Policy Management

`2021.1`

MiCT implements policies and procedures to maintain compliance and integrity of data. The Security Officer and Privacy Officer are responsible for maintaining policies and procedures and assuring all MiCT workforce members, business associates, customers, and partners are adherent to all applicable policies. Previous versions of policies are retained to assure ease of finding policies at specific historic dates in time.

Policy Statements

MiCT policy requires that:

(a) MiCT policies must be developed and maintained to meet all applicable compliance requirements adhere to security best practices, including but not limited to:

- HIPAA
- SOC 2

(b) All policies must be reviewed at least annually.

(c) All policy changes must be approved by MiCT Security Officer. Additionally,

- Major changes may require approval by MiCT CEO or designee;
- Changes to policies and procedures related to product development may require approval by the Head of Engineering.

(d) All policy documents must be maintained with version control, and previous versions must be retained for a minimum of seven years.

(e) Policy exceptions are handled on a case-by-case basis.

- All exceptions must be fully documented with business purpose and reasons why the policy requirement cannot be met.
- All policy exceptions must be approved by both MiCT Security Officer and COO.
- An exception must have an expiration date no longer than one year from date of exception approval and it must be reviewed and re-evaluated on or before the expiration date.

Controls and Procedures

Policy Management Process

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

Each document starts with the current version number in the format of `YYYY.#` (e.g. `2017.1`), followed by a brief summary. The remaining of the document is structured to contain the following subsections:

- Policy Statements
- Applicable Standards
- Controls and Procedures

Versioning Each MiCT policy document contains a version and optionally a revision number. The version number is the four digit year followed by a number, to indicate the year and sequence number of the policy at which time it was written or updated.

The version number shall be incremented by one with each material change to the policy content. For example, if a new policy statement is added or a technical control/procedure is updated to `2017.1` version of a policy, the new version should be numbered `2017.2`.

The policy document may also include a revision number, in the format of `rev.#`, immediately following the main version number. A revision number indicate minor, non-material changes to the document, such as formatting changes, fixing typos, or adding minor details.

Numbering If sequencing numbers are included in the policy headings:

- Policy may be referenced by its statement number, such as `§2.1(a)`, in internal/external communications as well as in other MiCT policies or technical/business documentation for cross reference.
- As such, to maintain cross referencing integrity, starting from version `2017.2`, all numbering shall remain intact for policy documents and statements.
- When updating, avoid reordering and renumbering of policy documents and statements. For example:
  - Append at the end of the list by adding new statement(s) as needed instead of inserting.
  - If a policy or policy statement is no longer applicable, mark it deprecated instead of removing the file or statement completely.

Review and Maintenance of Policies

1. All policies are stored and up to date to maintain MiCT compliance with HIPAA,

   SOC 2 and other relevant standards. Updates and version control are done similar to source code control.

2. Policy update requests can be made by any workforce member at any time. Furthermore, all policies are reviewed annually by the Security and Privacy Officer to assure they are accurate and up-to-date.

3. MiCT employees may request changes to policies using the following process:

    1. The MiCT employee initiates a policy change request by creating an Issue in the Github Security project. The change request may optionally include a pull request from a separate branch or repository containing the desired changes.

    2. The Security Officer or the Privacy Officer is assigned to review the policy change request.

    3. Once the review is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review and documentation.

    4. If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.

    5. If the policy change requires technical modifications to production systems, those changes are carried out by authorized personnel using MiCT's change management process.

    6. If the change results in a new version instead of a new revision (see §3.3.1 for definitions), the current version of the policy document(s) must be saved to archive under the corresponding version number prior to the new policy being adopted/published and prior to merging the pull request containing the changes. This allows easy reference to previous versions if necessary.

    !!! important

    ```
    * Changes are made on the `drafts` (or equivalent) branch instead of on the `master` b
    * If multiple authors are working on the changes, additional separate branches and pul
    * Changes must not be merged to `master` without the approval of Security and Privacy
    * Changes must not be merged to `master` without archiving the existing version of pol
    * Once the changes are final and approved, a pull request shall be created from the `d
    * Policy update communication and training for non-development staff is conducted sepa
    ```

4. All policies are made accessible to all MiCT workforce members. The current master policies are published at https://mict-international.org/security.

    - Changes are automatically communicated to all MiCT team members through integrations between and Slack that log changes to a predefined MiCT Slack Channel.
    - The Security Officer also communicates policy changes to all employees via email. These emails include a high-level description of the

policy change using terminology appropriate for the target audience.

5. All policies, and associated documentation, are retained for 7 years from the date of its creation or the date when it last was in effect, whichever is later

    1. Version history of all MiCT policies is done via .
    2. Backup storage of all policies is done with AWS S3 and/or internal file share (e.g. Microsoft Office365 SharePoint or Box).

6. The policies and information security policies are reviewed and audited annually, or after significant changes occur to MiCT's organizational environment, by the security committee members. Issues that come up as part of this process are reviewed by MiCT management to assure all risks and potential gaps are mitigated and/or fully addressed. The process for reviewing polices is outlined below:

    1. The Security Officer initiates the policy review by creating an Issue in the Github Security project or via a Pull Request (PR).
    2. The Security Committee members and additional reviewers are notified by email or via the PR to review the current policies.
    3. If changes are made, the above process is used. All changes are documented in the Issue/PR.
    4. Once the review is completed, the Security Officer approves or rejects the Issue/PR. If the Issue/PR is rejected, it goes back for further review and documentation.
    5. If the review is approved, the Security Officer then marks the Issue as Done, or merges the PR into master branch, adding any pertinent notes required.
    6. Policy review is monitored using Github or reporting to assess compliance with above policy.

Additional documentation related to maintenance of policies is outlined in Roles and Responsibilities.