UNIVERSITÄT
BERN

Directives on basic ICT protection 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 Basic ICT Protection Policy defines the minimum requirements regarding information security at the University of Bern and supports the implementation of the security objectives defined in the Governance Information Security directives of the University of Bern.

Systematic processes and procedures must be established to ensure that the requirements contained in these directives are implemented effectively and sustainably. Compliance with the specifications must be checked regularly by those responsible.

2. Area of application

These directives apply to all employees of the University of Bern who operate and provide ICT systems on-premise or in the cloud for the University of Bern. Students and their IT resources are excluded.

External third parties must be contractually obliged to implement basic ICT protection accordingly.

3. Basic principles

- **Virtualization** – basic ICT protection applies regardless of whether an item to be protected is operated on dedicated hardware or a virtualization solution.
- **State of the art** – the protective measures used correspond to the current state of the art.
- **Need to know/least privilege** – permissions are granted only if necessary to perform work-related tasks. This means that no permissions are granted automatically. The principle applies to ICT systems [3], network zones and information.
- **Security by default** – all ICT systems [3] must be developed, configured and operated in such a way that all sensible security and protection mechanisms (e.g. encryption) are activated by default and can be effective without the users having to worry about it.
- **Attack surface reduction** – ICT systems [3] only offer features and duties that are absolutely necessary for performing services. To reduce the attack surface of ICT systems, unnecessary duties and functions must be disabled or removed.

4. Organization and responsibilities

This chapter describes the roles and tasks in the context of these directives.

The individual requirements are assigned to the respective roles in section 6. This assignment is shown in the table in the “Responsible” column. If a requirement cannot be uniquely assigned to a role, it is assigned to the managing director. They may delegate the implementation of the requirements within their organization to other offices.

4.1 Managing directors

- The managing directors (**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 relevant requirements (such as directives, specific laws and regulations, e.g. the Human Research Act) are known and implemented in their impact areas.
- They are responsible for ensuring that these instructions are implemented in their organization.
- They provide the necessary human and financial resources to cover the defined tasks as far as possible.

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

4.2 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 Services Office and the employees. Their main duties under these directives are to:

- develop security measures (basic ICT protection).
- regularly update basic ICT protection due to new threats or new requirements, e.g. new laws and ordinances.
- report to the University Executive Board – reporting on information security.

4.3 Information owners

The information owners (IO) 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 are regulated in the column “Responsible” in section 6.

4.4 Information Security Officer

The Information Security Officer (ISO) is the extended arm of the CISO and represents their interests in the respective organizational unit. The most important tasks in the context of these directives are to:

- point of contact for information security issues.
- identify and document information security risks and deviations from basic ICT protection.
- develop, where necessary and sensible, complementary security measures to basic ICT protection in their area of responsibility.
- assist with the implementation of basic ICT protection.
- report identified deviations from the basic ICT protection of the CISO.

The ISO are appointed by the managing directors.

The tasks of the ISO in the context of these directives are regulated in the column “Responsible” in section 6.

4.5 Technology managers (TM)

The technology managers (TM) are responsible for the technical implementation of information security requirements in the faculties and institutes in accordance with the column “Responsible” in section 6.

4.6 IT Services Office

There are no technology managers in the IT Services Office (ID). Analogously, the "Responsible" column in section 6 also lists the ID if it is responsible.

5. Protection concept

Basic ICT protection guarantees basic protection (based on the *CIS Controls* in version 8) against known threats and vulnerabilities in ICT. Information and *ICT systems* with a greater need for protection can be protected by means of additional protective measures. The need for protection can be determined by means of a *protection needs analysis* or a *risk analysis*.

Aids	Need for protection	Protection levels
Directives on basic ICT protection	Normal need for protection	Basic ICT protection
Protection needs analysis/risk analysis	Greater need for protection	Is determined on a case-by-case basis

The CIS controls can be used as an aid for identifying pragmatic measures. The implementation of the CIS controls as a supplement to basic ICT protection is recommended. The *CIS Controls UniBE* document can be used as an assessment aid.

