Business Continuity and Disaster Recovery

`2021.1`

The MiCT Contingency Plan establishes procedures to recover MiCT following a disruption resulting from a disaster. This Disaster Recovery Policy is maintained by the MiCT Security Officer and Privacy Officer.

HIPAA: This MiCT Contingency Plan has been developed as required under the Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, November 2000, and the Health Insurance Portability and Accountability Act (HIPAA) Final Security Rule, Section §164.308(a)(7), which requires the establishment and implementation of procedures for responding to events that damage systems containing electronic protected health information.

Policy Statements

MiCT policy requires that:

(a) A plan and process for business continuity and disaster recovery (BCDR), including the backup and recovery of systems and data, must be defined and documented.

(b) BCDR shall be simulated and tested at least once a year. Metrics shall be measured and identified recovery enhancements shall be filed to improve the BCDR process.

(c) Security controls and requirements must be maintained during all BCDR activities.

Controls and Procedures

BCDR Objectives and Roles

Objectives The following objectives have been established for this plan:

1. Maximize the effectiveness of contingency operations through an established plan that consists of the following phases:
   - *Notification/Activation phase* to detect and assess damage and to activate the plan;
   - *Recovery phase* to restore temporary IT operations and recover damage done to the original system;
   - *Reconstitution phase* to restore IT system processing capabilities to normal operations.
2. Identify the activities, resources, and procedures needed to carry out MiCT processing requirements during prolonged interruptions to normal operations.

3. Identify and define the impact of interruptions to MiCT systems.
4. Assign responsibilities to designated personnel and provide guidance for recovering MiCT during prolonged periods of interruption to normal operations.
5. Ensure coordination with other MiCT staff who will participate in the contingency planning strategies.
6. Ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

Example of the types of disasters that would initiate this plan are natural disaster, political disturbances, man made disaster, external human threats, and internal malicious activities.

MiCT defined two categories of systems from a disaster recovery perspective.

1. *Critical Systems.* These systems host production application servers/services and database servers/services or are required for functioning of systems that host production applications and data. These systems, if unavailable, affect the integrity of data and must be restored, or have a process begun to restore them, immediately upon becoming unavailable.
2. *Non-critical Systems.* These are all systems not considered critical by definition above. These systems, while they may affect the performance and overall security of critical systems, do not prevent Critical systems from functioning and being accessed appropriately. These systems are restored at a lower priority than critical systems.

Line of Succession The following order of succession to ensure that decision-making authority for the MiCT Contingency Plan is uninterrupted. The Chief Operating Officer (COO) is responsible for ensuring the safety of personnel and the execution of procedures documented within this MiCT Contingency Plan. The Head of Engineering is responsible for the recovery of MiCT technical environments. If the COO or Head of Engineering is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the CEO shall function as that authority or choose an alternative delegate. To provide contact initiation should the contingency plan need to be initiated, please use the contact list below.

- Klaas Glenewinkel, COO: klaas@mict-international.org
- Adam Burns, Head of Engineering: burns@mict-international.org
- Klaas Glenewinkel, CEO: klaas@mict-international.org

Response Teams and Responsibilities The following teams have been developed and trained to respond to a contingency event affecting MiCT infrastructure and systems.

1. **IT** is responsible for recovery of the MiCT hosted environment, network devices, and all servers. The team includes personnel responsible for the daily IT operations and maintenance. The team leader is the IT Manager who reports to the COO.
2. **HR & Facilities** is responsible for ensuring the physical safety of all MiCT personnel and environmental safety at each MiCT physical location. The team members also include site leads at each MiCT work site. The team leader is the Facilities Manager who reports to the COO.
3. **DevOps** is responsible for assuring all applications, web services, platform and their supporting infrastructure in the Cloud. The team is also responsible for testing re-deployments and assessing damage to the environment. The team leader is the Head of Engineering.
4. **Security** is responsible for assessing and responding to all cybersecurity related incidents according to MiCT Incident Response policy and procedures. The security team shall assist the above teams in recovery as needed in non-cybersecurity events. The team leader is the Security Officer.

Members of above teams must maintain local copies of the contact information of the BCDR succession team. Additionally, the team leads must maintain a local copy of this policy in the event Internet access is not available during a disaster scenario.

All executive leadership shall be informed of any and all contingency events. Current members of MiCT leadership team include the Security Officer, Privacy Officer, CTO, COO.

General Disaster Recovery Procedures

Notification and Activation Phase This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to MiCT. Based on the assessment of the Event, sometimes according to the MiCT Incident Response Policy, the Contingency Plan may be activated by either the COO or Head of Engineering. The Contingency Plan may also be activated by the Security Officer in the event of a cyber disaster.

The notification sequence is listed below:

- The first responder is to notify the COO. All known information must be relayed to the COO.
- The COO is to contact the Response Teams and inform them of the event. The COO or delegate is responsible to begin assessment procedures.
- The COO is to notify team members and direct them to complete the assessment procedures outlined below to determine the extent of damage and estimated recovery time. If damage assessment cannot be performed

locally because of unsafe conditions, the COO is to following the steps below.

  - Damage Assessment Procedures:
  - The COO is to logically assess damage, gain insight into whether the infrastructure is salvageable, and begin to formulate a plan for recovery.
  - Alternate Assessment Procedures:
  - Upon notification, the COO is to follow the procedures for damage assessment with the Response Teams.

