System Audits, Monitoring and Assessments

`2021.1`

MiCT shall audit, monitor, and assess the access and activity of systems and applications that process or store production and/or sensitive data such as personally identifiable information (PII) and electronic protected health information (ePHI) in order to ensure compliance.

It is required by the HIPAA Security Rule, that healthcare organizations to implement reasonable hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

Audit activities may be limited by application, system, and/or network auditing capabilities and resources. MiCT shall make reasonable and good-faith efforts to safeguard information privacy and security through a well-thought-out approach to auditing that is consistent with available resources.

It is the policy of MiCT to safeguard the confidentiality, integrity, and availability of applications, systems, and networks. To ensure that appropriate safeguards are in place and effective, MiCT shall audit access and activity to detect, report, and guard against:

- Network vulnerabilities and intrusions;
- Breaches in confidentiality and security of sensitive information;
- Performance problems and flaws in applications;
- Improper alteration or destruction of sensitive information;
- Out of date software and/or software known to have vulnerabilities.

This policy applies to all MiCT systems that store, transmit, or process sensitive information.

Policy Statements

MiCT policy requires that:

(a) All critical computing systems and software, both virtual and physical, must enable audit logging.

(b) Audit logs must include sufficient information to identify who did what, when, where.

(c) An annual audit of MiCT security controls must be conducted, either by a designated internal audit team or a qualified external audit firm.

Controls and Procedures

Types of System Audits

MiCT's auditing processes include the following.

1. **Configuration and Activity Monitoring:** This refers to the logging, monitoring, scanning and alerting of a system, account, or environment, which may be achieved using real-time automated scripts/software or a manual review/testing. This type of auditing is performed *continuously* as part of MiCT operations.

   !!! tip "Examples include:"

   ```
   * User: User and account-level audit trails generally monitor and log all commands dir
   * Application: Application-level audit trails generally monitor and log all user activ
   * System: System-level audit trails generally monitor and log user activities, applica
   * Network: Network-level scans or audit trails generally monitor information on what i
   * Traffic: Traffic refers to the incoming and outgoing traffic into and out of product
   * Data: Data includes all successful and failed attempts at production data access and

   *Data associated with above events will include origin, destination, action performed,
   ```

2. **Access Review:** This refers to the review of all user and service accounts and permissions across MiCT operational environments, including on-premise systems, cloud environments such as AWS accounts, and other applications such as collaboration software, ticketing system and code repos.

   - MiCT developed an internal tool to automatically pull configurations from our cloud based environments, including
     - AWS access configuration from IAM policies, EC2 VPC and security group settings, S3 bucket policies, Lambda and API Gateway resources, etc.;
     - Users, groups, application access from Okta IdP;
     - Network access settings from Cisco Meraki, etc.
   - The data is collected either on demand triggered by security team or by changes in the operational environment.
   - The data is used by the tool to aggregate and analyze user and application access.
   - Access to other systems and applications that are not covered by this automated tool are reviewed manually on a quarterly basis or with any significant change to the target environment.
   - As a result of each review, unused or invalid access will be removed.

3. **Compliance and Controls Audit:** This refers to the audit performed against the Technical, Administrative, and/or Physical controls as defined in MiCT policies and procedures, to measure their adoption and effectiveness. This type of auditing is typically performed by either a designated internal audit team or an external audit firm, at *defined intervals* or prompted by a *trigger event*.

   !!! tip "Potential trigger events include:"

   ```
   * Scheduled compliance audit/assessment (e.g. annual risk assessment)
   ```

```
* High risk or problem prone incidents or events, or as part of post-incident activiti
* Business associate, customer, or partner complaints
* Identification of significant security vulnerabilities
* Atypical patterns of activity
* Failed authentication attempts
* Remote access use and activity
* Activity post termination
* Random audits
```

Security Events Analysis

Security logs, events, and audit trails are reviewed by the security team with the assistance of automated systems and processes.

- Auditing logs are automatically analyzed and correlated by the monitoring solutions and/or a centralized security information and event management system.
- The systems are configured with rules/policies to identify suspicious activities, vulnerabilities and misconfigurations.

- Alerts are triggered upon identification of an issue based on the policy configuration.

- The alerts are sent immediately to the responsible staff (e.g. security team) for analysis. The alerts may be sent via email, Slack messaging, or as notification on the monitoring dashboard.
- Analysis is prioritized based on alert severity. High severity alerts are typically reviewed within 24 hours.
- Incident response process is followed, as needed.
- Patches and updates will be applied to all systems in a timely manner.

Internal/Manual Auditing Activities

Additional manual reviews, such as user accounts and access auditing, may be necessary from time to time. These activities may be triggered by the events listed above.

