IT Interruption and Business Continuity Plan

IT Interruption and Business Continuity Plan
Sponsor: Head of Operations
Version 2.0 (September 2024)
Next review: September 2025

1. Introduction

1.1 **Purpose -** The purpose of this IT Interruption and Business Continuity Plan is to provide a structured approach to managing and responding to IT interruptions that may affect the organisation's ability to carry out critical business functions. This plan outlines the procedures to ensure the rapid restoration of IT services and to minimise the impact on business operations, most importantly the 'student experience'.

1.2 **Scope -** This plan applies to all departments, systems, and processes of MLA College. It covers all IT-related interruptions, including but not limited to, system failures, data breaches, cyber-attacks, natural disasters, and other incidents that could disrupt the normal operation of IT services. The scope includes:

- Critical IT systems such as servers, databases, network infrastructure, and cloud services.
- Business processes that rely on IT systems and need to be maintained during an interruption.
- Stakeholders, including employees, customers, suppliers, and partners, who may be affected by IT interruptions.

1.3 **Objectives -** The primary objectives of this plan are:

a. Minimise Downtime: Ensure the swift and efficient restoration of IT systems to minimize the downtime and disruption to business operations.
b. Ensure Business Continuity: Maintain critical business functions and services during IT interruptions to meet the organisation's obligations to students, partners, and stakeholders.
c. Protect Data Integrity: Safeguard the integrity, confidentiality, and availability of the organisation's data during and after an IT interruption.
d. Effective Communication: Provide clear and effective communication channels to inform stakeholders of the situation and recovery efforts.
e. Compliance: Ensure that the response to IT interruptions aligns with regulatory requirements and industry best practices.

2. Roles and Responsibilities

2.1 This section outlines the key roles and responsibilities of individuals and teams involved in the execution of the IT Interruption and Business Continuity Plan. Clear definition of roles ensures that everyone understands their duties during an IT interruption, enabling an organised and efficient response.

2.2 **Crisis Management Team -** The Crisis Management Team (CMT) is responsible for the overall coordination of the response to an IT interruption. This team will assess the situation, make decisions regarding the activation of the Business Continuity Plan, and manage communication with stakeholders.

Crisis Management Leader: In the event of an IT Interruption the Head of Operations will assume the role of Crisis Management Leader. Primary responsibility will be to report information of problem to 3rd Party IT Support and liaise until issues are rectified.

Deputy Crisis Management Leader: The Vice-Rector (Professional Services) will act as second-in-command, assuming the leader's responsibilities if they are unavailable.

Communication Officer: A Business Intelligence Officer will assume the role of Communications Officer and will be tasked with providing clear and concise information to students, staff and stakeholders.

2.3 **IT Recovery Team -** The IT Recovery Team is responsible for the technical recovery of IT systems and services. This team will work to identify the cause of the interruption, restore affected systems, and ensure that data integrity is maintained.

2.4 MLA College relies on external 3rd Party IT support. In the event of an IT outage, the external IT Support Contractor will assume the role of IT Recovery Team.

2.5 **Employees -** All employees have a role to play in ensuring the effectiveness of the IT Interruption and Business Continuity Plan.

- General Staff: Follow instructions provided by the Crisis Management Team and their department heads. Report any IT issues immediately to the Head of Operations or Operations Assistant.

- Managers: Ensure that their teams are informed and that business continuity procedures are followed during an IT interruption.

2.6 **External Stakeholders -** External parties who may be involved in the recovery process or need to be informed during an IT interruption.

- Service Providers: External vendors responsible for providing IT services or support. They must be available to assist with recovery efforts.

- Regulatory Bodies: Any relevant authorities that must be notified in case of a significant IT interruption, especially if it involves data breaches or compliance issues.

- Students and Partners: Prompt communication will be provided to inform students and partners of any interruptions that may affect them, if deemed relevant.

3. Risk Assessment

3.1 **Identifying Potential Threats -** This subsection outlines the different types of threats that could lead to an IT interruption. These threats can be broadly categorised into the following:

- **Natural Disasters:**
  - Floods: Potential to damage data centres, IT equipment, and disrupt network infrastructure.
  - Earthquakes: Risk of physical damage to buildings, servers, and other critical IT infrastructure.
  - Storms and Severe Weather: Power outages and physical damage to infrastructure caused by wind, lightning, and heavy rainfall.

- **Technical Failures:**
  - Hardware Failures: Malfunction of servers, storage devices, network components, or other critical hardware.
  - Software Failures: Bugs, crashes, or incompatibilities in critical software applications or operating systems.
  - Power Outages: Loss of power can cause system shutdowns, data loss, and hardware damage.

