HR and Personnel Security

2021.1

MiCT is committed to ensuring all workforce members actively address security and compliance in their roles at MiCT. We encourage self management and reward the right behaviors. This policy specifies acceptable use of end-user computing devices and technology. Additionally, 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.

Policy Statements

In addition to the roles and responsibilities stated earlier, MiCT policy requires all workforce members to comply with the Acceptable Use Policy for End-use Computing and HR Security Policy.

MiCT policy requires that:

(a) Background verification checks on all candidates for employees and contractors should be carried out in accordance with relevant laws, regulations, and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risk.

(b) Employees, contractors and third party users must agree and sign the terms and conditions of their employment contract, and comply with acceptable use.

(c) Employees will go through an onboarding process that familiarizes them with the environments, systems, security requirements, and procedures MiCT has in place. Employees will also have ongoing security awareness training that is audited.

(d) Employee offboarding will include reiterating any duties and responsibilities still valid after terminations, verifying that access to any MiCT systems has been removed, as well as ensuring that all company owned assets are returned.

(e) MiCT and its employees will take reasonable measures to ensure no sensitive data is transmitted via digital communications such as email or posted on social media outlets.

(f) MiCT will maintain a list of prohibited activities that will be part of onboarding procedures and have training available if/when the list of those activities changes.

(g) A fair disciplinary process will be utilized for employees are suspected of committing breaches of security. Multiple factors will be considered when deciding the response such as whether or not this was a first offense, training, business contracts, etc. MiCT reserves the right to terminate employees in the case of serious cases of misconduct.

Controls and Procedures

HR Management and Reporting

MiCT uses to manage its workforce personnel records.

Organization Structure

A reporting structure has been established that aligns with the organization's business lines and/or individual's functional roles. The organizational chart is available to all employees via the and/or posted on the internal web portal.

Job Functions and Descriptions

Position / Job descriptions are documented and updated as needed that define the skills, responsibilities, and knowledge levels required for certain jobs.

Performance Reviews and Feedback

Employees receive regular feedback and acknowledgement from their manager and peers. Formal performance reviews are conducted annually using EaseCentral. Performance measures, incentives, and other rewards are established by management according to responsibilities at all levels, reflecting appropriate dimensions of performance and expected standards of conduct.

Acceptable Use of End-user Computing

MiCT requires all workforce members to comply with the following acceptable use requirements and procedures, such that:

(a) Per MiCT security architecture, all workforce members are primarily considered as remote users and therefore must follow all system access controls and procedures for remote access.

(b) Use of MiCT computing systems is subject to monitoring by MiCT IT and/or Security team.

(c) Employees may not leave computing devices (including laptops and smart devices) used for business purpose, including company-provided and BYOD devices, unattended in public.

(d) Device encryption must be enabled for all mobile devices accessing company data, such as whole-disk encryption for all laptops.

(e) Use only legal, approved software with a valid license installed through a pre-approved application store. Do not use personal software for business purposes and vice versa.

(f) Encrypt all email messages containing sensitive or confidential data.

(g) Employees may not post any sensitive or confidential data in public forums or chat rooms. If a posting is needed to obtain technical support, data must be sanitized to remove any sensitive or confidential information prior to posting.

(h) Anti-malware or equivalent protection and monitoring must be installed and enabled on all endpoint systems that may be affected by malware, including workstations, laptops and servers.

(i) All data storage devices and media must be managed according to the MiCT Data Classification specifications and Data Handling procedures.

(j) It is strictly forbidden to download or store any sensitive data on end-user computing devices, including laptops, workstations and mobile devices.

(k) Mobile devices are not allowed to connect directly to MiCT production environments.

Employee Screening Procedures

MiCT publishes job descriptions for available positions and conducts interviews to assess a candidates technical skills as well as culture fit prior to hiring.

Background checks of an employee or contractor is performed by HR/operations and/or the hiring team prior to the start date of employment.

Employee Onboarding Procedures

A master checklist for employee onboarding is maintained by HR/Facilities.
It is published in the HR system or the HR folder on MiCT's internal file sharing site.

The HR Representative / Facility Manager is responsible to create an Issue in the Github HR & Facilities project to initiate and track the onboarding process. The onboarding process should include the following IT/Security items:

1. Training.

    - New workforce member is provided training on MiCT security policy, acceptable use policy, and given access to the Employee Handbook.
    - HIPAA awareness training is provided to new workforce member.
    - Records of training and policy acceptance is kept in the HR system (currently EaseCentral).
    - The training and acceptance must be completed within 30 days of employment.

2. Access.

    - Standard access is provisioned according to the job role and approval as specified in the HR onboarding Github ticket.

- Non-standard access requires additional approval following the access request procedures.
- Request for modifications of access for any MiCT employee can be made using the procedures outlined in the Access Establishment and Modification policy and procedures.

3. System configuration.

    - The end-user computing device (e.g. workstation or laptop) may be provisioned by IT to install necessary software, malware protection, security agents, and setting system configurations.
    - Users in a technical role, such as Development, may choose to self configure their system. In this case, the user is given configuration guidelines defined by IT and Security. The system must have the required security configuration and endpoint agents installed for monitoring and to ensure compliance.

Employee Exiting/Termination Procedures

A master checklist for employee existing/termination is maintained by HR/Facilities. It is published in the HR system or the HR folder on MiCT's internal file sharing site.

1. The Human Resources Department (or other designated department), users, and their supervisors (HR) are required to notify Security upon completion and/or termination of access needs and facilitating completion of the "Termination Checklist".

