# Brain-CODE

## Security Policy

*Version 3.0*

*November 1, 2022*

# 1. Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of the Brain-CODE platform and the platform's data.

# 2. Scope

This policy applies to the Brain-CODE platform (including all hardware, operating systems and applications), its data and its users. The policy also applies to organizations engaged in the development, maintenance, and administration of the Brain-CODE including: the Ontario Brain Institute (OBI); and the Service Group comprised of Indoc Research; Queen's University at Kingston, as represented by the Centre for Advanced Computing (CAC); and Baycrest Centre for Geriatric Care, as represented by the Rotman Research Institute (RRI-CSR).

# 3. Roles and Responsibilities

The OBI Board of Directors is responsible for overseeing the governance of cyber risk for Brain-CODE, approving OBI's overall cyber security strategy and ensuring it is aligned with OBI's objectives and risk tolerance.

The OBI Executive, led by the President and Scientific Director, are responsible for overseeing the implementation of the Board of Directors' strategic direction in regards to cyber risk. This includes ensuring measures are taken to protect the Brain-CODE platform, and its data, that are appropriate given the value of the assets, available resources and organizational risk tolerance.

The OBI staff assigned to the Brain-CODE team, including the Manager of Informatics and Analytics and the Senior Lead of Informatics Privacy and Security have oversight over the implementation of this policy as part of the day-to-day operations of Brain-CODE.

The Service Group, as contractors and sub-contractors of OBI, are responsible for ensuring this policy is implemented as part of the services they provide to OBI in relation to Brain-CODE.

Authorized Brain-CODE users, and Participating Institutions, are responsible for carrying out their responsibilities under this policy as part of the agreements they have with OBI in relation to Brain-CODE.

# 4. Risk Identification and Mitigation

OBI and the Service Group will meet on a regular basis to identify and review cyber security threats to Brain-CODE and develop appropriate mitigation strategies.

OBI, with the cooperation and support of the Service Group, will commission a threat risk assessment once every three years, and on an annual basis, commission penetration tests and vulnerability scans of the Brain-CODE platform including tests of the network boundary to identify security control gaps. OBI and the Service Group will develop a plan to respond or address risks that are identified.

## 5. Cyber Security Incident Response Standard Operating Procedure

A cyber security incident occurs when there is an event which has caused, or has the potential to cause, damage to OBI information assets, damage to OBI reputation, negative financial consequences, information to be transferred to someone who is not entitled to receive it, the corruption of data, or the unavailability of the platform or critical components of the platform.

OBI, with the cooperation and support of the Service Group, will develop and implement a Cyber Security Incident Response Standard Operating Procedure that includes the specific steps to contain and control a cyberattack upon discovery. The plan will include, among other things:

- clearly defined roles and responsibilities;
- an immediate and coordinated response;
- data backup and recovery strategy;
- internal reporting and communication;
- external reporting and communication (including to the organization's insurer);
- protocol for engaging external security experts.

OBI will centrally store records of incidents so that they can be used for the analysis of trends and correlations in relation to security events and cyber losses.

The Cyber Security Incident Response SOP will align with OBI's Privacy Breach Protocol.

OBI and the Service Group will conduct regular simulated cyber-attacks and recovery scenarios and/or table-top exercises using the Cyber Security Incident Response Standard Operating Procedure.

## 6. Identity and Access Management

OBI and the Service Group will develop and implement an Identity and Access Management Standard Operating Procedure (IAM SOP). The IAM SOP will:

- include a standardized identity and access management process that supports an effective administration of user accounts (e.g., granting, revoking, and managing user access to systems, processes, and network drives);

- ensure accounts are provisioned following the 'least privilege' principle, providing the minimum functionality necessary for tasks and restricting administrator privileges to an as-required basis;
- include a process to ensure accounts and/or functionality is removed in a timely manner when users no longer require these for their tasks
- provide policies on password length and reuse
- enforce password changes on suspicion or evidence of compromise
- require virtual private network (VPN) connectivity for remote access into corporate networks where appropriate as agreed upon between OBI and the Service Group.