- **Human Error:**
  - Accidental Deletion or Corruption of Data: Unintentional actions by employees that lead to data loss or system misconfiguration.

- Misconfiguration of Systems: Incorrect setup or maintenance of IT systems that lead to failures or vulnerabilities.
- Lack of Training: Insufficient training leading to improper use or handling of IT systems.

- **Cyber Threats:**
  - Cyber Attacks: Including hacking, ransomware, phishing, and distributed denial of service (DDoS) attacks.
  - Data Breaches: Unauthorised access to sensitive information that could lead to legal and financial consequences.
  - Malware and Viruses: Infection of systems with malicious software that can disrupt operations or compromise data integrity.

- **External Factors:**
  - Third-Party Service Failures: Interruptions or failures from cloud service providers, ISPs, or other critical vendors.
  - Supply Chain Disruptions: Delays or failures in obtaining critical hardware or software components due to supplier issues.

3.2 **Mitigation Strategies**

- Preventative Measures: Steps to prevent the risk from occurring, such as regular maintenance, employee training, and implementing robust cybersecurity practices.

- Response Strategies: Plans for minimising the impact if the risk does materialise, such as having backup systems in place, data recovery plans, and alternative work arrangements.

4. Incident Response Plan

4.1 The Incident Response Plan outlines the steps to be taken immediately following the detection of an IT interruption. This section ensures that the organisation can respond swiftly and effectively to minimise damage and restore normal operations as quickly as possible.

4.2 **Detection and Reporting -** This subsection details how IT interruptions will be detected, reported, and escalated within the organisation.

- Initial Reporting Procedures:
  - Who to Notify: First stage report should be provided to Head of Operations or Operations Assistant. Vice-Rector (Professional Services) and Vice-Rector (Academic) will be notified by Head of Operations.
  - Information to Report: The following information must be included:
    1. Nature of the issue
    2. Systems affected
    3. Time detected
    4. Immediate impact.

- Escalation Process:
  - Criteria for Escalation: If Operations Department are unable to rectify the issue, a call must be made to External IT Support Contractor. This call should detail the above information. Clarity must be gained on estimated time to rectification and advice sought on any further implications to business continuity. CEO, Rector and Vice-Rector (Academic or Professional Services) must be notified at the earliest opportunity.

4.3. **Initial Response**

- Incident Confirmation:
  - Verify the Incident: Steps to confirm that an IT interruption has occurred, including checks by the IT Support Contractor or automated system logs.
  - Assessment of Scope: In collaboration with IT support Contractor quickly assess the scope and scale of the interruption (e.g., affected systems, geographical impact, estimated duration).

- Activation of the Response Plan:
  - Crisis Management Team Activation: Procedures for mobilising the Crisis Management Team, including notification protocols and initial briefings.
  - Internal Communication: Immediate communication to all employees informing them of the incident and any immediate actions they need to take.

- Containment Measures:
  - Containment Actions: Under the guidance of IT Support Contractor steps to contain the incident, such as isolating affected systems, stopping the spread of malware, or shutting down specific services to prevent further damage will be implemented.
  - Temporary Workarounds: Identify and implement temporary workarounds to allow critical business functions to continue operating while the incident is being managed.

4. **Communication Plan -** Effective communication is essential during an IT interruption. This subsection outlines how information will be shared with internal and external stakeholders.

- Internal Communication:
  - Channels: If possible, staff will be notified of any serious incident via email, MLA Whatsapp, and company email.
  - Frequency: Updates will be provided as required, either to inform of any progress towards rectification or to advise on required actions.

- External Communication - The nature of any IT interruption will be assessed by the Crisis Management Team and determination on whether external communication is required will be agreed. If deemed relevant:
  - Students: All active students will receive notification via email which will include the expected duration and any impact on services.
  - Partners and Stakeholders: Partners and Stakeholders will be notified by email, particularly if their services are affected or required for recovery efforts.
  - Media and Public Relations: If necessary and appropriate, company social media channels will be utilised to communicate news of any impact on services.

- Regulatory Notification:
  - Legal Requirements: Any issues involving Data Protection or Data Breach will be processed through ICO protocol to determine the need for full reporting.

5. Recovery Strategies

5.1 **Data Recovery -** Data recovery is crucial to ensure that critical information is restored with minimal loss.

5.2 **System Recovery -** This subsection outlines the steps for restoring IT systems and infrastructure to operational status.

