Roles, Responsibilities and Training

`2021.1`

Security and compliance is everyone's responsibility. MiCT is committed to ensuring all workforce members actively address security and compliance in their roles. Statistically, cybersecurity breaches typically start with compromise of end-user computing devices, social engineering, human error or insider threat. Therefore, users are the first line of defense and yet usually the weakest link. As such, training is imperative to assuring an understanding of current best practices, the different types and sensitivities of data, and the sanctions associated with non-compliance.

In this and all related policy documents, the term "employees" and "workforce members" may be used interchangeably to include all full-time and part-time employees in all job roles, contractors and subcontractors, volunteers, interns, managers and executives at MiCT.

The Security Officer, in collaboration with the Privacy Officer, is responsible for facilitating the development, testing, implementation, training, and oversight of all activities pertaining to MiCT's efforts to be compliant with the applicable security and compliance regulations and industry best practices. The intent of the Security Officer Responsibilities is to maintain the confidentiality, integrity, and availability of critical and sensitive data. The Security and Privacy Officer is appointed by and reports to the Board of Directors and/or the CEO.

MiCT has appointed Adam Burns as the Security Officer and Maren Hornung as the Privacy Officer.

An official **Security Committee** has been formed, chaired by the Security Officer, and represented by the select members of the senior leadership team (Security Officer, Privacy Officer, CTO, COO).

Policy Statements

MiCT policy requires that:

(a) A Security and Privacy Officer [164.308(a)(2)] must be appointed to assist in maintaining and enforcing safeguards towards security, compliance, and privacy.

(b) Security and compliance is the responsibility of all workforce members (including employees, contractors, interns, and managers/executives). All workforce members are required to:

- Complete all required security trainings, including annual regulatory compliance training, security awareness, and any additional role-based security training as part of the ongoing security awareness program and as required by job role.

- Complete annual HIPAA awareness training
- Follow all security requirements set forth in MiCT security policy and procedures, including but is not limited to access control policies and procedures and acceptable use policy for end-user computing.
- See something, say something: follow the incident reporting procedure to report all suspicious activities to the security team.

(c) All workforce members are required to report non-compliance of MiCT's policies and procedures to the Security Officer or designee. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

(d) All workforce members are required to cooperate with federal, state and local law enforcement activities and legal investigations. It is strictly prohibited to interfere with investigations through willful misrepresentation, omission of facts, or by the use of threats against any person.

(e) Workforce members found to be in violation of this policy will be subject to sanctions.

(f) Segregation of Duties shall be maintained when applicable to ensure proper checks and balances and minimize conflict of interests. This helps reduces the possibility of fraud and insider threat considerably, and eliminates single points of compromise to critical systems.

Controls and Procedures

Assignment of Roles and the Security Committee

MiCT has appointed Adam Burns as the Security Officer and Maren Hornung as the Privacy Officer.

The security committee is chaired by the Security Officer, and represented by the select members of the senior leadership team, including Security Officer, Privacy Officer, CTO, COO, in addition to the Security and Privacy Officer.

General Responsibilities of the Security and Privacy Officer The authority and accountability for MiCT's information security program and privacy program is delegated to the Security and Privacy Officer. The Security Officer and the security team are required to perform or delegate the following responsibilities:

- Build and maintain security and privacy program to satisfy regulatory and contractual requirements.
- Establish, document, distribute and update security policies, standards and procedures.

- Oversee, enforce and document all activities necessary to maintain compliance and verifies the activities are in alignment with the requirements;
- Monitor, analyze, distribute and escalate security alerts and information.
- Develop and maintain security incident response and escalation procedures to ensure timely and effective handling of all situations.
- Administer user accounts, including additions, deletions, and modifications.
- Monitor and control all access to critical systems and data.
- Perform risk assessment, remediation, and ongoing risk management.
- Provide regular security awareness and compliance training, as well as periodic security updates and reminder communications for all workforce members.
- Maintains a program that incentivizes right behaviors, supports timely and proper reporting and investigation of violations, implements effective and practical mitigation, and applies fair sanctions when necessary.
- Assist in the administration and oversight of business associate agreements.
- Facilitate audits to validate compliance efforts throughout the organization.
- Work with the COO/CFO to ensure that any security objectives have appropriate consideration during the budgeting process.

