08

**Fall**

**Brandeis University 2015 Disaster Recovery**

**Tabletop Exercise Plan (ExPlan)**

Table of Contents

[Exercise Agenda 3](#_Toc429057865)

[Acknowledgments 3](#_Toc429057866)

[Participant List 4](#_Toc429057867)

[Introduction 5](#_Toc429057868)

[Purpose 5](#_Toc429057869)

[Scope 5](#_Toc429057870)

[Goals 5](#_Toc429057871)

[Objectives 5](#_Toc429057872)

[Planning Assumptions 6](#_Toc429057873)

[Structure 6](#_Toc429057874)

[Guidelines 6](#_Toc429057875)

[Ground Rules 6](#_Toc429057876)

[Module 1: Incident & Initial Response (9-10am) 8](#_Toc429057877)

[Module 1: Discussion Questions 10](#_Toc429057878)

[Module 2: Secondary Impact (10-11am) 12](#_Toc429057879)

[Module 2: Discussion Questions 13](#_Toc429057880)

[Module 3: Tertiary Impact (11-11:30) 15](#_Toc429057881)

[Module 3: Discussion Questions 16](#_Toc429057882)

[Hotwash (11:30-12) 17](#_Toc429057883)

[FEMA Online Training 18](#_Toc429057884)

# Exercise Agenda

|  |
| --- |
| 0830–0900 Welcome and opening remarks |
| 0900–1000 Module 1 |
| 1000–1010 [Break] |
| 1015–1100 Module 2 |
| 1100-11:30 Module 3 |
| 1130–1200 Combined Discussion  |

At 8:55 am, the operations team will call the leadership team meeting location and a round of introductions will take place. As long as the exercise does not preclude it, electronic services (e.g., Google Apps) may be used.

# Acknowledgments

This document was prepared by Michael Corn, Deputy CIO, Library and Technology Services at Brandeis University. Christina Maryland provided valuable feedback regarding emergency communications and Peter Nash provided valuable feedback regarding professional services training.

# Participant List

Note: some last minute delegation, substitutes, or observers should be expected

|  |  |  |
| --- | --- | --- |
| **Name**  | **Unit** | **Role in TTX** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## Introduction

All organizations experience unexpected and unwanted disruptions to their day-to-day operations. Too often organizations view an IT emergency as something solely handled by their IT unit. However as more and more of the University’s mission requires a working IT infrastructure, it becomes increasingly important to look at the broader impact of an IT systems or infrastructure disaster on Brandeis’ operations.

Fortunately while it is impossible to predict when and what sort of emergency will occur, it is possible to prepare in advance. Only by regularly practicing responding to a simulated disaster can an organization gain confidence that when a real incident occurs, it’ll be prepared to respond.

## Purpose

A tabletop exercise is a review of the processes and procedures that would generally be used during a real crisis. The goal of this exercise is to detect issues that may interfere with response and recovery during an actual emergency.

## Scope

The scope of this exercise should be strictly limited to online education and specifically the impact of the Latte system being unavailable. Do not spend time discussing how to recover from additional systems that would (in a real event) also be disabled by the simulated incident. Aspects of the exercise are necessarily contrived – some suspension of belief is always required.

Note to all participants and facilitator: due to the compressed nature of the ‘incident time’ vs. actual time, it will be necessary to treat incident time in an elastic fashion. Once the exercise begins the facilitator will start the ‘incident clock’ and we will attempt to work to the degree possible in real-time. However the facilitator should feel free to move forward in incident time if necessary to push the discussion forward.

## Goals

The primary objective of this exercise is to explore many of the issues that will arise during an IT disaster scenario, some technical, some mission related. This is the first step to the creation of a rigorous disaster recovery plan and thus to provide Brandeis with the capabilities to respond and recover effectively. We want to identify gaps and establish best practices that should be addressed when creating a disaster recovery plan. Although this is a timed event, our goal is not to race to some arbitrary point of resolution.

## Objectives

* Exercise teamwork: focus on relationship and team building
* Provide us tools for crisis response, and a forum for discussing and developing emergency plans
* Test assumptions
* Enhance Brandeis emergency resiliency

## Planning Assumptions

The participants in this exercise will be separated into two teams, one operations and one leadership. The operations team should focus on returning impacted services to availability. The leadership team will be discussing questions related to general emergency response (such as the availability of an emergency operations center) and addressing questions related to policy or resources beyond the capacity or authority of the operations team. Both rooms will have phones in them, though participants are free to communicate with others as desired and within the constraints of the scenario.

## Structure

This will be a facilitated tabletop exercise (TTX). Players will participate in the following three distinct modules:

* Module 1: Incident + Initial Response
* Module 2: Secondary Impact
* Module 3: Tertiary Impact

Each module begins with an update that summarizes the key events occurring within a specific time period. Following the updates, participants review the situation and engage in a plenary group discussion of appropriate response issues.

Questions have been included after each module to stimulate discussion and the flow of information around departmental procedures and encourage interdepartmental collaboration.

