



# Business Continuity And Disaster Recovery Plan

August 2019

|   |   |
|---|---|
| PUBLICATION NOTE                                      | 3 |
| DOCUMENT MANAGEMENT                                   | 3 |
| DOCUMENT APPROVAL AND ACCEPTANCE                      | 3 |
|   |   |
| 1. PURPOSE  | 4 |
| 2. SCOPE  | 4 |
| 3. POLICY   | 4 |
|   |   |
| 4. CONTINUITY & RECOVERY PLANNING                     | 4 |
| 1. PLAN OBJECTIVES                                    | 4 |
| 2. ASSUMPTIONS  | 4 |
| 3. DISASTER DEFINITION                                | 4 |
| 4. RECOVERY TEAM RESPONSIBILITIES                     | 5 |
| 5. INSTRUCTIONS FOR USING THE PLAN                    | 5 |
| 5.1 INVOKING THE PLAN                                 | 5 |
| 5.2 DISASTER DECLARATION                              | 5 |
| 5.3 NOTIFICATION                                      | 5 |
| 5.4 EXTERNAL COMMUNICATIONS                           | 5 |
| 6. EMERGENCY MANAGEMENT STANDARDS                     | 6 |
| 6.1 DATA BACKUP POLICY                                | 6 |
| 6.2 EMERGENCY MANAGEMENT PROCEDURES                   | 6 |
| 6.3 IN THE EVENT OF A NATURAL DISASTER                | 7 |
| 6.4 IN THE EVENT OF A FIRE                            | 7 |
| 6.5 IN THE EVENT OF A NETWORK SERVICE PROVIDER OUTAGE | 8 |
| 6.6 IN THE EVENT OF A FLOOD OR WATER DAMAGE           | 9 |

|  |        |
|--|--------|
| 7. PLAN REVIEW, TESTING & MAINTENANCE  | 9      |
| 8. ALERT / VERIFICATION / DECLARATION PHASE (1-4 HOURS)                      | 10     |
| 8.1 NOTIFICATION OF INCIDENT AFFECTING PHYSICAL OFFICE                       | 10     |
| 8.2 PROVIDE STATUS TO RECOVERY TEAM  | 10     |
| 8.3 DECIDE COURSE OF ACTION  | 10     |
| 8.4 INFORM RECOVERY TEAM OF DECISION   | 10     |
| 8.5 RESPONSE COORDINATOR NOTIFIES ACCOUNT TEAMS & CUSTOMERS                  | 11     |
| 8.6 CONTACT GENERAL VENDORS  | 11     |
| 8.7 CONDUCT DETAILED DAMAGE ASSESSMENT                                       | 11     |
| 8.8 DECIDE WHETHER TO CONTINUE TO BUSINESS RECOVERY PHASE                    | 11     |
| 9. BUSINESS RECOVERY PHASE (96 HOURS – FULL RECOVERY)                        | 12     |
| 9.1 PRODUCTION SERVICE RECOVERY  | 12     |
| 9.2 NOTIFY RESPONSE COORDINATOR AND MURSION CORPORATE OF RECOVERY<br>STARTUP | 12     |
| 9.3 OPERATIONS RECOVERED   | 12     |
| 5. AMENDMENT/TERMINATION OF THIS POLICY                                      | 12     |
| 6. EXCEPTIONS  | 12     |
| 7. VIOLATIONS/ENFORCEMENT  | 12     |
| <br>APPENDIX A: ROLE DEFINITIONS   | <br>13 |
| 1. RESPONSE COORDINATOR  | 13     |
| 2. RECOVERY TEAM   | 13     |
| 3. ENGINEERING   | 13     |
| APPENDIX B: RECOVERY TEAM CONTACT LIST                                       | 14     |
| 1. RECOVERY TEAM   | 14     |
| 2. IT OPERATIONS   | 14     |
| APPENDIX C: CONTACT LIST   | 15     |
| APPENDIX D: FORMS  | 16     |
| CRITICAL EQUIPMENT STATUS ASSESSMENT AND EVALUATION FORM                     | 18     |
| APPENDIX E: GENERAL CONTACT  | 19     |
| SERVER AND COMPUTER EQUIPMENT SUPPLIERS                                      | 19     |
| COMMUNICATIONS AND NETWORK SERVICES SUPPLIERS                                | 19     |
| MECHANICAL ENGINEERING (HVAC, FACILITIES, ETC.)                              | 19     |
| PLUMBING   | 20     |
| BUILDING MANAGEMENT AND SITE SECURITY SERVICES                               | 20     |