2. HR are required to notify Security to terminate a user's access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and is filed with the Privacy Officer):

    - The user has been using their access rights inappropriately;
    - A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password);
    - An unauthorized individual is utilizing a user's User Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).

3. Security will terminate users' access rights immediately upon notification, and will coordinate with the appropriate MiCT employees to terminate access to any non-production systems managed by those employees.

4. Security audits and may terminate access of users that have not logged into organization's information systems/applications for an extended period of time.

Employee Issue Escalation

MiCT workforce members are to escalate issues using the procedures outlined in the Employee Quick Reference. Issues that are brought to the Escalation Team are assigned an owner. The membership of the Escalation Team is maintained by the Chief Executive Officer or his delegate.

Security incidents, particularly those involving sensitive data, are handled using the process described in Incident Response. If the incident involves a breach of sensitive data, the Security Officer will manage the incident using the process described in Breach Notification. Refer to Incident Response for a list of sample items that can trigger MiCT's incident response procedures; if you are unsure whether the issue is a security incident, contact the Security team immediately.

It is the duty of the incident owner to follow the process outlined below:

1. Create an Issue in the Github Security Project.
2. The Issue is investigated, documented, and, when a conclusion or remediation is reached, it is moved to Review.
3. The Issue is reviewed by another member of the Escalation Team. If the Issue is rejected, it goes back for further evaluation and review.
4. If the Issue is approved, it is marked as Done, adding any pertinent notes required.
5. The workforce member that initiated the process is notified of the outcome via email.

Whistleblower Policy and Process

The MiCT requires all workforce members to observe high standards of business and personal ethics in the conduct of their duties and responsibilities. All workforce members must practice honesty and integrity in fulfilling their responsibilities and comply with all applicable laws and regulations.

(a) Reporting Responsibility. Each workforce member is required and encouraged to report serious concerns so that MiCT can address and correct inappropriate internal conduct and actions. This includes

- questionable or improper accounting or auditing matters,
- violations and suspected violations of company policies or ethics, or
- suspected violations of law or regulations that govern MiCT's operations

(b) Acting in Good Faith. Anyone filing a written complaint concerning a violation or suspected violation must be acting in good faith and have reasonable grounds for believing the information disclosed indicates a violation. Any allegations that prove not to be substantiated and which prove to have been made maliciously or knowingly to be false will be viewed as a serious disciplinary offense.

(c) Confidentiality. Insofar as possible, the confidentiality of the whistleblower will be maintained. However, identity may have to be disclosed to conduct a thorough investigation, to comply with the law, and to provide accused individuals their legal rights of defense.

(d) No Retaliation. Workforce members, in good faith, reporting a concern under the Whistleblower Policy shall NOT be subject to retaliation or adverse employment consequences. Moreover, any workforce member who retaliates against someone who has reported a concern in good faith is subject to disciplinary actions up to and including termination of employment.

(e) Reporting. Reports of concerns may be filed directly with the company CEO, COO, and/or the Compliance Officer. Additional reporting procedure details can be found in the employee handbook.

Employee Performance Review Process

Formal performance reviews are conducted annually using Small Improvements.

- 360 feedback is collected from team members working directly with the employee
- Employee provides their own self assessment for both performance outcome and behavior
- Manager reviews employee self-assessment and peer feedback, and documents the final review and rating
- The final review and rating is reviewed and signed by both the employee and their manager

Employee Incentives and Rewards

MiCT encourages employees to go above and beyond to contribute to the business objectives and help their peers and customers. Employees are recognized and rewarded for positive behavior on a regular basis via peer recognition, appreciation, feedback, and rewards using Motivosity.

Continuous Education and Skills Development

MiCT provides employees the opportunity to attend conferences, trade shows, and/or ongoing training/studies relevant to their job function and business objectives.

Non-Compliance Investigation and Sanctions

Workforce members shall report non-compliance of MiCT's policies and procedures to the Security Officer or other individual as assigned by the Security Officer. 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.

1. The Security Officer promptly facilitates a thorough investigation of all reported violations of MiCT's security policies and procedures. The Security Officer may request the assistance from others.

   - Complete an audit trail/log to identify and verify the violation and sequence of events.
   - Interview any individual that may be aware of or involved in the incident.
   - All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.
   - Provide individuals suspected of non-compliance of the Security rule and/or MiCT's policies and procedures the opportunity to explain their actions.
   - The investigator thoroughly documents the investigation as the investigation occurs. This documentation must include a list of all employees involved in the violation.

2. Violation of any security policy or procedure by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including business associates, customers, and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.

   - A fair disciplinary process will be utilized for employees are suspected of committing breaches of security. Multiple factors will be considered when deciding the response such as whether or not this was a first offense, training, business contracts, etc.
   - MiCT reserves the right to terminate employees in the case of serious cases of misconduct.
   - A violation resulting in a breach of confidentiality (i.e. release of sensitive data to an unauthorized individual), change of the data integrity, or inability to access data by other users, requires immediate termination of the workforce member from MiCT.

3. The Security Officer facilitates taking appropriate steps to prevent recurrence of the violation (when possible and feasible).

4. In the case of an insider threat, the Security Officer and Privacy Officer are to set up a team to investigate and mitigate the risk of insider malicious activity. MiCT workforce members are encouraged to come forward with information about insider threats, and can do so anonymously.

5. The Security Officer maintains all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of seven years after the conclusion of the investigation.

6. When the Security Officer identifies a violation and begins a formal sanction process, they will notify the appropriate management or supervisors within 24 hours. That notification will include 1) identifying the individual sanctioned, 2) the reason for the sanction, and 3) specific procedures for service or account restriction / revocation or other disciplinary actions as required.

Warning Notice Template