Each exercise participant will receive this Exercise Plan (ExPlan), which provides a written scenario and situation updates. Following each module is a series of questions that highlight pertinent issues for consideration. These questions are supplied as catalysts for the group discussions; participants are not required to answer every question, nor are they limited to those topics. Participants are encouraged to use this ExPlan as a reference throughout the exercise.

## Guidelines

Although you may look ahead in this plan, it is important to address only the current and prior events in each module. You may not move forward or discuss items that have not yet occurred.

This is a time to discuss the specific actions you will—or be assigned—to undertake. Always consider how long each action might take. Take whatever time is necessary to discuss your process, procedures and protocol.

## Ground Rules

The follow ground rules will apply to this exercise:

* This is a no-fault exercise and is not a test.
Varying viewpoints, even disagreements, are expected. This is intended to be an open, low-stress environment.
* The exercise setting is the ideal opportunity to consider different approaches and suggest improvements to current resources, plans, and training.
* Responses should be based on current capabilities.
* **Fight the problems, not the scenario.**
* Respect the speaker.
* Start on time, end on time, and use the timers.
* Look through the windshield and not the rear view mirror.
* Enough, Let’s Move On (E.L.M.O.) will be used to keep the group moving forward and avoid becoming entrenched in the minutiae
* There are no “hidden agendas” or trick questions intended to mislead participants.
* All participants will receive the same information at the same time.

# Module 1: Incident & Initial Response (9-10am)

Incident Background

Incident

Monday, November 2nd 2015 at 3:00am

### Event 1: 3am November 2nd 2015

At 3am a disgruntled ex-employee entered Feldberg – he were terminated on October 30th and his card access had not yet be terminated so he was able to enter the building and all LTS communications rooms and data centers.

Once in the building he took a crow bar and smashes the CISCO ACE 30 load balancer impacting Moodle services and then he pulled the alarm bar and turned off building power (by pressing the circuit disconnect in room 104A).

### Event 2: 3:15am November 2nd

Brandeis University police arrive and seeing the smashed equipment quickly disable the alarm and declare the data center a crime scene. The police do not allow anyone to touch the core power switch for the building until a fingerprint expert arrives and tests the switch for fingerprints.

### Event 3: 5am November 2nd

After hiding in the Library for the last couple of hours, the ex-employee made his way to the Goldfarb data center and physically removes the CISCO ACE 30 in this data center. This load balancer is also crushed and left on the floor in pieces.

Current Situation

Anyone who feels they would have already been engaged in the incident should summarize what they believe their actions would have been.

**Inject 1, 9am:** The LTS Helpdesk opens to a queue of 100 messages from students reporting that they are unable to log into Latte. 30 similar messages are from faculty who have early morning classes and are unable to access Latte.

**Inject 2, 9:45**: Social media is describing some sort of event requiring law enforcement on campus and the first calls from worried parents are starting to come in. The main Brandeis website ([www.brandeis.edu](http://www.brandeis.edu)) is seeing an increasing load. (nb: this inject will primarily be of significance to the communications staff and the leadership team).

Planning Considerations:

The following services are affected (i.e., “in play”):

* Latte
* Feldberg and Goldfarb data center

The following services are unaffected (i.e., “out of play”):

* DNS
* Internet connectivity
* Other systems running on the virtualized infrastructure

# Module 1: Discussion Questions

Group

1. In an actual incident, what would have taken place by the time of the exercise kick-off?
2. Based on the information presented, what are your top priorities at this time?
3. What department is the lead in response?
4. Who will be coordinating between departments?
5. How would you be alerted to a possible access breach and large-scale service interruption?
6. Where would the leadership meet in an actual incident (where is the EOC)? How would they have been notified? What is the chain of command for institutionally scoped decisions?

University Services

1. What processes or procedures would you implement in response to the situation presented? What procedures are in place to access the environmental hazard from the liquid in Goldfarb?
2. Who would you look to coordinate your response?
3. Who or when would you engage the University’s leadership?

Library and Technology

1. What alarms or monitoring would have been triggered by the incident as described?
2. What coordination among departments is necessary at this point?
3. What plans, policies, and/or procedures are in place to prevent or respond to a large-scale service interruption?
4. What information sources could you contact to get further information about this service interruption?
5. Due to the information presented, would there be any immediate operational changes in your department? Would this involve a change in security protocol, either physical or logical?

Academic Units

1. How would you expect to first hear about the incident?
2. What procedures or communications might you undertake once learning about the incident?

Communications

1. When would you expect to be notified?
2. How does Office of Communications respond to this type of incident?
3. Is this protocol discussed in the Brandeis Crisis Communications Plan? Has this plan been provided to communications liaisons university-wide? Are they aware of the protocol?

Public Safety

1. Does the University police department possess resources or personnel capable of investigating access breaches/crimes?
2. What coordination among departments is necessary at this point?
3. What information sources at LTS would you contact to get further information?
4. Due to the information presented, would there be any immediate operational changes in your department? Would this involve a change in security protocol, either physical or logical?

