SPHN/BioMedIT Information Security Policy

Document Number: PL-001

Version: 2.0

Revision History

Version	Date	Authors	Remarks
1.0	23 Aug 2020	Document editor: Heinz Stockinger (SIB Swiss Institute of Bioinformatics). In collaboration with: Marcel Hausherr (TEMET AG), Christian Bolliger (ETH Zurich), Dorothée Caminiti (ETH Zurich), Roberto Fabbretti (SIB), Marc Filliettaz (SIB), Anja Harder (ETH Zurich), Christian Iseli (SIB), Adrien Lawrence (SPHN, SAMS), Sergio Maffioletti (University of Zurich), Warren Paulus (SIB), Gunnar Rätsch (ETH Zurich), Bernd Rinn (ETH Zurich), Torsten Schwede (SIB & University of Basel), Thierry Sengstag (SIB & University of Basel), Nora Toussaint (ETH Zurich)	First version of the Information Security Policy
2.0	8 Oct 2020	Frédéric Erard, Martin Fox, Guillermo Losilla, Warren Paulus, Bernd Rinn, Thierry Sengstag, Heinz Stockinger	Minor updates to reflect the implementation status of BioMedIT. Used DTUA instead of DUA. Clarification about exam, BioMedIT Security WG. Reference to BioMedIT Security Design. Added Section 5.3 Data Provider.

A project of SAMW ASSM
Schweizerische Akademie der Medizinischen Wissenschaften
Académie Suisse des Sciences Médicales
Accademia Svizzera delle Scienze Mediche
Swiss Academy of Medical Sciences

SIB Swiss Institute of Bioinformatics

SIB Swiss Institute of Bioinformatics
Personalized Health Informatics Group (PHI)
Elisabethenstrasse 43
CH-4051 Basel

The Personalized Health Informatics Group manages
the SPHN Data Coordination Centre and the BioMedIT project

Table of Contents

1 Purpose and Scope

The purpose of this policy is to establish a framework to meet SPHN's responsibilities in matters of Information Security with respect to compliance with the applicable regulations regarding the management, oversight and audit of Information Security. Additionally, it clarifies the roles and responsibilities of various parties relative to Information Security.

This policy applies to (i) research IT infrastructure providers at Swiss academic institutions (e.g., BioMedIT Nodes), (ii) Project Leaders, (iii) Data Providers and (iv) data Users within SPHN projects and related projects where applicable (e.g., PHRT sfa-phrt.ch). In particular, this policy defines the technical and organizational measures that are necessary to operate IT infrastructures supporting SPHN projects and provides additional technical guidelines for data protection complementing the SPHN Ethical Framework for Responsible Data Processing[1] and associated policies.

This document uses the term BioMedIT Node representative for any research IT infrastructure used in the context of SPHN. This policy does *not* apply to IT infrastructures within hospitals.

This policy is a reference and should be applied wherever possible. For research projects with special requirements, and subject to approval of the CISO of a BioMedIT Node's organization, alternative measures providing an equivalent or stricter level of security can be implemented.

Overview of typical usage scenarios and responsibilities

The following paragraphs illustrate on a non-exhaustive basis typical usage scenarios and responsibilities based on research studies performed within SPHN using the BioMedIT infrastructure. The example is provided to facilitate the understanding of the SPHN Information Security Policy and will refer to the respective chapters for technical details.

All projects performed within SPHN need to comply with the SPHN **Ethical Framework for Responsible Data Processing**[1], the SPHN Information Security Policy (i.e., this document), as well as specific policies of the respective academic host organizations.

A research project is typically led by an **Investigator** (Project Leader, Research Team leader), who is responsible for obtaining ethical approval for the planned research project[2] and entering into a project specific Data Transfer and Use Agreement[3] with the data provider (usually a Swiss hospital), before data can be transferred and processed on the IT infrastructure. As Controller/Recipient (cf. Chapter 4), the Project Leader is responsible for **classifying** the data (or applying an existing classification) according to risk and data privacy requirements (as described in *Section 4.2 Classification of Information Assets*). The Project Leader (or the designated Data

[1] https://sphn.ch/document/ethical-framework-version-2-version-07-05-2018/
[2] http://www.swissethics.ch/
[3] https://sphn.ch/services/documents/ethics-legal-governance/

