UNIVERSITY of HOUSTON
UNIVERSITY INFORMATION TECHNOLOGY

Continuity of Operations Plan (COOP)

Version 4.12

September 2018

Approval and Implementation

This plan applies to all University of Houston IT units (UIT) with assigned emergency and service continuity responsibilities, as described in this plan.

THIS PLAN IS HEREBY APPROVED FOR IMPLEMENTATION AND SUPERSEDES ALL PREVIOUS EDITIONS.

Dr. Dennis Fouty Date
Associate Vice Chancellor, UHS
Associate Vice President, UH
Chief Information Officer, UHS/UH

Mary Dickerson Date
Assistant Vice Chancellor, UHS Information Security
Assistant Vice President, UH Information Security
Chief Information Security Officer, UHS/UH

David Johnson Date
Assistant Vice President, UIT Technology Services and Support

Keith Martin Date
Assistant Vice Chancellor, UHS Enterprise Systems
Assistant Vice President, UIT Enterprise Systems

Table of Contents

Section 1: Plan Overview

1.1 Purpose

The University of Houston (UH) University Information Technology (UIT) Continuity of Operations Plan (COOP) is intended to establish procedures and organizational structure for response to events that are of a magnitude to cause a significant disruption of the functioning of all or portions of UIT services. This plan describes the roles and responsibilities of UIT departments and personnel during these incidents. Since events may be sudden and without warning, these procedures are designed to be flexible in order to accommodate contingencies of various types and magnitudes.

Through the use of appendices, this COOP addresses specific types of incidents providing guidelines for the stabilization and continuity of UIT services throughout the incident. These include emergency instructions and references in a concise format for the individuals designated to manage UIT resources.

The goal of this plan is to reduce the consequences of any disruptive incident to UIT Services to non-service affecting levels and to participate with the UH Emergency Management team.

The Continuity Plan is a static document, and represents a framework and references. Nothing in this plan shall be construed in a manner that limits or prevents the use of good judgment and common sense in matters not foreseen or covered by the elements of the plan.

1.2 Alignment with UH Emergency Management Plan

This plan outlines the preparation, preparedness, response, assessment, recovery, and mitigation of UIT resources. The UIT COOP is consistent with established practices relating to interoperability of emergency response actions.

Plans and activities required for protecting the safety and welfare of the university's students, faculty, staff and visitors may be found in the UH Emergency Management Policy, MAPP 06.01.01 and in the UH Business Continuity Policy, MAPP 06.01.02.

This plan incorporates the use of the National Incident Management System (NIMS) National Response Framework (NRF), Incident Command (IC) and National Fire Protection Association (NFPA) 1600, Standard on Disaster/Emergency Management and Business Continuity Programs to facilitate interoperability within the university and between responding mutual-aid agencies.

1.3 Annual Preparedness Activities

By June 1st of each year, the following tasks will be completed:

- All UIT staff will ensure their contact information is correct and complete within PASS.
- All UIT staff will ensure they have the appropriate tools for working remotely if required to do so during an incident. A planning guide is available at www.uh.edu/workingoffcampus.
- UIT Ride Out Team primary and backup members will be confirmed and training requirements verified.
- UIT emergency supplies will be inspected: replace batteries, broken and depleted items and ensure sufficient food and water provisions and accommodations for the Ride Out Team during an incident.
- UIT core locations will be reviewed to ensure preparation: equipment up off the floor, fuel in generator, cameras for real-time monitoring operational.
- ITAC communication methods will be verified to ensure that they are in working order and fully charged: MiFi, cell phones, 2-way radios, conference bridges, satellite phone.

- The UIT Continuity Of Operations plan will be reviewed to ensure it is up-to-date, tested and posted to the ITAC website at www.uh.edu/itac.

1.4 Testing the Plan

UIT Information Security is responsible for continuity planning and for conducting a test to determine the effectiveness of the plan and areas where the plan needs modification. This will consist of one of the following exercises: Orientation Seminar, Drill, Tabletop, Functional, or Full-Scale exercise. All UIT Managers and staff will jointly step through the plan's prescribed steps and activities to ensure that everyone agrees that the steps will serve to effectively continue services affected during the incident. At the end of the test, an After Action Review will be conducted in order to update the current plan. **The most recent test of the plan was done as a Tabletop on TBD, 2018**.

