



Cybersecurity: Governance and Data Privacy Policy

1. POLICY INFORMATION

Organization Name: **Solutions Biotonix Inc.**

Effective Date: **August 1, 2023**

Revision Date: **February 4, 2025** (*Next revision scheduled for August 2025*)

1.1 Policy Scope

The Solutions BIOTONIX Data Security Policy applies to all entities under the organization's purview. The measures outlined herein apply uniformly across the entire organization to ensure consistent protection and compliance.

Regarding data processors, the company partners with Solulan (SOC 2 certified) as a trusted collaborator to strengthen cybersecurity efforts and secure the Office 365 environment. Solulan's advanced backup and Data Loss Prevention (DLP) systems significantly enhance Solutions BIOTONIX's data protection measures. The use of premium Microsoft products, optimized by this partner, ensures a superior level of security.

BIOTONIX is committed to enforcing rigorous governance regarding cybersecurity and data privacy. Under the supervision of the Vice President of Technology, Sébastien Lacoste, the organization adheres to best practices in data protection and complies with the requirements of Quebec's Law 25.

1.2 Policy Statements

1.2.1 Solutions BIOTONIX holds personal and sensitive data.

1.2.2 The organization's approach to data security is built on a firm commitment to the following pillars:

1.2.3 Compliance with Laws and Best Practices: The company adheres to legal standards and adopts best practices to ensure proactive compliance.

1.2.4 Protection of Individual Rights: The rights of individuals are central to Solutions BIOTONIX's operations, in accordance with legal and ethical standards.

1.2.5 Transparency and Communication: The company maintains a transparent and honest relationship with data subjects, respecting confidentiality while providing necessary information.

1.2.6 Staff Training and Support: Solutions BIOTONIX trains and supports its team to ensure the consistent and prudent management of personal data.

1.2.7 Voluntary Notification to the Information Commissioner: The company voluntarily reports incidents, demonstrating a commitment to accountability and transparency.

1.2.8 Ultimately, these pillars guide Solutions BIOTONIX's commitment to protecting data proactively, ethically, and in regulatory compliance.

1.3 Key Risks

- Loss of user data.
- Data leakage originating from an unsecured work environment.

2. RESPONSABILITIES

2.1 Executive Management

The management of Solutions BIOTONIX holds the overall responsibility for ensuring the organization complies with its legal obligations.

2.2 Data Protection Officer (DPO)

This role is held by the Vice President of Technology, Sébastien Lacoste, a computer engineer. This central role guarantees the implementation of security best practices. Responsibilities include:

- Informing the Board of Directors of data protection responsibilities.
- Reviewing data protection policies and related documentation.
- Advising staff on complex data protection issues.
- Ensuring that data protection onboarding and training are completed.
- Processing subject access requests.
- Approving unusual or controversial disclosures of personal data.
- Approving contracts with data processors.

2.3 BIOTONIX Employees

All staff members are required to read, understand, and accept all policies and procedures regarding the personal data they handle during their duties.

3. SECURITY

3.1 Security Measures

To ensure enhanced protection, all employees must log out of their sessions at the end of their workday. Additionally, Multi-Factor Authentication (MFA) is mandatory for all access to Office 365 accounts, limiting the risk of unauthorized access. Backup responsibilities are delegated to Solulan in accordance with the agreement between them and Solutions BIOTONIX.

3.2 Data Storage

Sensitive data generated by BIOTONIX applications is securely stored in Microsoft Azure on servers located in Canada, benefiting from the platform's advanced protections. Furthermore, our partnership with Solulan (SOC 2 certified) reinforces cybersecurity, particularly within the Office 365 environment, through advanced Data Loss Prevention (DLP) solutions and automated backups.

3.3 Data Retention

In compliance with current laws and Solutions BIOTONIX's commitment to transparency, users retain ownership of their data and may permanently delete it at any time via the option available in the mobile application. Solutions BIOTONIX also enforces a data retention policy to ensure compliance with regulations and operational needs:

- **Active User Data:** Retained as long as the account remains active.
 - **Inactive User Data:** Deleted after 24 months of inactivity, unless a legal retention obligation exists.
 - **Transactional Data:** (Payments, invoices, login history, etc.) Retained for a minimum of 7 years for regulatory compliance and audit purposes.
- Anonymized Data:** Certain data may be retained in an anonymized format for statistical analysis and service improvement, with no possibility of user re-identification.

Users may request the immediate deletion of their personal data via the mobile app or, if necessary, by submitting a written request to the Data Protection Officer. In the event of a cybersecurity incident requiring investigation, certain data may be temporarily retained beyond these periods until the investigation is concluded.

3.4 Access Rights

Roles and permissions are assigned based on a strict interpretation of the principle of least privilege, ensuring each employee holds only the access rights necessary for their specific tasks.

4. CYBERSECURITY INCIDENT MANAGEMENT PLAN

4.1 Incident Definition

An incident may include:

- Unauthorized access to systems or data.
- Leakage or loss of sensitive data.
- Malware or ransomware infection.
- Phishing attacks.
- Failure of a critical system that exposes data.

4.2 Incident Response Process

4.2.1 Detection and Alerting

- Monitor and detect threats via cybersecurity tools (e.g., antivirus, SIEM, access logs).
- Establish an internal reporting channel (dedicated email, Teams) for reporting incidents.
- Prioritize incidents based on severity (minor, moderate, critical) .

4.2.2 Containment

- Immediately isolate compromised systems or accounts (e.g., disable an account, block access).
- Implement countermeasures (e.g., activate a temporary firewall).
- Notify relevant stakeholders (Management, Data Protection Officer, technical partner Solulan).

4.2.3 Analysis and Remediation

- Identify the root cause of the incident (e.g., human error, external attack, software vulnerability).
- Assess damages incurred and data affected.
- Apply security patches (e.g., updates, credential changes, procedure reviews).

4.2.4 Communication and Notification

- Notify the *Commission d'accès à l'information* (CAI) if required (pursuant to Law 25).
- Inform affected users if there is a risk to their data.
- Communicate with processors and partners if the incident impacts them.

4.2.5 Learning and Prevention

- Draft an incident report (events, actions taken, lessons learned).
- Adapt procedures and staff training to prevent recurrence.
- Implement a continuous improvement plan.