Publication Note


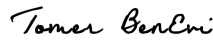
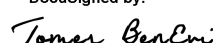
This policy is the property of Mursion and is exclusively for the use of Mursion employees, authorized agents, and affiliated companies. It contains Mursion confidential and proprietary information, and under no circumstances is it to be delivered or disclosed to any person not employed by Mursion, its authorized agents, or affiliated companies, without the express written authorization of an officer of Mursion.

Document Management

Version History

| Revision | Release Date | Updated by | Remarks/Comments |
|----------|--------------|------------|------------------|
| O.1      | 5/6/19       | M. Cooper  | Initial draft    |
| O.2      | 5/17/2019    | T.Ben-Evi  | Second draft     |

Document Approval and Acceptance

| Name          | Signature  | Date                     |
|---------------|--|--------------------------|
| Tomer Ben-Evi | <div>DocuSigned by:<br/><br/>80DE9222D94343D...</div>   | 12/20/2019   2:45 PM PST |
| Tomer Ben-Evi | <div>DocuSigned by:<br/><br/>A1112A21C6D546F...</div>   | 8/20/2020                |
| Tomer Ben-Evi | <div>DocuSigned by:<br/><br/>A1112A21C6D546F...</div> | 7/26/2021                |





## **1. Purpose**

The purpose of this Business Continuity and Disaster Recovery Plan is to prepare Mursion in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame. For all Mursion sites and our production environment, Mursion shall implement preventive measures to minimize network failure and to recover as rapidly as possible when a failure occurs.

## **2. Scope**

The scope of this plan is limited to Mursion production services and infrastructure components. Mursion's physical offices do not host any production service components or critical business applications. In the event of a disaster at a Mursion physical office, staff shall work from home or an alternate location until the office is accessible or new office space is established. Disaster recovery processes for physical offices shall be limited to that which is needed to ensure the confidentiality of data, systems, and records located at the office.

## **3. Policy**

Mursion shall plan, design, and regularly test processes needed to maintain the continuity of business services and information security, and recover from any disaster that affects the confidentiality, availability, or integrity of business critical or production service applications, systems, and networks.

## **4. Continuity & Recovery Planning**

### **1. Plan Objectives**

- Serves as a guide for the Mursion recovery teams.
- References and points to the location of any data that resides outside this document.
- Provides procedures and resources needed to assist in recovery.
- Identifies vendors and customers that must be notified in the event of a disaster.
- Assists in avoiding confusion experienced during a crisis by documenting, testing, and reviewing recovery procedures.
- Documents storage, safeguarding, and retrieval procedures for vital records.

### **2. Assumptions**

- Key people (Team Leaders or Alternates) will be available following a disaster.
- A national disaster such as nuclear war is beyond the scope of this plan.
- This document and all vital records are stored in a secure off-site location and not only survived the disaster but are accessible immediately following the disaster.

### **3. Disaster Definition**

Disaster is defined as any event that causes an interruption, or loss of data integrity or availability, in the Mursion production service for more than four (4) hours, or the physical destruction or compromise of a Mursion facility.



#### **4. Recovery Team Responsibilities**

- Maintain a current, protected, copy of this plan in an internet accessible storage location not dependent on the availability of Mursion physical offices or production service account
- Report to the Response Coordinator in disaster situations
- Restore production services as quickly as possible and within 48 hours of the incident in the worst-case scenario
- Recover business application services within two (2) business days of an incident or disaster
- All the members should keep a copy of this plan and an updated calling list of their work team members' work, home, cell phone numbers both at home and at work.
- All team members should familiarize themselves with the contents of this plan. See Appendix A for Role Definitions.
- Following a disaster, document the restoration and recovery steps taken and determine any lessons learned.

