Security Program Overview

`2021.1`

MiCT is committed to protecting its employees, partners, clients/customers and the company itself from damaging acts either malicious or unintentional in nature. This includes implementation of policies, standards, controls and procedures to ensure the Confidentiality, Integrity, and Availability of systems and data according to their risk level.

The MiCT security program and policies are developed on the principles that (1) security is everyone's responsibility and (2) self-management is best encouraged by rewarding the right behaviors.

!!! TLDR

`[Quick Reference / Employee Handbook](employee-handbook.md)`

Controls and Procedures

Information Security Program and Scope

MiCT has developed a security program and implemented controls to meet and exceed all compliance requirements, including but not limited to HIPAA,

SOC 2 Common Criteria and other applicable industry best practices.

On a high level, MiCT's information security program covers:

1. Inventory and protection of all critical assets
2. Visibility into and the management of data lifecycle, from creation to retention to deletion
3. Protection of data-at-rest, data-in-transit, and data-in-use
4. Segmented network architecture
5. Automated security configuration and remediation
6. Centralized identity and access management
7. Secure product development
8. Continuous monitoring and auditing
9. Validated plan and practice for business continuity, disaster recovery, and emergency response
10. End-user computing protection and awareness training

More information about the MiCT Security and Privacy program can be found at https://mict-international.org/security and https://mict-international.org/privacy.

The information security program and its policies and procedures cover all MiCT workforce members, including full-time and part-time employees in all job roles, temporary staff, contractors and subcontractors, volunteers, interns, managers, executives employees, and third parties.

The information security program is managed by dedicated security and compliance personnel, using JupiterOne as a GRC platform.

Understanding the Policies and Documents

Policies are written in individual documents, each pertaining to a specific domain of concern.

Each document starts with the current version number and/or last updated date, followed by a brief summary. The remaining of the document is structured to contain two main sections:

- Policy Statements
- Controls and Procedures

All policy documents are maintained, reviewed, updated and approved following standards and procedures outlined in Policy Management.

Review and Reporting

The information security program, policies, procedures and controls are reviewed on a regular basis internally by cross functional team members and externally by qualified assessors.