UNIVERSITÄT
BERN

Administrative Director's Office

IT Services Office

General Terms and Conditions (GTC) relating to ISDP in performing IT services for the IT Services Office of the University of Bern

1. General terms and conditions

1.1 Purpose

The purpose of the GTC is to protect the personal rights of people whose data is processed and to guarantee information security when IT services are performed by service providers for the University of Bern.

1.2 Object and scope

These GTC apply to IT services that are performed by service providers for the University of Bern and that involve processing data, as well as to any of the service providers' related business processes.

These GTC also apply to subcontractors, representatives, auxiliaries, and employees of the service providers that work with University of Bern data, systems, and processes.

1.3 Relationship to contractual provisions

These GTC form part of a contract between service providers and the University of Bern. If these stipulate that other GTC apply, for instance the GTC of the Swiss Conference on Informatics (GTC SIK), the provisions of these GTC shall supersede the information security and data protection provisions of the other GTC.

Otherwise, the provisions of the other parts of the contract shall take precedence over these GTC.

2. Rights and obligations

2.1 Information obligation

At the request of the University of Bern, service providers shall provide information and documentation pertaining to the methods and processes used to perform the contractual services that are relevant to compliance with ISDP. The University of Bern shall be entitled to consult those documents in situ and to see a demonstration of the relevant operating procedures.

Service providers shall inform the University of Bern about any extraordinary events that affect the data, systems and processes of the University of Bern, for instance serious violations of ISDP.

2.2 Complying with basic ISDP security

Service providers shall ensure basic ISDP security in accordance with Annex 1 of these ISDP GTC.

2.3 Complying with additional ISDP regulations in accordance with the ISDP concept

If the ISDP requirements of the University of Bern exceed the level of basic ISDP security, the contract contains an ISDP concept that shall govern the relevant requirements and measures.

2.4 Obligations in accordance with data protection law

Service providers acknowledge that Art. 16 of the Cantonal Data Protection Law of February 19, 1986 (KDSG, BSG 152.04) states:
"Anyone who processes personal data on behalf of an authority is subject to the law in the same way as the client. They require the express permission of the client to disclose personal details to third parties."

2.5 Involvement of third parties

The contract or any other applicable GTC shall determine whether and under what circumstances service providers may involve third parties. However, a written confidentiality agreement in accordance with Paragraph 2 is always a prerequisite for involving third parties.

The service providers shall commit any third parties involved (Clause 1.2 Paragraph 2 of these GTC) in writing to maintain confidentiality (Clause 2.6) and shall stipulate compliance with the statutory and contractual ISDP provisions in the employment contract along with staff employed at the University of Bern. They shall inform these third parties about the statutory and contractual ISDP provisions.

2.6 Confidentiality

Facts and data which are neither evident nor publicly available shall be kept confidential. In case of any doubt, facts and data shall be treated confidentially. Duties of confidentiality shall also apply before the contract is concluded and after termination of the contractual relationship or after the agreed services have been performed. Statutory information obligations shall remain reserved.

2.7 Disclosing data and information

Unless otherwise authorized, service providers may only use University of Bern data for the university and may only disclose it to the university. Information disclosure requests by private parties (whether or not affected by the processing of the data) or other entities shall be forwarded to the University of Bern.

2.8 ISDP audits

With regard to its data, systems and processes, the University of Bern can arrange for ISDP audits to be carried out on the service providers. The audits are performed by internal or external, professionally independent experts following widely accepted methods. The service providers are not obliged to work with auditors who are their competitors. The University of Bern shall make the audit report available to the service providers.

If the service providers are certified in accordance with widely accepted information security and data protection standards and are regularly audited as part of this, they shall provide the University of Bern with the audit report insofar as this affects the data, systems and processes of the University of Bern.

The contract shall govern the specifics if this is the case.

2.9 Supervision and control

When dealing with the University of Bern's data, systems and processes are involved, the service providers are subject to supervision by the Cantonal Data Protection Supervisory Authority (Art. 32ff. FADP), supported by the IT security officer (IT SO) of the Cantonal Department of Informatics and Organization.

The Data Protection Supervisory Authority can carry out controls or have controls carried out as part of its statutory function. The service providers shall support them in this without payment.

2.10 Support from the service recipient

The University of Bern shall support the service provider in performing its obligations in accordance with these GTC.

3. Sanctions

If Clause 2.5 Paragraph 2, 2.6, and 2.7 of these GTC are violated, the provisions of the applicable GTC SIK, January 1, 2004 version on sanctions in the event of violation of duties of confidentiality shall apply (GTC SIK 1, Clause 12.4; GTC SIK 2, Clause 7.4; GTC SIK 3, Clause 9.5; GTC SIK 4, Clause 8.4; GTC SIK 5, Clause 9.4). If the contract does not state that any of the GTC SIK are applicable, Clause 12.4 of the GTC SIK 1 shall apply to purchasing overall IT systems as well as to producing individual software.

4. Place of jurisdiction and applicable law

Where other constituent parts of the Agreement do not stipulate the place of jurisdiction or applicable law, the jurisdiction shall be Bern and Swiss law shall apply without regard to conflict of law provisions.