#### **5. Instructions For Using The Plan**

##### *5.1 Invoking The Plan*

This plan becomes effective whenever production services have been unavailable or severely compromised for four (4) hours. Normal problem management procedures will initiate the plan, and remain in effect until production services are resumed and fully functional.

Plans for securing data and systems at physical offices shall be invoked immediately following any disaster the renders the office unusable.

##### *5.2 Disaster Declaration*

The Response Coordinator is responsible for declaring a disaster and activating the Recovery Team as outlined in this plan.

##### *5.3 Notification*

Regardless of the disaster circumstances, or the identity of the person(s) first made aware of the disaster, the Recovery Team must be activated immediately in the following cases:

- Production services are unavailable or severely compromised for more than 4 hours
- Disaster at a physical office rendering the office unusable

##### *5.4 External Communications*

The Response Coordinator is designated as the principal contact for customers, partners, the media (radio, television, and print), regulatory agencies, government agencies, and other external organizations following a formal disaster declaration.

It is the responsibility of the Response Coordinator to prepare answers to basic questions, such as:

- What happened?
- How did it happen?
- What is going to be done about it?



## 6. Emergency Management Standards

### 6.1 Data Backup Policy

Mursion utilizes regionally distributed cloud architecture for essential and critical architecture components to maintain more than one disaster-ready version of the core product architecture and business critical data.

A technical restore test of at least one critical backup shall be performed as part of the annual disaster recovery plan test or disciplinary action in accordance with Company procedures. Mursion may advise law enforcement agencies when a criminal offense may have been committed.

| Key Business Process                   | Backup Strategy  |
|--|--|
| IT Operations                          | Regionally distributed cloud architecture. Local files backed up to G Suite. Source code, configurations, and technical documentation stored on GitHub, AWS, and SVN.          |
| Email                                  | Utilize G suite and its distributed nature, rely on Google's standard service level agreements.  |
| Finance and HR                         | Utilize online payroll, bill pay, and accounting software services and rely on their distributed nature and vendor service level agreements. Local files backed up to G Suite. |
| Sales, Delivery, Finance and Marketing | Utilize SaaS vendor services and rely on their distributed nature and vendor standard service level agreements. Local files backed up to G Suite.                              |

### 6.2 Emergency Management Procedures

The following procedures are to be followed by IT operations personnel and other designated Mursion personnel in the event of an emergency at a Mursion facility.

- The Recovery Coordinator shall ensure that the physical office is inspected following a disaster and that appropriate steps are taken to secure systems and data. Physical sites may be secured by locking physical doors and windows, public safety or emergency responder perimeters, building management personnel, or security guards.
- Anyone not recognized by Mursion staff around physical offices as normally having business in the area must be challenged by the staff who should then notify the police, building management, security personnel, and the Recovery Coordinator as needed.
- In the event of any situation where access to a building housing a system is denied, personnel shall work from home or any available off-site location until further instructions are provided.
- In the event of an emergency, all personnel must attempt to contact their immediate supervisor or management via email, chat, or telephone. Phone numbers and email addresses are included in this document.



### 6.3 In The Event Of A Natural Disaster

In the event of a natural disaster affecting production services at an Mursion facility, immediately notify the Response Coordinator.

| Procedure | Step | Backup Strategy   |
|-----------|------|---|
|           | 1    | Notify Response Coordinator of pending event, if time permits.  |
|           | 2    | <p>If impending natural disaster can be tracked, begin preparation of site within 72 hours as follows:</p> <ul style="list-style-type: none"> <li>• Notify Response Coordinator of impending disaster and prepare to shut down all equipment and vacate the site</li> <li>• Notify all staff to work from home until further notice</li> <li>• Document any equipment that will be removed from the site as needed and where it will be stored</li> </ul> |
|           | 3    | <p>24 hours prior to event:</p> <ul style="list-style-type: none"> <li>• Back up any critical system or data elements</li> <li>• Fuel personal vehicles and charge all mobile equipment batteries</li> <li>• Shut down all equipment and secure the site</li> <li>• Notify Response Coordinator that site is vacated and secured</li> </ul>   |

### 6.4 In The Event Of A Fire

In the event of a fire or smoke in any of the facilities, the guidelines and procedures in this section are to be followed.

