BIC's Technical and Organizational Security Measures (TOM)
Last modified: Jun 12, 2023 - template model inspired from draft.io

Description of the technical and organizational measures implemented by the Brain Imaging Center (BIC) to ensure an appropriate level of security, taking into account the nature, scope, context, and purpose of the processing, and the risks for the rights and freedoms of natural persons:

1. Measures of pseudonymization and encryption of Research Data

No data encryption is enforced at the BIC, whether at rest or otherwise but users are free to do so with various available methods. We do otherwise enforce data encryption when in transit, using for example ssh, rsync, sftp or https. Imaging data is anonymized while some modalities may also undergo a defacing procedure when deemed necessary.

2. Measures for ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services

These include the following:

Access to production systems is regulated essentially through McGill University's VPN, leveraging unique accounts and role-based access within operational and research environments. Authorization requests for access are tracked and logged on a regular basis.

Removal of access for employees upon termination or change of role.

Multi-factor Authentication (MFA) is enforced at the VPN level. Strong passwords are required and encrypted in transit. We do however allow ssh connections to a special login server, w/o the use of the VPN, where connections are closely monitored and where brute force attacks are mitigated with the use of fail2ban, which limits the number of failed attempts. In fact all systems within the BIC are bound to fail2ban mitigation and firewalled locally, while also firewalled at the edge of McGill University's network.

Users must comply with all applicable federal and provincial laws for the use of research data, along with McGill's Confidential Data Policy, described in section 5.1 of https://www.mcgill.ca/secretariat/files/secretariat/responsible-use-of-mcgill-it-policy-on-the.pdf

We encourage but we do not enforce strict permissions on data accessibility, as data owners have control over how they share their data.

3. Measures for ensuring the ability to restore the availability and access to Personal or Research Data in a timely manner in the event of a physical or technical incident

We have external data mirroring and tape backup processes in place for those who opt for these services.

4. Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing

While we monitor access to our services, McGill University's IT Security group perform frequent penetration tests for various components of our services, http/https/ssh, and maintain security incident management policies and procedures. They also notify us if and when our systems are impacted by any security threats or vulnerabilities.

We also enable automatic package security updates within our Debian/Ubuntu O/S environments to minimize the risks to such threats or vulnerabilities.

5. Measures for user identification and authorization

Access to our services by BIC personnel and other users is uniquely identifiable, logged, and monitored. Access to back-end infrastructure by BIC personnel requires multiple layers of authentication including requiring unique identifiers, optimal password strength and/or SSH keys, and in some instances the use of Multi-factor Authentication.

6. Measures for the protection of data during transmission

We employ TLS 1.2/1.3 encryption for web services and widely accepted encryption algorithms for SSH/SFTP services.

7. Measures for the protection of data during storage

Data access can be given via web services or directly at the linux shell level to authorized users. Access permissions are controlled by domain, linux groups, file permissions and ACLs (Access Control Lists).

8. Measures for ensuring the physical security of locations where Research Data is processed

Physical access to our infrastructure at all locations is strictly restricted to personnel via the use of FOB keys and monitored via security cameras. Our facilities are designed to withstand adverse weather and other reasonably predictable natural conditions and supported by on-site backup generators and uninterruptible power supplies (UPS) in the event of a power failure.

9. Measures for ensuring events logging

We log authorization requests by users to our servers, and capture configuration changes and updates, up to roughly one year.

10. Measures for ensuring system configuration, including the default configuration

All of our systems are subject to configuration automation to insure consistency and we monitor changes to mitigate the risk of undetected changes to production systems.

11. Measures for internal IT and IT security governance and management

We are bound by all applicable federal and provincial laws for the use of research data, along with McGill's responsible use of IT policies available at https://www.mcgill.ca/it/it-policies/.

12. Measures for certification/assurance of processes and products

We strive in our commitment to implement controls and safeguards, while providing an environment that is conducive to research.

13. Measures for ensuring data minimization, as it relates to privacy

Data is collected and processed in accordance with stated purposes. Access is provisioned and restricted in accordance with roles and requirements for job responsibilities.

14. Measures for ensuring data quality

We have various in house methods to insure the quality of Research Data Acquisition and curation. Such methods have also been peer-reviewed.

15. Measures for ensuring limited data retention

Automatic deletion of temporary data is implemented to enforce some level of data retention limitations. User accounts that are inactive for more than 12 months are automatically locked. Their related account data is preserved unless the principal investigator requests the data to be deleted from production.