Access

`2021.1`

Access to MiCT systems and application is limited for all users, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants, and any other entity, is allowable only on a minimum necessary basis. All users are responsible for reporting an incident of unauthorized user or access of the organization's information systems.

These safeguards have been established to address the HIPAA Security regulations and industry best practices.

Policy Statements

Access Control Policy

MiCT policy requires that

(a) Access to all computing resources, including servers, end-user computing devices, network equipment, services and applications, must be protected by strong authentication, authorization, and auditing.

(b) Interactive user access must be associated to an account or login unique to each user.

(c) All credentials, including user passwords, service accounts, and access keys, must meet the length, complexity, age, and rotation requirements defined in MiCT security standards.

(d) Use strong password and multi-factor authentication (MFA) whenever possible to authenticate to all computing resources (including both devices and applications).

(e) MFA is required to access any critical system or resource, including but not limited to resources in MiCT production environments.

(f) Unused accounts, passwords, access keys must be removed within 30 days.

(g) A unique access key or service account must be used for different application or user access.

(h) Authenticated sessions must time out after a defined period of inactivity.

Access Authorization and Termination

MiCT policy requires that

(a) Access authorization shall be implemented using role-based access control (RBAC) or similar mechanism.

(b) Standard access based on a user's job role may be pre-provisioned during employee onboarding. All subsequent access requests to computing resources must be approved by the requestor's manager, prior to granting and provisioning of access.

(c) Access to critical resources, such as production environments, must be approved by the security team in addition to the requestor's manager.

(d) Access must be reviewed on a regular basis and revoked if no longer needed.

(e) Upon termination of employment, all system access must be revoked and user accounts terminated within 24 hours or one business day, whichever is shorter.

(f) All system access must be reviewed at least annually and whenever a user's job role changes.

Shared Secrets Management

MiCT policy requires that

(a) Use of shared credentials/secrets must be minimized and approved on an exception basis.

(b) If required by business operations, secrets/credentials must be shared securely and stored in encrypted vaults that meet the MiCT data encryption standards.

(c) Usage of a shared secret to access a critical system or resource must be supported by a complimenting solution to uniquely identify the user.

Privileged Access Management

MiCT policy requires that

(a) Users must not log in directly to systems as a privileged user.

- A privileged user is someone who has administrative access to critical systems, such as a Active Directory Domain Administrator, root user to a Linux/Unix system, and Administrator or Root User to an AWS account.

(b) Privilege access must only be gained through a proxy, or equivalent, that supports strong authentication (such as MFA) using a unique individual account with full auditing of user activities.

(c) Direct administrative access to production systems must be kept to an absolute minimum.

Controls and Procedures

Standards for Access Provisioning

Workforce Clearance

1. The level of security assigned to a user to the organization's information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user's job classification and/or to a user needing access to carry out treatment, payment, or healthcare operations.
2. All access requests are treated on a "least-privilege" principle.
3. MiCT maintains a minimum necessary approach to access to Customer data. As such, MiCT, including all workforce members, does not readily have access to any ePHI.

Access Authorization

1. Role based access categories for each MiCT system and application are pre-approved by the Security Officer.
2. MiCT utilizes hardware-defined and/or software-defined boundaries to segment data, prevent unauthorized access, and monitor traffic for denial of service attacks.

Person or Entity Authentication

1. Each workforce member has and uses a unique user ID and password that identifies him/her as the user of the information system.
2. Each Customer and Partner has and uses a unique user ID and password or OpenID Connect that identifies him/her as the user of the information system. This is enforced through the use of **AWS Cognito**.
3. All customer support interactions must be verified before MiCT support personnel will satisfy any request having information security implications.

Unique User Identification

1. Access to the MiCT Platform systems and applications is controlled by requiring unique User Login IDs and passwords for each individual user and developer.
2. Passwords requirements mandate strong password controls (see below).
3. Passwords are not displayed at any time and are not transmitted or stored in plain text.
4. Default accounts on all production systems and environments, including root, are disabled/locked.
5. Shared accounts are not allowed within MiCT systems or networks.

Automatic Logon and Logoff

1. Automated log-on configurations that store user passwords or bypass password entry are not permitted for use with MiCT workstations or production systems.
    - Automatic log-on may only be permitted for low-risk systems such as conference room PCs connecting to a Zoom Room.