If fire or smoke is present in the facility, evaluate the situation and determine the severity, categorize the fire as Major or Minor and take the appropriate action as defined in this section. Call 911 as soon as possible if the situation warrants it.

- Call 911 immediately if any fire is observed or detected
- If it is safe to do so, personnel may attempt to extinguish minor fires (e.g., single hardware component or paper fires) using hand-held fire extinguishers located throughout the facility. Any other fire or smoke situation will be handled by qualified building personnel until the local fire department arrives.
- In the event of a major fire, call 911 and immediately evacuate the area.
- In the event of any emergency, system site security and personal safety are the major concern. If possible, the senior staff person or his or her designee should remain present outside the facility until the fire department has arrived.
- Once it is safe to do so, notify the Response Coordinator.



| Procedure | Step | Action  |
|-----------|------|---|
|           | 1    | Dial 9-1-1 to contact the fire department.  |
|           | 2    | Provide them with your name, extension where you can be reached, building and room number, and the nature of the emergency. Follow all instructions given.  |
|           | 3    | Immediately notify all other personnel in the facility of the situation and evacuate the area.  |
|           | 4    | Alert the Response Coordinator when safe to do so.<br><i>Note: During non-staffed hours, security or building personnel will notify the Mursion site contact on file who should then notify the Response Coordinator.</i>   |
|           | 5    | Notify Building Management.<br>Local building management personnel should establish security at the location and not allow access to the site unless notified by the Response Coordinator or their designated representative.   |
|           | 6    | Contact appropriate vendor personnel (i.e. protective services) to ensure the protection of files and equipment if needed.  |
|           | 7    | All personnel evacuating the facilities will meet at their assigned outside location and follow instructions given by the designed authority. <b>Unless medically necessary, personnel should not leave without notifying the Response Coordinator or local manager so that all staff can be accounted for.</b> |

## 6.5 In The Event Of A Network Service Provider Outage

Information about any emergency that could impact Mursion's online platform or the ability to maintain Mursion services must be reported immediately upon discovery. In the event of a network service provider outage to production services or any facility, the guidelines and procedures in this section are to be followed.

| Procedure | Step | Action  |
|-----------|------|---|
|           | 1    | Notify Response Coordinator of outage.<br>Determine cause of outage, any impact to data, and timeframe for its recovery.  |
|           | 2    | If production services outage will be greater than 4 hours, enact Recovery Team<br><br>If the network outage affects an office facility, send staff to work from home or an alternate location. |
|           | 3    | As needed, switch production services to an alternate cloud region or availability zone.  |





## 6.6 In The Event Of A Flood Or Water Damage

In the event of a flood or broken water pipe within any computing facilities, the guidelines and procedures in this section are to be followed.

| Procedure | Step | Action  |
|-----------|------|---|
|           | 1    | Assess the situation and determine if outside assistance is needed; if this is the case, dial 911 immediately.  |
|           | 2    | Immediately notify building management and all other personnel in the facility of the situation and to be prepared to cease operations accordingly.   |
|           | 3    | If water is originating from above the equipment, power down the individual devices if safe to do so.   |
|           | 4    | Water detected on the floor may have different causes: <ul style="list-style-type: none"> <li>• If water is slowly dripping from an air conditioning unit or pipes, and not endangering equipment, contact building management or repair personnel immediately.</li> <li>• If water is of a major quantity and flooding beneath the floor (i.e. water main break), immediately implement power-down procedures. While power-down procedures are in progress, evacuate the area and follow management's instructions.</li> </ul> |

## 7. Plan Review, Testing & Maintenance

This plan is intended to be a living document and as such must be reviewed on a regular basis. The plan will be reviewed and exercised on an annual basis. The test may be in the form of a walk-through, mock disaster, or component testing. Additionally, with the dynamic environment present within Mursion, it is important to review the listing of personnel and phone numbers contained within the plan regularly.