Manager) needs to make a **Data Transfer Request** [R1] to the DCC (SPHN's Data Coordination Center) and the respective Data Provider(s) **before the first data is transferred** in order to ensure appropriate measures are in place (no further notification is normally required for additional data transfers for the same project). The Project Leader is also responsible for maintaining an **up-to-date inventory** of all confidential data used under any active or past Data Transfer and Use Agreement (cf. Section 4.1*).* Additionally, the Project Leader is responsible for the **full data life cycle management** (including backup/archiving as well as deletion of data where appropriate). The Project Leader (or the designated Permissions Manager) must specify which research team members have access to the data and take the appropriate steps to revoke user access as soon as it is no longer needed.

Members of a **research team** (Users) are authorized by the Project Leader or a delegate [R2] on a per project basis to access private project data. All Users of the IT system (e.g., a BioMedIT Node) are assigned User accounts. They need to authenticate themselves - typically with a username, a password and a second factor - to access the data, software and compute infrastructure. For detailed User responsibilities when accessing SPHN infrastructure and data, refer to *Section 5.2 Project Leaders, Users and Responsibilities*. A high-level summary is given below:

1. **Confidential data** (considered as *confidential* according to the classification in Chapter 4) must be securely transferred to or from BioMedIT Nodes, either by **encrypting files** or use of an **encrypted channel** (cf. Chapter 8).
2. On BioMedIT Nodes, Users are not allowed to **use or install software** that **harms** the system, other Users or SPHN in general.
3. Users and Project Leaders need to follow a **security awareness training and pass a respective exam** to correctly deal with confidential data on BioMedIT's infrastructure (cf. Chapter 12).

Note that Chapters 6 to 11 are mainly addressed to **BioMedIT Nodes** and their respective IT infrastructures.

2 Terms and Definitions

2.1. Terms Used for People, Organizations and Technology

For definitions of many of the terms used in this policy please refer to the **SPHN glossary** (PDF file) at https://sphn.ch/document/sphn-glossary/.

Anonymization: cf. SPHN glossary. Note that anonymization must not be confused with pseudonymization!

Authentication: cf. SPHN glossary

Authorization: cf. SPHN glossary

Availability: cf. SPHN glossary

BioMedIT Node: cf. SPHN glossary

Confidentiality: cf. SPHN glossary

Controls: cf. SPHN glossary

Controller (**Provider** or **Recipient**): cf. SPHN glossary

Data Manager: responsible for cryptographic keys and decryption of data from a Data Provider and for placing the Data Transfer Requests for transfers between Data Provider(s) and the BioMedIT Nodes.

Data Provider: hospital, technical platform etc. that provides data to be used on a BioMedIT Node. Must be 'onboarded' to the BioMedIT Node or Nodes to which transfer of data is made.

Information Assets: cf. SPHN glossary

Information Security: cf. SPHN glossary

Information Security Incident: cf. SPHN glossary

IT Infrastructure: cf. SPHN glossary

Investigator: cf. SPHN glossary also referred to as **Project Leader** in this policy

Least Privilege Principle: is the concept and practice of restricting access rights for Users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities. Privilege itself refers to the authorization to bypass certain security restraints.

Media: refers to storage media such as USB sticks, external hard drives, optical drives etc. Note that the term media does *not* include storage provided by a BioMedIT Node.

Monitoring: cf. SPHN glossary

Permissions Manager: assigns the User Roles of "(default) User" and "Data Manager" to authorized BioMedIT users and with that granting them access to the project space, also revokes roles and access.

Personal Data: cf. SPHN glossary

Processor: cf. SPHN glossary

Pseudonymization: cf. SPHN glossary

Researcher: cf. SPHN glossary

Risk Analysis: process to comprehend the nature of risk and to determine the level of risk.

Risk Management: is the process of taking actions to assess risks and avoid or reduce risks to acceptable levels.

Secure Jump Host: a specially secured machine (whitelisted gateway machine) where Users can login and from where they can further access machines in a secure environment, for instance, login nodes of HPC clusters

Security Controls: cf. SPHN glossary

Service Provider / Third Party: cf. SPHN glossary

System Administrator: technical staff administering and operating the IT Infrastructure.