Test Exercise Procedures:

1. UIT Information Security will be responsible for coordinating the annual test exercise, which could be unannounced, and determining the type of exercise and testing procedure.

2. UIT managers will execute the procedures noted in the COOP during the exercise.

3. UIT Information Security will conduct an After Action Review of the exercise within 48 hours of completion of the exercise.

4. Any problems detected by the exercise will be logged and assigned to a person for resolution. Based on the severity of the problem, exercises may be run again after the fix has been made or implemented.

The Manager, IT Security Risk Management and Compliance has primary responsibility for collecting and publishing changes to this COOP. Any changes in personnel, hardware, software or telecommunications can create significant changes in the recovery plan. As key members of the plan change positions, the plan must be updated with new contact information and responsibilities. Similarly, system changes must be promptly reflected in the COOP. The Manager, IT Security Risk Management and Compliance will rely on UIT managers to furnish this information on a timely basis. However, the plan will be reviewed annually to insure updates are being made.

The current version of this plan is posted on the ITAC website. www.uh.edu/itac.

1.5 Business Impact Analysis

Business Impact Analysis (BIA) is the process of identifying Critical Information Resources (CIR) required to resume academic and business operations to a non-service affecting level. A BIA distinguishes between critical and non-critical resources.

Functional Area	Business Functions and Processes (People, Property, Processes) Descriptions	1. Critical Program Space and Facilities Are Damaged or Unavailable				2. Critical Equipment is Damaged or Unavailable.			
		Impact H-M-L (High=1)	Probability H-M-L (High=1)	Maximum Tolerable Downtime (MTD in days)	Rank	Impact H-M-L (High=1)	Probability H-M-L (High=1)	Maximum Tolerable Downtime (MTD in days)	Rank
ES	Critical Core Services	1	3	0.005	0.02	1	2	0.005	0.01
ES	Mission Critical Applications/Services	1	3	0.005	0.02	1	2	0.005	0.01
ES	Telecommunications Services	1	2	0.01	0.02	1	2	0.01	0.02
TSS	IT Support Services	2	3	0.5	3	2	2	0.5	2
SEC	Information Security Services	2	3	1	6	2	2	1	4

Functional Area	Business Functions and Processes (People, Property, Processes) Descriptions	3. Centrally Provided Power Unavailable				4. Communications (Phone, Fax, Email, and Internet) Unavailable			
		Impact H-M-L (High=1)	Probability H-M-L (High=1)	Maximum Tolerable Downtime (MTD in days)	Rank	Impact H-M-L (High=1)	Probability H-M-L (High=1)	Maximum Tolerable Downtime (MTD in days)	Rank
ES	Critical Core Services	2	3	0.005	0.03	2	1	0.005	0.01
ES	Mission Critical Applications/Services	2	3	0.005	0.03	1	1	0.005	0.01
ES	Telecommunications Services	1	2	0.01	0.02	1	1	0.01	0.01
TSS	IT Support Services	2	3	0.5	3	2	1	0.5	1
SEC	Information Security Services	2	3	1	6	2	1	1	2

(continued on page 8)

Functional Area	Business Functions and Processes (People, Property, Processes) Descriptions	5. Central InfoSys are Non-functional				6. Local InfoSys are Non-Functional			
		Impact H-M-L (High=1)	Probability H-M-L (High=1)	Maximum Tolerable Downtime (MTD in days)	Rank	Impact H-M-L (High=1)	Probability H-M-L (High=1)	Maximum Tolerable Downtime (MTD in days)	Rank
ES	Critical Core Services	1	2	0.005	0.01	1	2	0.005	0.01
ES	Mission Critical Applications/Services	1	2	0.005	0.01	1	2	0.005	0.01
ES	Telecommunications Services	1	2	0.01	0.02	1	2	0.01	0.02
TSS	IT Support Services	2	2	0.5	2	2	2	0.5	2
SEC	Information Security Services	2	2	1	4	2	2	1	4

