# Data Management Policy

`2021.1`

This policy outlines the requirements and controls/procedures MiCT has implemented to manage the end-to-end data lifecycle, from data creation/acquisition to retention and deletion.

Additionally, this policy outlines requirements and procedures to create and maintain retrievable exact copies of electronic protected health information(ePHI), PII and other critical customer/business data.

Data backup is an important part of the day-to-day operations of MiCT. To protect the confidentiality, integrity, and availability of sensitive and critical data, both for MiCT and MiCT Customers, complete backups are done daily to assure that data remains available when it needed and in case of a disaster.

## Policy Statements

MiCT policy requires that

(a) Data should be classified at time of creation or acquisition according to the MiCT data classification model, by labeling or tagging the data.

(b) Maintain an up-to-date inventory and data flows mapping of all critical data.

(c) All business data should be stored or replicated to a company controlled repository, including data on end-user computing systems.

(d) Data must be backed up according to its level defined in MiCT data classification.

(e) Data backup must be validated for integrity.

(f) Data retention period must be defined and comply with any and all applicable regulatory and contractual requirements. More specifically,

- Data and records belonging to MiCT platform customer must be retained per MiCT product terms and conditions and/or specific contractual agreements.

(g) By default, all security documentation and audit trails are kept for a minimum of seven years, unless otherwise specified by MiCT data classification, specific regulations or contractual agreement.

## Controls and Procedures

### Data Classification Model

MiCT defines the following four classifications of data:

- **Critical**
- **Confidential**
- **Internal**
- **Public**

**Definitions and Examples** **Critical** data includes data that must be protected due to regulatory requirements, privacy, and/or security sensitivities.

Unauthorized disclosure of critical data may result in major disruption to business operations, significant cost, irreparable reputation damage, and/or legal prosecution to the company.

External disclosure of critical data is strictly prohibited without an approved process and agreement in place.

*Example Critical Data Types* includes

- PII
- PHI or ePHI
- Production Security data, such as
  - Production secrets, passwords, access keys, certificates, etc.
  - Production security audit logs, events, and incident data

**Confidential** and proprietary data represents company secrets and is of significant value to the company.

Unauthorized disclosure may result in disruption to business operations and loss in value.

Disclosure requires the signing of NDA and management approval.

*Example Confidential Data Types* includes

- Business plans
- Employee/HR data
- News and public announcements (pre-announcement)
- Patents (pre-filing)
- Specialized source codes
- Non-production Security data, including
  - Non-prod secrets, passwords, access keys, certificates, etc.
  - Non-prod security audit logs, events, reports, and incident data
  - Audit/compliance reports, security architecture docs, etc.

**Internal** data contains information used for internal operations.

Unauthorized disclosure may cause undesirable outcome to business operations.

Disclosure requires management approval. NDA is usually required but may be waived on a case-by-case basis.

*Example Internal Data Types* includes

- Internal documentation
- Policies and procedures
- Product roadmaps
- Most source codes

**Public** data is Information intended for public consumption. Although non-confidential, the integrity and availability of public data should be protected.

*Example Internal Data Types* includes

- News and public announcements (post-announcement)
- Marketing materials
- Product documentation
- Contents posted on company website(s) and social media channel(s)

### Data Handling Requirements Matrix

Requirements for data handling, such as the need for encryption and the duration of retention, are defined according to the MiCT Data Classifications.

| Data | Labeling or Tagging | Segregated Storage | Endpoint Storage | Encrypt At Rest | Encrypt In Transit | Encrypt In Use | Controlled Access | Monitoring | Destruction at Disposal | Retention Period | Backup Recovery |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Critical** | Required | Required | Prohibited | Required | Required | Required | Access is blocked to end users by default; Temporary access for privileged users only | Required | Required | 7 years for audit trails; Varies for customer-owned data† | Required |

| Data | Labeling or Tagging | Segregated Storage | Endpoint Storage | Encrypt At Rest | Encrypt In Transit | Encrypt In Use | Controlled Access | Monitoring | Destruction at Disposal | Retention Period | Backup Recovery |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Confidential** | Required | N/R | Allowed | Required | Required | Required | All access is based on need-to-know | Required | Required | 7 years for official documentation; Others vary based on business need | Required |
| **Internal** | Required | N/R | Allowed | N/R | N/R | N/R | All employees and contractors (read); Data owners and authorized individuals (write) | N/R | N/R | 7 years for official documentation; Others vary based on business need | Optional |

| Data | Labeling or Tagging | Segregated Storage | Endpoint Storage | Encrypt At Rest | Encrypt In Transit | Encrypt In Use | Controlled Access | Monitoring | Destruction at Disposal | Retention Period | Backup Recovery |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Public** | N/R | N/R | Allowed | N/R | N/R | N/R | Everyone (read); Data owners and authorized individuals (write) | N/R | N/R | Varies based on business need | Optional |

N/R = Not Required

† customer-owned data is stored for as long as they remain as a MiCT customer, or as required by regulations, whichever is longer. Customer may request their data to be deleted at any time; unless retention is required by law.