User: A User is a natural person using the IT infrastructure. A User is technically matched to a computer system account.

2.2 Laws, Regulations and Standards

In instances where local, cantonal, state or foreign legal requirements also apply, Users must understand and abide by those standards.

The following laws and regulations provide support and direction relative to the security requirements applicable to SPHN. They were referred to (either implicitly or explicitly) in writing this policy and include (non-exhaustive list):

Switzerland:

- Federal Act on Data Protection (SR 235.1)
- Federal Data Protection Ordinance (SR 235.11)
- Cantonal Acts on Data Protection
- Human Research Act (SR 810.30)
- Human Research Ordinance (SR 810.301)
- Swiss Penal Code (SR 311.0)

European Union:

- General Data Protection Regulation (Regulation (EU) 2016/679)

This Information Security program has been developed with the following standards in mind:

- ISO/IEC 27001:2013 Information Technology – Security Techniques – Information security – management systems – requirements
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- NIST Cybersecurity Framework

3 IT Security Governance

3.1 Objectives

This Information Security Policy provides management direction and support for Information Security in accordance with SPHN requirements, relevant laws and regulations. It controls the way the Confidentiality, Integrity, and Availability of information is handled, preventing misuse and malicious damage that will affect SPHN.

SPHN is committed to safeguarding its human, intellectual, financial and physical assets. To do so, SPHN requires a robust security infrastructure that meets SPHN's legal, regulatory and ethical expectations with respect to protecting assets and preventing fraud, waste and abuse. This includes:

- A safe and secure Information Technology working environment.
- The support of SPHN and BioMedIT Nodes through strategic and tactical Information Security programs.
- Participation in the planning, evaluation and implementation of significant new initiatives to determine that appropriate Information Security requirements are met and that any Information Security risk to operations is properly identified and managed.

3.2 Organization of Information Security

Any organization providing IT infrastructure for SPHN (e.g., BioMedIT Node) shall manage information to ensure that:

- compliance to this policy can be monitored through an internal audit inside SPHN;
- the types of information processed within the systems are identified, and any risks associated to the information are documented, actioned and monitored;
- all breaches of Information Security - actual or suspected - are reported promptly, investigated and lessons learned and the root cause recorded; and
- a review of security processes is carried out on a yearly basis - this includes a yearly review of the Information Security Policy.

In addition, all persons interacting with the IT infrastructure for SPHN shall be made aware of the requirements of this policy and undertake training relevant to their job roles.

3.3 Roles and Responsibilities

Role	Responsibility
SPHN NSB	For overall commitment to information governance and Information Security with delegated responsibilities to roles as detailed below. (NSB: National Steering Board)
SPHN DCC Director	Leads the coordination of the DCC (Data Coordination Centre) and related activities with respect to interoperability, data privacy and security
BioMedIT Security Working Group	Composed of the Security Officers of the BioMedIT Nodes: ● Responsible for Information Security processes as defined in this SPHN Information Security Policy ● Handles policies and security incidents ● Needs to notify authorities if security incidents need to be escalated ● Plans and performs audits ● Defines necessary actions in case of violation of this policy The BioMedIT Security WG reports to the SPHN DCC Director and fulfils the role of a “CISO” (Chief Information Security Officer) for SPHN.
Security Officer of BioMedIT Node	Is responsible for the security of IT systems including how policies and procedures are developed, monitored and reviewed in accordance with the relevant legislation and guidance. The Security Officer reports functionally to the BioMedIT Security Working Group.
Users, Project Leaders, System Administrators	To make informed decisions to protect the security of IT systems and the data held on the systems.
BioMedIT Node Manager	Person who 1) has full responsibility for the operation of a BioMedIT Node and 2) is the supervisor of all personnel employed by the node (i.e., System Administrators, Security Officer and related personnel).

3.4 Information Security Risk Management

A risk assessment is to be carried out at regular intervals and whenever significant changes in workflows occur. Such assessment shall address administrative, technical and physical safeguards as appropriate and examine the potential risks and vulnerabilities to the confidentiality, availability and integrity of all sensitive data and related processes.

A formal risk management process is to be established and describes how risks are:

- identified
- assessed

- reduced, eliminated or accepted.