Functional Area	Business Functions and Processes (People, Property, Processes) Descriptions	7. Staff is Impacted and Unavailable				8. Critical Vendors/Partners Unavailable			
		Impact H-M-L (High=1)	Probability H-M-L (High=1)	Maximum Tolerable Downtime (MTD in days)	Rank	Impact H-M-L (High=1)	Probability H-M-L (High=1)	Maximum Tolerable Downtime (MTD in days)	Rank
ES	Critical Core Services	2	3	0.005	0.03	2	2	0.005	0.02
ES	Mission Critical Applications/Services	2	3	0.005	0.03	2	2	0.005	0.02
ES	Telecommunications Services	2	3	0.01	0.06	2	2	0.01	0.04
TSS	IT Support Services	1	3	0.5	1.5	3	2	0.5	3
SEC	Information Security Services	2	3	1	6	3	2	1	6

1.6 Impact Assessment of Major UIT Provided Services

No.	Business Activities	Business Owner	Impact[1] (High=1)	Probability (High=1)	Rank (Impact * Prob)
CRITICAL CORE SERVICES					
1	DNS	Charles Chambers	2	2	4
2	DHCP	Charles Chambers	2	2	4
3	Active Directory	Eric Block	2	2	4
4	Emergency Web Presence	Diane Trippel	2	2	4
5	Emergency Email	Eric Block	2	2	4
6	Emergency Listserv	Diane Trippel	2	2	4
CRITICAL INFORMATION RESOURCES					
1	UH/UHV Blackboard	Jeff Morgan	2	2	4
2	UH.edu Web Farm	David Johnson	2	2	4
3	Data Warehouse	Susan Moreno Barbara Duarte	2	2	4
4	Lync	David Johnson			
5	Email Service	David Johnson	2	2	4
6	PS-UH/UHCL/UHV Student System	Mara Affre	2	3	6
7	PS - UHS HR/Payroll	Joan Nelson	2	3	6
8	PS - Finance	Karin Livingston	2	3	6
9	PS – UHS Portal	Mara Affre			
10	University Advancement	Steve Mueller	2	2	4
11	Remedy	Leroy Mays	3	2	6
12	Post office SMTP email services	Eric Block	2	2	4
13	Everbridge	Malcolm Davis	2	2	4
14	LDAP (alias)	David Johnson	2	2	4
15	File Services	Eric Block	2	2	4
16	Cougar Card	Deborah Marks	2	2	4
17	TSM	David Johnson	3	2	6
18	Fax Server	David Johnson	3	2	6
19	SharePoint	David Johnson	2	2	4
20	AccessUH	David Johnson	2	2	4
21	Print Services	Eric Block			
22	FAMIS	David Oliver			
23	UH Go	Lisa Holdeman	2	2	4
24	SendIt	David Johnson	2	2	4

(Continued on page 10)

[1] Degree of impact considers political or sensitivity, and financial costs

TELECOMMUNICATIONS SERVICES CRITICAL CORE SERVICES					
1	Network Infrastructure	Charles Chambers	2	2	4
2	VPN	Charles Chambers	2	2	4
3	Voice System/ ACD/Phone Mail	Charles Chambers	2	2	4
4	Internet	Charles Chambers	2	3	6
5	Internet 2	Charles Chambers	2	3	6
INFORMATION SECURITY CRITICAL INFORMATION RESOURCES					
1	SSL Certificates	Jana Chvatal	2	2	4

Impact Assessment is the result of identifying the CIR Business Owner, assessing the CIR on degree of impact and probability of occurrence, and ranking on the product of impact and probability. Additionally, the BIA also identifies and ranks the Critical Core Services, which are resources that are required to have an infrastructure in place for the Critical Information Resources. The rank for each of activity will be considered in determining the function's criticality.

