

Information Technology Department

**Emergency Response Plan**

Version 1

October, 2013

**Table of Contents**

[1. INTRODUCTION 3](#_Toc369681367)

[1.1 PURPOSE 3](#_Toc369681368)

[1.2 APPLICABILITY 3](#_Toc369681369)

[1.3 SCOPE 3](#_Toc369681370)

[1.3.1 Planning Principles 3](#_Toc369681371)

[1.3.2 Assumptions 4](#_Toc369681372)

[1.4 REFERENCES/REQUIREMENTS 4](#_Toc369681373)

[2. CONCEPT OF OPERATIONS 5](#_Toc369681374)

[2.1 SYSTEM DESCRIPTION AND ARCHITECTURE 5](#_Toc369681375)

[2.2 LINE OF MANAGEMENT SUCCESSION 5](#_Toc369681376)

[2.3 RESPONSIBILITIES 5](#_Toc369681377)

[3. NOTIFICATION AND ACTIVATION PHASE 12](#_Toc369681378)

[4. RECOVERY OPERATIONS 13](#_Toc369681379)

[5. RECONSTITUTION PHASE 13](#_Toc369681380)

[Appendix A – Personnel Contact List 14](#_Toc369681381)

[Appendix B – Application Criticality 14](#_Toc369681383)

[Appendix C – Vendor Contact List & Service Level Agreements 15](#_Toc369681384)

[Appendix D – Computer Operations 16](#_Toc369681385)

**1. INTRODUCTION**

## 1.1 PURPOSE

This Emergency Response Plan establishes procedures to recover all SUNY MARITIME COLLEGE applications and IT infrastructure components following a disruption. The following objectives have been established for this plan:

* 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 from damage done to the original systems

**Reconstitution phase -**  to restore IT system processing capabilities to normal operations

* Identify the activities, resources, and procedures needed to carry out processing during prolonged interruptions to normal operations.
* Assign responsibilities to designated IT personnel and provide guidance for recovering all systems during prolonged periods of interruption to normal operations.
* Ensure coordination with SUNY MARITIME COLLEGE staff from other departments that will participate in the contingency planning strategies and ensure coordination with external points of contact and vendors who will participate in the contingency planning strategies.

## 1.2 APPLICABILITY

The plan applies to the functions, operations, and resources necessary to restore and resume operations on campus or in the future establish alternate locations for all SUNY MARITIME COLLEGE Information Technology supported systems. The IT Dept. Emergency Response Plan is supported by the College’s Cyber Security Policy, which requires that the department maintain a program for ensuring the continuity of business. Procedures outlined in this plan are coordinated with and support the Continuity of Business Plan, which provides the necessary procedures established by the University Police Department to conduct business functions in the event of a disaster.

## 1.3 SCOPE

### 1.3.1 Planning Principles

Various scenarios were considered to form a basis for the plan, and multiple assumptions were made. The applicability of the plan is predicated on key principles.

* The SUNY MARITIME COLLEGE Data Center in the Science and Engineering building is inaccessible; therefore, The College is unable to perform data processing for normal business activities.
* Executive Management in coordination with University Police will determine alternate operating facilities in the event that the campus is inaccessible.
* SUNY MARITIME COLLEGE will use the alternate site and IT resources to recover data processing functionality during an emergency situation that prevents access to the campus.
* The alternate site will be used to continue critical application recovery and processing throughout the period of disruption until returning to normal operations.

### 1.3.2 Assumptions

Based on these principles, the following assumptions were used when developing the IT Emergency Response Plan

* Critical applications are inoperable at the primary SUNY MARITIME COLLEGE data center.
* Key IT Dept. personnel have been identified and trained in their emergency response and recovery roles; they are available to activate the Emergency Response Plan.
* Data center equipment, including components supporting critical applications and IT infrastructure, are connected to an uninterruptible power supply (UPS) that provides 10 – 20 minutes of electricity during a power failure.
* The SUNY Maritime data center is **NOT** equipped with a generator onsite that is capable of providing power to the data center for approximately 72 hours without requiring fuel delivery.
* Current backups of the application software and data are intact and available to be deployed at an alternate offsite facility.
* The hardware, software, communications and power required to operate all critical applications from one data center are available at the alternate site.
* Service agreements are maintained with hardware, software, and communications providers to support the emergency system recovery.

The Emergency Response Plan does not apply to the following situations:

* Overall recovery and continuity of business operations. The Continuity of Business Plan (COBP) is established and maintained by the University Police Department.
* Emergency evacuation of personnel. The Fire Drill and Evacuations Procedure is established and maintained by the system Facilities Department.