4 Asset Management

Proper management of SPHN's information assets (i.e., data processed within SPHN as well as other documentation, files etc. as defined in Chapter 2) helps ensure the asset is protected according to its value and confidentiality. Where appropriate, all assets must have an owner or a responsible person. In case of data, it is typically the Controller (Data Recipient using the data on a BioMedIT Node) who has responsibility. The Controllers may delegate some administrative responsibilities; however, they retain accountability for the security and appropriate use of information.

Both, **Project Leaders** and **BioMedIT Nodes,** need to collaborate to make sure data is protected with respect to its classification (cf. Section 4.2), risk and confidentiality. This section outlines the main principles and obligations for Project Leaders, Users and BioMedIT Nodes. In summary, the responsibilities are assigned as follows:

- **Project Leaders need to classify data or use the existing classification** (according to classification in Section 4.2) that should be used on BioMedIT and inform the BioMedIT Node about the confidentiality of data, so the necessary technical and organizational measures can be taken to physically protect that data. Other responsibilities:
    - Maintain inventory of confidential data used under any active or past Data Transfer and Use Agreement of the Project Leader.
    - Responsibility for **data life cycle** including archiving. When data is no longer needed, responsible for the deletion or return of data, in accordance with the Data Provider's directions.
    - Ensure that data is backed up either within a BioMedIT Node or external to SPHN's infrastructure following this Information Security Policy.
- **BioMedIT Nodes** have responsibility for operating physical hardware and software systems (incl. inventory of equipment) and to provide technical means to protect data hosted on the nodes' infrastructures.

4.1 Inventory and Responsibility of Assets

Organizational assets must be identified, and appropriate protection responsibilities must be defined.

Inventory and Ownership

Assets associated with information and information processing facilities shall be identified, and an inventory of these assets established and maintained. This applies to material assets (equipment, infrastructure) as well as immaterial (confidential information).

All SPHN material assets involved in confidential data processing must have an owner. Ownership is defined when the asset is created or put in production (i.e., fully functional and accessible by Users).

Return of Assets

Data deletion or return is the responsibility of the User (in particular, the Project Leader of the respective project).

4.2 Classification of Information Assets

A security classification system and accompanying controls help ensure that appropriate levels of security are applied to confidential and high-value information assets and provide guidance to management on where to focus security controls. SPHN must use security classifications to indicate the need and priorities for protection of confidential or high-value information assets and communicate the need for special handling measures. SPHN must ensure that all confidential personal information is protected and used in a manner consistent with applicable law and acceptable use.

Classification of Information

All information assets will be classified based on their risks of loss or compromise, importance to research activities, and the definitions provided in this document:

- **Public**: information that is or can be shared and made available outside of SPHN. This includes properly anonymized research findings and/or aggregated data.

- **Internal**: information that may be shared within SPHN. This information is not intended to be shared outside SPHN and respective projects/initiatives. The impact of the information leaking outside of SPHN would be minor.

- **Confidential**: the access to this information must be restricted only to those parties within SPHN that have a legitimate need to have access to it. All personal data (either identifying data or pseudonymized) are confidential unless explicitly classified differently. The impact of leaking this information without valid justification to parties within SPHN or to the public may cause major harm to the person from whom the data originate, to the original Data Provider (Controller), to the research organization, or to SPHN.

A detailed document and respective training will be available to help correctly classifying data.

Labelling & Treating of Information

All information systems processing confidential personal information should inform Users of the confidentiality of personal data accessible from the system (e.g., at start-up or log-in), i.e., privacy and security awareness shall be raised explicitly.

Handling of Information Assets

BioMedIT Nodes maintain records of assets (data sets) and their authorized Users limited to the projects, including information about the Users, the data space, and the project documentation (as specified in Data Transfer and Use Agreements or related documents).

Temporary as well as permanent copies of information assets must be handled according to the classification of the original information.

4.3 Media handling

SPHN strives to protect information stored on media to prevent unauthorized disclosure, modification, removal or destruction of the information.

Management of removable media

Removable media is considered to be a potential security risk and therefore may not be connected to or disconnected from the IT infrastructure of the BioMedIT Nodes without previous approval of respective System Administrators, IT security personnel or BioMedIT Node Manager. The BioMed IT Node maintains records of such removals to maintain an audit trail. Confidential data on removable media must be encrypted.