# Module 2: Secondary Impact (10-11am)

**Inject 3, 10am:** Brandeis University police, working with Waltham police have collected all the evidence they need from the Feldberg data center and allow LTS staff to re-enter to and to enable power to the building.

### **Inject 4, 10:15am:** The volume of calls to the Helpdesk and to the general Brandeis operator are so large that general phone service is starting to fail – callers are getting busy signals and in general the phones are of intermittent use, even on campus.

**Inject 5, 10:45am:** Using CCTV footage and in consultation with HR, Brandeis police were able to identify the suspect in the incident under discussion and are working with area law enforcement to apprehend him. He is not believed to be on campus at this time. The individual is an ex-LTS employee who was terminated for cause on Friday. The suspect had privileged access to all LTS facilities and professional knowledge of the Brandeis computing environment.

Planning Considerations:

The following services are affected (i.e., “in play”):

* Latte
* Feldberg and Goldfarb data center
* Brandeis phone system
* Brandeis primary website

The following services are unaffected (i.e., “out of play”):

* DNS
* Internet connectivity
* Other systems running on the virtualized infrastructure

# Module 2: Discussion Questions

Group question

1. Based on the information presented, what are your top priorities at this time?
2. Is there a list of critical contact information for network, security, or senior-level administrators? Where is this located?

University Services

1. With the partial or complete failure of the campus phone system, how are US operations affected?
2. Who are the building wardens? How is this information provided to staff? Do they play a role in your response?

Library and Technology

1. Specifically, what interdepartmental coordination is necessary at this point?
2. What steps must be taken to ensure critical evidence is preserved? Are procedures in place for this action?
3. Will this incident impact library operations for the day/week? What is the business continuity plan? If there is an impact, how will this be communicated to the staff and campus community?

Communications

1. How does this team respond to the incident as it escalates?
2. Who is notified of the disruptions, within your department and across the university or the public?
3. What coordination among departments is necessary at this point? When should the release of incident related information be provided to coordinating departments?
4. When are senior university leaders provided a brief of the incident scope?
5. What consideration is given to the release of service interruption alerts to campus community members? What is the protocol for rumor control?
6. Due to the information presented, would there be any immediate operational changes in your department?

Academic Units

1. What internal processes or communications with your faculty or students would you be implementing?
2. What information might you be putting on your website about this incident?
3. What information do you need to know to plan your response accordingly?

Public Safety

1. How are decisions made about protecting the system/data versus investigating this problem as a crime? Who makes the decision?
2. What steps must be taken to ensure critical evidence is preserved? Are procedures in place for this action?

# Module 3: Tertiary Impact (11-11:30)

**Inject 6, 11am:** A Facebook posting claims that a bomb went off on the Brandeis campus and that’s why no one can get through on the phone. The Brandeis homepage receives 100x of times its normal load and becomes unresponsive.

Planning Considerations:

The following services are affected (i.e., “in play”):

* Latte
* Feldberg and Goldfarb data center
* Brandeis phone system and primary website

The following services are unaffected (i.e., “out of play”):

* DNS
* Internet connectivity
* Other systems running on the virtualized infrastructure

# Module 3: Discussion Questions

Group question

1. Based on the information presented, what are your top priorities at this time?
2. What are the long-term effects associated with the situations presented?
3. What is your department’s role in the continuing investigation? How would this be coordinated with university efforts?

University Services

1. Can US assist in shifting IT operations to alternative facilities on campus? Is this feasible?
2. Can additional classroom space be made available for courses traditionally held online?

Library and Technology

1. What is the priority of repair or restoration of systems?

Communications

1. How would you monitor the dissemination of this rumor?
2. What previously untargeted departments or demographics would now require communications?

Academic Units

1. What is your role in responding to inquiries from parents or alumni?

Public Safety

1. How would you monitor the dissemination of this rumor?
2. What previously untargeted departments or demographics would now require communications?

# Hotwash (11:30-12)

At 11:30 the leadership team will move to the larger Gardner Jackson room where the operations team is located. A general discussion of the exercise and lessons learned will take place.

1. Based on this exercises would you take any proactive approaches to prepare for an actual event? How would you prepare?
2. Were the University phone operators prepared to respond to calls?
3. What is the maximum amount of time that Latte can be unavailable? How do we create procedures to address continuity of operations during this interval?
4. If Latte can only be restored from a backup – how far back in time can that back up come from (i.e., how many days of lost data can we tolerate?)
5. If resources need to be procured (IT equipment, leased space…) who can authorize these expenses?
6. What would be the reputational impact to Brandeis of this event and how would you address that?

# FEMA Online Training

FEMA provides a host of online incident training material. A few of the core courses are listed here; it is recommended that all members of the University’s and LTS’ leadership complete IS100 and IS 700.

* FEMA - Emergency Management Institute (EMI) Course | IS-700.A: National Incident Management System (NIMS) An Introduction

<https://training.fema.gov/is/courseoverview.aspx?code=IS-700.a>

* FEMA - Emergency Management Institute (EMI) Course | IS-100.B: Introduction to Incident Command System, ICS-100 <https://training.fema.gov/is/courseoverview.aspx?code=IS-100.b>