Acceptable Use Policy of SIB's IT Infranstructure

Version 2.0, 4 September 2020

Art. 1 Purpose

The SIB Swiss Institute of Bioinformatics provides a secure IT Infrastructure and services to support biomedical researchers in Switzerland and beyond (the "**IT Infrastructure**"). The IT Infrastructure allows for **processing of sensitive personal data** which require specific protection, in particular strict access restrictions. This is essential to guarantee **data confidentiality, integrity and availability** of the IT Infrastructure and all Data. Accordingly, this Acceptable Use Policy (the "**Policy**") defines the rules that each User of the IT Infrastructure must comply with when accessing and using the IT Infrastructure. **This Policy applies in addition to the SPHN Information Security Policy** (the "**ISP**") [1]. All Users must read and comply with all provisions of the ISP.

Art. 2 Terms and Definitions

Definitions of the terms **User, Project Leader** and **IT Infrastructure** are identical with the ones used in the ISP. **Data**: a set of files transferred to and processed on the IT Infrastructure for a specific scientific project under the responsibility of the Project Leader. Data can contain ‘sensitive personal data’ or other information. Furthermore, sensitive personal data is typically classified as ‘confidential’ in the context of SPHN/BioMedIT unless explicitly classified differently (see ISP).

Art. 3 Scope

This Policy applies to all Users who use or have access to the IT Infrastructure.

Art. 4 Roles and Responsibilities

For each scientific project that is carried out on the IT Infrastructure, an explicit Project Leader must be assigned who is responsible for the project and all Users accessing the IT Infrastructure and specific Data in relation with the project. Therefore, this policy explicitly distinguishes between the following roles which come with distinct responsibilities:

- **Project Leader**: person having full responsibility for the scientific project carried out on SIB's IT Infrastructure.
- **User**:person who is explicitly authorized by a Project Leader to access the IT Infrastructure and the respective Data. SIB can only grant access to a new User if the

Project Leader or an authorized delegate (such as a Permissions Manager [2]) gives explicit written consent (e.g., via Email). A Project Leader can also obtain an account on the IT Infrastructure: in this case, she/he needs to take all responsibilities of a User, too.

SIB acts as IT Infrastructure provider and therefore as Processor with respect to Project Leaders (Controllers) and Data Providers (Controllers).
A detailed summary of a the responsibilities of Project Leaders and Users is provided in Section 5.2 Project Leaders, Users and Responsibilities of the ISP. In this policy, a short summary is given, but **each Project Leader and User is expected to read and comply with the latest version of the ISP**.

Art. 5 Responsibilities of a Project Leader

1. Ensure that all **Data have been lawfully obtained and are lawfully handled** according to this Policy and all other applicable laws and regulations.
2. Apply **Data Classification** for all Data transferred to the IT Infrastructure as stated in Chapter 4 ISP, i.e., declare data as "confidential" where applicable. Note that "All Personal Data are classified as Confidential Data unless explicitly classified differently".
3. Execute a **Data Transfer and Use Agreement** or **Processing Agreement** where applicable.
4. Provide the **information** necessary to complete SIB's register of **processing activities**.
5. Submit **access requests for Users** - including immediate notification once access is no longer required. This responsibility can be delegated to a **Permissions Manager** [2] who is accountable to the Project Leader.
6. Take care of **data life cycle** for Data processed on IT Infrastructure (including removal of Data if access is no longer allowed or required).
7. Proactively **inform** IT infrastructure provider and SIB Data Protection Board and Security Board as soon as a data breach is identified.
8. Proactively **cooperate** with SIB and respective authorities in **case of data breaches**.

Art. 6 Responsibilities of a User

1. **Use** the IT Infrastructure and the Data only to the extend required for, and in a manner that is consistent with, the intended scientific research, in accordance with all applicable laws. All other uses are strictly forbidden.
2. **Follow** a Data Privacy and IT Security **training** and **present a respective certificate** of achievement of BioMedIT's Data Privacy and IT Security exam [3].
3. Take all the necessary actions to **secure the account** and preserve the confidentiality of respective credentials that are necessary to access the IT Infrastructure. In particular, Users must not share their credentials with any other person or store them in clear text in password directories.
4. **Install/manage a second factor** required for the Two Factor Authentication.
5. Take all necessary actions to **protect the confidentiality, availability and integrity** of all **Data** which is not public. Do not share such data with unauthorized personnel!
6. Ensure that all **Data transferred** to and from the IT infrastructure are **encrypted**.
7. **Report all irregularities** observed regarding the use of the IT Infrastructure and respective Data.

8. Do not circumvent any access protection or restriction mechanism, nor use or try to gain access to any Data which the User is not entitled to access.
9. **Inform** the Project Leader – and, for Project Leaders, SIB – immediately in case of a **data breach** or the identification of any other issue related to data integrity or security, and assist, to the best of their ability, with any investigation and attempts to stop and/or remedy the breach.
10. **Do not** install or use any software on the IT Infrastructure that might harm other Users, projects or the IT Infrastructure.
11. **Do not** connect to the IT Infrastructure or store Data on removable media without the prior written authorization of the respective Project Leader.
12.

Art. 7 Monitoring

SIB monitors compliance with this Policy and IT Security Training in accordance with data protection laws. It reserves the right to monitor activities on the IT Infrastructure on an individual basis where it suspects that there has been a breach of this Policy or the ISP.

Art. 8 Non-Compliance

A User who violates or circumvents this Policy or the ISP will have her/his access revoked, and her/his host institution will be notified immediately (disciplinary actions may follow).

Some violations may also constitute violations of laws or regulations and result in civil or criminal penalties.

Reference

[1] SPHN Information Security Policy

[2] BioMedIT User Management SOP, PHI_SOP-003_User Management_v1.0, 15 July 2020.

[3] BioMedIT Data Privacy and IT Security Training and on-line exam

Approval

This policy was approved by the **SIB Data Protection and Security Board** on 4 September 2020.

- Valérie Barbié, Head of Clinical Bioinformatics
- Marc Filliettaz, Data Protection Officer
- Mark Ibberson, Head of Vital-IT
- Warren Paulus, Cyber Security Officer
- Heinz Stockinger, Head of Core-IT