The plan will be stored on Box as well as in common locations where it can be viewed by system site personnel and the Recovery Team. The Recovery Team shall have its own directory with change management limited to the Response Coordinator.

The Response Coordinator will be responsible for the plan. His or her specific responsibilities are as follows:

- Lead the annual test and assign a team member to take notes and formally document the test results including lessons learned
- Ensure that annual test documentation is stored in a designated Box repository
- Review and update this plan as needed not less than annually, incorporating lessons learned from tests, exercises, and actual events.
- Ensure that team members can access this plan in Box, at home, in a personal car, or electronically via a hand-held device or laptop computer.
- Regularly review and update information in the disaster recovery plan (e.g., contact lists, equipment inventories). Communicate with responsible personnel to get up-to-date information periodically.
- Hold initial team meeting to get team members acquainted with the plan and hold annual meetings to review and test the plan on an ongoing basis
- Maintain an accurate record of critical internal and external contacts that will be needed in a disaster
- Ensure that at least one critical data backup is technically restored during each annual test. The technical backup restore test shall be documented as part of the annual test of the plan.

## **8. Alert / Verification / Declaration Phase (1-4 Hours)**

### *8.1 Notification Of Incident Affecting Physical Office*

#### **Business-hours:**

Upon observation or notification of a production service outage or potentially serious situation during working hours at an office facility, ensure that personnel on site have enacted standard emergency and evacuation procedures if appropriate and notify emergency responders and the Response Coordinator.

#### **After hours:**

Notify the Response Coordinator if you become aware of an after-hours emergency or disaster. Notify building management and/or emergency responders as needed.

### *8.2 Provide Status To Recovery Team*

The Response Coordinator will contact the Recovery Team and provide the following information when any of the following conditions exist: (See Appendix B for contact list).

- Production services are offline for four (4) or more hours
- Any production problem that would cause the above condition to be present or where there is certain indication that the above condition is about to occur.
- Unavailability of a physical office due to a disaster.

The Response Coordinator will provide the following information:

- Location or scope of the disaster
- Type of disaster (e.g., fire, hurricane, flood)
- Summarize the damage (e.g., minimal, heavy, total destruction)
- Directions and information for staff who are working remotely from home
- An estimated timeframe of when a damage assessment group can enter the facility (if possible)

### *8.3 Decide Course Of Action*

Based on the information obtained, the Response Coordinator decides how to respond to the event.

### *8.4 Inform Recovery Team Of Decision*

If a disaster is not declared, the Response Coordinator will continue to address and manage the situation through its resolution and provide periodic status updates to the Recovery Team and Mursion Corporate.

If a disaster is declared, the Response Coordinator will notify the Recovery Team members immediately for deployment.

Declare a disaster if the situation is not likely to be resolved within predefined time frames. The person who is authorized to declare a disaster must also have at least one (1) backup who is also authorized to declare a disaster in the event the primary person is unavailable.



### 8.5 *Response Coordinator Notifies Account Teams & Customers*

Using the call list in (Appendix B), Response Coordinator contacts Recovery Team members to inform them of the situation. If known, advise as to when operations will be restored or what actions will be taken to restore operations.

### 8.6 *Contact General Vendors*

Contact any affected or needed vendors per the procedure in Appendix E.

### 8.7 *Conduct Detailed Damage Assessment*

Under the direction of local authorities and/or the Response Coordinator, the Response Coordinator shall assess the damage to the affected location and/or assets. Include vendors/providers of installed equipment to ensure that their expert opinion regarding the condition of the equipment is determined ASAP.

*NOTE: Access to the facility following a fire or potential chemical contamination will likely be denied for 24 hours or longer.*

The Response Coordinator shall document assessment results using Assessment and Evaluation Forms contained in Appendix D.

