security processes and requirements. Key figures, management reviews and audits ensure that the ISMS is effective and efficient.

The core elements of the ISMS are an established security organization, security framework and risk management process that adequately counteracts specific threats and continuously improves the ISMS.

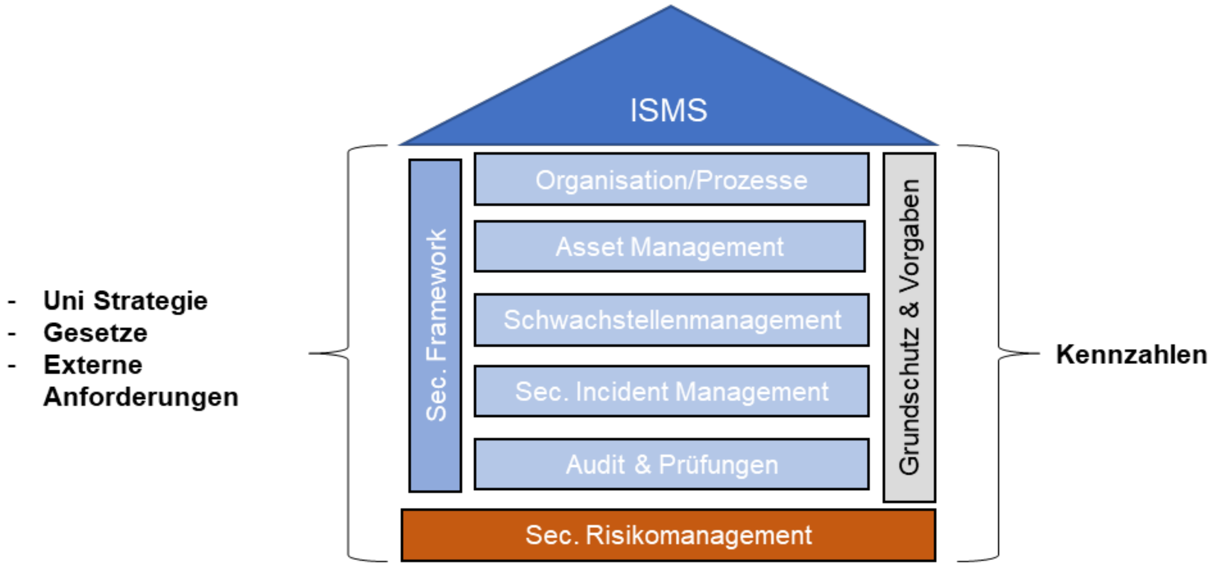


Figure 1

	University Strategy
	Legislation
	External parties
	Requirements
	ISMS
	Organization/processes
	Asset management
	Vulnerabilities management
	Sec. incident management
	Audit and inspections
	Sec. risk management
	Basic protection and requirements
	Key figures

6.1 Basic protection and requirements

The University of Bern uses recognized frameworks and standards to ensure information security. The basic ICT protection based on the CIS controls contains a large number of internationally recognized protective measures that counteract known threats. The basic ICT protection measures, including responsibilities and processes, are described in detail in the basic ICT protection directives.

In addition to basic ICT protection, further topic-specific requirements are issued in the context of information security. Together with the topic-specific directives, the basic ICT protection forms the security framework of the University of Bern.

6.2 Projects and plans

To ensure that information security and data protection are taken into account in projects in good time, the documents must be used in projects and plans in accordance with Table 1. The documents are based on the HERMES project methodology.

ISDP document	Description
Protection needs analysis	The protection needs analysis is used to determine the need to protect collections of information.

ISDP concept	The ISDP concept documents how the security and data protection measures (e.g. the basic protection) are implemented for a specific item to be protected/collection of information.
Risk analysis	If basic ICT protection measures cannot be implemented or can only be implemented partially, a risk analysis must be conducted.