    - Such systems are configured on separate network VLANs.

2. Users are required to make information systems inaccessible by any other individual when unattended by the users (ex. by using a password protected screen saver or logging off the system).
3. Information systems automatically lock users such as enabling password-protected screensaver after 2 minutes or less of inactivity.
4. Information systems automatically enter standby or log users off the systems after 30 minutes or less of inactivity.
5. The Security Officer must pre-approves any exception to automatic log off requirements.

Password Management

1. User IDs and passwords are used to control access to MiCT systems and may not be disclosed to anyone for any reason.
2. Users may not allow anyone, for any reason, to have access to any information system using another user's unique user ID and password.
3. On all production systems and applications in the MiCT environment, password configurations are set to require:
    - a minimum length of 12 characters;
    - a mix of upper case characters, lower case characters, and numbers or special characters;
    - a 60-day password expiration, or 60-day password expiration for administrative accounts;

    - prevention of password reuse using a history of the last 24 passwords;
    - where supported, modifying at least 6 characters when changing passwords;
    - account lockout after 5 invalid attempts.

    !!! check "Exceptions"

    ```
    Password expiration may be set to a greater interval if an account is always protected
    Currently, Okta SSO password rotation interval is set to 60 days.
    ```

4. All system and application passwords must be stored and transmitted securely.
    - Where possible, passwords should be stored in a hashed format using a salted cryptographic hash function (SHA-256 or stronger NIST compliant standard).
    - Passwords that must be stored in non-hashed format must be encrypted at rest pursuant to the requirements in Data Protection.

   - Transmitted passwords must be encrypted in flight pursuant to the requirements in Data Protection.

5. Each information system automatically requires users to change passwords at a pre-determined interval as determined by the system owner and/or Security, based on the criticality and sensitivity of the data contained within the network, system, application, and/or database.
6. Passwords are inactivated immediately upon an employee's termination (refer to the Employee Termination Procedures in HR policy).
7. All default system, application, and Vendor/Partner-provided passwords are changed before deployment to production.
8. Upon initial login, users must change any passwords that were automatically generated for them.
9. Password change methods must use a confirmation method to correct for user input errors.
10. All passwords used in configuration scripts are secured and encrypted.
11. If a user believes their user ID has been compromised, they are required to immediately report the incident to the Security team.
12. In cases where a user has forgotten their password, password reset procedures provided by the IdP shall be followed. The exact process depends on the system or application. If help is needed, users shall contact IT Support or Security
13. An approved password manager is used for to store or share non-critical business application passwords that are not integrated with our primary IdP through SSO.
    - The password manager locally encrypts the password vault with the user's master password before synchronizing to the cloud.
    - The master password must follow the password requirements listed above.
    - MFA must enabled in the password manager configuration.
    - Enrollment of the password manager is configured as an application in Okta.
14. An automated process/tool is implemented to ensure compromised passwords or common dictionary words are not used as passwords. This is currently implemented in Okta.

Single Sign On

- MiCT selected Okta as its primary Identity Provider (IdP) to control user access to systems and business applications.

- Single sign-on (SSO) should be used whenever possible instead of local authentication. This centralized approach improves user experience and simplifies access management.
- SSO is configured via industry standard SAML protocol between the IdP (Okta) and the target application.
- MiCT will not configure SSO to target applications unless they score a “B” rating or higher on the Qualys SSL Labs benchmark.
- Security team is responsible for the administration of the IdP / SSO system, including user and access provisioning. Security team may delegate administrative privilege to a subset of the system, such as a specific application.

Multi-factor Authentication

Multi-factor authentication (MFA) is a standard control used by MiCT to provide strong access control to critical systems and applications, and should be enabled whenever possible.

MiCT implements Okta for MFA.

!!! important

```
**Approved MFA methods include:**

- Push notification delivered through the Okta mobile app (default and preferred for end-use
- Hardware MFA token (required for the root user of AWS accounts)
- A unique cryptographic certificate tied to a device
- Time-based One-Time Password (TOTP) delivered through a mobile app, such as Google Authent
- One-time passcode delivered through SMS text message (if it is the only supported option)
- Secure physical facility (if the system or application can only be accessed at that locati
```

Role Based Access Control (RBAC)

By default, user access is granted based on the user’s job function / role. For example:

- Developer
- Security
- IT
- Administrative
- Marketing / Sales

This is defined as **user groups** in .