SPHN has no control over end-points (workstations, laptops, smartphones), including any removable media connected to them. SPHN relies on the User's compliance with the respective policy of the User's institution.

Disposal of media

Media containing confidential personal data should be stored and disposed of securely, e.g., by shredding, or securely erasing data before reuse inside or outside SPHN. Disposal of sensitive media should be logged in order to maintain an audit trail.

Physical media transfer

Media containing information must be protected against unauthorized access, misuse or corruption during transportation.

5 Access Control

5.1 IT Infrastructure Provider (BioMedIT Node)

Secure design and architecture

A BioMedIT Node needs to implement a secure architecture as defined in BioMedIT Infrastructure Security Design [R5].

Need to know and need to do

Access to data, systems and networks will be granted only when there is a reason to do so. Without sufficient justification, access will not be granted. Users who have a scientific need (i.e., an approved SPHN project) will be granted access to such data and systems commensurate with their roles and the sensitivity (classification) of the data in question.

Access to data, systems and networks shall be granted only to persons who have **formally agreed to comply with the SPHN Information Security Policy** by agreeing to a node-specific *Acceptable Use Policy* and who have passed the BioMedIT Information security awareness exam.

Least privilege

Access to data, systems and networks must follow the least privilege principle.

Authentication

Access to all operating systems, software applications and information resources shall, at a minimum, be controlled by using unique User IDs and strong passwords.

Access to systems holding confidential data must be protected by two factors of authentication, for instance, additional one-time passwords, certificates, etc.

Users are provided with a temporary password which must be changed to one of their choice when they first log on.

As a minimum, the identification and authentication mechanisms must guarantee that only a limited number of failed login attempts are possible: the time span allowed for login attempts must be restricted.

Passwords must not be stored in clear text in password directories.

User access to BioMed IT systems should only be possible via Secure Jump Hosts or similar security measures (e.g., reverse proxy).

Segregation of duties

Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Within BioMedIT it must be examined to what extent the management or execution of certain duties or areas of responsibilities can be separated in order to reduce opportunities for unauthorized modification or misuse of information or services.

User- and access rights management

Logical access rights (e.g., Users, rights / privileges, types of access paths) to confidential data, applications and systems must be allocated and administered (application, approval, installation / change / deletion) via an appropriate process which is determined, documented and in place before the assets are put into operation.

Every User account established for a User must have a specified expiration date.

All User IDs must automatically have the associated rights revoked or locked after a 6-months period of inactivity (i.e., no login to BioMedIT Node). Access rights should be administered in a mandatory centralized Identity and Access Management infrastructure (IAM). Any exception must be justified, documented and is subject to validation by the Security Officer of the BioMedIT Node.

A BioMedIT Node provisions the access to systems and data according to the Project Leader's requests.

When a User changes function, access rights must immediately be modified accordingly. When a User leaves her institution, her access rights must be revoked immediately (cf. responsibilities of Project Leader in Section 5.2).

Review of access rights

According to the principles of least privileges and the segregation of duties, accounts and access rights must be reviewed on a regular basis (at least twice a year) by BioMedIT Node System Administrators.

Privileged access

Administrative access to BioMed IT systems shall only be possible via Secure Jump Hosts or similar security measures (e.g., reverse proxy).

Access to data and system utilities shall be controlled and restricted to those authorized personnel who have a legitimate need, such as system or database administrators.

Creation and changes to privileged accounts are managed under a formal change control process.

Access with privileged accounts should be controlled and audited internally. Audit logs need to be protected.

Physical and logical access to diagnostic and configuration ports must be controlled.

Delegated processes, sessions, transactions and technical Users are managed in a way that their activities and permissions may be retraced.

Transport of credentials

The transport of credentials in a network is only allowed over encrypted connections.

5.2 Project Leaders, Users and Responsibilities

User Registration and De-Registration

Access requests to data and systems managed by SPHN are submitted by the responsible Investigator (Project Leader) via a Data Transfer and Use Agreement and/or additional information where appropriate (e.g., the BioMedIT portal). The requesting Project Leader is responsible for

- justifying that there is an agreed reason to provide access (stated in a Data Transfer and Use Agreement);
- notifying BioMedIT if a User in the project team does no longer need access to data or systems;
- ensuring that access rights are removed when the project purpose ends or ceases to be valid.