Table 1

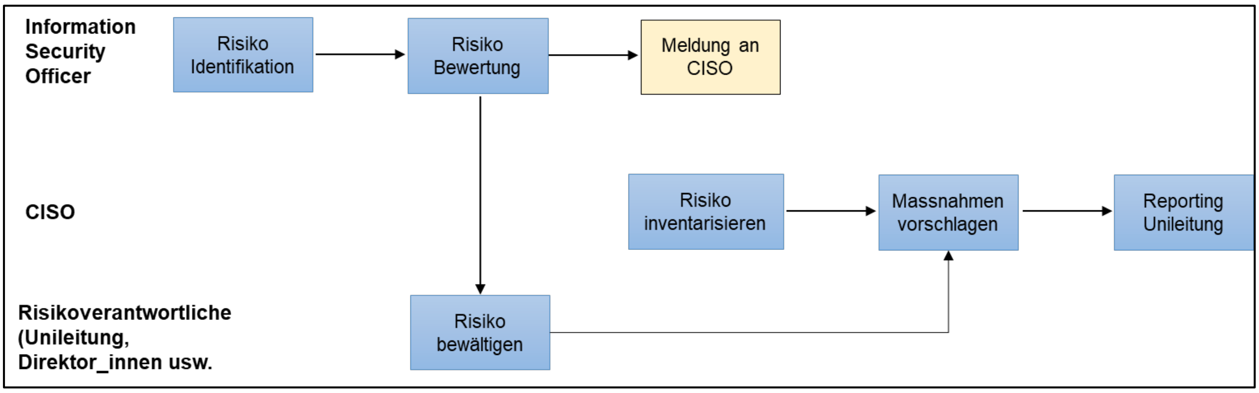
Any risks and the completed documents must be sent to the responsible ISO and CISO.

6.3 Risk management in the ISMS

Risk management is an essential part of the ISMS. It ensures that information security as a whole is continuously analyzed and optimized as needed.

Vulnerabilities (technical and organizational), threats and risks should be identified, evaluated and documented on a regular basis. Information Security Officers are required to report relevant information security risks to the CISO. The CISO is responsible for the centralized documentation of risks and reporting to the University Executive Board.

Figure 2



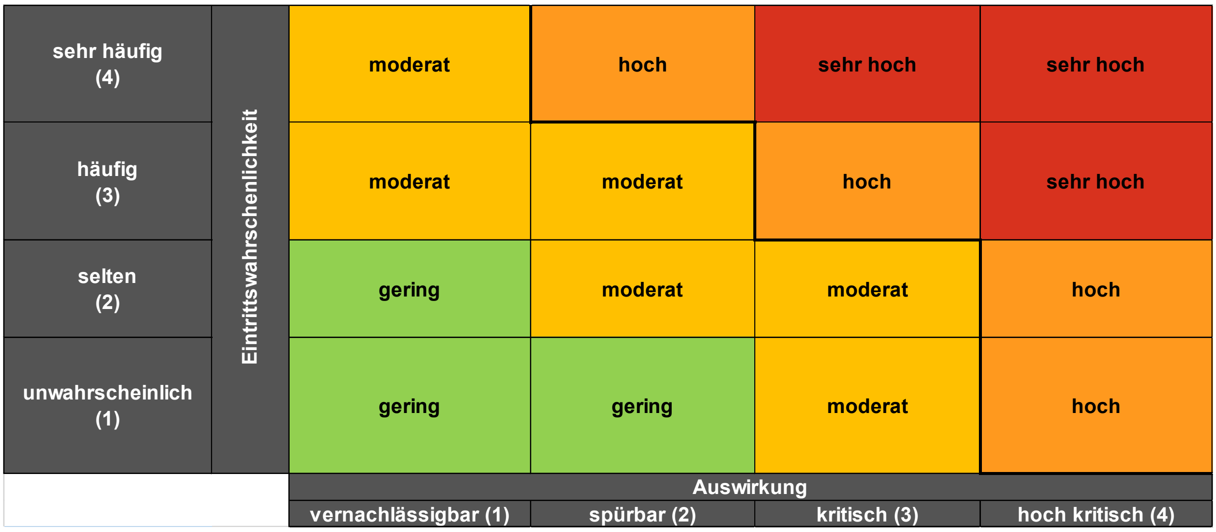
	Risk identification
	Risk assessment
	Report to the CISO
	CISO
	Inventory risk
	Propose measures
	Reporting to the University Executive Board
	Risk Manager (University Executive Board, directors, etc.)
	Manage risk

6.3.1 Risk matrix

By definition, a risk is a measure of the magnitude of a risk and includes the frequency or probability and extent of damage of an adverse event.