Degree of Impact
1 = Loss of mission-critical service to all students/staff
2 = Significant loss of service to some users
3 = Inconvenient for some users but not essential

Probability of Occurrence
1 = Most likely incident will occur
2 = Nominal chance of incident occurring
3= Little or no chance of incident occurring

Rank (Impact*Probability)
1-3 = Highly Critical
4-6 = Medium Critical
7-9 = Not Critical

Section 2: Emergency Declaration and Response

2.1 Authority to Declare an Emergency

Based on information obtained from authorities of the University or from the Information Technology Availability Center (ITAC), the University CIO or designee may declare an emergency based on the current situation or predetermined criteria outlined for specific scenarios. At the discretion of the CIO, portions of or the complete Continuity of Operations Plan may be activated as needed to mitigate the threat.

2.2 Criteria for Declaring an Emergency

An emergency may be declared based on one or more of the following criteria:

1. An emergency has been declared by the University.
2. UIT is experiencing a service affecting incident whose degree of impact affects all faculty, staff and students.
3. UIT is experiencing a significant loss of service to a group of users for more than 4 hours.
4. A significant external imminent threat (i.e., weather, pandemic, etc.) has been identified by a government agency.
5. At the discretion of the CIO or designee, based on the current situation (i.e., pandemic, center of attention).

2.3 Pre-Determined Criteria and Incident Response

UIT has pre-determined the following criteria and incident response for assistance in declaring an emergency in specific scenarios. Detailed response plans for these events are available in the noted Appendix.

Scenario	Criteria	Incident Response
Weather	• Threat is expected to occur within 96 hours.	Appendix B, Level 5
	• Threat is expected to occur within 72 hours.	Appendix B, Level 4
	• Threat is expected to occur within 48 hours.	Appendix B, Level 3
	• Threat is expected to occur within 24 hours.	Appendix B, Level 2
	• Threat is expected to occur within 12 hours.	Appendix B, Level 1
Computing Center on *Generator* Power	• Utility power lost • Failover to generator has occurred successfully	Appendix F Scenario 1
Computing Center on *UPS* Power	• Utility and generator power lost • Power supplied solely by UPS	Appendix F Scenario 2
Computing Center without Chiller	• Chiller power lost	Appendix TBD

2.4 Emergency Response and Assessment

Once an emergency has been declared, the following items should be completed for the event. If the emergency is one with a pre-determined response scenario, the following steps should be incorporated into the incident response as appropriate.

A. UIT Leadership/Staffing/Communication

1. Utilizing the UIT Order of Succession located in Section 3 of this document, **identify** the Incident Commander for UIT and the Incident Leader for each workgroup within UIT.
2. **Establish** an Information Technology Incident Command Post (IT-ICP). Unless otherwise specified by the Incident Commander, the IT-ICP will be located in the Computing Center, Room 216.
3. **Establish** a Technical Bridge. The bridge will be activated by ITAC and will remain open until the emergency has been resolved.
4. **Update** the ITAC site. ITAC will make regular updates throughout the incident to the ITAC site at www.uh.edu/itac.
5. **Establish** a Management Bridge. The bridge will be activated by ITAC, who is also responsible for notifying the appropriate personnel of the bridge.
    a. UIT Managers participating in the bridge are responsible for:
        1. Addressing the impact of the incident on their respective service(s)
        2. Identifying any needs for their service as a result of the incident
        3. Responding as requested to the incident
    b. The management bridge will:
        1. **Provide** an initial briefing on the incident, identifying the impact to UIT services.
        2. **Determine** internal UIT communication needs, such as the briefing schedule and appropriate staff communication. Refer to Appendix A, Communications Strategies, to determine the appropriate mode of communication for the incident.
        3. **Identify** immediate external communication needs to the following groups. Refer to Appendix A, Communications Strategies, to determine the appropriate mode of communication for the incident.
            a. IT affiliates: Technology Partners Program, Component Campuses
            b. General Population: Faculty, Staff, Students (for UIT emergencies only).
        4. **Result** in an Incident Action Plan, which ITAC will post on the ITAC site.
6. If the incident has a predefined trigger response in Section 2.3, UIT managers should **complete** the appropriate tasks outlined in the Appendix for the incident response.

B. Service Impact Mitigation

1. **Identify** if the affected service can be run out of the secondary data center while primary operations are restored.