#### **Building access permitting:**

- Conduct an on-site inspection of affected areas to assess damage to essential hardcopy records (files, manuals, contracts, documentation, etc.), electronic systems, and data
- Obtain information regarding damage to the facility (e.g., environmental conditions, physical structure integrity, furniture, and fixtures) from the Response Coordinator.

#### **Determine priorities:**

- Develop a Restoration Priority List, identifying facilities, vital records and equipment needed for resumption activities that could be operationally restored and retrieved quickly
- Develop a Salvage Priority List identifying sites and records which could eventually be salvaged
- Make recommendations for required resources
- Contact the Recovery Team and decide whether the situation requires the initiation of business recovery plans or if work can return to the primary location
- Determine whether the site remains physically secure or whether contract guard services are required.

### 8.8 *Decide Whether To Continue To Business Recovery Phase*

The business recovery phase of this plan will be implemented when resources are required to support full restoration of system and/or facility functionality at an alternate recovery site (e.g., another company office, vendor hot site, cold site) that would be used for an extended period.

*NOTE: During the Initial Response Phase, service may be shifted to alternate sites to allow operations to begin functioning and provide service to its customers. Initially reduced service may be provided until sites can be fully restored. Coordinate with management to ensure services are moved to alternate sites and functional within 48 hours/2 days.*

The Response Coordinator and Mursion management may determine that staff should work from home until the primary site is restored.



## **9. BUSINESS RECOVERY PHASE (96 HOURS – FULL RECOVERY)**

This section documents the steps necessary to activate business recovery plans to support full restoration of systems or facility functionality.

### *9.1 Production Service Recovery*

If a disaster is isolated to production services, the following restoration process must occur to restore to full service: Mursion Production Services Technical Disaster Recovery Procedure.

### *9.2 Notify Response Coordinator And Mursion Corporate Of Recovery Startup*

Using the call list in Appendix B, notify the appropriate company personnel. Inform them of any changes to processes or procedures, contact information, hours of operation, etc. (may be used for media information)

### *9.3 Operations Recovered*

Assuming all production services have been recovered, and employees are in place to support operations, the company can declare that it is functioning in a normal manner at the recovery location.

Using the call list in (Appendix B), Response Coordinator shall contact Recovery Team members to inform them of the situation. If known, advise as to when operations will be restored or what actions will be taken to restore operations.

Following a disaster at a physical office, once staff are accounted for and the site is secured, the disaster can be declared over and staff shall be informed of plans to work from home or alternate locations until access to the facility is restored or an alternate facility is established.

## **5. Amendment/Termination Of This Policy**

Mursion reserves the right to modify, amend or terminate this policy at any time. This policy does not constitute a contract between the company and its employees, partners, agents and contractors.

## **6. Exceptions**

Requests for an exception to this Policy must be submitted to authorized personnel for approval. All exception requests will be handled in accordance with the Information Security Exception Policy and Standard.

## **7. Violations/Enforcement**

Any known violations of this policy should be reported to the company's IT department. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures. The Mursion may advise law enforcement agencies when a criminal offense may have been committed.



## Appendix A: Role Definitions

### 1. Response Coordinator

Responsible for overall coordination of the disaster recovery effort, evaluation and determining disaster declaration, and communications with senior management. Following a disaster, the CEO, Chief Technology Officer, or Information Security Manager shall assign a Response Coordinator for the oversight of disaster response and recovery operations.

Support activities:

- Evaluate which recovery actions should be invoked and activate the Recovery Team.
- Evaluate and assess damage assessment findings
- Set restoration priority based on the damage assessment reports
- Provide senior management with ongoing status information
- Acts as a communication channel to corporate teams and major customers
- Work with vendors and Recovery Team to develop a rebuild/repair schedule

### 2. Recovery Team

The Recovery Team is formed to deploy to the disaster location when a disaster is declared. The Recovery team will typically consist of senior engineers.

