Information Security Policy

Context and Purpose

Tochtech Technologies Ltd (Tochtech) is committed to appropriately protecting the privacy of individuals and ensuring the security of their personal data and health information.

Tochtech is committed to safeguarding its IT ecosystem, to securing its data holdings and to protecting health information with administrative, physical and technical security safeguards appropriate to the sensitivity of the information. These safeguards protect Tochtech's data holdings against theft, loss, unauthorized use or disclosure, unauthorized copying, modification or disposal.

The purpose of the Information Security Policy is to:

• Provide Tochtech Staff with direction and support for information security in accordance with business requirements and relevant laws and regulations; and
• Outline the responsibilities of Tochtech Staff with respect to information security.

Scope

This policy and all related standards, guidelines and procedures apply to all Tochtech Staff, contractors, consultants, temporary employees and other workers at Tochtech.

Policy

Tochtech management supports the development and maintenance of the Information Security Program in accordance with business, legal and privacy requirements. This program must address, at minimum, the following control objectives and practices:

• A security governance framework;
• Privacy and Security Risk Management;
• Ongoing review of the security policies, procedures and practices implemented;
• An information security awareness and training program for all employees;
• Policies, standards, practices and/or procedures for ensuring the physical security of the premises, the security of information processing facilities and the protection of information throughout its life cycle (creation, acquisition, retention and storage, use, disclosure and disposition), including policies and procedures related to mobile devices, remote access and security of data at rest;
• An access management process for information and information processing facilities;
• Secure systems acquisition, development and maintenance;
• Technical vulnerability management;
• A cybersecurity program;
• Security audits;
• Acceptable use of information technology;
• Security in backup and recovery;
• Business continuity and disaster recovery;
• Information security incident management;
• Protection against malicious and mobile code; and
• Continuous improvement of the Information Security Program.

Tochtech is committed to ensuring that reasonable steps are taken to ensure that personal health information is protected against loss or theft, as well as against unauthorized access, disclosure, copying, use, modification and disposal.

Responsibilities

The following Tochtech individuals/groups have specific responsibilities for the Information Security Program:
• All Tochtech Staff
• Senior Management
• Chief Information Officer
• Director, Human Resources and Administration

• Manager, Information Security

Tochtech Staff

All information under the care and control of Tochtech is a corporate asset and must be securely managed throughout its life cycle. The protection of Tochtech information assets is a responsibility of all Staff, and Staff must understand and agree to their obligation to protect such assets throughout the information life cycle — creation, acquisition, retention and storage, use, disclosure and disposition. Tochtech Staff shall create, acquire, retain, store, use, disclose, transfer or dispose of information only in accordance with Tochtech's policies, standards and guidelines. Tochtech Staff must at all times engage in practices that are consistent with published information security policies, procedures, standards and guidelines. Additionally, Tochtech Staff are obliged and expected to report all information security incidents and suspected information security incidents immediately upon learning of them. (For more information, refer to the Privacy Breach Incident Response Plan.)

Senior Management

Senior Management shall provide the necessary guidance and support for the development and maintenance of the Information Security Program, in line with privacy and legal requirements and business strategy objectives. This support includes, but is not limited to, the following:

• Integrating information security goals into relevant processes;
• Providing clear direction and visible management support for information security initiatives;
• Providing the resources required for information security; and
• Approving assignment of specific roles and responsibilities for information security across the organization.

Chief Information Officer (CIO)

The CIO has overall responsibility for information security and represents Tochtech's Executive Committee. He or she shall ensure that information security goals are identified, meet organizational requirements and are addressed within the Information Security Program.

Director, Human Resources and Administration

The Director, Human Resources and Administration, is responsible for the following in support of Tochtech's information security objectives:

- The physical security of the premises;
- Records and information management policies, procedures and practices; and
- Security in Human Resources processes.

Glossary

Business record

Business records comprise any information created, received or maintained as evidence and information by Tochtech, in the transaction of business or in the pursuance of legal obligations. Business records may be in physical or electronic form and include, but are not limited to,

- Information collected from data providers, clients and stakeholders;
- Official organizational records;
- Transitory records; and
- Records in the public domain owned by Tochtech.

Information asset

For the purposes of this policy, information or information assets shall include the following:

- All health information maintained by Tochtech for the purposes of meeting our mandate; and

• All business records of the organization, regardless of the security classification. Information may be in physical or electronic format.

Information security

The concepts, techniques, technical measures and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification or loss.

Tochtech Staff

Any worker at Tochtech, including all full-time or part-time employees, secondments, temporary workers, students and contract employees, including external consultants or other third-party service providers whose role includes responsibility for the secure storage of personal health information.

For more information, please contact compliance@tochtech.com