SOP
DATA PROTECTION

Document number	1.02.004
Version	1.0
Category	Resource Management
Sub-category	IT
Authored by	Swiss Biobanking Platform
Effective date	

TABLE OF CONTENT

A. GENERAL INFORMATION ..... PAGE 2
- **A1. Scope**
- **A2. Objectives**
- **A3. Abbreviations and definitions**

B. PERSONNEL MANAGEMENT ..... PAGE 2
- **B1. Roles and responsibilities**

C. PROCESS MANAGEMENT ..... PAGE 3
- **C1. Procedures for data protection**
- **C2. Quality control**

D. RESOURCE MANAGEMENT ..... PAGE 4
- **D1. Materials and equipment**

E. REFERENCES ..... PAGE 5
- **E1. Reference to laws, regulations, and guidelines**
- **E2. Reference to other sbp documents**
- **E3. Appendices**
- **E4. Revision history**

SWISS BIOBANKING PLATFORM

A. GENERAL INFORMATION

A1. SCOPE

Biobanks are responsible and accountable for guarantying the privacy of the participants and safeguarding the integrity and confidentiality of the associated data stored in the Biobank database. This SOP covers the procedures for data protection by controlling the access to information and by preventing data loss, misuse, and damage.

A2. OBJECTIVES

- Ensure that the privacy rights of participants are protected.
- Ensure the authenticity, confidentiality, and integrity of data stored in the Biobank database.
- Ensure that only authorised qualified personnel access the Biobank database.
- Ensure that IT safety measures are implemented to prevent data loss, damage, and misuse.

A3. ABBREVIATIONS AND DEFINITIONS

For this document, the following abbreviations apply.

BB = Biobank
BIMS = Biobank Information Management System
QR = Quality Representative
SBP = Swiss Biobanking Platform
SOP = Standard Operating Procedure

See SBP Glossary for definitions of associated data and other terms

The SBP SOPs are based on Good Biobanking Practices to ensure an optimal setup for the biobanking activities.
Additionally, the SBP SOPs can serve as a reference for BBs to develop site-specific Work Instructions.

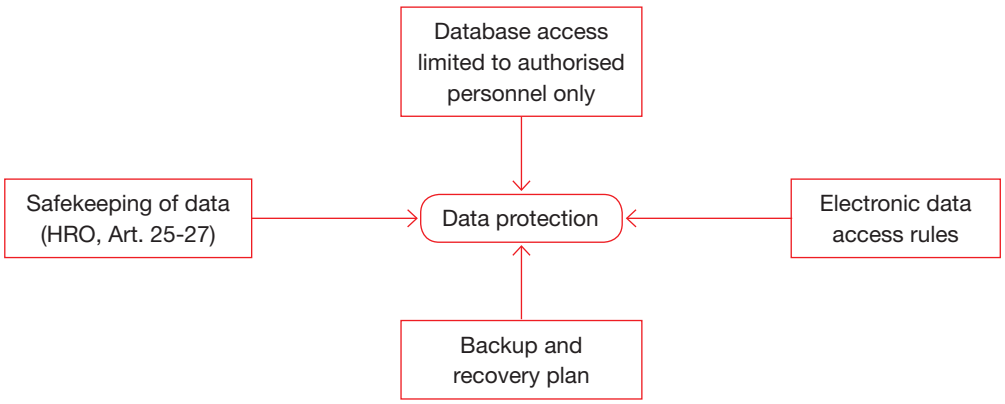
B. PERSONNEL MANAGEMENT

B1. ROLES AND RESPONSIBILITIES

BB personnel	Responsibility / role
BB Manager/Director	› Appoints Key-keeper › Administers confidentiality agreements › Authorises personnel to access the database › Defines backup and recovery plan
Key-keeper	› Keeps the key to coded data › Protects the key from disclosure
Qualified personnel	› If authorised, access the database
IT personnel	› Implement and administer the backup system › Recover data, when necessary › Implement IT safety measures › Require the use of “strong” passwords
QR	› Performs Quality Control

C. PROCESS MANAGEMENT

C1. PROCEDURES FOR DATA PROTECTION



C1.1. Limited access to authorised personnel

- The access to the database shall be granted to the personnel who are authorised to enter, audit, access, and process data stored in the database, according to the tasks described in the Personnel file (Document 2.02.001).
- When appropriate, the BB Manager/Director shall administer a confidentiality agreement to guests, visitors, outsourced employees, auditors/inspectors, and newly authorised/employed personnel.