Access to sensitive data and production customer data is highly restricted and further defined in its own section.

Temporary Access to AWS Accounts and Resources

Access to MiCT AWS accounts are permissible through temporary credentials / sessions only. No persistent users, passwords or access keys are allowed in AWS IAM configurations for end-user access, either to the AWS console or AWS CLI. This is achieved with the following processes:

AWS Console Access

- An organization master account (`MiCT-master`) in AWS is configured with IAM roles such as Developer and Security.
- SAML SSO and trust relationship is established between the roles in `MiCT-master` and an "AWS application" provisioned in Okta.
- Users are assigned their corresponding roles through application and role assignment in Okta.
- Via SSO, Users authenticate through Okta by using their Okta username, password, and MFA.
- Upon successful authentication and MFA validation, users are logged into `MiCT-master` using AWS Assume Role capability.
- The roles in `MiCT-master` by default has highly restricted access. For example, the `Developer` role does not have access to any services and resources in the master account.
- The user is required to Assume a Role in a sub-account, connected via cross-account trust policy defined at account bootstrap or through an approved change management process. For example, a Developer can assume the `Administrator` role in `MiCT-dev`, which is the sandboxed development environment in a separate AWS account.
- Assume Role access to a production AWS account is highly restricted.
    - Developers can only assume the `Developer` role in production which only has access to read CloudWatch logs, XRay system traces/service maps, CloudWatch metrics, resource group inventories, and CloudWatch dashboards.
    - Security can only assume the `Auditor` role in production which has the default Auditor IAM policy managed by AWS. This policy allows read-only access to account and resource configurations, but does not allow read access to any data such as S3 objects.

AWS CLI/SDK Access

- Okta AWS-CLI Tool is used to obtain temporary credentials (access keys) for developers to connect to AWS using the CLI or SDK.
- By running the Okta AWS-CLI Tool, developers are prompted to authenticate to Okta using their Okta credentials and MFA token/app.

- Upon successful authentication and MFA validation, a temporary access key and session token is inserted into the local configuration file (e.g. `~/.aws/credentials` and `~/.aws/config`).
- This temporary credentials expires after one hour and a new temporary credential must be obtained for access.
- Through this method, developers are granted the same permission as they would by assuming the `Developer` role through AWS console.
- Additional details are documented on the Development Wiki.

IAM Safety

- MiCT implements **Dome9** to monitor and protect its AWS environments. Dome9 provides an additional layer of defense on top of native IAM policies called **IAM Safety**.
- IAM Safety works by defining a set of risky actions, such as adding/remove IAM users to an **Explicit Deny** policy. The policy is attached to an IAM Group, and protected Users and/or Roles are assigned to this Group.
- Because explicit deny rules always take precedence in AWS IAM policy, this effectively restricts access and prohibits execution of the risky actions as defined in the policy, even if the user/role may have administrative privilege.
- Original access can be temporarily restored through the Dome9 web console or its mobile app.
- Privilege Roles, such as Security role in master account and Administrator role in production account, are protected by IAM Safety.
- Additional details can be found on Dome9's product documentation.

Troubleshooting / Support Access

In normal operations, troubleshooting is performed with log analysis in Sumo Logic, outside of the production environments in AWS. A separate Support role is created for temporary troubleshooting and support access when log access is insufficient to determine the cause. Support access should be minimized and is designed to involve manual approval and provision process.

- The Support role by default is NOT assigned to anyone.
- The Support role is configured with Read level access to the services used by MiCT platform services and applications. It does NOT have permission to make any configuration changes and does NOT have access to production data.
- A PRODCM ticket is used to request temporary support access and must be approved by Head of Engineering and Security.
- Upon approval of the support access PRODCM ticket, Security grants the requestor temporary access to by assigning the Support role to that particular individual user in Okta.
- The Support role is protected by Dome9 with IAM Safety and it must be explicitly allowed by the Security team for it to assume the Support role in the target production environment.

- By default, temporary Support access is limited to one hour. This can be extended by the Security team.
- The role assignment is removed from Okta immediately after the support session and Dome9 IAM Safety is re-enabled.