Access to SPHN services will be granted by a BioMedIT Node upon the Project Leader's request. The Project Leader can delegate this task to a Permissions Manager as stated in BioMedIT's Standard Operating Procedure (SOP) for User Management [R2].

Every User account has a specified expiration date and will be renewed on the User's request and in accordance with the Project Leader.

The access rights of all Users to data and systems must be removed upon termination of their association with the Project Leader (e.g., no more work contract with the Project Leader's institution) or adjusted upon change of role.

Access to confidential data will be reviewed and validated twice a year by the BioMedIT Node (i.e., Security Officer or responsible System Administrator). It is the responsibility of the Project Leader to provide information when requested.

Service Provider Access

A written agreement which includes a binding commitment to abide by SPHN's security policies and procedures must be received by SPHN staff prior to the establishment of a User ID for any third party (e.g., vendor or external technical support). If the third party is another organization, then the agreement must be signed by an authorized officer.

Access for vendor or external technical support must only be activated for the specific support task with limited time.

When third party access to BioMedIT Node infrastructure is no longer needed, the involved BioMedIT Node Manager within SPHN must immediately notify the relevant System Administrators.

Personal User IDs and Credentials

Users are responsible for all activities they perform with their personal User IDs. They must not permit others to perform any activity with their User IDs, and they must not perform any activity with IDs belonging to other Users.

User IDs must be protected via strong passwords and two factor authentication (e.g., via eduid.ch).

Users must not provide their credentials (e.g., passwords, private keys, etc.) to any other person (including project collaborators) or third parties. Such disclosures not only cause the involved Users to be responsible for all damage that another person may cause, but this behavior is also a justifiable cause for a BioMedIT Node to terminate a User's account and access rights on its systems.

Use of personal computers (end-points)

Users must not share their personal computers, if used for SPHN projects, with any other person unless a multi-user environment is correctly configured. The respective security personnel (e.g., a local System Administrator) must ensure that personal computers have been configured so that separate User IDs and privilege profiles are supported for each individual User. Any exception must be specifically approved.

End-points that are used to connect to the BioMedIT Node (i.e., via jump host or reverse proxy) must always be locked and protected via password (or equivalent) when unattended.

End-points must have an up to date operating system and additional security measures implemented (e.g., anti-malware protection, firewall, disk encryption).

A User must be vigilant and careful with respect to security in order to avoid that a BioMedIT Node is in danger (negligent behaviour with respect to security is not acceptable).

5.3 Data Providers

Secure connection to a dedicated BioMedIT Node

BioMedIT implements a data-transfer architecture where each individual Data Provider is connected to a specific BioMedIT Node (“snowflake” architecture). A secure, dedicated network connection must be established between a Data Provider and a BioMedIT Node (i.e., a Landing Zone).

Single Point of Exit

A Data Provider such as a Swiss University Hospital, should have a single point of exit for data transfer. In this context a ‘single point of exit’ could be a Clinical Data Warehouse or other nominated data transmission facility.

Usage of dedicated transfer tool

It is highly recommended that BioMedIT’s dedicated transfer tool **sett** [R4] and the defined operating procedures are applied [R1], [R3].

6 Operations Management

6.1 Operational Procedures and Responsibilities

Documented Operating Procedures

Responsibilities and procedures for the management of all information processing facilities must be documented to ensure the correct and secure operation of information processing facilities.

Change Management

Changes to the BioMed IT Node organization, processes, information processing facilities and systems that affect information security shall be controlled and follow a formal change management process.

All system changes must be subject to appropriate review before implementation to verify that changes do not compromise the confidentiality, integrity and availability of information and systems.

Capacity Management

The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.

6.2 Protection from Malware

Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate User awareness.

Systems and networks should be isolated where feasible to reduce the impact or spreading of malware.

Systems processing confidential data should not have direct internet access.

6.3 Backup

Backup procedures and controls must maintain the integrity and availability of IT services. They must protect the confidentiality of data on backup media such as employing encryption for media holding confidential data (outside of the control of BioMed IT Node service providers).