# 7. Hardware Asset Management

CAC will implement an Information Technology Asset Management (ITAM) process to manage the lifecycle and inventory of hardware assets used for the Brain-CODE platform. The ITAM process will include industry best practices related to securing all active and inactive devices appropriately, including decommissioning of assets that are past their end of life. The ITAM process will also include risk assessment activities as to whether to replace any hardware.

# 8. Baseline Controls – Technical Safeguards

## 8.1 Physical Architecture

CAC will ensure security zones will be employed to separate operations on Brain-CODE. The boundaries between such zones must be physical and robust in nature.

Systems must be placed between firewalls in a demilitarized network segment, to protect them from internal and external threats.

## 8.2 Patching

OBI and the Service Group will have a patch management process in place to address defects and security vulnerabilities in a timely manner.

## 8.3 Anti-Malware

For the network file system, the Service Group will utilise industry standard anti-malware solutions that update and scan automatically.

### 8.4 Firewalls

CAC will ensure internet traffic is mediated by firewalls. Firewalls will have stateful, layer 3 designs to enforce network policies.

### 8.5 Monitoring – IDS/IPS

The Service Group will be responsible for ensuring industry standard systems are implemented for ongoing monitoring including:

- real-time network traffic and host availability and
- an intrusion detection and/or intrusion prevention system

### 8.6 Web Applications

The Service Group will use the following as a reference to assess Brain-CODE web applications:

- the Open Web Application Security Project (OWASP) top 10 most critical security concerns for web application security; and
- the OWASP Application Security Verification Standard (ASVS) security verification Level 2.

## 9. Data Storage, Backups, Continuity

CAC will ensure that Brain-CODE backups are stored securely in an encrypted state and access to backups are restricted to those who must access them for the testing or use of restoration activities.

The Service Group will ensure that recovery mechanisms effectively and efficiently restore these systems from back-up.

## 10. Training

OBI (including OBI Steering Committees and the Data Access Committee) and the Service Group will ensure all Brain-CODE users are required to successfully complete any platform related security training prior to being given access to the platform.

## 11. Physical Safeguards

In physical premises, controlled by OBI or members of the Service Group, which house elements of the Brain-CODE platform or its data, the following physical safeguards will be implemented:

- Access to premises is limited to authorized personnel only.
- Access to premises is controlled by an electronic security locking system.
- The premises are continually monitored against intrusion. All entrances and exits will be monitored by Closed Circuit Television CCTV with all images securely stored on a video recording system and maintained for a minimum of 90 days.
- All cabinets and computing resources within the secured premises are locked.
- The CAC data center will be equipped with:
    - Filtered, conditioned, power connected to an appropriately sized uninterruptible power supply
    - Backup power supplied through a generator
    - Fire suppression, heating, ventilation, and air conditioning appropriate for a commercial data processing facility

Processes must be in place to ensure appropriate OBI or Service Group personnel or contractors are alerted in a timely fashion in order to respond to any security or environmental incidents.

## 1.0 Contractors / Vendors / Third Parties

OBI, and the Service Group, will take all necessary steps to satisfy themselves that any contractor engaged to use or perform work on any components of the Brain-CODE platform will have in place security measures appropriate to the sensitivity, level of access and use of the platform and its data. These may include, among other things, agreements containing assurances that reasonable security measures will be taken and/or requiring industry standard certifications and/or audit reports.

## 12. Insurance

OBI and the Service Group will carry cyber security insurance policies that provide coverage for losses and costs associated with a serious cyber incident, including the cost of data recovery, repair or replacement of hardware used for Brain-CODE, legal actions, fines, forensic investigations, and identity recovery protection for individuals whose privacy may have been compromised.

## 13. Exceptions

OBI's Manager of Informatics and Analytics, with the advice of the Senior Lead of Informatics Privacy and Security, will assess the risk posed by any proposed exception to this policy. The Manager may approve an exception. If exception is approved, the Manager will promptly notify the VP, Integrated Discovery and Analytics of the exception and the rationale deviating from this policy including the risks, costs and benefits.

All exceptions must be centrally documented by OBI (including the risk assessment and the justification for permitting the exception) and wherever possible, the exception should time limited.