## 1.4 REFERENCES/REQUIREMENTS

This plan complies with the overall Maritime College contingency planning policy as follows:

* The organization shall develop a contingency planning capability to meet the needs of critical supporting operations in the event of a disruption.
* The procedures for execution of such a capability shall be documented in a formal contingency plan and shall be reviewed at least annually and updated as necessary.
* Personnel responsible for critical systems shall be trained to execute contingency procedures for those systems.
* The plan, recovery capabilities, and personnel shall be tested to identify weaknesses of the capability at least annually.

The Emergency Response Plan also complies with the following federal and state policies:

* Federal Information Security Management Act of 2002
* OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000.
* Federal Preparedness Circular (FPC) 65, Federal Executive Branch Continuity of Operations, June 2004
* Presidential Decision Directive (PDD) 67, Enduring Constitutional Government and Continuity of Government Operations, October 1998
* PDD 63, Critical Infrastructure Protection, May 1998
* Federal Emergency Management Agency (FEMA), The Federal Response Plan (FRP), April 1999
* Defense Authorization Act (Public Law 106-398), Title X, Subtitle G, “Government Information Security Reform,” October 30, 2000
* NYS Cyber Security Policy P03-002, Information Security Policy, July 2010

# 2. CONCEPT OF OPERATIONS

## 2.1 SYSTEM DESCRIPTION AND ARCHITECTURE

The SUNY MARITIME COLLEGE data processing environment for communications consists of VPNs, LANs, and WANs. Computer hardware and Operating Systems are comprised of Windows, NetApp, Dell, and HP blade servers. Database management consists of SQL Server and Oracle databases. End User Computing consists of Dell desktops/laptops, smartphones, tablets, and various other peripheral devices.

## 2.2 LINE OF MANAGEMENT SUCCESSION

The SUNY MARITIME COLLEGE sets forth an order of management succession, in coordination with the order set forth by the IT department to ensure that decision-making authority for the Emergency Response Plan is uninterrupted. The Chief Information & Technology Officer (CITO) is responsible for ensuring the safety of IT personnel and the execution of procedures documented within this Emergency Response Plan. If the CITO is unable to function as the overall authority or chooses to delegate this responsibility to a successor, the Deputy CIO shall function as that authority.

## 2.3 RESPONSIBILITIES

The Emergency Response Plan establishes several teams assigned to participate in recovering data processing operations. The combination of these individual groups will comprise the ‘Incident Response Team’. The Incident Response Team is responsible for recovery of the entire data processing environment and applications. Members of the team include personnel who are also responsible for the daily operations and maintenance of networks, applications, and all related IT infrastructure. There will be an ‘Incident Commander’ who will direct the Incident Response Team.

**INCIDENT COMMAND STRUCTURE**

**Purpose**

The purpose of the Incident Command Structure is to establish and direct plans of action to be followed in the event of a disaster.

**Organization & Planning**

The Incident Command Structure (ICS) for a given emergency will consist of an Incident Commander, a designated Operations Section Chief and support staff and teams as needed to support recovery. This organizational structure is modular in design and changes based on the size and complexity of the incident.

The Incident Commander will administer and manage the execution of the Emergency Response Plan. The Operations Section Chief, usually the Deputy CIO or Director (Networks or Applications) with the largest stake in recovery operations, will provide tactical direction of the other personnel required based on the type of incident. In the case of a major service disruption, the CITO will be the Operations Section Chief. Please refer to the organization chart below for the current Incident Command Structure to be employed for major service disruptions. Contact information for all IT management staff is detailed in Appendix A.

**Incident Response Team**

The Incident Response Team is a group of people who prepare for and respond to any emergency incident, such as a natural disaster or an interruption of business operations. This team is generally composed of specific members designated before an incident occurs, although under certain circumstances the team may be an ad-hoc group of willing volunteers.

**SUNY MARITIME COLLEGE Incident Command Structure**



**Incident Commander**

The Incident Commander is responsible for overall management of the incident. During an emergency situation, the Incident Commander will activate and direct all activities until the emergency is under control. Additionally, the commander is responsible for the following:

**Responsibilities:**

* Coordinate the updates and evaluation of the Emergency Response Plan to assure that all emergency situations have been adequately considered and that appropriate corresponding contingency plans have been prepared.
* To ensure that the Incident Response Team and other employees receive proper training of emergency plans and procedures. This process is incorporated into the annual review of the plan. The coordinator will work with other IT Managers to ensure that new employees are properly trained and that certain emergency procedures are reviewed as frequently as necessary.
* Keep all members of the Incident Response Team fully briefed on all aspects of the disaster plan.
* Evaluate the readiness & proficiency of the Incident Response Team.
* Evaluate the appropriateness of the Incident Response Team assignments.
* Keep management informed of the status of the Incident Response Team & the Emergency Response Plan.
* Communicate the status of emergency situations to management promptly & efficiently
* Maintain liaison with local fire & police agencies, other emergency locations, and all involved parties as appropriate.