6. Requirements

The following requirements apply to ICT systems on-premise and in the cloud (IaaS, PaaS), which are set up and operated by employees of the University of Bern.

6.1 Training and raising awareness

No.	Requirement	Responsible
1	Persons who process *sensitive data/information* of the University of Bern must be trained and instructed about the correct handling of security and protective measures (e.g. data protection training, instructions) and about possible sanctions.	ISO

6.2 Inventory

No.	Requirement	Responsible
	An inventory process should be established that ensures that a complete inventory of ICT systems (physical and virtual instances), including software and licenses, is available. The inventory should contain at least the following items: • Name of the item • Location • Responsible persons (owner) • Criticality, Recovery Time Objective (RTO), Recovery Point Objective (RPO) • Confidentiality level: derived from the classified data • Type of hardware • Software name • Software version	ISO

6.3 Documentation and ISDP documents

No.	Requirement	Responsible
1	Documentation must be created for all ICT systems and kept up-to-date throughout the entire life cycle. The documentation must include the following aspects: • Intended use • Responsibilities • Criticality (level of confidentiality, RTO, RPO, level of integrity) • Data protection-specific measures • Security-related components, features and configurations • The applicable Service Level Agreement (SLA) • Supply chain • Contractual agreements	TM/ID
2	At the start of the project (preliminary phase) or in the event of major changes to ICT systems, a protection needs analysis must be created or updated. If the protection needs analysis shows that the data/information are in need of greater protection, an ISDS concept must be created. If the requirements for prior checking (Art. 17a of the Cantonal Data Protection Act (KDSG)) are met (e.g. when processing particularly sensitive personal data), the ISDS concept must also be submitted to the *Datenschutzaufsichtsstelle des Kantons Bern (DSA, the Data Protection Supervisory Authority of the Canton of Bern)*. In such a case, the CISO and the Legal Services Office (Data Protection Office) must be involved.	TM/ID

6.4 Identity and account management

All (internal and external) employees of the University of Bern and technical resources must be clearly identified and authorized prior to exercising an activity or role.

No.	Requirement	Responsible
1	Each person must be identified before a personal account can be assigned. As a rule, this occurs as part of the employment process. Identities must be clearly and centrally recorded.	MD
2	An account must always be identified with multi-factor authentication (MFA) whenever possible. MFA is **mandatory** for the following cases: • Use of privileged accounts, e.g. administrators. • Access from untrusted networks (e.g. Internet, remote access, support access) to non-public data and information of the University of Bern. • Access from unknown devices (e.g. BYOD) to data and information of the University of Bern.	TM/ID
3	Passwords must contain at least 12 characters (14 characters for admin accounts) and a combination of three of the following four elements. (Uppercase letters, lowercase letters, numbers, special characters) and must be technically enforced.	TM/ID
4	After 10 invalid login attempts, an account must be blocked for a certain amount of time.	TM/ID

5	For the first registration of new users, randomly generated initial passwords must be assigned, which must be changed after one use. If possible, the request must be technically enforced.	TM/ID
6	Passwords may not be transmitted or stored in plain text. A secure password hashing algorithm with salt (randomly selected character string) must be used to store passwords. If possible, the request must be technically enforced.	TM/ID
7	Passwords are personal and must not be shared. Business passwords must not be used for private purposes.	User
8	Whenever possible, no local accounts should be used and to use a central directory. Local accounts must be documented and assigned to a responsible person.	TM/ID
9	Procedures must be established (automated if possible) to ensure that user accounts (local and central): • in the event of a departure (termination), the departure date is disabled or deleted. • in the event of an express departure (termination without notice, dismissal), the identity/account is disabled immediately.	TM/ID
10	Unused user accounts must be deleted or, if this is not possible for traceability, disabled.	TM/ID
11	Privileged activities must be performed using specific administrator accounts or documented, orderable, time-limited, logged, and MFA-protected privileged roles. General activities such as surfing the Internet, editing e-mails or using Office applications must be carried out with the personal, non-privileged user account.	TM/ID
12	Impersonal accounts, e.g. service accounts, should be avoided wherever possible. Where they are necessary, the accounts must be documented (reason, date, duration, person responsible) and assigned to a person with technical responsibility.	TM/ID
13	Dedicated service accounts with the necessary privileges must be used for different system services. The same account cannot run multiple system services and programs.	TM/ID