- Responsibility for audit activity is assigned to MiCT's Security Officer. The Security Officer shall:
  - Assign the task of generating reports for audit activities to the workforce member responsible for the application, system, or network;
  - Assign the task of reviewing the audit reports to the workforce member responsible for the application, system, or network, the Privacy Officer, or any other individual determined to be appropriate for the task;
  - Organize and provide oversight to a team structure charged with audit compliance activities (e.g., parameters, frequency, sample sizes,

report formats, evaluation, follow-up, etc.).
  - All connections to MiCT are monitored. Access is limited to certain services, ports, and destinations. Exceptions to these rules, if created, are reviewed on an annual basis.

- The manual review process shall define and include:
  - Description of the activity as well as rationale for performing the audit.
  - Identification of personnel to perform the review (workforce members shall not review audit logs that pertain to their own system activity).
  - Frequency of the auditing process.
  - Determination of significant events requiring further review and follow-up.
  - Identification of appropriate reporting channels for audit results and required follow-up.

- Manual audits and reviews activities are tracked in Github.

- Auditing, reviews and testing may be carried out internally or provided through an external third-party vendor. 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).

Audit Requests

1. A request may be made for an audit for a specific cause. The request may come from a variety of sources including, but not limited to, Privacy Officer, Security Officer, Customer, Partner, or an Application owner or application user.

2. A request for an audit for specific cause must include time frame, frequency, and nature of the request.

3. A request for an audit must be reviewed and approved by MiCT's Privacy Officer and/or Security Officer before proceeding. Under no circumstances shall detailed audit information be shared with parties without proper permissions and access to see such data.

    - Should the audit disclose that a workforce member has accessed sensitive data inappropriately, the minimum necessary/least privileged information shall be shared with MiCT's Security Officer to determine appropriate sanction/corrective disciplinary action.
    - Only de-identified information shall be shared with Customer or Partner regarding the results of the investigative audit process. This information will be communicated to the appropriate personnel by MiCT's Privacy Officer or designee. Prior to communicating with customers and partners regarding an audit, it is recommended that

MiCT consider seeking guidance from risk management and/or legal counsel.

Review and Reporting of Audit Findings

1. Audit information that is routinely gathered must be reviewed in a timely manner, at least monthly, by the responsible workforce member(s). Additional reviews are performed as needed to assure the proper data is being captured and retained.
2. The reporting process shall allow for meaningful communication of the audit findings to relevant workforce members, Customers, or Partners.
    - Significant findings shall be reported immediately in a written format. MiCT's security incident response form may be utilized to report a single event.
    - Routine findings shall be reported to the sponsoring leadership structure in a written report format.
3. Reports of audit results shall be limited to internal use on a minimum necessary/need-to-know basis. Audit results shall not be disclosed externally without administrative and/or legal counsel approval.
4. Security audits constitute an internal, confidential monitoring practice that may be included in MiCT's performance improvement activities and reporting. Care shall be taken to ensure that the results of the audits are disclosed to administrative-level oversight structures only and that information which may further expose organizational risk is shared with extreme caution. Generic security audit information may be included in organizational reports (individually-identifiable information shall not be included in the reports).
5. Whenever indicated through evaluation and reporting, appropriate corrective actions must be undertaken. These actions shall be documented and shared with the responsible workforce members, Customers, and/or Partners.

Remediation of Control Deficiencies

Most controls are continuously monitored and reported via automation on the JupiterOne platform.

Control deficiencies identified as a result of an internal or external system audit are documented and reviewed with management.

Security team works with the corresponding control owner to prioritize and mitigate the control deficiency, including applying corrective actions, implementating additional controls or adjusting existing controls as needed.

Audit Trails and Application Security Events Logging Standard

MiCT logging standards requires application and system logs to contain sufficient information to determine **who did what, when, where** to ensure recording of security and audit events and to generate evidence for unauthorized activities.

All systems and software developed at MiCT must have the following security events logging enabled as part of or in addition to standard application logging.