Dual Control for Root Access

MiCT implements a Dual Control / Split Knowledge process to protect the Root user access to our AWS accounts. The process works as follow:

- Security Lead has access to the root account credentials.
  - The credentials are stored encrypted in the master account.
  - Security Lead obtains temporary access to the master account following the process listed above (MFA is required).
  - Security Lead must assume a role with permission to access the credential (e.g. Administrator), which is protected by an additional layer of IAM Safety.
- Engineering Lead has access to the Hardware Tokens associated with the root users.
  - The tokens are stored in secured facility with restricted badge reader access.
  - The token serial is mapped per account and documented in MiCT Engineering Wiki.

When root access is required for business or operational needs, a Github Issue is created that requires the Security Lead and Engineering Lead to jointly perform the action.

Remote Access / VPN

- VPN remote access to non-production and non-privileged environments in AWS are permissible and implemented using **Pritunl**.
- VPN remote access to master and production accounts are prohibited.
- VPN remote access to MiCT office network(s) is configured via **Pritunl**, and should be used whenever connecting from public networks.

Access to PHI/ePHI

1. Access to ePHI is permitted to genomics science staff, or staff that otherwise has a business need to access.
2. Access to any on-premise server that contains ePHI is restricted and monitored. *Currently MiCT has no on-premise server that stores or processes ePHI.*
3. Access to ePHI in MiCT's production environments in the cloud is strictly prohibited. Access is protected via multiple layers of security controls such

as IAM policies, restricted IAM roles, VPC configuration, S3 bucket policy, external monitoring, etc.

4. Users may not download ePHI to any workstations or end-user computing devices.

Platform Customer Access to Systems

MiCT does not allow direct system access by customers. Access is only available through the Web UI or API interface, with valid authentication and authorization detailed in the Product Security, Architecture, and Security pages of the engineering wiki.

Access Establishment, Modification and Termination

1. Requests for access to MiCT Platform systems and applications is made formally using the following process:

    1. An access request is created in Github through either the new employee onboarding request or a specific access request from MiCT Internal Support site.

    2. The Security team will grant standard access to per job role as part of new employee onboarding. A standard set of accounts that are default for all employees are created as part of the onboarding process. This includes

        - User account for local system/laptop
        - Okta user in the Everyone group, and additional group based on role such as Development, IT, Security
        - Office365 account for access to Outlook email, SharePoint, etc.
        - Ataata account for security awareness training
        - HR accounts for paperwork, benefits management, payroll, expense reporting, etc.
        - Github access for submitting support requests
        - Additional role based access (e.g. and https://localhost access for a developer)

    3. Standard access may be provisioned at any time by account owners/administrators at any time during or after onboarding with approval of account owners and/or manager.

    4. If additional access is needed in addition to the above, a separate access request (through Github) is required and the requester must include a description and justification as part of the access request.

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

6. If the review is approved, IT or Security team provisions access, then marks the Issue as Done, adding any pertinent notes required.
   - New accounts will be created with a temporary secure password that meets all password requirements, which must be changed on the initial login.
   - All password exchanges must occur over an authenticated channel.
   - For on-premise systems, access grants are accomplished by adding the appropriate user account to the corresponding LDAP/AD group.
   - For cloud accounts, access grants are provisioned in Okta or using the access control mechanisms built into those services/applications.
   - Account management for non-production systems may be delegated to a MiCT employee at the discretion of the Security Officer.

2. Special access, including access to production environments, is not granted until receipt, review, and approval by the MiCT Security Officer.
3. The request for access is retained for future reference.
4. Temporary accounts are not used unless absolutely necessary for business purposes.
   - Accounts are reviewed every 90 days to ensure temporary accounts are not left unnecessarily.
   - Accounts that are inactive for over 90 days are removed.
5. In the case of non-personal information, such as generic educational content, identification and authentication may not be required.

Access Termination IT Manager or Security team receives access termination requests in one of the following conditions and processes it accordingly:

- Employee existing/termination, as defined by the process in HR & Employee Security;
- Employee access to a system is no longer required as a result of job role change or similar event, in which case a access termination request may be submitted by the employee or his/her manager via the Internal Help portal or an email request to Security team;
- As the result of a Access Review, as defined in System Auditing.
- Non-standard access is revoked by default after 30 days of inactivity, unless an exception/extension is requested and approved.

Access Reviews

- All access to MiCT systems and services are reviewed and updated following the procedures specified in System Auditing to ensure proper authorizations are in place commensurate with job functions.
- In cases of increased risk or known attempted unauthorized access, immediate steps are taken by the Security and Privacy Officer to limit access and reduce risk of unauthorized access.