**Deputy Commander**

The Deputy Commander is responsible for ensuring the Commander’s guidance and intent is effectively communicated, understood, and executed. During an emergency situation, the Deputy Commander will perform all activity of the Incident Commander in his absence. The Deputy Commander is also responsible for the financial and administrative functions that are critical to IT Department operations in the event of a disaster. Additionally, the Deputy Commander is responsible for the following:

**Responsibilities:**

Recovery

Coordinate and manage expenses related to the recovery process Coordinate with vendors in obtaining necessary repairs or replacement of server hardware.

Coordinate and manage expenses related to the recovery process

Reconstitution

Coordinate with Purchasing, Finance, Insurance, and other departments in equipment salvage, insurance claims, and financing for replacement server equipment.

**Applications Section Chief**

**Purpose:** The Applications Section Chief is responsible for coordinating the application recovery teams while in disaster mode.

**Network Section Chief**

**Purpose:** The Network Section Chief is responsible for coordinating all infrastructure activities while in disaster mode.

**Systems Administrator**

**Purpose:** The System Administrator is responsible for coordinating all Systems Administration and Email activities while in disaster mode.

**Damage Assessment Team**

**Purpose:** The Incident Commander will appoint individuals to the Damage Assessment Team at the time of disaster declaration. The team will be comprised of senior management from the IT department infrastructure and application sections as appropriate.

**Responsibilities:**

Notification/Activation

* The Damage Assessment Team is responsible for assessing the damage to all application and infrastructure components including data and is not responsible for assessing structural damages of the data center.

Reconstitution

* The team will be asked to confirm if any permanent damages have occurred to any of the application and/or infrastructure components.

**Recovery Functions**

The following have been identified as Recovery functions in the event of a disaster or major emergency. The Incident Commander and/or the Incident Response Team will activate the appropriate Recovery function according to the nature of the emergency.

* **IT Security Function**
* **IT Disaster Recovery Function**
* **Applications Function**
* **Network and Voice Communications Function**
* **End User Computing Function**
* **Server Infrastructure Function**
* **Facilities Infrastructure Function**
* **Database Administration Function**
* **Technology Support Center Function**

Designated leaders of the Recovery Functions and their contact information are identified in Appendix A.

**IT Security Function:**

**Purpose:** The purpose of the Security Team is to assist with any task that may include but not be limited to: firewall rule modifications, access rights assignments, troubleshooting, hardware or software configuration or installation.

**IT Disaster Recovery Function:**

**Purpose:** The purpose of the Disaster Recovery Team is to ensure that all recovery staff have access to detailed application recovery plans and follow the established recovery and reconstitution procedures.

**Applications Function:**

**Purpose:** The purpose of the applications teams is to assist in the recovery of SUNY MARITIME COLLEGE IT Department supported applications.

**Responsibilities:**

Recovery

* In an emergency, the Applications Teams will participate as needed to install, configure, and validate the application environment where production operations will be recovered.
* If additional problems are identified with how an application is operating at the contingency site, the Applications Teams must prepare, document, and coordinate implementation of solutions for the problems.
* Coordinate with end-users to determine work that was in progress at the time of the disaster. When operations are restored at the contingency site, the Applications Teams will first attempt to recover any lost data.

Reconstitution

* Once the primary environment has been recovered, coordinate with the users to synchronize the data on the disaster recovery systems with the primary production systems.
* If applicable, the Applications Teams will participate as needed and will validate the application environment where production operations will be restored back to the primary processing environment.

**Network and Voice Communications Team**

**Purpose:** The Network and Voice Communications Function is responsible for all voice & data communication infrastructure as well as repair or replacement of all lines and associated communications hardware.

**Responsibilities:**

Recovery

* To ensure that all voice and data infrastructure is functioning as intended
* Make any necessary adjustments to voice/data infrastructure to ensure application availability
* Coordinate with vendors in obtaining necessary repairs or replacement of hardware as needed to ensure that the recovery site is functioning as intended
* Coordinate with the Deputy Commander for equipment salvage, insurance claims, and financing of replacement communications infrastructure equipment.

