Swiss Institute of Bioinformatics

Terms of Use

Version 1.0, 21 June 2021

Objective

The following document defines the Terms of Use (ToU) of IT services offered by the SENSA platform (sensa.sib.swiss) dedicated to a **specific research project** dealing with sensitive personal data.

Table of Contents

1 Service Description

1.1 Overview

The **S**ecure s**ENS**itive data processing pl**A**tform (**SENSA**) offers biomedical researchers a full service for the processing of sensitive data, from a tailored compute and storage environment to expertise in data protection and bioinformatics support. SENSA being connected to the national network of secure IT infrastructures (BioMedIT), it also acts as a gateway to the Swiss Personalized Health Network (SPHN.ch) to enable nationwide biomedical projects.

A basic overview of the service components is provided below:

Access control

- **Access** to the platform is restricted to **trusted network locations** such as white-listed IP addresses or ranges (incl. VPN)
- Federated identity management via SWITCH *edu-ID*, including 2-factor authentication (2FA)
- **Isolation of distinct project spaces** via **virtualization** based on *OpenStack* technology, compliant with the legal requirements for sensitive personal data
- **Network-protected project space**: By default, there is no inbound nor outbound network connection to/from a project space. If external services need to be accessible, network access needs to be explicitly requested, and the service request will be reviewed.
- Users interact with the platform through a **remote desktop in a web browser** (via the Apache *Guacamole* web application) or through a Secure Shell (SSH)-based terminal

Encrypted transfer and storage

- **Encrypted data transfer** into and out of the platform via a Secure File Transfer Service and the sett tool (https://sett.readthedocs.io)
- Superior data protection via an **encrypted storage system** (*WekaIO* and *Ceph*)
- Unless agreed otherwise, the infrastructure providers have no access to the data

Hardware resources

- 10 CPU nodes with 40 cores each (400 CPU cores in total) - 64 to 512 GB RAM
- 2 GPU nodes with 20 cores each (graphics cards for optimised computation) - 64 GB RAM
- 200 TB of encrypted storage

Virtualized services

- By default, services are provided using the GNU/Linux operating system, currently, mainly CentOS 7 and 8.
- In exceptional cases, software might be deployed on Windows but this requires specific licenses and extra costs.

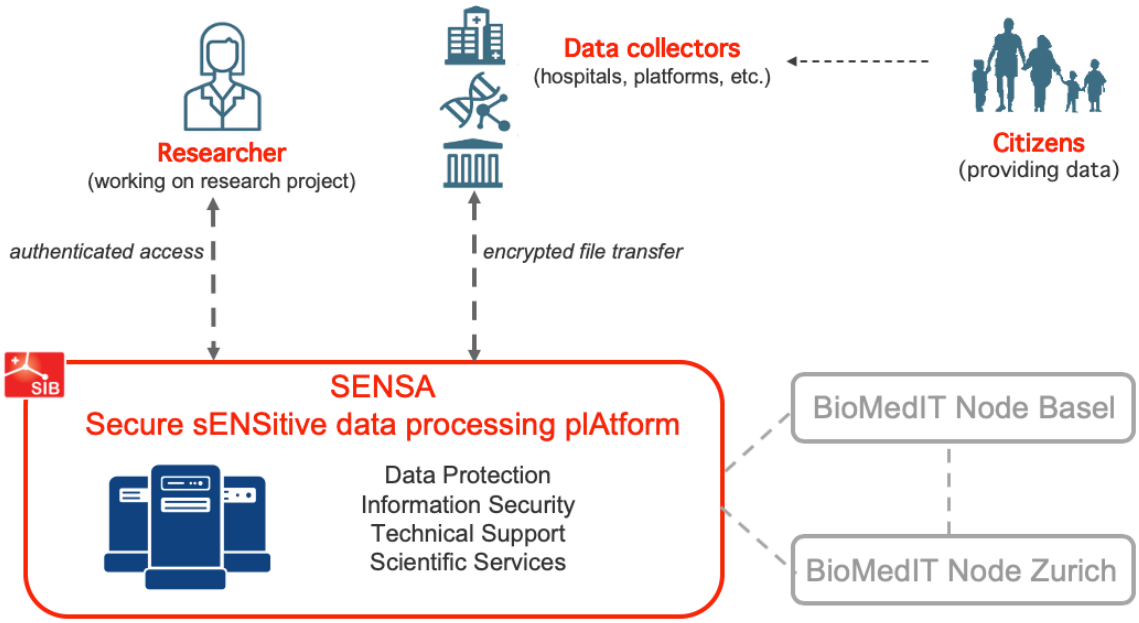

Figure 1. Overview of the SENSA platform. Note that SENSA typically receives sensitive personal data via Data Providers (called “Data collectors"), rather than via direct interaction with citizens.