### Data Inventory and Lifecycle Management

MiCT Security team uses an automated system to query across our cloud-based infrastructure, including but is not limited to AWS, to obtain detailed records of all data repositories, including but not limited to:

- AWS S3 repositories
- AWS RDS and DynamoDB instances
- AWS EC2 volumes
- Source code repositories
- Office 365
- On-premise storage systems (manually maintained)

The records are stored in a database system maintained by MiCT security team. Records are tagged with owner/project and classification when applicable. All records are kept up to date via automation. The system is also designed to track movement of data and update/alert accordingly.

### AWS S3 Object Lifecycle Management

The MiCT platform will automatically adjust the storage class for certain types of data based on its usage pattern and age. This allows the MiCT platform to provide competitive pricing while still allowing the customer to store large amounts of data.

AWS provides the following storage classes:

- General Purpose
- Infrequent Access
- Archive (Amazon Glacier)

S3 lifecycle policies are used to manage the storage class for certain types of data. In most cases, the MiCT platform automatically adjusts the storage class but we may give customers the ability to adjust the storage class manually to meet their pricing or performance needs.

MiCT performs regular full backups of all production data. We leverage S3 lifecycle policies to automatically remove old backup data. This allows older data to "age out" instead of having to explicitly delete it. S3 lifecycle policies are also used to adjust the storage class of data backups based on the age of the backup.

**Other Business Data**

All internal and confidential business records and documents, such as product plans, business strategies, presentations and reports, are stored outside of an employee workstation or laptop.

- Official records are stored in record management systems such as
  - Github (tickets),
  - (source code),
  - (HR),
  - (expense reports), etc.
- Unstructured business documents such as Word documents, Excel spreadsheets and PowerPoint presentations are stored on MiCT internal file share.
- Confidential business documents/records are be stored in encrypted form and with access control enabled on a need-to-know basis.

**Transient Data Managemet**

Data may be temporarily stored by a system for processing. For example, a storage device may be used to stage temp/raw files prior to being uploaded to the production environment in AWS. These transient data repositories are not intended for long term storage, and data is purged immediately after use.

*MiCT currently does NOT use transient storage for any sensitive data.*

### Backup and Recovery

**Customer Data** MiCT stores data in a secure production account in AWS, using a combination of S3, DynamoDB, and Aurora SQL databases. By default, Amazon S3 provides durable infrastructure to store important data and is designed for durability of 99.999999999% of objects.

All data store services and platforms in use are HIPAA compliant.

MiCT performs automatic backup of all customer and system data to protect against catastrophic loss due to unforeseen events that impact the entire system. An automated process will back up all data to a separate AWS region in the same country (e.g. US East to US West). By default, data will be backed up daily. The backups are encrypted in the same way as live production data.

Customers can also utilize the MiCT Application Programming Interface (API) to extract and store their data elsewhere. Standard API usage fees will apply.

**Source code** MiCT stores its source in git repositories hosted by .

Source code repositories are backed up to MiCT's AWS S3 infrastructure account on a weekly basis with a common set of configuration for each repository to enforce SDLC processes.

In the event that suffers a catastrophic loss of data, source code will be restored from the backups in AWS S3.

Because AWS and can both host git repositories, we are able to leverage git's ability to maintain a full history of all changes to our git repos via the commit log.

**Business records and documents** Each data owner/creator is responsible for maintaining a backup copy of their business files local on their laptop/workstation to the appropriate location on MiCT SharePoint team site. Examples of business files include, but are not limited to:

- Documents (e.g. product specs, business plans)
- Presentations
- Reports and spreadsheets
- Design files/images/diagrams
- Meeting notes/recordings
- Important records (e.g. approval notes)

Unless the local workstation/device has access to **Critical** data, backups of user workstations/devices are self managed by the device owner. Backups may be stored on an external hard drive or using a cloud service such as iCloud if and only if the data is both encrypted and password protected (passwords must meet MiCT requirements).

### Data Deletion Procedures

**For Platform Customers** Despite not being a requirement within HIPAA, MiCT understands and appreciates the importance of health data retention. Acting as a subcontractor/service provider, and at times a business associate, MiCT is not directly responsible for health and medical records retention as set forth by each state.

MiCT has created and implemented the following procedures to make it easier for MiCT Customers to support data retention laws.

Some types of customer data may be automatically transitioned to a storage class that is appropriate for archival or infrequent usage. The guidelines for transitioning data to different storage classes is at the discretion of MiCT.

Customer data is retained for as long as the account is in active status. Data enters an expired state when the account is voluntarily closed. Expired account data will be retained for 14 days. After 14 days, the project/account and related data will be removed. Customers that wish to voluntarily close their account should download their data manually or via the API prior to closing their account.

If an account is involuntarily suspended, then there is a 14 day grace period during which the account will be inaccessible but can be re-opened if the customer meets their payment obligations and resolves any terms of service violations. If a customer wishes to manually backup their data in a suspended account, then they must ensure that their account is brought back to good standing so that the API and user interface will be available for their use. After 14 days, the suspended account will be closed and the data will be permanently removed (except when required by law to retain).

**For patient data as as a Covered Entity** MiCT is NOT a covered entity. Should we become a covered entity in the future, we would be required by law to retain healthcare records for up to 10 years beyond when service was last provided when providing healthcare services directly to patients. Any patient data that is marked for deletion will be archived for the time required by law. This archived data can be retrieved by the customer as long as it is retrieved within 10 years from date of last service.