Reconstitution

* Ensure voice and data communication infrastructure is operational at the primary data center.
* Coordinate with Purchasing, Finance, Insurance, and other departments in equipment salvage, insurance claims, and financing for replacement equipment.

**End User Computing Team**

**Purpose:** The User Computing Team is responsible for end-user hardware and software considerations during a disaster. This includes providing information about the status of services and alternatives.

**Responsibilities:**

Recovery

* In the event of a disaster, assess the extent of damage or the effect of failures on desktop computers.
* Install and test all new/replacement desktop hardware and supervise problem solving when problems or failures are encountered.
* Coordinate with the Deputy Commander for equipment salvage, insurance claims, and financing of replacement end user equipment.

Reconstitution

* Ensure availability of desktops and other peripherals to end users and supervise all solutions when problems or failures are encountered.

**Server Infrastructure Team**

**Purpose:** The Server Infrastructure Team is responsible for the hardware, operating system and various application software for all production servers.

**Responsibilities:**

Recovery

* In the event of a disaster, assess the extent of damage or the effect of failures on server infrastructure.
* Coordinate with vendors in obtaining necessary repairs or replacement of server infrastructure.
* Work with the Deputy Commander to coordinate equipment salvage, insurance claims, and financing of replacement server infrastructure equipment.
* Install and test all new/replacement server hardware, and supervise solutions when problems or failures are encountered.

Reconstitution

* Ensure availability of SUNY MARITIME COLLEGE client/server and network storage environments

**Facilities Infrastructure Team**

**Purpose:** The Facilities Infrastructure Team is responsible for ensuring that the infrastructure is adequate at the datacenters.

**Responsibilities:**

Recovery

* Verify IT Infrastructure services are functioning at the alternate site and contact any vendor or other SUNY MARITIME COLLEGE department if necessary to help expedite the process.

Reconstitution

* Verify IT Infrastructure services are established at the primary site.
* Ensure availability of architectural, security, electrical, mechanical, fire suppression, HVAC infrastructure are available to support the existing IT department service level agreement

**Database Administration Team**

**Purpose:** The Database Administration Team is responsible for all production databases.

**Responsibilities:**

Recovery

Verify all production databases supported by continuity of business have automatically failed over.

* In the event of a disaster, assess the extent of damage or the effect of failures on all production databases.
* Coordinate with vendors in obtaining necessary support to aid in database recovery.
* Install and test all new/replacement databases, and supervise solutions when problems or failures are encountered as a result of a disaster.

Reconstitution

* To ensure availability of database environments upon return of normal operations.

**Technology Support Center Team**

**Purpose:** The Technology Support Center Team is responsible for resuming IT department call center functions during a disaster.

**Responsibilities:**

Recovery

* Assemble the Technology Support Center staff to report to an alternate site to establish a temporary call center to provide a channel for end user communication or any other assistance if requested by the Incident Commander or the Incident Response Team

Reconstitution

* To maintain call center functions during the return to regular operating status.
* Ensure IT call center procedures; escalation procedures and vendor contact information are available at the alternate site.

# 3. NOTIFICATION AND ACTIVATION PHASE

This phase addresses the initial actions taken to detect and assess damage inflicted by a disruption to SUNY Maritime College’s data center. An Incident Commander will be appointed based on the assessment of the event. The SUNY MARITIME COLLEGE IT Department’s top priority is to preserve the health and safety of its staff before proceeding to the Notification and Activation procedures.

Contact information for key personnel is located in Appendix A. The notification sequence is defined below:

* The first responder from the SUNY MARITIME COLLEGE IT Dept. is to notify the CITO/Incident Commander.
* The Incident Commander is to notify the DCIO/Deputy Commander to direct completion of 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, a decision will be made to work from the alternate data center.

**Damage Assessment Procedures**:

**Damage Assessment**

Work in conjunction with other team members, vendors, Police, Fire Dept., EMS, Utility Co. Personnel, etc., to assess the situation. Use the chart below:

|  |  |  |  |
| --- | --- | --- | --- |
| **DAMAGE ASSESSMENT** | **ESTIMATED TIME TO REPAIR** | **ASSESED BY** | **Incident Commander****Informed** |
| Physical Damage to Building |   |  |  |
| Physical Damage to Data Processing Equipment |   |  |  |
| Physical Damage to Telephone Equipment |   |  |  |
| Site Accessibility Problems |   |  |  |
| Damage to Power Supplies |   |  |  |
| Damage to Tape Library |   |  |  |
| Other: |   |  |  |

##### Conditions for Disaster Declaration

Using the chart below, classify the disaster based on damage assessment and recovery time.

|  |  |  |
| --- | --- | --- |
| **Classification** | **Length of Interruption** | **Action to Take** |
| **Class I** | 1-12 Hours | Cancel or delay the formal declaration of a disaster |
| **Class II** | 12-24 Hours | Evaluate workload impact and make decision |
| **Class III** | 24 + Hours | Formally declare a disaster |

If the plan is to be activated, the Incident Commander is to identify and notify all team leaders and inform them of the details of the event and if relocation is required.