1.2 Scope

This SLA applies to the service components that are part of SENSA. In particular, services hosted in SIB’s VMware, OpenStack and Weka systems.

1.3 Ordering and Costs

For enquiries and ordering resources in SENSA, please contact it-support@sib.swiss.

The costs related to the service provision are available upon request.

Invoicing is done twice a year.

The **basic service maintenance package** includes:

- Installation of one or more virtual machines (VM)
- Installation and basic configuration of web server(s)
- Installation and updates of client software packages in project space (typically, open-source software running on supported operating systems)
- IP whitelisting for end users
- Regular updates with the latest security patches. Customers are informed at least three days in advance except for emergency situations or in case of an immediate security risk.
- Regular backups, as agreed with the Customer
- Reviewing, authorizing and setting up of inbound/outbound network connections
- Minor system administration tasks (adding new users, changing configuration of systems and firewalls, etc.).

The following services are not included in the basic package and require additional support hours at extra costs:

- Major upgrade of the Linux operating system

- Installation and configuration of complex services
- Scientific data management services (e.g., installation/configuration of a data management system, data preparation, analysis, etc.)
- Backup restoration
- Licenses for commercial software applications.

2 Service provided to the Customer

For each Customer (usually a research group) a tailored service is provided that serves a well-defined scientific project which requires access to and processing activities of sensitive personal data. The service can include one or several virtual machines that are operated in a protected environment. A project space can contain encrypted storage, compute nodes and additional services installed upon request.

The detailed services need to be defined by the Project Leader and discussed with the SENSA personnel before the service can be made accessible.

2.1 Project phases

In order to allow for production use of a service in the project space, the service activation for a project goes through the following phases, which might take from one to several weeks.

Each scientific project is divided into the following phases:

- **Definition of requirements**
  - Definition of hardware infrastructure (virtual machines, storage capacity, network connectivity), software services and tools to be installed as well as data management needs.
  - Preparation and signature by the Customer of the legal documents concerning sensitive personal data, approved by SIB Legal department. For instance, a Data Transfer and Processing Agreement (DTPA) needs to be worked out with the legal departments of SIB and the Customer.
  - If personal data is to be transferred and used, the Customer should demonstrate compliance with law (e.g., ethical approval by the relevant ethics commission if appropriate).
- **Installation and test phase**
  - Installation and configuration of the individual service components (incl. the network settings to access the service from outside SIB's network).
  - Security review of all components. SIB typically reviews all components that are planned to be installed and might suggest changes to comply with common security standards and best practices.
  - The installation and configuration scope must be defined upfront as the support work of SIB may require support fees that are beyond the basic maintenance package (see Section 1.3).
- **Pre-production**
  - In this phase, the project space can only be used with test data, not with real data.
  - External (web) services of the Customer must therefore not yet assume production quality of services in project spaces: only preproduction tests are tolerated.
- **Production**

    - Production can start once the technical setup is finished, and all legal requirements and documents are signed (e.g., DTPA). The quality of service as defined in Section 3 will be ensured.
    - If sensitive personal data are used, an entry to the Record of Processing system [1] must have been completed where applicable. The relevant information must be provided by the Customer and is filled in by SIB into the system.
- **End of life**
    - Each project needs to have a clearly defined end. That date determines the end of the service provided to the Customer. The end date of service may however be extended in the course of a project by mutual agreement between SIB and the Customer. However, SIB is not committed to accepting such an extension.
    - SIB needs to return and/or remove all data within the provided project space, as per the legal documents.
    - All user access is removed, and the infrastructure is released.
    - Backups can be provided to the Customer on demand before definitive closure of the project.

Within the limits of availability, the compute and/or storage capacity can be increased at any time during the production phase. However, such an increase may result in a planned service downtime, as well as additional costs.