6.5 Roles and permissions

No.	Requirement	Responsible
1	A transparent application and approval process is required for assigning permissions and roles to confidential/highly confidential classified information. The assignment of permissions and roles must be planned and documented and kept up-to-date in an permission concept for each application.	IO
2	It must be ensured that the permissions are checked and removed if necessary when employees (including external employees) join, transfer and leave.	IO
3	Permissions are assigned in accordance with the need-to-know principle and must be carried out via established and documented processes.	IO

	When assigning permissions, the classification of data and information must be taken into account	
4	The permissions must be checked periodically or in the event of changes, but at least annually, and documented in a traceable manner.	IO

6.6 Technical vulnerability management

No.	Requirement	Respon-sible
1	It is a process incl. roles that ensures that technical vulnerabilities in ICT systems are identified and remedied within an appropriate period. The following factors determine the response time and prioritization of vulnerabilities: • Vulnerability severity based on CVSS score; • Exposure of the affected ICT equipment • Criticality of the affected ICT system	TM[1]/ID
2	A vulnerability scan must be performed regularly, but at least four times a year.	TM/ID
3	Patching procedures must be established which ensure that: • emergency patches (0-day) are closed within 24h; • highly critical vulnerabilities (CVSS 7-10) are closed within 30 days; • critical (CVSS 4.1-6.9) are closed within 60 days; • and all others are closed within 180 days; or alternative protection measures are implemented.	TM/ID

6.7 ICT infrastructure

No.	Requirement	Respon-sible
1	The software of the ICT systems (e.g. applications, middleware, end devices, network components) must be kept up-to-date (stable release of a major version under maintenance recommended by the manufacturer).	TM/ID
2	Only software and hardware supported by the manufacturer may be used.	TM/ID
3	Software errors and vulnerabilities must be corrected or closed by the manufacturers within a reasonable period of time. Appropriate agreements must be made with the manufacturers and renewed if necessary.	TM/ID
4	Defective hardware must be replaced within a reasonable period, depending on availability requirements. Appropriate agreements must be made with the manufacturers or sufficient replacement material must be procured.	TM/ID
5	ICT systems must be configured securely (hardening), e.g. according to the manufacturer's recommendation or according to hardening	TM/ID

[1] The NETSEC Group of the IT Services Office operates infrastructure for scanning technical vulnerabilities and is available for support.

	guidelines, e.g. ID-hardening guidelines or CIS benchmarks. Minimum requirements are: • Best practice from the manufacturer must be taken into account. • Only services (software) that are necessary for the intended operation of the system may be installed or activated. No automatic installation/activation. • Preconfigured accounts (e.g. guest) must be deleted or disabled. • Services may only have the permissions they require (no root/admin rights). • Initial passwords must be changed. • Turn off error and debug messages for end users and only enable them if necessary.	
6	Development, integration and production environments must be separated.	TM/ID
7	It must be ensured that there is no connection to systems used by other customers or clients.	TM/ID
8	ICT systems must be designed in accordance with the availability criteria defined in the *protection needs analysis*. This means that critical ICT systems must be configured with a high level of availability and/or location redundancy.	TM/ID
9	Only software libraries (e.g. dll, ocx, so files) from trusted sources may be used.	TM/ID
10	Data media must be safely disposed of or destroyed. Appropriate procedures must be established.	TM/ID

6.8 Application security/software development

No.	Requirement	Responsible
1	The requirements for the security of applications are based on the current recommendations (de facto standards) in accordance with *OWASP*. These fundamentals must be adequately considered throughout the entire development and operating process, taking into account risks and cost-effectiveness.	TM/ID
2	Access to repositories must be clearly regulated and kept to a minimum.	TM/ID
3	Software must be tested systematically before it is launched and after each major release.	TM/ID
4	Applications that access central systems must be approved before they are purchased, commissioned or used by the IT Services Office. In the case of risks relating to data protection laws, the CISO and the Legal Services Office must be involved.	TM