Privileged Access

Privileged users must first access systems using standard, unique user accounts before elevating the privilege or switching to privileged users and performing privileged tasks. Examples include:

- `sudo` in Linux/macOS
- `Run as Administrator` in Windows
- `Assume role` in AWS

Service Accounts

- All application to application communication using service accounts is restricted and not permitted unless absolutely needed. Automated tools are used to limit account access across applications and systems.
- Services that are part of MiCT platform leverage AWS IAM policy configurations and/or OAuth for authorization.
- Generic accounts are not allowed on MiCT systems.
- Direct system to system, system to application, and application to application authentication and authorization are limited and controlled to restrict access.
- In AWS, service accounts are implemented in the form of IAM Roles, and their access defined by the corresponding IAM policies. The creation of these IAM roles and policies is implemented as code, which follows the secure development, review and production change approval process.
- An inventory of all Service accounts is maintained by AWS IAM and Terraform and reviewed periodically.

Employee Workstation / Endpoints Access and Usage

All workstations at MiCT are company owned, using one the following approved hardware vendors and operating systems:

- Apple, Dell, or Lenovo
- macOS, Linux (Ubuntu or Debian), or Windows 10

1. Workstations may not be used to engage in any activity that is illegal or is in violation of organization's policies.
2. Access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or "X-rated". Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition shall be transmitted or maintained. No abusive, hostile, profane, or offensive language is to be transmitted through organization's system.
3. Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization's best interests. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
4. Solicitation of non-company business, or any use of organization's information systems/applications for personal gain is prohibited.
5. Users may not misrepresent, obscure, suppress, or replace another user's identity in transmitted or stored messages.
6. Workstation hard drives will be encrypted using FileVault (macOS), BitLocker (Windows) or equivalent.
7. All workstations must have host firewalls enabled to prevent unauthorized access unless explicitly granted.
8. All workstations must have endpoint security software installed and actively running, if supported by the operating system.

Office Network and Wireless Access

1. MiCT production systems are not accessible directly over wireless channels.

2. Wireless access is disabled on all production systems.

3. When accessing production systems via remote wireless connections, the same system access policies and procedures apply to wireless as all other connections, including wired.

4. Wireless networks managed within MiCT non-production facilities (offices, etc.) are secured with the following configurations:

    - All data in transit over wireless is encrypted using WPA2 encryption;
    - Passwords are not currently on a rotation schedule because the office environments are considered insecure.

    - Passwords are changed immediately should a suspicious activity or indicator of compromise is detected.
    - Guest wireless access is on a separate SSID configured with different password and traffic VLAN.
    - Wireless access is managed by the IT Manager.

- Wireless access points connected to the network are automatically scanned; rogue access points identified are immediately removed.

Production Access and Secrets Management

MiCT leverages a combination of https://localhost credentials store, credstash, and Amazon EC2 Systems Manager Parameter Store to securely store production secrets. Secrets are always encrypted; access to secrets is always controlled and audited.

Details and usage are documented on the MiCT Engineering Wiki.

Production Data Access

The following requirements and controls are in place for accessing production data by internal personnel:

- There is no pre-provisioned, persisted "internal" access to production data stores. Access such as direct SSH to the production database servers and direct access to data objects in production S3 buckets are prohibited.
- Access to customer data is granted on a per-account basis.
- Access requests follow the same production access processes. Access must be approved by both the data owner and the security team.
- Access to production data is granted only through an approved platform with strong centralized access control, with MFA.
- An audit list of who has access to which customer data is maintained and reviewed monthly. Access is revoked when no longer needed.

Password Reset and other Helpdesk Requests

MiCT employees have the ability to obtain self-service support directly from supported business applications, such as password reset via the SSO/IdP tool.

If needed, users may use our internal service desk or email request to obtain IT and Security support.

A ticket is opened in Github for each support request and assigned to the appropriate personnel. The person assigned must verify the identity of the requester and ensure the ticket has appropriate approval before implementing or providing support. The verification step and confirmation of "User identity verified" should be included as a comment in the ticket by the support personnel. Additionally, if a password or security credential has been created or supplied, confirm user has received it via another channel like slack/email/phone/zoom and document receipt in the ticket.