Workforce Supervision Responsibilities Although the Security Officer is responsible for implementing and overseeing all activities related to maintaining compliance, it is everyone's responsibility (i.e. team leaders, supervisors, managers, co-workers, etc.) to supervise all workforce members and any other user of MiCT's systems, applications, servers, workstations, etc. that contain sensitive data.

1. Monitor workstations and applications for unauthorized use, tampering, and theft and report non-compliance according to the Security Incident Response policy.
2. Assist the Security and Privacy Officers to ensure appropriate role-based access is provided to all users.
3. Take all reasonable steps to hire, retain, and promote workforce members and provide access to users who comply with the Security regulation and MiCT's security policies and procedures.

Segregation of Duties MiCT has dedicated team/personnel assigned the job function of security and compliance. Segregation of duties are achieved via a combination of assignment of roles and responsibilities to different personnel, and automation enforcement for software-defined processes.

Checks and balances are ensured via such segregation of duties and related review/approval processes. When applicable, reviews and approvals must be obtained from designated personnel separate from the individual performing

the work.

Policy and Compliance Training

1. The Security & Privacy Officer facilitates the training of all workforce members as follows:
    1. New workforce members within their first month of employment;
    2. Existing workforce members annually;
    3. Existing workforce members whose functions are affected by a material change in the policies and procedures, within a month after the material change becomes effective;
    4. Existing workforce members as needed due to changes in security and risk posture of MiCT.
2. Documentation of the training session materials and attendees is retained for a minimum of seven years.
3. The training session focuses on, but is not limited to, the following subjects defined in MiCT's security policies and procedures:
    1. SOC 2 Security Principals and Controls;
    2. HIPAA Privacy, Security, and Breach notification rules;
    3. Risk Management procedures and documentation;
    4. Auditing. MiCT may monitor access and activities of all users;
    5. Workstations may only be used to perform assigned job responsibilities;
    6. Users may not download software onto MiCT's workstations and/or systems without prior approval from the Security Officer;
    7. Users are required to report malicious software to the Security Officer immediately;
    8. Users are required to report unauthorized attempts, uses of, and theft of MiCT's systems and/or workstations;
    9. Users are required to report unauthorized access to facilities
    10. Users are required to report noted log-in discrepancies (i.e. application states users last log-in was on a date user was on vacation);
    11. Users may not alter sensitive data maintained in a database, unless authorized to do so by a MiCT Customer;
    12. Users are required to understand their role in MiCT's contingency plan;
    13. Users may not share their user names nor passwords with anyone;
    14. Requirements for users to create and change passwords;
    15. Users must set all applications that contain or transmit sensitive data to automatically log off after 15 minutes of inactivity;
    16. Supervisors are required to report terminations of workforce members and other outside users;
    17. Supervisors are required to report a change in a users title, role, department, and/or location;

18. Procedures to backup sensitive data;
19. Procedures to move and record movement of hardware and electronic media containing sensitive data;
20. Procedures to dispose of discs, CDs, hard drives, and other media containing sensitive data;
21. Procedures to re-use electronic media containing sensitive data;
22. Secrets management (such as SSH key) and sensitive document encryption procedures.

Ongoing Awareness Training

MiCT leverages KnowBe4 to deliver innovative, fun and engaging security awareness contents to all employees monthly. This security awareness training shall include modules on

- phishing,
- social engineering,
- proper internet use (social media, email, clicking, etc),
- access control (proper passwords, 2FA, screen locking, etc),
- mobile device security,
- data protection, and
- system security (anti-malware, patches, secure configuration, etc).

Progress is tracked individually for each employee and reported on KnowBe4's cloud-managed learning platform.

HIPAA Awareness Training

MiCT requires all employees to take a HIPAA awareness training within 30 days of onboarding and annually thereafter. The training record is captured within the HR record and/or the learning system KnowBe4.

Internal Business Communications

Company-wide updates MiCT holds a company-wide roundtable at least quarterly to communicate updates across all aspects of business operations, performance and objectives.

Senior management sends out additional company-wide announcements as appropriate through pre-established internal communication channels such as email or messaging (e.g. Slack #general channel).

Departmental, team and/or project status updates Regular performance and status updates are communicated by each department, functional team, and/or designated individuals through pre-established channels.

Additionally, each project team maintains team updates at their own committed cadence and channel – for example, daily development standups/scrum or weekly team meetings.