- Restoration Procedures:
  - Hardware Replacement: Will be discussed and agreed with External IT Support Contractor, in collaboration with Head of Operations and CEG.
  - Software Reinstallation: If required, details of any reinstallation will be provided by External IT Support Contractor.
  - Network Recovery: Instructions for restoring network services, such as reconfiguring routers, switches, and firewalls will be provided by External IT Support Contractor. In the event of system failure, a representative of the IT Support Contractor will be based on site to oversee network recovery.

- Testing and Validation:
  - System Testing: Ensure that all restored systems are thoroughly tested to verify that they are functioning correctly and securely.
  - User Acceptance Testing (UAT): Involve end-users in testing to ensure that systems meet operational needs and that no critical functionality is missing.

5.3 **Alternative Work Locations -** If the primary business location is unavailable, alternative work locations may be necessary to maintain business continuity.

- Identification of Alternative Locations:
  - Remote Working Options: Due to the nature of MLA College's operations, all staff may be required to work from home, or a suitable premises which will enable uninterrupted connection to company systems.

- Logistics and Support:
  - Workstation Setup: All staff are issued with portable IT equipment upon joining and should follow advice given during DSE assessments when setting up a home workstation.
  - IT Support: Usual IT support remains available to all staff through External IT Support Contractor. All portable IT equipment is setup during initial setup phase to allow remote access operation to External IT Support Contractor.

5.4 **Communication During Recovery -** Maintaining clear and effective communication is vital throughout the recovery process.

- Internal Updates:
  - Regular Briefings: Schedule regular updates to keep employees informed about the recovery status, including expected timelines and any required actions.
  - Communication Channels: Specify the communication channels to be used for updates. Nature of incident will determine relevant channels.

- External Communication:
  - Customer and Partner Updates: Provide timely updates to customers and partners about the status of services and expected recovery timelines.
  - Media and Public Relations: If necessary, manage communications with the media and the public, especially if the interruption has a significant impact on the organisation's reputation.

6. Plan Activation

6.1 **Decision Criteria -** This subsection outlines the specific criteria that must be met for the IT Interruption and Business Continuity Plan to be activated. These criteria help ensure that the plan is only activated when necessary and that the response is proportionate to the incident.

- Severity of the Incident:
  - Critical Systems Affected: The plan should be activated if key IT systems critical to business operations are disrupted.
  - Scope of Impact: The plan should be activated if the interruption affects multiple departments or has the potential to significantly impact business operations.

- Type of Incident:
  - Cybersecurity Breach: Any confirmed data breach or cyber-attack, particularly those involving sensitive or regulated data, should trigger plan activation.
  - Natural Disasters: In the event of a natural disaster that affects IT infrastructure or business locations, the plan should be activated.
  - Extended Power Outages: Prolonged power outages that exceed backup power capabilities should trigger the activation of the plan.

6.2 **Activation Procedures**

- Initial Assessment:
  - Crisis Management Team Notification: The Crisis Management Leader should be immediately notified of the incident. They will assess the situation based on the decision criteria.
  - Incident Verification: The IT Recovery Team should verify the nature and extent of the interruption to confirm whether plan activation is necessary.

- Activation Decision:
  - Crisis Management Leader's Decision: The Crisis Management Leader is responsible for making the final decision to activate the plan. This decision should be based on the severity of the incident, potential impact, and input from the IT Recovery Team.
  - Documenting the Decision: The decision to activate the plan should be documented, including the reasons for activation, the time of the decision, and the individuals involved.

- Plan Activation Announcement:
  - Internal Communication: Immediately notify all employees that the IT Interruption and Business Continuity Plan has been activated. Provide clear instructions on what actions they should take.
  - External Communication: If necessary, inform students, partners, and other stakeholders that the plan has been activated and outline any immediate impacts on services.

6.3 **Deactivation of the Plan -** Once the situation has been stabilised and normal operations are ready to resume, the plan can be deactivated. This subsection outlines the criteria and process for deactivation.

- Criteria for Deactivation:
  - Restoration of Critical Systems: The plan can be deactivated once all critical IT systems have been successfully restored and tested.
  - Resolution of the Incident: The underlying cause of the IT interruption has been resolved, and there is no further risk of recurrence.

- Confirmation from Stakeholders: All relevant stakeholders, including department heads and the IT Recovery Team, confirm that their areas are ready to return to normal operations.

- Deactivation Procedures:
  - Crisis Management Leader's Decision: The Crisis Management Leader makes the final decision to deactivate the plan, based on input from the IT Recovery Team.
  - Communication of Deactivation: Notify all employees and external stakeholders that the plan has been deactivated and normal operations are resuming.

- Post-Incident Review:
  - Once the plan is deactivated, conduct a post-incident review to assess the effectiveness of the response, identify lessons learned, and recommend improvements to the plan.