UNIVERSITÄT BERN

Administrative Director's Office

IT Services Office

Annex 1: Basic ISDP security

Basic ISDP (information security and data protection) security measures are based on the basic ISDP security certification that was prepared in collaboration with the Data Protection Supervisory Authority of the Canton of Bern.
The provisions of the basic ISDP security measures catalog for which the service providers are responsible are set out below. Any particulars specific to the service must be governed in the contract (Clause 2.2 of the ISDP GTC)

1. Access controls (physical)

Goal: Preventing unauthorized people from accessing rooms in which University of Bern data is being processed.

1.1 Organizational measures

1.1.1 Sensitive rooms (e.g. server rooms, rooms with essential telecommunications equipment, rooms holding back-up copies, archives) must be designated as security zones.

1.1.2 Access to computer rooms and resources must be regulated using binding and traceable access authorization. This must be appropriately graded.

1.1.3 A locking up plan must be prepared and documented that governs how the means of access are administered, issued and returned and who is responsible for them.

1.2 Technical measures

1.2.1 The entrances to the security zones must have a secure locking and entry system.

1.2.2 Locking and entry systems must be checked regularly to make sure they are working properly.

1.2.3 Access via other openings to the building must be prevented using room security measures such as bars on windows, security shutters, etc.

2. Access controls

Goal: Preventing the unauthorized use of IT systems, services, and applications and communications equipment as well as access to data output from the University of Bern.

2.1 Organizational measures

2.1.1 The process of issuing user rights must be compulsorily regulated, documented and monitored.

2.1.2 Accounts and access rights that are no longer needed (e.g. when a user leaves) or that have not been used for a long time must be disabled or deleted.

2.1.3 In areas open to the public (e.g. counters, secretary's offices), ancillary equipment such as screens and printers must be placed such that unauthorized people are not able to view any data.

2.2 Technical measures

2.2.1 Authorized access to systems is via a user ID and secure password. A secure password comprises at least eight characters and contains characters from at least three categories. More details on the categories can be found at https://ktools.unibe.ch.

Passwords are personal and secret.

2.2.2 Failed access attempts (blocked accounts) must be recorded and the records must be analyzed regularly.

3. Access controls (logical)

Goal: Preventing unauthorized access to University of Bern data by authorized system users.

3.1 Organizational measures

Not relevant under these GTC.

3.2 Technical measures

3.2.1 Users must identify and authenticate themselves on the system with a personal user ID and a secure password (see Paragraph 2 above).

4. Disclosure controls

Goal: Preventing loss of confidentiality, availability and integrity of University of Bern data during transfer.

4.1 Organizational measures

4.1.1 Data storage devices (paper, discs, CDs, etc.) with classified data must be marked and recognizable as such.

4.1.2 Data storage devices must be packed and addressed appropriately when posting.

4.1.3 Measures must be taken to determine and control which users and operators are permitted to use which network services.

4.2 Technical measures

4.2.1 The confidentiality and integrity of authentication data, keys or other critical system data must be protected when transferring data via the network.

4.2.2 Transfers from/to external networks must be recorded (connection set-up, user).

5. Input control

Goal: Conserving evidence relating to user activities

5.1 Organizational measures

5.1.1 It must be compulsory to regulate who is permitted to process which data and who bears responsibility for data protection and data quality.

5.2 Technical measures

None stipulated.

6. Order controls

Goal: Guaranteeing that University of Bern data is processed in accordance with orders.

6.1 Organizational measures

Not relevant under these GTC.

6.2 Technical measures

6.2.1 Access must be limited to specifically defined data and applications.

6.2.2 External access via the network must be prevented using sound authentication procedures.

7. Availability controls

Goal: Protecting University of Bern data from limited availability, destruction and loss.

7.1 Organizational measures

7.1.1 Authentication data belonging to people responsible for the system or other privileged system operators must be stored in a secure form for use by a representative in the event of an emergency.

7.1.2 Any documentation necessary for safe operation and for use and maintenance of systems and applications must be available from those responsible for the systems and applications at all times.

7.2 Technical measures

7.2.1 Computer rooms and systems must be appropriately protected against physical factors (break-in, fire, water, etc.).

7.2.2 Systems must be safeguarded using overvoltage protection, an uninterruptible power supply (UPS) and by an appropriate air conditioning system.

7.2.3 Procedures for backing up data to storage devices and restoring data must be regularly monitored.

7.2.4 Mobile data storage devices must be kept in a protected place that is separate from the operational environment.

8. Separation controls

Goal: Ensuring compliance with the requirement to state a purpose

Extract from Art. 5 KDSG (Canton Data Protection Law):

- The purpose of the data processing must be defined.
- The personal data and type of processing must be suitable and necessary for fulfilling the task.

8.1 Organizational measures

Not relevant under these GTC.

8.2 Technical measures

8.2.1 Test and production data must be processed separately. A reliable and logical form of separation is sufficient.

9. Other control goals

Goal: Overall guarantee of information security

9.1 Organizational measures

9.1.1 Suitable precautions must be taken in case of malfunction, emergency and catastrophe.

9.2 Technical measures

9.2.1 Systems and applications must be protected against malicious software (viruses, spyware, etc.) using recognized procedures and products.