    Secondary Data Center Location
    University of Houston – Victoria
    3007 Ben Wilson Room 204b
    Victoria, TX 77901
    Gabe Striedel, Manager, Network Operations, 361.570.4887, striedelga@uhv.edu
    Contact Howard Jares for configuration changes or updates

UIT Personnel with access to SDC: Sam Longoria, Howard Jares, David Frankfort

Applications Currently Available in Secondary Data Center

- Blackboard
- CougarNet Active Directory
- Emergency ListServ
- Emergency UH web presence
- Infoblox

2. If the affected service cannot be run out of the secondary data center, **identify** available options for continuing the affected service or providing an alternative to the service for affected users.

C. Facilities and Infrastructure Impacts

1. An assessment of each facility where UIT staff and/or equipment is located must be conducted to make necessary adjustments to continue operations to the greatest extent possible during the incident.

- **Determine** the impact the incident has on the physical spaces occupied by UIT staff:
  - Computing Center
  - General Services Building
  - UH Technology Bridge, Building 3
  - MD Anderson Library Basement
  - Leroy & Lucile Melcher Center for Public Broadcasting
  - Ezekiel W. Cullen
- **Determine** the impact the incident has on the UIT critical infrastructure areas:
  - Computing Center
  - Cullen College of Engineering 2, room E125
  - Fred J. Heyne, room 119
  - Multi-Disciplinary Research and Engineering Building, rooms 105 & 217
  - Philip Guthrie Hoffman Hall, rooms 10, 116, & 116A
  - TDECU Stadium , room S124
  - UH Technology Bridge – Building 3, room 236
  - University of Houston Science Center, room 100F
- **Determine** the impact the incident has on the Secondary Data Center.
- **Determine** the need and/or feasibility of relocating equipment or providing an alternative service delivery method.
- **Determine** the need to relocate staff from an affected building to an alternate work location, either on campus or by sending staff home to continue working as appropriate.

2. An assessment of critical core services must be conducted to identify and rank where recovery efforts should be focused to ensure service is restored in an appropriate manner. Refer to Section 1.6 Impact Assessment of Major UIT Services for a complete listing of critical core services.

D. Personnel Accountability

1. In the event the Ride-Out Team requires activation for an emergency, ride-out team members will be identified and contacted by UIT senior management. Members must ensure their contact information is current in PeopleSoft.
2. UIT will utilize the check-in Kiosk located in the front lobby of the UHS Computing Center for recording of ride-out personnel, recovery personnel or any other UIT personnel on campus. If the Kiosk is not operational or available, the IT Incident Command Post (IT-ICP) will establish and maintain a manual log of personnel for the incident.
3. Ride-out team members are required to stay in designated areas during the emergency unless authorized by the Incident Commander.
4. When Ride-out team members rotate shifts or are released from the emergency, any items such as keys, radios, etc. must be left with the IT-ICP.
5. Any UIT personnel asked to assist during an emergency must keep a log of their time worked and activities conducted during the emergency.
6. IT-ICP will be responsible for reporting this accountability information forward to the UH Emergency Operations Center. This responsibility includes the initial report and any status changes, (people leaving or returning, or new personnel arriving on campus) that may take place.

2.5 Travel to Campus

Various weather conditions can make travel to and from campus hazardous. When the potential or conditions develop that would make travel to and from the campus hazardous, the following steps will be followed:

1. ITAC and UH Office of Emergency Management will monitor the National Weather Service broadcasts and local reports, and will monitor the TXDOT Road Conditions Web page located at http://www.txdot.gov/travel/road_conditions.htm. Upon receipt of information that would make travel hazardous, ITAC will work with UH OEM to identify the potential impact on the campus and the immediate area. If conditions threaten UIT operations, ITAC will contact the ITAC manager and advise him/her of the situation. The ITAC manager will instruct ITAC on what course of action to take and what notifications to distribute based on the conditions and directives from UH OEM.
2. Only the University President will determine if campus operations are suspended and the campus will be closed. Upon notification that the campus is closed, UIT personnel should monitor the UH Emergency Operations Center website at alerts.uh.edu.
3. UIT personnel may be asked by UIT management to support systems remotely or come to campus if able and they feel safe, to mitigate service affecting incidents with Critical Core Systems and/ or Critical Information Resources.
4. ITAC will secure the UHS Computing Center and stand up the IT Incident Command Post to continually monitor weather, news, road condition reports, and maintain communications between UIT and the UH Emergency Operations Center.
5. Once conditions have stabilized, all hazards have been mitigated, and UH OEM has advised that the campus has been reopened, the IT-ICP will notify all IT personnel of the all clear, and stand down the IT Incident Command Post. Once the IT Incident Command Post is stood down, ITAC will resume normal operations.

Section 3: Personnel and Contact Information

3.1 UIT Order of Succession

	UIT Leader	Job Title
	Dennis Fouty	Assoc VP, IT/Chief Info Ofcr
1st Successor	David Johnson	Asst VP, UIT Tech Svcs & Suprt
2nd Successor	Mary Dickerson	Asst VP/VC, IT Security / CISO
	Mary Dickerson	Asst VP/VC, IT Security, CISO
1st Successor	Jana Chvatal	Mgr, IT Sec Risk Mgmt & Comp
2nd Successor	Debbie Samuels	Mgr, Enterprise App Sec & Invs
	David Johnson	Asst VP, UIT Tech Svcs & Suprt
1st Successor	Diane Trippel	Dir, Web & Comm
2nd Successor	Leroy Mays	Dir, IT Customer Services
	Keith Martin	Asst VP/VC, UIT Enterprise Sys
1st Successor	Haseen Mazhar	Exec Dir, Entprs Sys Univ Svcs
2nd Successor	Charles Chambers	Mgr, Network Planning/Develop

	UIT Leader	Job Title
	Rita Barrantes	Dir, IT Customer Services
1st Successor	James Schexneider	Mgr, Telecommunications
2nd Successor	Omar Farooq	Mgr, Telecommunications
	Reggie Beavers	Mgr, Enterprise Computing
1st Successor	Jerry Raschke	Systems Administrator 3
2nd Successor	Kinglsey Erowele	Systems Administrator 2
	Anita Bhakta	Technical Svcs Spec 4
1st Successor	Kim Moody	Systems Analyst 3
2nd Successor	Lannette Baptiste	User Services Spec 3
	Khalid Bhatti	Mgr, Enterprise Computing
1st Successor	Richard Wall	ES Application Developer 2
2nd Successor	Meredith Coleman	ES Application Developer 2
	Robert Birkline	Mgr, Web Technology
1st Successor	Anita Bhakta	Technical Svcs Spec 4
2nd Successor	Kim Moody	System Analyst 3

	Phil Booth	Mgr, Instructional TV
1st Successor	Don Price	Video Producer
2nd Successor	Scott Wharton	Developer, Digital Media
	Eric Block	Dir, Enterprise Sys Architect
1st Successor	Jitender Kumar	Mgr, Enterprise Sys Databases
2nd Successor	Shivi Pawa	Mgr, Enterprise Computing
	Deadera Broussard	Supv, UH Contact Center
1st Successor	Carolyn Crowell	Contact Center Rep
2nd Successor	Paula McZeal-Lemelle	Contact Center Rep
	Matthew Castillo	Admnstr, UH Web
1st Successor	Ryan Reynolds	Developer, Web 2
2nd Successor	Iggy Harrison	Analyst, Systems 2
	Charles Chambers	Mgr, Network Planning/Develop
1st Successor	Tesfaye Kumbi	Network Analyst, Lead
2nd Successor	Reza Golshan	ES Network Administrator 2
	Ron Chance	Mgr, ITAC
1st Successor	Mike Kahanic	Analyst, Systems 2
2nd Successor	Leroy Mays	Dir, IT Customer Services
	Mike Chang	Mgr, Enterprise Computing
1st Successor	Adekunle Buraimoh	Application Developer 4
2nd Successor	Krishnaveni Mandalreddy	Application Developer 4
	Jana Chvatal	Mgr, IT Sec Risk Mgmt & Comp
1st Successor	Ric Rodriguez	Analyst 3, Enterprise IT Sec
2nd Successor	Debbie Samuels	Mgr, Enterprise App Sec & Invs
	Keith Crabb	Mgr, High Performance Computing
1st Successor	Jeffrey Sarlo	Systems Administrator 3
2nd Successor	Alan Pfeiffer-Traum	Systems Administrator 3
	Ivey Davis	Lead, User Services Spec
1st Successor	Amy Ma	Lead, User Services Spec
2nd Successor	Maricela Rodriguez	Coord 2, IT Documentation
	Omar Farooq	Mgr, Telecommunications
1st Successor	Brian Dooling	Analyst, Telecom 3
2nd Successor	Ray Hernandez	Analyst, Telecom 3