1. All security log events must have the following attributes at minimum:
    - Timestamp of the event (synchronized to approved time server)
    - Identifier of the principal performing the action (such as user ID)
    - Location including both origin (such as hostname/IP) and target (such as host/service/resource)
    - Activity or action (such as log in, log out, create, read, update, delete of a resource)
        - the action may be logged as and determined by the HTTP request method and the API endpoint
    - Event description and additional details may be logged depending on the system or application
2. The following types of security events must be logged at minimum:
    - User and group administration activities (user or group added, updated, deleted, access granted/revoked)
    - All login attempts, successful and unsuccessful including the source IP address
    - All interactive logoffs
    - Privileged actions (configuration changes, application shutdown/restart, software update etc)
    - Major application events (e.g. application failure, start and restart, shutdown)
    - Any and all actions performed on critical resources such as production data
3. All application and system logs must not include (removed or masked):
    - Any sensitive information, including protected health information (PHI), personally identifiable information (PII)
        - except for IP addresses
        - usernames/logins may/should be logged as part of authentication logging
        - for user action auditing, opaque IDs should be used instead of usernames/logins whenever possible
    - Authentication and session tokens, user credentials
4. Security events and audit logs must be:

- Always accessible to the monitoring system/team
- Protected from any changes
- Monitored with alerting mechanism in place (including alert for not receiving log events for a certain period of time)

5. All MiCT IT infrastructure must have system clock synchronized

Examples of recommended application events for logging and their auditing purpose:

Events	Purpose
Client requests and server responses	forensics and debugging - details level is defined by application
Successful and unsuccessful login attempts	authentication
Successful and failed access to application resources	authorization, escalation of privileges
Excessive amount of requests from the client	brute-forcing, malicious bots, denial of service attacks
E-mails sent by an application	spamming, social engineering

Details of the logging configuration is documented at

- Application Logging - documented on the Engineering Wiki
- Identity and Access Activity Logs via Okta
- AWS Cloudtrail
- AWS S3 Server Access Logs

Audit Trail Integrity - Security Controls and Log Retention

1. Audit logs shall be protected from unauthorized access or modification, so the information they contain will be made available only if needed to evaluate a security incident or for routine audit activities as outlined in this policy.

2. All audit logs are protected in transit and encrypted at rest to control access to the content of the logs.

3. Whenever possible, audit logs shall be stored on a separate system to minimize the impact auditing may have on the privacy system and to prevent access to audit trails by those with system administrator privileges.

    - Separate systems are used to apply the security principle of "separation of duties" to protect audit trails from hackers.
    - MiCT logging servers may include Elasticsearch, Logstash, and Kibana (ELK) as part of their baseline configuration to ease reviewing of audit log data. The ELK toolkit provides message summarization, reduction, and reporting functionality.

4. Reports summarizing audit activities shall be retained for a period of seven years.
5. Audit log data is retained locally on the audit log server or in the source environment for a period of one month. Beyond that, log data is encrypted and moved to warm storage (currently S3) using automated scripts, and is retained for a minimum of one year.
6. Raw event data may be purged after one month / 30 days as long as the required details are sufficiently covered in aggregated audit logs/reports.

Auditing Customer and Partner Activity

1. Periodic monitoring of Customer and Partner activity shall be carried out to ensure that access and activity is appropriate for privileges granted and necessary to the arrangement between MiCT and the 3rd party. MiCT will make every effort to assure Customers and Partners do not gain access to data outside of their own environments.
2. If it is determined that the Customer or Partner has exceeded the scope of access privileges, MiCT's management and security must remedy the problem immediately.
3. If it is determined that a Customer or Partner has violated the terms of the HIPAA business associate agreement or any terms within the HIPAA regulations, MiCT must take immediate action to remediate the situation. Continued violations may result in discontinuation of the business relationship.

Auditing and Assessment Tools

MiCT's Security Officer is authorized to select and use assessment tools that are designed to detect vulnerabilities and intrusions. Use of such tools against MiCT systems and environments are prohibited by others, including Customers and Partners, without the explicit authorization of the Security Officer. These tools may include, but are not limited to:

- Scanning tools and devices;
- Password cracking utilities;
- Network "sniffers";
- Security agents installed locally on servers and endpoints;
- Passive and active intrusion detection systems; and
- Penetration testing tools.

Vulnerability testing software may be used to probe the network to identify what is running (e.g., operating system or product versions in place), whether publicly-known vulnerabilities have been corrected, and evaluate whether the system can withstand attacks aimed at circumventing security controls.

Training, Education, Awareness and Responsibilities

1. MiCT workforce members are provided training, education, and awareness on safeguarding the privacy and security of business and data. MiCT's commitment to auditing access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies. MiCT workforce members are made aware of responsibilities with regard to privacy and security of information as well as applicable sanctions/corrective disciplinary actions should the auditing process detect a workforce member's failure to comply with organizational policies.

2. MiCT Customers are provided with necessary information to understand MiCT auditing capabilities. Platform Customers are responsible for the logging, auditing and retention of any application hosted outside of MiCT environments, even though the applications may integrate with MiCT Platform API. Customer applications hosted within the MiCT environments will follow the auditing standards and procedures defined in this document.