Backups must be protected adequately against physical and environmental threats as well as against unauthorized access.

Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy. This needs to be combined with a test of the restoration procedures and checked against the restoration time required.

A BioMedIT Node can offer different systems with different backups, for instance, 1) /scratch not backed-up; 2) /home small storage, backed-up by default, 3) long-term archive with backup. The User is responsible to put the data into the right systems or do encrypted backups herself outside of SPHN.

All data stored on external/removable media must be encrypted.

6.4 Logging and Monitoring

Event logging

Event logs recording User activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.

Protection of log information

Logging facilities and log information must be protected against tampering and unauthorized access.

Administrator and operator logs

System Administrator and system operator activities should be logged. These logs should be protected and regularly reviewed.

Audit logs

Audit logs for applications, operating systems, security devices, and network devices like firewalls, routers, switches shall be in place covering at least the following events:

- login / logoff
- failed login
- create, disable, enable User account activity
- administrator actions
- configuration changes
- system start-up / shutdown
- access to protected information
- changes to logs

Logs shall be collected, stored and protected in a way that it can be used as evidence to support legal actions. For that such logs shall be kept for a period of 6 months (or for a longer time period if there is a specific, explicitly documented request/need).

Timestamps

The timestamps of all relevant information processing systems within an organization or security domain shall be synchronized.

6.5 Control of Operational Software

Procedures should be implemented to control the installation of software on operational systems.

6.6 Technical Vulnerability Management

Management of technical vulnerabilities

Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.

Information resources shall be identified and used to gather information about technical vulnerabilities of all systems and technologies in use.

Once a potential technical vulnerability has been identified, the associated risks and the necessary actions to be taken must be identified. Such actions could involve patching of vulnerable systems or applying other controls.

Patches shall be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls need to be considered, such as:

- turning off services or capabilities related to the vulnerability;
- adapting or adding access and security controls, e.g., firewall rules;
- increased monitoring to detect actual attacks;
- raising awareness of the vulnerability.

An audit log shall be kept for all procedures undertaken.

Systems at high risk need to be addressed first.

An effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur.

Specialized procedural and technical controls and assurance activities, such as independent penetration and vulnerability assessments should be applied.

Restrictions on software installation

Rules governing the installation of software by Users should be established and implemented.

Users must not install/use any software that harms others or the stability of the overall infrastructure.

7 Physical and Environmental Security

Physical protection

BioMedIT Node equipment must be physically protected from security threats and environmental hazards to prevent loss, damage or compromise of information assets and interruption to business activities.

Access to facilities that are dedicated to computer processing (i.e., data centers, computer rooms) should be protected by a range of physical controls.

Strict access control

Areas and offices hosting BioMedIT Node infrastructure that handle, process or store confidential information must be deemed restricted areas and access restricted to authorized Users only. Keys, entry codes and swipe cards must have a security management process to ensure prompt detection of loss or theft and to reduce the likelihood of inappropriate activity.

Server rooms are classified as highly restricted and must be protected from unauthorized access at all times.

8 Cryptography

General

Encryption shall be used to protect confidential data during transport to/from and at rest outside the SPHN environment.

Full disk encryption shall be implemented on desktops and laptops processing confidential data.

Portable external storage devices used to store or transfer confidential data shall be encrypted either in hardware or using volume or file/folder encryption. All backups of confidential data must be encrypted.

All cryptographic keys must be protected against modification and loss. Secret and private keys shall be protected against unauthorized use as well as disclosure. Equipment used to generate, store and archive keys shall be physically protected.

Encryption Algorithms and Protocols

Cryptographic algorithms and protocols for symmetric/asymmetric key encryption, hashes, key lengths and usage practices shall be selected according to best practice and shall be limited to those which have received substantial public review and acceptance and which have been proven to work effectively.

Key Management

Secure processes for key management must be in place. These include generating, storing, changing or updating, archiving, retrieving, distributing, recovering, revoking and destroying cryptographic keys.

9 Communications Security

Networks shall be managed and controlled to protect information from risks concerning confidentiality, integrity and availability. Access to the networks shall be restricted. Security mechanisms, service levels and management requirements of all network services shall be identified and included in network service agreements.

