INTRODUCTION
The Information Technology Incident Management Plan (IMP) is a framework that outlines how incidents are managed from the onset to recovery and is activated once an incident has occurred. The IMP provides systematic steps leading to the restoration of normal business operations supported by IT infrastructure in the most effective and efficient way possible.

INCIDENT DEFINITION
As defined by ITILv3 an incident is an unplanned interruption to an IT service, or a reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service is also an incident. The purpose of the actions outlined in this plan is to restore services as soon as possible. Disaster incidents are defined as any IT service interruption estimated to be more than 72 hours.

EXECUTIVE INCIDENT MANAGEMENT TEAM
The Executive Incident Management Team (EIMT) consists of the Vice President for Information Technology (EIMT Leader) and each IT Director. This official body is only activated when a potential or actual incident occurs.

Responsibilities are as follows:
- Assess the situation and declare an incident
- Select the appropriate Team Leader and Alternate Team Leader
- Approve and support funding for all disaster recovery efforts
- Communicate with the GC Community and CUNY CIS during the incident and upon recovery
- Ensure that resources required by the IT Incident Management Team (IMT) are provided when needed

INCIDENT MANAGEMENT TEAM
The Incident Management Team (IMT) is charged with managing the intricacies of the incident and the recovery of business activities. IMT is responsible for: leading response and recovery activities, implementing recovery resources and monitoring the recovery process.

The IMT includes any combination of the Information Technology Management Team Plus (ITMT+), Sr. Technicians and Network Administrators who have the expertise required to manage an incident and recover business activities.
The IMT’s composition includes:
- Team Leader
- Alternate Team Leader
- Communications Leader
- IT Services Representative
- Sr. Technician Representative
- Infrastructure Representative
- Administrative Services Representative
- Systems Administrator

TEAM LEADER AND ALTERNATE TEAM LEADER
The Team Leader and Alternate Team Leader are selected by the EIMT based on the incident and the required areas of expertise.

The remaining members are assigned by the Team Leader based on the nature of the incident and skills needed for recovery.

ROLES
Team Leader – Leads the IMT in efforts to recover from the incident and restore services. *This position is assigned to IT managers only.* The Team Leader also selects one of the team members to serve as the Communications Leader.

Alternate Team Leader – Assists the Team Leader in decision making and leads the team in the absence of the Team Leader.

Communications Leader – Shares with EIMT all decisions made to recover, recovery milestones, budgetary needs, and any issues encountered on behalf of the Team Leader. The Communications Leader makes announcements and provides updates to the entire Information Technology Department.

The remaining members are responsible for assisting the IMT Leader and Alternate Leader in decision-making by contributing ideas, testing methods and solutions during the recovery process.

MANAGING THE INCIDENT

The Incident
Any technician who encounters an issue that appears to be an incident should contact his/her manager immediately to initiate assessment of the problem.

Initial Assessment
The EIMT will assess the situation and conduct necessary fact-finding, affirm the Incident Level and select the Team Leader and Alternate Leader. The Team Leader consults with the EIMT to
decide who should be a part of the IMT. *Incidents take first priority over other assignments and projects.*

**Appoint IMT Members**
The IMT Leader will appoint the IMT Members and direct the team to report to the appropriate Command Center. At the Team Leader’s discretion, either the Systems Table or Console Room (2408) will serve as the Command Center.

**Recovery Efforts**
The IMT Leader will delegate responsibilities to each IMT Member based on expertise and the necessary corrective measures required to restore systems and business activities. Team Members will provide periodic status reports to the IMT Leader and the Communications Leader will keep the EIMT abreast of recovery efforts.

**Notify Graduate Center Community**
The Communications Leader will inform the Graduate Center Community of the incident and that the IMT is working diligently to restore systems and business activities.

**Final Damage Assessment**
Based on updated damage assessment provided by The IMT Leader, the EIMT will decide whether to issue a Disaster declaration.

If a Disaster is declared the EIMT Leader will:
- assign Communications Leader to update CUNY CIS and the GC Community
- follow the GC Emergency Operations Plans

**POST INCIDENT EVALUATION**
Upon recovery and before disbanding the IMT, a post incident evaluation will be conducted and forwarded to the EIMT Leader. The IMT Leader will:
- identify root cause and take appropriate steps not to allow incident to occur again
- give a summary of what caused the incident
- assign Communications Leader to update CUNY CIS and the GC Community
- provide a list of corrective measures taken to restore services
- submit lessons learned from the activities engaged to restore services
- congratulate the team on a job well done