Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

NEXUS Personalized Health Technologies

ETH Zürich
Daniel Stekhoven
Director
SWS L 641
Wagistrasse 18
8952 Schlieren, Switzerland

+41 44 632 21 61
stekhoven@nexus.ethz.ch
www.nexus.ethz.ch

NEXUS Data Usage and Processing Policy

Version 1.2, 2024-03-19

1. Purpose of this policy

1.1. The purpose of this policy is to prevent breach of confidentiality, integrity, or availability of all data entrusted to NEXUS Personalized Health Technologies.

1.2. The policy defines the guidelines for receiving, storing, processing, and sharing different types of data.

1.3. It is based on the *IT Guidelines and IT Baseline Protection Rules of ETH Zurich*[1] and extends or clarifies them where necessary.

2. Data types

2.1. All data entrusted to or generated at NEXUS needs to be classified by the project owner into one of four data confidentiality levels[2].

2.2. Classification levels are PUBLIC, INTERNAL, CONFIDENTIAL, and STRICTLY CONFIDENTIAL.

3. Data use and processing policies

3.1. Data must only be used for the intended purposes.

3.2. All devices used to access and process CONFIDENTIAL and STRICTLY CONFIDENTIAL data at NEXUS have to be encrypted.

3.3. Emails from NEXUS employers have to be digitally signed and whenever possible encrypted.

3.4. Radius authentication passwords (“NETHZ password”) have to be unique and all passwords have to comply with ETH Zurich password and PIN rules[1].

3.5 Personal passwords and private keys must not be shared with anyone.

3.6. Devices have to be locked when unattended[1].

3.7 Backup disks have to be encrypted. The encryption password needs to be deposited with the NEXUS secretariat[3].

[1] RSETHZ 203.23 (https://rechtssammlung.sp.ethz.ch/Dokumente/203.23.pdf)

[2] RSETHZ 203.25 (https://rechtssammlung.sp.ethz.ch/Dokumente/203.25.pdf)

[3] Data backups for clients (https://unlimited.ethz.ch/display/nexuswiki/Data+Backups+for+Clients)

4. Policies related to confidential data classification

4.1. PUBLIC:
- No restrictions.

4.2. INTERNAL:
- Data must only be accessible by authorized users.
- Data can be shared by email.

4.3. CONFIDENTIAL and STRICTLY CONFIDENTIAL:
- Data must only be accessible by authorized users.
- Data must only be processed and stored on encrypted devices.
- STRICTLY CONFIDENTIAL data is either designated directly in the file(s) or accompanied by a designating text file located in the same directory.
- For high performance computing the Leonhard Med secure high performance computing infrastructure[4] has to be used.
- Data must not be shared by email unless encrypted.
- Data may only be transferred using an access-controlled and secure infrastructure, e.g., Globus[5].

5. Data lifecycle

5.1. Governance of data entrusted to and generated by NEXUS is organized in the Data Lifecycle Management of NEXUS[6].

5.2. All data associated with a project is kept for a maximum of 6 months after the final handover of deliverables.

5.3. Extensions of this time frame need to be requested and motivated in writing 1 month before the expiration date.

5,4 Once the final handover is done, associated project data will be moved away from the everyday operations storage server to cost defined storage server for another four years. If required, archived data can be restored to an active production environment on the basis of the request from project leader.

5.5 project data will be removed from cost defined storage servers (archives) when it exceeds the required retention period (four years) or no longer serves a meaningful purpose to NEXUS. This will be informed to the project lead a month in advance.

[4] RSETHZ 438.1 (https://rechtssammlung.sp.ethz.ch/Dokumente/438.1.pdf)

[5] Data Transfer with Globus (https://www.globus.org/data-transfer)

[6] NEXUS DLM (link follows soon)