The internal network within a BioMedIT Node shall be segregated (physically or logically), and access to these segments restricted [R5].

Measures shall be put in place in each BioMedIT Node to protect the transfer of information.

Agreements made in relation to the use of the BioMedIT network shall address the secure transfer of information.

Information involved in electronic messaging shall be appropriately protected.

10 Information Security Incident Management

The objective of Information Security Incident management is to ensure that Information Security events and incidents as well as weaknesses associated with information systems are communicated in a manner, allowing timely corrective action to be taken.

Security events, incidents or weaknesses must be reported promptly through the correct management channels and resolved by suitable professionals. Details are specified in a separate “Incident Response Plan” document.

Information Security events, incidents and weaknesses should be identified, responded to, recovered from, and followed up using an Information Security Incident management process to continuously identify and resolve Information Security incidents quickly and effectively minimize their impact and reduce the risk of similar incidents occurring.

The BioMedIT Security Working Group handles incidents in close coordination with the BioMedIT Nodes (System Administrators and BioMedIT Node Managers if appropriate).

11 Business Continuity and Disaster Recovery

It is the responsibility of the management of each BioMedIT Node to ensure that impact assessment (i.e., impact of security incidents), business continuity and disaster recovery plans are produced for the critical information systems used within the BioMedIT network.

12 Information Security Awareness Training

Users, Project Leaders and System Administrators must be made aware of and motivated to comply with their obligations under this Information Security Policy, associated standards, procedures, guidelines, laws and regulations.

Training activities shall be undertaken by Users, Project Leaders and System Administrators. This will take the form of a security awareness program designed to promote security awareness to all individuals who access the information and information systems of SPHN and BioMedIT Nodes.

System Administrators shall also be trained in how to correctly manage the systems and how to develop and apply relevant and appropriate Information Security controls.

Prior to being granted access to the BioMedIT network all users shall undertake and pass an online exam to demonstrate they have the necessary level of awareness of the need for security on the BioMedIT network. On-line [R6] and classroom training is available for all prospective Users.

13 Compliance and Auditing

The BioMedIT Security Working Group is responsible for monitoring compliance with this policy. Security monitoring enables the early identification of security issues or new security vulnerabilities and can help prevent security incidents or at least minimize the potential impact of such incidents.

Right to monitor activities

All Information and Information Technology equipment, including but not limited to servers, workstations, and network access devices used on the BioMedIT network is subject to ongoing monitoring. The inappropriate use of any of these systems and/or networks which violates this policy will be investigated as needed.

Non-Compliance

Any employee or User who violates or circumvents this policy will have access removed, and the host institution will be notified immediately (disciplinary actions may follow).

Auditing

Internal and external audits of operational systems should be planned and performed on a regular basis.

The BioMedIT Security Working Group conducts periodical internal and external audits. It establishes an audit plan covering operational aspects and processes. The audit plan is communicated to the NSB and the DCC Director.

14 Exception Management

Any questions, interpretations, or exception requests to this policy should be directed to the BioMedIT Security Working Group. The BioMedIT Security Working Group is responsible for approving policy exceptions. Any exceptions to these policies must be documented.

15 Next Review and Changes

A review is planned within one year of the effective date of this policy.

Planned changes will be documented and communicated in a specific document called “Roadmap” in order to have them in place and implemented by BioMedIT Nodes when a new version of the Information Security Policy is available.

References

[R1] BioMedIT Data Transfer SOP, v1.0, 20 May 2020.

[R2] BioMedIT User Management SOP, v1.0, 15 July 2020.

[R3] BioMedIT Data Provider SOP, draft v0.1, 30 July 2020.

[R4] Secure Encryption & Transfer Tool components description, Draft 0.2, 13 March 2020.

[R5] BioMedIT Infrastructure Security Design, v3.0, 29 May 2020.

[R6] BioMedIT On-line Security Awareness Course: “SPHN/BioMedIT Data Privacy and IT Security Training”, https://edu.sib.swiss/course/view.php?id=424

Approval

Version 1.0 of policy was approved by: SPHN’s Scientific Expert Board.

Version 2.0 had only minor changes with respect to version 1.0 and was approved by the BioMedIT Security Working Group as well as the BioMedIT Heads of Nodes on 8 October 2020.