Data Protection

`2021.1`

MiCT takes the confidentiality and integrity of its customer data very seriously. As stewards and partners of MiCT Customers, we strive to assure data is protected from unauthorized access and that it is available when needed. The following policies drive many of our procedures and technical controls in support of the MiCT mission of data protection.

Production systems that create, receive, store, or transmit Customer data (hereafter "Production Systems") must follow the requirements and guidelines described in this section.

Policy Statements

MiCT policy requires that:

(a) Data must be handled and protected according to its classification requirements and following approved encryption standards, if applicable.

(b) Whenever possible, store data of the same classification in a given data repository and avoid mixing sensitive and non-sensitive data in the same repository. Security controls, including authentication, authorization, data encryption, and auditing, should be applied according to the highest classification of data in a given repository.

(c) Workforce members shall not have direct administrative access to production data during normal business operations. Exceptions include emergency operations such as forensic analysis and manual disaster recovery.

(d) All Production Systems must disable services that are not required to achieve the business purpose or function of the system.

(e) All access to Production Systems must be logged, following the MiCT Auditing Policy.

(f) All Production Systems must have security monitoring enabled, including activity and file integrity monitoring, vulnerability scanning, and/or malware detection, as applicable.

Controls and Procedures

Data Protection Implementation and Processes

Data is classified and handled according to the MiCT Data Handling Specifications and Data Classification document.

Critical, confidential and internal data will be tagged upon creation, if tagging is supported. Each tag maps to a data type defined in the data classification scheme, which then maps to a protection level for encryption, access control,

backup, and retention. Data classification may alternatively be identified by its location/repository. For example, source codes in MiCT's repos are considered "Internal" by default, even though a tag is not directly applied to each source file.

Critical and confidential data is always stored and transmitted securely, using approved encryption standards. More details are specified in MiCT's Data Classification and Handling document.

All IT systems that process and store sensitive data follow the provisioning process, configuration, change management, patching and anti-malware standards as defined in Configuration and Change Management document.

Customer/Production Data Protection MiCT hosts on Amazon Web Services in the US-East (Ohio) region by default. Data is replicated across multiple regions for redundancy and disaster recovery.

All MiCT employees, systems, and resources adhere to the following standards and processes to reduce the risk of compromise of Production Data:

1. Implement and/or review controls designed to protect Production Data from improper alteration or destruction.
2. Ensure that confidential data is stored in a manner that supports user access logs and automated monitoring for potential security incidents.
3. Ensure MiCT Customer Production Data is segmented and only accessible to Customer authorized to access data.
4. All Production Data at rest is stored on encrypted volumes using encryption keys managed by MiCT. Encryption at rest is ensured through the use of automated deployment scripts referenced in Configuration and Change Management.
5. Volume encryption keys and machines that generate volume encryption keys are protected from unauthorized access. Volume encryption key material is protected with access controls such that the key material is only accessible by privileged accounts.
6. Encrypted volumes use approved cipher algorithms, key strength, and key management process as defined in §12.3.1 above.
7. Raid volume drives are individually encrypted and assembled on boot requiring a manual input of the key to mount the encrypted volume.

Access MiCT employee access to production is guarded by an approval process and by default is disabled. When access is approved, temporary access is granted that allows access to production. Production access is reviewed by the security team on a case by case basis.

Separation Customer data is logically separated at the database/datastore level using a unique identifier for the institution. The separation is enforced at the API layer where the client must authenticate with a chosen institution and

then the customer unique identifier is included in the access token and used by the API to restrict access to data to the institution. All database/datastore queries then include the institution identifier.

Backup and Recovery For details on the backup and recovery process, see controls and procedures defined in Data Management.

Monitoring MiCT uses AWS CloudWatch/CloudTrail to monitor the entire cloud service operation. If a system failure and alarm is triggered, key personnel are notified by text, chat, and/or email message in order to take appropriate corrective action. Escalation may be required and there is an on-call rotation for major services when further support is necessary.

MiCT uses a security agent to monitor production systems. The agents monitor system activities, generate alerts on suspicious activities and report on vulnerability findings to a centralized management console.

The security agent is installed on all on premise Linux servers. It is also built into Amazon Machine Images (AMIs) for use in MiCT AWS environments.

Protecting Data At Rest

Encryption of Data at Rest All databases, data stores, and file systems are encrypted with AES-256 using separate keys for each storage type. The keys are rotated periodically.

Local Disk/Volume Encryption Encryption and key management for local disk encryption of on-premise servers and end-user devices follow the defined best practices for Windows, macOS, and Linux/Unix operating systems, such as Bitlocker and FileVault.

Protecting Data In Transit

1. All external data transmission is encrypted end-to-end using encryption keys managed by MiCT. This includes, but is not limited to, cloud infrastructure and third party vendors and applications.
2. Transmission encryption keys and systems that generate keys are protected from unauthorized access. Transmission encryption key materials are protected with access controls, and may only be accessed by privileged accounts.
3. Transmission encryption keys use a minimum of 4096-bit RSA keys, or keys and ciphers of equivalent or higher cryptographic strength (e.g., 256-bit AES session keys in the case of IPSec encryption).
4. Transmission encryption keys are limited to use for one year and then must be regenerated.

5. For all MiCT APIs, enforcement of authentication, authorization, and auditing is used for all remote systems sending, receiving, or storing data.
6. System logs of all transmissions of Production Data access are kept. These logs must be available for audit.

Encryption of Data in Transit All internet and intranet connections are encrypted and authenticated using TLS 1.2 (a strong protocol), ECDHE_RSA with P-256 (a strong key exchange), and AES_128_GCM (a strong cipher).

Data protection via end-user messaging channels Restricted and sensitive data is not allowed to be sent over electronic end-user messaging channels such as email or chat, unless end-to-end encryption is enabled.

Protecting Data In Use

Data in Use, sometimes known as Data in Process, refers to active data being processed by systems and applications which is typically stored in a non-persistent digital state such as in computer random-access memory (RAM), CPU caches, or CPU registers.

Protection of data in use relies on application layer controls and system access controls. See the Production Security / SDLC and Access sections for details.

MiCT applications implement logical account-level data segregation to protect data in a multi-tenancy deployment. In addition, MiCT applications may incorporate advanced security features such as Runtime Application Self Protection (RASP) modules and Attribute Based Access Control (ABAC) for protection of data in use.

Encryption Key Management

MiCT uses AWS Key Management Service (KMS) for encryption key management.

- KMS keys are unique to MiCT environments and services.
- KMS keys are automatically rotated yearly.

Certificate Management

MiCT uses AWS Certificate Manager (ACM) and LetsEncrypt for certificate management.

- Certificates are renewed automatically.
- Security team monitors the certificates for expiration, potential compromise and use/validity. Certificate revocation process is invoked if the certificate is no longer needed or upon discovery of potential compromise.

Data Integrity Protection

When appropriate, MiCT engineering should implement "Versioning" and "Lifecycle", or equivalent data management mechanism, such that direct edit and delete actions are not allowed on the data to prevent accidental or malicious overwrite. This protects against human errors and cyberattacks such as ransomware.

In AWS, the IAM and S3 bucket policy in production will be implemented accordingly when the environments are configured. When changes must be made, a new version is created instead of editing and overwriting existing data.

- All edits create a new version and old versions are preserved for a period of time defined in the lifecycle policy.
- Data objects are "marked for deletion" when deleted so that they are recoverable if needed within a period of time defined according to the data retention policy.
- Data is archived offsite – i.e. to separate AWS account and/or region.

Additionally, all access to sensitive data is authenticated, and audited via logging of the infrastructure, systems and/or application.