Compliance Audits and External Communications

`2021.1`

MiCT may be requested occasionally to share additional details regarding its compliance, privacy and security program by an external entity such as a customer, media, legal or law enforcement. Such external communication, beyond what is already publicly published, needs to comply with the following policies and procedures.

Policy Statements

MiCT policy requires that:

(a) MiCT operations must comply with all applicable laws, regulations, security standards and frameworks. External audits shall be conducted accordingly to each applicable compliance requirement.

- HIPAA/HITECH. MiCT must comply with all requirements listed in the HIPAA (Health Insurance Portability and Accountability Act of 1996) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.

(b) All external communications related to compliance and customer/employee privacy must follow pre-established procedures and handled by approved personnel. This includes but is not limited to distribution of audit reports, assessment results, incidents and breach notification.

(c) Audit and compliance reports may be shared with an external party only when under signed NDA and approved by MiCT Security and/or Privacy Officer.

Controls and Procedures

Compliance Program Management

MiCT management and security/compliance team has identified and regularly reviews all relevant statutory, regulatory, and contractual requirements.

MiCT's compliance policy includes requirements to meet any and all applicable compliance requirements.

Additionally, the Vendor Risk Management policies and procedures specify the details related to contractual agreements with clients, partners and vendors, as well as requirements and process related to intellectual property rights and the use of proprietary software products.

Requesting Audit and Compliance Reports

MiCT, at its sole discretion, shares audit reports, including any Corrective Action Plans (CAPs) and exceptions, with customers on a case by case basis. All audit reports are shared under explicit NDA in MiCT format between MiCT and party to receive materials. Audit reports can be requested by MiCT workforce members for Customers or directly by MiCT Customers.

The following process is used to request audit reports:

1. A request may be sent by email to compliance@mict-international.org or by submitting a request via MiCT Internal Support Portal or Email. In the request, please specify the type of report being requested and any required timelines for the report.
2. An Issue with the details of the request into the MiCT Security Project on Github, which is used to track requests status and outcomes.
3. MiCT security team will confirm if a current NDA is in place with the party requesting the audit report. If there is no NDA in place, MiCT will send one for execution.
4. Once it has been confirmed that an NDA is executed, MiCT staff will move the Github Issue to "Under Review".
5. The MiCT Security Officer or Privacy Officer must Approve or Reject the Issue. If the Issue is rejected, MiCT will notify the requesting party that we cannot share the requested report.
6. If the Issue has been Approved, MiCT will send the customer the requested audit report and complete the Github Issue for the request.

See detailed policy and procedures in Breach Notification

External Audits of Information Access and Activity Prior to contracting with an external audit firm, MiCT shall:

- Outline the audit responsibility, authority, and accountability
- Choose an audit firm that is independent of other organizational operations
- Ensure technical competence of the audit firm staff
- Require the audit firm's adherence to applicable codes of professional ethics
- Assign organizational responsibility for supervision of the external audit firm
- Obtain a signed HIPAA business associate agreement, if any ePHI will be shared/accessed during the audit

Whenever possible, a third party auditing vendor should not be providing the organization IT oversight services (e.g., vendors providing IT services should not be auditing their own services to ensure separation of duties).

Contacts for External Communications Requests Direct all other communication requests to one of the following:

- For incident reporting, vulnerability disclosure and other security related inquiries:
  - security@mict-international.org
  - https://mict-international.org/security
- For privacy concerns, including report of violation:
  - privacy@mict-international.org
  - https://mict-international.org/privacy
- For all compliance related issues, including request of audit reports:
  - compliance@mict-international.org

Continuous Compliance Monitoring

The status of compliance is tracked via JupiterOne. Compliance dashboards are configured with applicable internal and external standards and frameworks. Any potential gaps detected are reported on the compliance dashboards.