# 4. RECOVERY OPERATIONS

Upon notification from the Incident Commander, Section Chiefs are to notify their respective teams. Team members are to be informed of all applicable information and be prepared to respond and relocate as necessary. The Incident Commander or his designated representative is to notify the off-site storage facility that a contingency event has been declared and to ship the necessary materials (as determined by damage assessment) to the alternate site.

# 5. RECONSTITUTION PHASE

When the data center at the original or new site becomes available, operations must be transitioned back. The goal is to provide a seamless transition of operations from the alternate site to the original data center. Establish networking, Microsoft infrastructure, Domain Name Services and Microsoft Exchange email.

# Appendix A – Personnel Contact List

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NAME** | **TITLE** | **OFFICE** | **CELL** | **Email****@sunymaritime.edu** |
| Scott Dieterich | Chief Information & Technology Officer | (718) 409-7362 | (516) 790-8829 | smdiete |
| Phil Robertson | Deputy CIO | (718) 409-3591 | (646) 532-9313 | probertson |
| Jasvinder Singh | Chief, Network Section | (718) 409-5986 | (646) 595-8737 | jsingh |
| Margie Maillard | Chief, Applications Section | (718) 409-4855 | (917) 574-7676 | mmaillard |
| Vinny Pagano | Systems Administrator | (718) 409-4043 | (347) 835-0428 | vpagano |
| Michael Mastromarino | Helpdesk Technician | (718) 409-5380 | (347) 852-1900 | mmastromarino |
| Joseph DiChiara | Helpdesk Technician | (718) 409-7487 | (646) 691-8223 | jdichiara |
| Polina Grzhibek  | Programmer | (718) 409-7490 | (917) 693-2733 | pgrzhibek |
| Vacant | Helpdesk Technician | (718) 409-7487 | N/A | N/A |
| Vacant | Helpdesk Technician | (718) 409-7487 | N/A | N/A |
| Vacant | Programmer | (718) 409-7490 | N/A | N/A |

#

**Appendix B – Application Criticality**


#

# Appendix C – Vendor Contact List & Service Level Agreements

**ePLUS**: Allen Stein

 (631) 478-6531 – Business

 (631) 291-1591 – Cell

 astein@eplus.com

**ITEC**:  Information Technology Exchange Center

Mike Radomski

Chief Technology Office

(716) 878-4832

Mike.radomski@itec.suny.edu

Joe Lofft (Technical POC)

Database Administrator

(716) 878-4832

Joe.lofft@itec.suny.edu

**SICAS**: Student Information and Campus Administrative System

Bill Grau

Executive Director

(607)-436-2181

Bill.grau@oneonta.edu

Stephanie Kot (Technical POC)

DBA – Assistant Director for Remote Services

Stephanie.kot@oneonta.edu

# Appendix D – Computer Operations

# Disaster Recovery Backup Site

The current recovery site backup vendor is: **TBD**

**Personnel Authorized to Declare an IT Disaster**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NAME** | **TITLE** | **OFFICE** | **CELL** | **Email****@sunymaritime.edu** |
| Scott Dieterich | Chief Information & Technology Officer | (718) 409-7362 | (516) 790-8829 | smdiete |
| Phil Robertson | Deputy CIO | (718) 409-3591 | (646) 532-9313 | probertson |
| Jasvinder Singh | Chief, Network Section | (718) 409-5986 | (646) 595-8737 | jsingh |
| Margie Maillard | Chief, Applications Section | (718) 409-4855 | (917) 574-7676 | mmaillard |

#### Notification of a Disaster – Off-Site Data Storage Notification

The current off-site storage facility for backup tapes is: **TBD**

**RECORD OF CHANGES**

Modifications made to this plan since the last printing are as follows:

|  |
| --- |
| **Record of Changes** |
| **Page No.** | **Change Comment** | **Date of Change** | **Changed By** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |   |  |  |
|  |   |  |  |
|  |   |  |  |
|  |   |  |  |
|  |   |  |  |
|  |   |  |  |
|  |   |  |  |
|   |   |  |  |