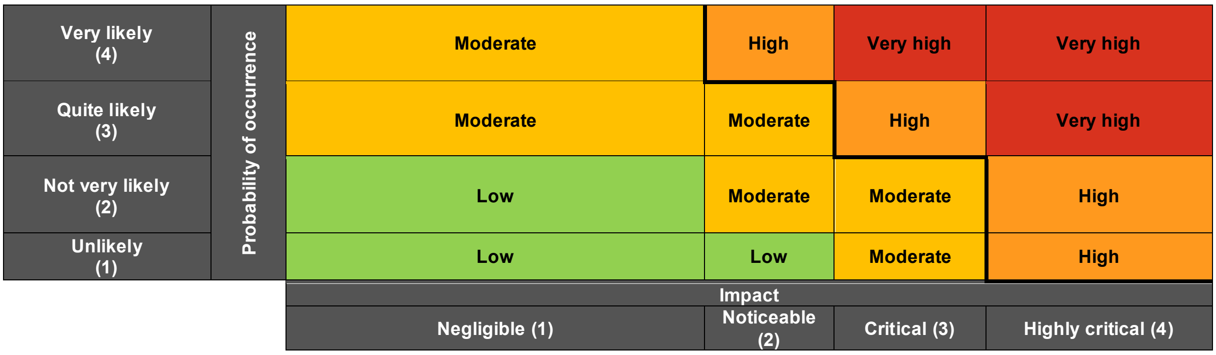
Risk = damage x probability of occurrence

Risk scenarios are evaluated by the respective information owners in accordance with the risk matrix in Figure 4. The specialist group (FGIS) can provide support if necessary.



Eintrittswahrscheinlichkeit	Auswirkung			
	vernachlässigbar (1)	spürbar (2)	kritisch (3)	hoch kritisch (4)
sehr häufig (4)	moderat	hoch	sehr hoch	sehr hoch
häufig (3)	moderat	moderat	hoch	sehr hoch
selten (2)	gering	moderat	moderat	hoch
unwahrscheinlich (1)	gering	gering	moderat	hoch

Figure 3 Risk matrix



Probability of occurrence	Impact			
	Negligible (1)	Noticeable (2)	Critical (3)	Highly critical (4)
Very likely (4)	Moderate	High	Very high	Very high
Quite likely (3)	Moderate	Moderate	High	Very high
Not very likely (2)	Low	Moderate	Moderate	High
Unlikely (1)	Low	Low	Moderate	High

Probability of occurrence

Highly likely	Likely	Not very likely	Unlikely
Several times a month	Once a month – once a year	Every one to five years	Every five years or less frequently

Table 2

Impact/damage

	Negligible	Noticeable	Critical	Highly critical
Confidentiality	Certain information can be viewed by unauthorized persons.	Sensitive information can be viewed to a limited extent by unauthorized persons.	Sensitive information can be viewed to a large extent by unauthorized persons.	Sensitive information can be viewed to an almost complete extent by unauthorized persons.
Availability	Failure/interruption of individual services or features.	Failure/interruption of individual services or an application.	Several applications or a business process are compromised or no longer available.	One or more business processes are compromised or no longer available.
Integrity	Certain information is no longer integer.	Information which is sensitive to a limited	Information which is sensitive to a large	Information which is sensitive to an almost

		extent is no longer integer.	extent is no longer integer.	complete extent is no longer integer.
Reputation	Negative reporting on one occasion or a few dissatisfied employees, students or researchers.	One to two days of negative reporting or larger groups of dissatisfied employees/students or researchers.	At least three days of negative reporting or many dissatisfied employees, students, researchers and supervisors.	Extensive, multi-day to multi-week negative reporting or mostly dissatisfied employees, students, researchers and superiors.
Legal consequences	Minimal violations. No risk of litigation or punishment.	Violations that could result in litigation or punishment.	Violations that are likely to result in litigation or punishment.	Violations that result in litigation or punishment.