2.2 Minimal Service

The minimal service to be set up for an individual project consists of the following components:

- URL: project-name.sensa.sib.swiss.
- Guacamole: web interface to project space.
- Project space with a single virtual machine using 2 CPU-cores, 4 GB RAM and 200 GB of encrypted disk space on Weka.
- SFTP access to upload data to the project space
- Access for 2 users using edu-ID accounts and 2-factor-authentication (eduid.ch)
- Regular backups on a project-specific basis.

Alternatively, instead of a Guacamole web portal, an internet-facing web server can be provided. This requires additional security checks on the web application which result in higher costs that are not included in the minimal service.

2.3 Access to the service

Access to the service can be provided at several levels, covering the following roles:

- **User**: access via edu-ID account and 2FA. Each User needs to sign the Acceptable Use Policy (sib.swiss/aup) and must be trained in data privacy and IT security before accessing the infrastructure:
  https://edu.sib.swiss/course/view.php?id=424
- **Privileged user**: this is a Linux account with specific privileges to operate a service. For instance, a privileged user might have sudo rights to restart a web server.
- **Service provider**: that can be an external Service Provider who requires root access on identified machines to install and/or operate a service. A Service Provider typically

receives (temporary) SSH-based access to access a specific machine. An explicit non-disclosure or confidentiality agreement needs to be signed for each Service Provider.

2.4 Scope of service

SENSA is dedicated to scientific projects dealing with sensitive personal data requiring a high level of IT security and data protection.

Compute or data intensive scientific projects only dealing with open data or non-sensitive data are not intended for use on SENSA. For these types of applications, the relevant HPC infrastructure of each academic or research institution should be used.

2.5 Compliance

The Customer must ensure that all legal and ethical requirements are fulfilled and is accountable for the activities of all users under their supervision.

3 Quality of Service

3.1 Service availability

Technical support is provided during **business hours**:

- 9:00 – 17:00 on normal workdays from Monday to Friday
- Not included: public holidays of the Canton of Vaud and weekends

Outside business hours, services are provided on a “best effort” basis. No 24x7 support is provided.

3.2 Backup and disaster recovery

By default, data stored in Weka is kept highly redundant and fault tolerant. The system automatically deals with hardware and software failures to guarantee maximum availability of sensitive data.

User errors such as unintended modification or deletion of data are not prevented but can be mitigated by **activating backups** with data versioning.

Additional **backup** of data and service information can be done **on request**.

Natural catastrophes or disasters yielding to the full or partial destruction of the SENSA hardware or software are not covered.

Electric power failures are covered by a redundant UPS and a respective generator. That allows SENSA to be functional even if there is a temporary, unforeseen power cut.

3.3 Downtimes and planned service maintenance

Any planned service downtime is announced at least **3 days** in advance.

In case of emergency or catastrophic failures, services might be **shut down** any time without prior notice.

Interruptions may also occur in case of failure of a critical, non-redundant component, or in case of simultaneous failure of redundant components.

3.4 Security

The architecture of the SENSA platform follows the BioMedIT General Security Concept [2]. The SENSA implementation can be found in [3] and is outlined in Figure 2.