6.9 Malware defense

No.	Requirement	Responsible
1	ICT systems must implement measures to detect and prevent malware. • Signature and behavior-based detection should be supported. • The programs must be updated regularly.	TM/ID

	When using removable media (e.g. USB stick), a malware scan must always be carried out beforehand.	
2	E-mails incl. attachments should be scanned for malware before being delivered to the mailbox.	TM/ID
3	Measures must be implemented to prevent falsification or alteration of e-mails.	TM/ID
4	It must be ensured that only current and manufacturer-supported e-mail clients and web browsers are used.	TM/ID
5	The central DNS servers of the IT Services Office must be used for DNS resolution. This ensures that the Switch DNS Firewall is used. Internal DNS servers in institutions must forward recursive queries to the central DNS servers of the IT Services Office. (DNS forwarding)	TM/ID
6	Unnecessary file types must be blocked on the mail server.	TM/ID

6.10 Data security

No.	Requirement	Responsible
1	Information and *collections of information* must be classified in terms of confidentiality, availability and integrity. The protection needs analysis is used to determine the protection needs of information/collections of information.	IO
2	*Sensitive data* must be encrypted during transmission.	TM/ID
3	Data storage devices must be encrypted.	TM/ID
4	Sensitive data at rest on servers, applications and databases must be encrypted at the client or application level.	TM/ID
5	No sensitive data should be stored on end devices (notebook, PC, mobile phone, etc.). If it is, the end device must be encrypted, e.g. with Windows BitLocker®, Apple FileVault® or Linux® dm-crypt.	TM/ID
6	A data management process is to be established based on the applicable legal and operational requirements. The process is designed to ensure that a data owner/information owner is designated and that retention and deletion regulations are known and adhered to.	MD
7	The processing and storage of sensitive data should be (technically or organizationally) separated from non-sensitive data.	TM/ID
8	All collections of information with a high need for protection must be inventoried and reported to the CISO.	ISO
9	Personal data as defined in *FADP/KDSG* on development and test systems must be anonymized or synthesized.	TM/ID
10	If test or development data cannot be anonymized or synthesized, the same security measures must be observed as in the production environment (complete basic protection including permissions).	TM/ID

6.11 Network security

No.	Requirement	Responsible

1	Access to sensitive data on the network must be restricted to the essentials (outbound and inbound traffic) by means of firewalls.	TM/ID
2	If possible and supported, “local” firewalls on servers must be enabled and managed.	TM/ID
3	Firewalls on end devices of the user must be enabled and managed.	TM/ID
4	Network traffic to critical systems and sensitive data must be authenticated and authorized.	TM/ID
5	The network must be divided into different network zones (segmentation).	ID
6	Each network zone type must have a policy. The policy should at least regulate the following: - Name of the zone - Inbound and outbound traffic - Authentication of network traffic - Recording level (what is logged) - Monitoring (what is monitored)	ID
7	Network traffic in and out of network zones with critical ICT systems must be monitored and logged.	TM/ID
8	Network documentation must be available and kept up-to-date.	ID
9	Remote access to the network of the University of Bern must be managed, encrypted, authenticated and recorded (log files) via a central gateway. In addition, only the required systems should be made accessible.	ID
10	Transport encryption must be implemented wherever possible and secure protocols used. (e.g. SFTP instead of FTP).	TM/ID

6.12 Backup and restore

No.	Requirement	Responsible
1	Data and configuration files of applications and systems required for operations must be backed up regularly (automatically) in accordance with the business availability requirements (see RPO in Protection Needs Analysis).	TM/ID
2	The restore of backup data must be tested regularly.	TM/ID
3	Backup data must be protected against malware/ransomware. It must be ensured by means of offline storage or other measures (e.g. air-gap, dedicated network zone) that backup data is not endangered by malware/ransomware.	TM/ID

6.13 Logging and monitoring

No.	Requirement	Responsible
1	Logs of systems exposed to the Internet must be connected to a security log/monitoring infrastructure.	TM/ID
2	Logs of systems with sensitive data must be connected to a security log/monitoring infrastructure.	TM/ID