C1.2 Electronic data access rules

- IT personnel shall implement IT safety measures to prevent and detect security breaches of the database.
- Electronic data access should be monitored, audited, and documented.
- IT personnel should require the use of “strong” (or non-intuitive) passwords to access the database. The definition of “strong” password should be included in the BB Work Instructions.
- IT personnel should encourage the personnel to log off from the database when moving from the workplace.
- Accounts shall be unique and personal. Shared accounts or access to the database with another user’s account shall be forbidden.
- The passwords allowing access to data shall be kept confidential. Personnel shall not share with anyone nor write down the password.
- IT personnel should require BB personnel to change the passwords on a regular basis.
- If an account or a password is suspected to have been compromised, the password shall be immediately changed or the account shall be blocked, following the procedures reported in the Non-conformity Management SOP (Document 1.04.002).

C1.3 Safekeeping of coded data

- In the presence of coded data, a Participant Identification Log (Document 2.01.002) shall be filled out for each participant. Since this document allows the coding/decoding of participant’s biological resources, it shall be kept confidential.
- At no time, the Participant Identification Log (Document 2.01.002) shall be copied or given outside the BB or to any person involved in the research project.
- A key-keeper shall be appointed by the BB Manager/Director to access and manage the Participant Identification Log (Document 2.01.002). The appointed key-keeper shall not be involved in the research project based on the coded data of which he/she has the key, according to the Human Research Ordinance (HRO) of 20 September 2013, 2013 (Status as of 1 January 2018) Art. 26:
  The key must be stored separately from the material or data collection and in accordance with the principles of Article 5 paragraph 1, by a person to be designated in the application who is not involved in the research project.

- The decoding of human participant's biological resources shall follow the Human Research Ordinance (HRO) of 20 September 2013 (Status as of 1 January 2018), Art. 27:
  For coded biological material and coded health-related personal data, the code may only be broken if:
  - breaking the code is necessary to avert an immediate risk to the health of the person concerned;
  - a legal basis exists for breaking the code; or
  - breaking the code is necessary to guarantee the rights of the person concerned, and in particular the right to revoke consent.

C1.4 Safekeeping of anonymised data

- In the presence of anonymised data, qualified personnel should ensure that the personal data are irreversibly masked or deleted, in agreement with the Human Research Ordinance (HRO) of 20 September 2013 (Status as of 1 January 2018), Art. 25:
  - For the anonymisation of biological material and health-related personal data, all items which, when combined, would enable the data subject to be identified without disproportionate effort, must be irreversibly masked or deleted.
  - In particular, the name, address, date of birth, and unique identification numbers must be masked or deleted.

C1.5 Safekeeping of anonymised data

- The BB Manager/Director together with the IT personnel shall define and implement a backup routine and recovery plan to protect data against misuse, loss, and damage.
- The backup shall be performed automatically and on a regular basis. The frequency of the backups is defined by the BB Work Instructions and depends on the frequency of data modifications.
- In case of user error, failure of equipment, catastrophic event, or deliberate intrusion or hacking, the personnel shall implement Immediate Corrective actions and follow the procedures described in the Non-conformity Management SOP (Document 1.04.002).
- Documentation related to the implementation of backup routine and recovery plan shall be made accessible for internal and external audits, as further explained in the Internal audit SOP (Document 1.04.004).

C2. QUALITY CONTROL

- Control that the personnel, which are authorised to access the database, are qualified and trained to access data, according to the job descriptions in the Personnel file (Document 2.02.001) and as explained in the Personnel Management SOP (Document 1.02.001)
- Control that the appointed key-keeper is not involved in the research project based on the coded data of which he/she has the key.
- Control that the backup is up-to-date so that the database can be entirely and accurately recovered.
- Every time the QR performs quality control on the process outputs, quality control details (date of QC, outcomes) shall be recorded in the Quality Control Results (Document 2.04.009).

D. RESOURCE MANAGEMENT

D1. MATERIALS AND EQUIPMENT

The materials and equipment in the following list are recommendations only and may be substituted by alternative/equivalent products more suitable for the specific task or procedure.

Materials and equipment
Backup hard disks

E. REFERENCES

E1. REFERENCE TO LAWS, REGULATIONS, AND GUIDELINES

- SBP - Ethical, legal and professional compliance list for human research biobanks applicable in Switzerland [Status as of 1 March 2018]

E2. REFERENCE TO OTHER SBP DOCUMENTS

- 1.04.001 Document Management SOP
- 1.02.001 Personnel Management SOP
- 1.04.002 Non-conformity Management SOP
- 1.04.004 Internal Audit SOP

E3. APPENDICES

- 2.02.001 Personnel file
- 2.02.006 Participant Identification Log
- 2.04.009 Quality Control Results.

E4. REVISION HISTORY

Document number	Revision date	Author	Details of revision
1.02.004		SBP	Initial release