- The MiCT Contingency Plan is to be activated if one or more of the following criteria are met:

  - MiCT will be unavailable for more than 48 hours.
  - On-premise hosting facility or cloud infrastructure service is damaged and will be unavailable for more than 24 hours.
  - Other criteria, as appropriate and as defined by MiCT.

- If the plan is to be activated, the COO is to notify and inform team members of the details of the event and if relocation is required.

- Upon notification from the COO, group leaders and managers are to notify their respective teams. Team members are to be informed of all applicable information and prepared to respond and relocate if necessary.

- The COO is to notify the hosting facility partners that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.

- The COO is to notify remaining personnel and executive leadership on the general status of the incident.

- Notification can be message, email, or phone.

Recovery Phase This section provides procedures for recovering MiCT infrastructure and operations at an alternate site, whereas other efforts are directed to repair damage to the original system and capabilities.

Procedures are outlined per team required. Each procedure should be executed in the sequence it is presented to maintain efficient operations.

Recovery Goal: The goal is to rebuild MiCT infrastructure to a production state.

The tasks outlines below are not sequential and some can be run in parallel.

1. Contact Partners and Customers affected to begin initial communication - DevOps
2. Assess damage to the environment - DevOps

3. Create a new production environment using new environment bootstrap automation - DevOps
4. Ensure secure access to the new environment - Security
5. Begin code deployment and data replication using pre-established automation - DevOps
6. Test new environment and applications using pre-written tests - DevOps
7. Test logging, security, and alerting functionality - DevOps and Security
8. Assure systems and applications are appropriately patched and up to date - DevOps
9. Update DNS and other necessary records to point to new environment - DevOps
10. Update Partners and Customers affected through established channels - DevOps

Reconstitution Phase This section discusses activities necessary for restoring full MiCT operations at the original or new site. The goal is to restore full operations within 24 hours of a disaster or outage. If necessary, when the hosted data center at the original or new site has been restored, MiCT operations at the alternate site may be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the computer center.

1. Original or New Site Restoration
    - Repeat steps 5-9 in the Recovery Phase at the original or new site / environment.
    - Restoration of Original site is unnecessary for cloud environments, except when required for forensic purpose.
2. Plan Deactivation
    - If the MiCT environment is moved back to the original site from the alternative site, all hardware used at the alternate site should be handled and disposed of according to the MiCT Media Disposal Policy.

Testing and Maintenance

The COO and/or Head of Engineering shall establish criteria for validation/testing of a Contingency Plan, an annual test schedule, and ensure implementation of the test. This process will also serve as training for personnel involved in the plan's execution. At a minimum the Contingency Plan shall be tested annually (within 365 days). The types of validation/testing exercises include tabletop and technical testing. Contingency Plans for all application systems must be tested at a minimum using the tabletop testing process. However, if the application system Contingency Plan is included in the technical testing of their respective support systems that technical test will satisfy the annual requirement.

Tabletop Testing Tabletop Testing is conducted in accordance with the CMS Risk Management Handbook, Volume 2. The primary objective of the tabletop test is to ensure designated personnel are knowledgeable and capable of performing the notification/activation requirements and procedures as outlined in the CP, in a timely manner. The exercises include, but are not limited to:

- Testing to validate the ability to respond to a crisis in a coordinated, timely, and effective manner, by simulating the occurrence of a specific crisis.

Simulation and/or Technical Testing The primary objective of the technical test is to ensure the communication processes and data storage and recovery processes can function at an alternate site to perform the functions and capabilities of the system within the designated requirements. Technical testing shall include, but is not limited to:

- Process from backup system at the alternate site;
- Restore system using backups; and
- Switch compute and storage resources to alternate processing site.

Work Site Recovery

In the event a MiCT facility is not functioning due to a disaster, employees will work from home or locate to a secondary site with Internet access, until the physical recovery of the facility impacted is complete. The recovery shall be performed by the facility management firm under contract with MiCT, and coordinated by the Facility Manager and/or the Site Lead.

MiCT's software development organization has the ability to work from any location with Internet access and does not require an office provided Internet connection.

Application Service Event Recovery

MiCT will develop a status page to provide real time update and inform our customers of the status of each service. The status page is updated with details about an event that may cause service interruption / downtime.

A follow up root-cause analysis details (RCA) will be available to customers upon request after the event has transpired for further details to cause and remediation plan for the future. Event Service Level

Short (hours)

- Experience a short delay in service.
- MiCT will monitor the event and determine course of action. Escalation may be required.

Moderate (days)

- Experience a modest delay in service where processes in flight may need to be restarted.
- MiCT will monitor the event and determine course of action. Escalation may be required.
- MiCT will notify customers of delay in service and provide updates on MiCT's status page.

Long (a week or more)

- Experience a delay in service and processes in flight may need to be restarted.
- MiCT will monitor the event and determine course of action. Escalation may be required.
- MiCT will notify customers of delay in service and provide updates on MiCT's status page.

Production Environments and Data Recovery

Production data is to be synchronized across multiple S3 buckets in AWS. Additionally, it is backed up to AWS Glacier for long term storage and recovery. In an event that requires data to be recovered, it will be retrieved from Glacier.

MiCT assumes that in the worst-case scenario, that one of the production environments suffers a complete data loss, the account will be reconstructed from code, and the data restored from Glacier that is hosted within a different AWS account and geolocation.

Recovery of production Environments and data should follow the procedures listed above and in Data Management - Backup and Recovery