	Jody Gillit	Mgr, IT Project
1st Successor	Andy Moon	Technical Svcs Spec 4
2nd Successor	Tom Carroll	User Services Spec 3
	Tuong Ho	Mgr, Enterprise Computing
1st Successor	Yun Cui	ES Application Developer 2
2nd Successor	Roy Ding	ES Application Developer 2
	Howard Jares	Mgr, Enterprise Computing
1st Successor	David Frankfort	Systems Administrator 3
2nd Successor	Tilak Brahmbhatt	Systems Administrator 2
	Jitender Kumar	Mgr, Enterprise Sys Databases
1st Successor	Carol Pena	ES Database Adminstrator 4
2nd Successor	Zeandra Mathura	ES Database Adminstrator 4
	Robert Li	Mgr, Enterprise Computing
1st Successor	Alan Alejandro	Application Developer 3
2nd Successor	Michael Burns	ES Application Developer 1
	Sam Longoria	Mgr, Technology Facilities
1st Successor	Keith Crabb	Mgr, High Performance Computing
2nd Successor	Bill Spindler	Dir, Business Svcs
	Amy Ma	Lead, User Services Spec
1st Successor	Ivey Davis	Lead, User Services Spec
2nd Successor	Maricela Rodriguez	Coord 2, IT Documentation
	Leroy Mays	Dir, IT Customer Services
1st Successor	Ivey Davis	Lead, User Services Spec
2nd Successor	Amy Ma	Lead, User Services Spec
	Haseen Mazhar	Exec Dir, Entprs Sys Univ Svcs
1st Successor	Tuong Ho	Mgr, Computing Systems
2nd Successor	Robert Li	Mgr, Computing Systems
	Leo Moreno	Mgr, Enterprise Computing
1st Successor	Annette Culberson	Application Developer 4
2nd Successor	Brian Thompson	ES Application Developer 2

	Shivi Pawa	Mgr, Enterprise Computing
1st Successor	Anshul Singla	Systems Administrator 3
2nd Successor	Tim Schlicher	Systems Administrator 2

	Fidel Ramirez	Mgr, Enterprise Computing
1st Successor	Suzanne Caillouet	Application Developer 4
2nd Successor	Rick DiPersio	Application Developer 4
	Mark Rosanes	Mgr, Web Technology
1st Successor	Scott Elder	Developer, Web 3
2nd Successor	Jesus Lozano	Analyst, Systems 2
	Debbie Samuels	Mgr, Enterprise App Sec & Invs
1st Successor	Will Moon	Analyst 3, Enterprise IT Sec
2nd Successor	Jana Chvatal	Mgr, IT Sec Risk Mgmt & Comp
	James Schexneider	Mgr, Telecommunications
1st Successor	Brandon Stratton	ES Network Administrator 3
2nd Successor	Ana Spaunhorst	ES Network Administrator 2
	Muhammad Soonasra	Mgr, Computing Systems
1st Successor	Evan Clayson	ES Application Dev II
2nd Successor	Asim Naqvi	ES Application Dev II
	Bill Spindler	Dir, Business Svcs
1st Successor	Sonia Morales	Admnstr, Business, Department
2nd Successor	Rowena Castro	Admnstr, Business,Asst-Finance
	Diane Trippel	Dir, Web & Comm
1st Successor	Robert Birkline	Mgr, Web Technology
2nd Successor	Mark Rosanes	Mgr, Web Technology
	Danny Truong	Mgr, Asst, Classroom Tech
1st Successor	Randy Dupre	User Services Spec 2
2nd Successor	Leroy Mays	Dir, IT Customer Services
	Brian Walker	Mgr, Enterprise IT Security
1st Successor	Jana Chvatal	Mgr, IT Sec Risk Mgmt & Comp
2nd Successor	Debbie Samuels	Mgr, Enterprise App Sec & Invs
	Steve Webb	Dir, Enterprise Sys, Stu Admin
1st Successor	Leo Moreno	Mgr, Enterprise Computing
2nd Successor	Khalid Bhatti	Mgr, Enterprise Computing