Table 3

6.3.2 Risk management and assessment

Table 3 shows which position/role in principle has the power to define how to deal with risks (risk management). Managing directors can delegate the power to manage moderate and low risks within their organization.

Possible coping strategies:

- Avoid risk – the business/project is discontinued
- Minimize risk – measures are implemented to reduce risk
- Accept risk – the risk is accepted
- Transfer risk – by contract or insurance

Risk	Risk owner	Notification obligation	Description
Low	Managing directors or according to delegation	No	The security measures already implemented or at least provided for in the security concept provide adequate protection. In practice, it is common to accept low risks and still observe the hazard.
Moderate	Managing directors or according to delegation (See chapter 5.2)	No	The security measures already implemented or at least provided for in the security concept may not be sufficient to prevent the occurrence of an event and to ward off the damage completely. In practice, efforts are being made to reduce moderate risks, taking into account costs and benefits.
High	Managing directors (See chapter 5.2)	Yes	The security measures already implemented or at least provided for in the security concept do not provide adequate protection against the risk in question. In practice, high risks are rarely accepted.
Very high	University Executive Board (see chapter 5.1)	Yes	The security measures already implemented or at least provided for in the security concept do not provide adequate protection against the risk in question. In practice, very high risks are not accepted.

Table 4

7. Definitions of terms

Term	Description
Impact/extent of damage	Impact (in the context of risk management) describe the totality of all consequences from one or more events. The impact can be both negative (damage) and positive (benefit).
Threat/danger	State or operation that may cause damage to an item to be protected.
CIS controls	The CIS Controls (formerly CIS Critical Security Controls) are a collection of recommended security measures designed to address the most common and dangerous cyber attacks.
Probability of occurrence	The possibility of a specific event occurring in a specific situation (risk scenario) or time period.
Collection of information	A collection of information is a collection of mostly structured information that is used in a specific context, regardless of how it is stored. As a rule, a collection of information is edited using an application. Examples include applications (incl. databases), business records, research data, archive (physical or digital).
Information	Information is equated with meaning or knowledge. For example, information can take the form of text, images or sound recordings. Unlike collections of information, information is usually unstructured documents such as contracts, protocols, requirements, concepts, wiki, Intranet or e-mails.
ISMS	Information Security Management System. These are all activities such as organization, processes, requirements and technical aids that ensure that an organization’s information security risks are identified and can be permanently reduced to an acceptable level.
NIST	National Institute of Standards and Technology from the USA
Privacy	Is the English term for data protection, i.e. for the protection of personality and privacy.
Project	A project is a one-off project with a specific objective. Actions must be planned and implemented in order to achieve the goal. The project has a beginning and an end.
Risk	A risk is a measure of the magnitude of a risk and includes the frequency or probability and extent of damage of an adverse event.
Risk owner	A role that decides how risks are handled. The risk owner decides whether risks are reduced, accepted, transferred or avoided. The role must have the necessary powers in the organization. The role is performed by the University Executive Board/Rector or a managing director.
Risk scenario	A general description of a potential event or development and the resulting impact on items to be protected.
Vulnerability	A vulnerability in the context of risk management describes a missing or ineffective technical or organizational protection measure.
Cybersecurity Framework (NIST)	The Cybersecurity Framework of the U.S. National Institute of Standards and Technology (NIST CSF) defines comprehensive measures for the protection of critical infrastructure in the USA. The NIST CSF has become a de facto standard

	in cybersecurity in recent years and is used by various Swiss regulatory authorities as a testing standard.

Table 5

8. Final provisions

8.1 Conflicting provisions

Any existing provisions which conflict with these directives are hereby repealed.

8.2 Entry into force

These directives enter into force with immediate effect.

Deviations from these directives must be identified and remedied within a reasonable period of time or recorded as a risk and accepted by the risk owner.

Bern, November 7, 2023

On behalf of the Executive Board
of the University of Bern:

Prof. Dr. Christian Leumann
Rector