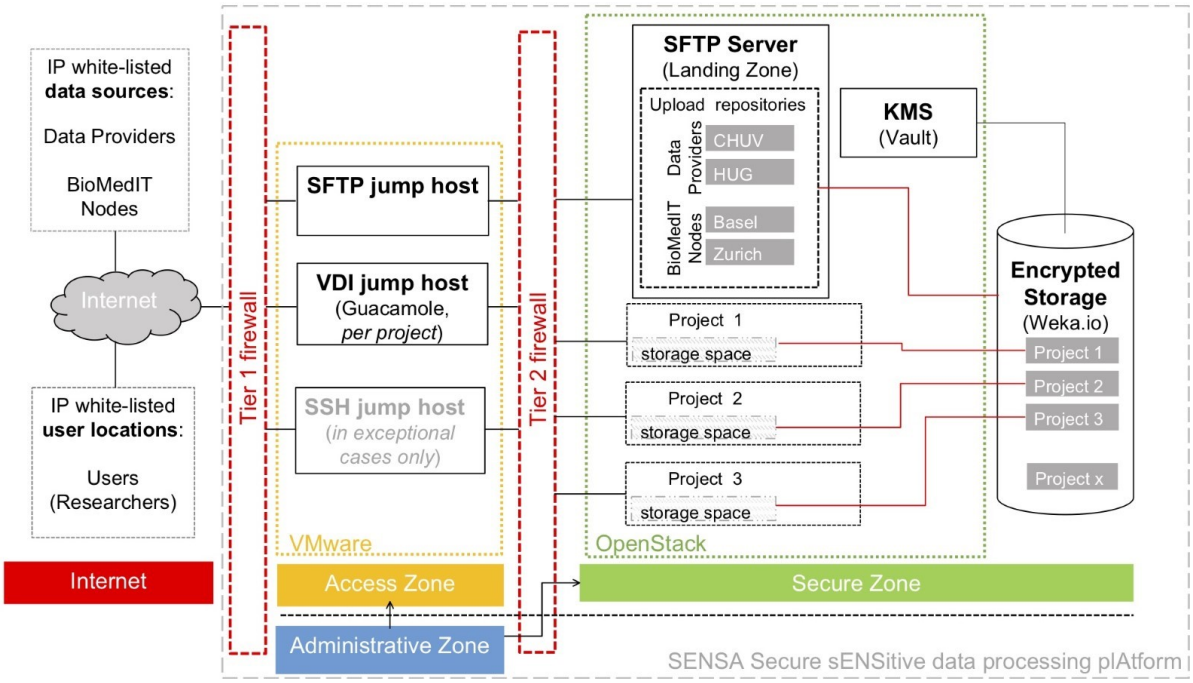

Figure 2. SENSA's security architecture and implementation. On the left, the two main stakeholders are shown: Data Providers and Users (researchers). In order to grant them access to SENSA, their network locations must be trusted, and their IP addresses need to be white-listed in SENSA's firewall. The stakeholders use different access methods (services): A Data Provider typically uses the file transfer service to transfer data to SENSA. A Researcher connects to SENSA to process/analyze data. This typically happens via a VDI/Guacamole jump host that is dedicated to a single project; SSH jump hosts are only used in exceptional cases and for specific users.

Location of the infrastructure (physical security)

The SENSA infrastructure is located in the computer centre of the University of Lausanne. Access to the machine room is granted only to authorized system administrators of SIB or UNIL. The doors of the computer room are opened on request by a security company.

Security audit of the platform

In January/February 2021, a leading Swiss IT security company did a full audit of the SENSA infrastructure, pen-testing access to the services and networks. The Executive Summary of the audit reports states:

> *Given the current implementation, the […] Security team considers that the infrastructure that hosts sensitive personal data is suitably protected against external attackers.*

Further security audits will take place on a regular basis.

3.5 Lifecycle management

In order to keep the hardware state-of-the-art, continuous maintenance is performed. As owner of the hardware, SIB reserves the right to upgrade, repair, replace or decommission any component at any time, without notifying the Customer, as long as these operations do not affect the resources or the quality of service provided to the Customer.

3.6 Monitoring

The system and the relevant services are continuously monitored for availability and performance.

Access to systems is logged. The information may be used for intrusion detection and other security purposes.

3.7 Limitations of the SLA

SIB applies the necessary effort, knowledge and personnel to avoid any issues or breaches with the SLA from the service provider side. The following cases are not considered a breach of the SLA:

- Planned and notified interruptions due to maintenance work.
- System compromise by malevolent third-parties (hackers) or software (e.g., viruses) when SIB has shown due diligence in preventing such disruptions.
- Customer-caused disruption of service.
- Force majeure (floods, earthquakes, fire, etc.).

4 Technical support

Technical support is available during business hours and can be contacted via the following email address:

> it-support@sib.swiss

A first response to a request is typically provided within two business days.

For exceptional or emergency requests, the Core-IT group can also be contacted via telephone at the numbers indicated at:

https://sib.swiss/core-it

Click on the name of the person to obtain the phone number.

References

[1] GDPR Art. 30, Records of processing activities, https://gdpr-info.eu/art-30-gdpr/

[2] BioMedIT General Security Concept, v1.0, 24 June 2020.

[3] Brief Overview of SENSA's Security Concept, v1.0, 12 June 2020