3	Changes to system configurations (in applications and IT systems) must be logged by the systems.	TM/ID
4	Log files of critical ICT systems or ICT systems with sensitive data must be kept for 180 days.	TM/ID
5	Access to sensitive data must be traceable (logs).	TM/ID

6.14 Emergency planning

No.	Requirement	Respon-sible
1	An emergency plan must be established for all items to be protected that support a relevant business process. The emergency plan describes the planning and disaster preparedness of the item to be protected in order to ensure the maintenance and restoration of legal capacity in exceptional situations. The relevance of a business process can be determined by means of a protection needs analysis, a business impact analysis or a risk analysis.	IO/TM/ID

6.15 Physical security

No.	Requirement	Respon-sible
1	ICT systems (users' end devices are an exception) must be operated in designated rooms. The following security measures must be taken into account: • Access only for authorized persons – only identified persons who actually need access in the course of their work-related activities will be authorized. • Regular control of access permissions • Accesses should be traceable (e.g. by means of a badge system) and logged. The logs must be kept for at least 180 days • Room security measures on windows and doors • Fire detection system • Fire seals/fire zones • Flooding/water protection • Surge suppressor • Climate control	MD

6.16 Outsourcing/cloud

No.	Requirement	Responsible
1	A contract must be concluded with each ICT service provider which, depending on the service purchased, "at least" regulates the following aspects: • Maintenance and support • License management • Information security and data protection requirements (GTC/ISDS) • Reporting security and privacy incidents • Disaster and emergency preparedness (for critical services) • Audit and the right to audit • Non-Disclosure Agreement • Regulation on outsourcing data processing (when processing personal data)	MD
2	An inventory of all external service providers and services must be created and kept up-to-date. The inventory must contain at least the following information: • Service provider • Contacts • Criticality of the service and outsourced data	ISO
3	When outsourcing critical services or sensitive data/information, a risk analysis must also be carried out in advance, in which the essential aspects of data protection and information security are examined in particular. Furthermore, an exit strategy must be created that shows how the services/data can be withdrawn/taken back or outsourced to another partner in the event of an emergency.	MD

7. Glossary/referenced documents

Terms/abbreviations	Description
GTC/ISDS	General Terms and Conditions (GTC) relating to ISDP in performing IT services for the IT Services Office of the University of Bern.
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.
CIS controls UniBE	Sheet for conducting a gap analysis and identifying risks.
ICT systems	Information and Communication Technology ICT: All devices (hardware) and applications (software) used to store, process, and transmit data, information and voice.
Collections 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.
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.
OWASP	The Open Worldwide Application Security Project (OWASP) is an open community committed to enabling organizations to develop, acquire and maintain trusted applications and APIs.
Risk analysis	Document for assessing and documenting ICT risks
RPO	Recovery Point Objective = maximum data loss
RTO	Recovery Time Objective
Protection needs analysis	SchuBAn – a tool for identifying critical, sensitive data and information.
Sensitive data/information	Data/information that, according to the protection needs analysis are in greater need of protection.
Technical resources	ICT systems, functions or services of an ICT system.
Directives on Information Security Governance	The Directives on Information Security Governance define the basic objectives, principles, responsibilities and processes of information security at the University of Bern.
Critical systems/services	Are facilities, systems or parts thereof that are essential for the maintenance of important functions and services at the University of Bern.
Particularly sensitive personal data	Particularly sensitive personal data includes: Information on religious, philosophical, political or trade union views or activities, health, privacy or race, social assistance measures and administrative or criminal prosecutions and sanctions. Personality profiles: Compilation of data that makes it possible to perform an assessment of essential aspects of a natural person's personality. Profiling: automated processing of personal data to evaluate, analyze or predict certain personal aspects. Genetic data and biometric data that uniquely identify a natural person.
DSG/ KDSG	The FADP is the Federal Act on Data Protection and applies to both private individuals and federal bodies. The KDSG is the Cantonal Act on Data Protection and applies to cantonal authorities such as the University of Bern.
Hardening guidelines	Minimum requirements which must be taken into account.

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, December 5, 2023

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

Prof. Dr. Christian Leumann
Rector