Support activities:

- Provide the following information to the Response Coordinator in the event of an outage:
  - o Type of event
  - o Location of occurrence
  - o Time of occurrence
  - o Recovery time and work effort estimates
  - o Ongoing recovery progress status reports
- Coordinate resumption of voice and data communications:
  - o Work with management to restore or re-route voice and data lines
  - o Verify voice mail and electronic mail are operational for staff
- Coordinate resumption of information system operations:
  - o Work with management to recover critical systems, applications, and infrastructure
  - o Recover critical data files and related information as needed
  - o Ensure that network and perimeter security is re-established
  - o Verify normal, secure operation of systems and servers at alternate sites

### 3. Engineering

Engineering will facilitate technology restoration activities.

Support activities:

- Upon notification of disaster declaration, review and provide support as follows:
  - o Facilitate production service recovery and restoration activities
  - o Coordinate removal of salvageable equipment at disaster site



Appendix B: Recovery Team Contact List

1. Recovery Team

| Name | Address | Home | Mobile/Cell Phone |
|------|---------|------|-------------------|
|      |         |      |                   |
|      |         |      |                   |
|      |         |      |                   |
|      |         |      |                   |

2. IT Operations

| Name | Address | Home | Mobile/Cell Phone |
|------|---------|------|-------------------|
|      |         |      |                   |
|      |         |      |                   |
|      |         |      |                   |
|      |         |      |                   |





**Appendix C: Contact List**

| Name | Address | Home | Mobile/Cell Phone |
|------|---------|------|-------------------|
|      |         |      |                   |
|      |         |      |                   |
|      |         |      |                   |
|      |         |      |                   |





Appendix D: Forms

Incident/Disaster form

Upon notification of an incident/disaster situation the senior on-site manager will make the initial entries into this form. It will then be forwarded to the Response Coordinator, where it will be continually updated. This document will be the running log until the incident/disaster has ended and “normal business” has resumed.

Time And Date

---

Type of Event

---

---

---

---

---

---

---

Location

---

---

Building Access Issues

---

---





---

---

---

---

## This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins or other markings on the paper.



Critical Equipment Status Assessment And Evaluation Form

Recovery Team: \_\_\_\_\_

[-----STATUS-----]

| Equipment | Condition | Salvage | Comments |
|-----------|-----------|---------|----------|
| 1.        |           |         |          |
| 2.        |           |         |          |
| 3.        |           |         |          |
| 4.        |           |         |          |
| 5.        |           |         |          |
| 6.        |           |         |          |
| 7.        |           |         |          |
| 8.        |           |         |          |
| 9.        |           |         |          |
| 10.       |           |         |          |
| 11.       |           |         |          |
| 12.       |           |         |          |
| 13.       |           |         |          |
| 14.       |           |         |          |
| 15.       |           |         |          |

Legend

- Condition:
- OK - Undamaged
  - DBU - Damaged, but usable
  - DS - Damaged, requires salvage before use
  - D - Destroyed, requires reconstruction





Appendix E: General Contact

Server And Computer Equipment Suppliers

| Company Name | Contact | Work | Mobile/Cell Phone |
|--------------|---------|------|-------------------|
|              |         |      |                   |
|              |         |      |                   |
|              |         |      |                   |
|              |         |      |                   |

Communications And Network Services Suppliers

| Company Name | Contact | Work | Mobile/Cell Phone |
|--------------|---------|------|-------------------|
|              |         |      |                   |
|              |         |      |                   |
|              |         |      |                   |
|              |         |      |                   |

Mechanical Engineering (Hvac, Facilities, Etc.)

| Company Name | Contact | Work | Mobile/Cell Phone |
|--------------|---------|------|-------------------|
|              |         |      |                   |
|              |         |      |                   |
|              |         |      |                   |
|              |         |      |                   |





**Plumbing**

| Company Name | Contact | Work | Mobile/Cell Phone |
|--------------|---------|------|-------------------|
|              |         |      |                   |
|              |         |      |                   |
|              |         |      |                   |
|              |         |      |                   |

**Building Management And Site Security Services**

| Company Name | Contact | Work | Mobile/Cell Phone |
|--------------|---------|------|-------------------|
|              |         |      |                   |
|              |         |      |                   |
|              |         |      |                   |
|              |         |      |                   |