3.2 Ride-Out Team

Name	Title	Ride Out Team Role
Aaron, Eli	Systems Administrator 2	Enterprise Systems Windows OS – Alternate
Adam, Arshad	ES Network Administrator 2	Network Planning & Development - Alternate
Beavers, Reggie	Mgr, Enterprise Computing	Enterprise Systems Linux OS - Primary
Bull, Vincent	Analyst, Systems 1	ITAC – Primary
Chambers, Charles	Mgr, Network Planning/Develop	Network Planning & Development - Primary
Chance, Ron	Mgr, ITAC	UIT Deputy Team Lead
Dickerson, Mary	Assistant VP, IT Security / CISO	UIT Senior Management
Dominguez, Michael	Telecom Tech 2	Network Operations Technician - Alternate
Ellis, George	Analyst, Systems 1	ITAC – Alternate
Fouty, Dennis	Associate VP, IT / CIO	UIT Senior Management
Frankfort, David	Systems Administrator 3	Enterprise Systems Infrastructure/VM - Primary
Gutierrez, Mary	ES Network Administrator 2	Network Operations Analyst - Alternate
Hotz, Randy	Lan Administrator	Network Operations Analyst - Alternate
Jares, Howard	Mgr, Enterprise Computing	Enterprise Systems Infrastructure/VM – Alternate
Johnson, David	Asst VP, UIT Tech Svcs & Support	UIT Incident Commander – Team Lead Primary
Jones, Sr., Lorenzo	Telecom Tech 3	Network Operations Technician – Primary
Kahanic, Mike	Analyst, Systems 2	ITAC – Alternate
Longoria, Sam	Mgr, Technology Facilities	UIT Facilities – Primary
Martin, Keith	Asst VP/VC, UIT Enterprise Sys	UIT Incident Commander – Team Lead Alternate UIT Facilities - Alternate
Nagji, Shabnam	Analyst, Systems 1	ITAC – Alternate
Plant, Robert	Analyst, Systems 1	ITAC – Primary
Schlicher, Tim	Systems Administrator 2	Enterprise Systems Windows OS – Primary
Smith, David	Analyst, Systems 1	ITAC – Alternate
Stewart, William	Analyst, Systems 1	ITAC – Primary
Truong-Vu, Quy	Analyst, Systems 1	ITAC – Alternate
Williams, Quinton	ES Network Administrator 2	Network Operations Analyst - Primary
Wilson, Curtis	User Services Spec 2	ITAC – Primary
Zhang, Tong	Systems Administrator 1	Enterprise Systems Linux OS - Alternate

3.3 UIT Incident Command Post

Location: University of Houston
Computing Center (Entrance 17), Room 216
4213 Elgin, Houston, Texas 77004
Primary Phone: 713.743.2700
IP Phone: 832.842.2700
Mobile Phone: 281.960.7718
Analog Phone: 713.747.0601
Briefing Conference Bridge: 866.557.8511 (Activated on management request)
E-Mail: ITAC@UH.edu or ITAC@Central.uh.edu
Web: www.uh.edu/itac

3.4 UH System Campus Contact Information

UH Main Number - 713.743.1000
UH Police
    Emergency - 911
    Non-Emergency - 713.743.3333
UH On Call - 713.743.2255

UH Emergency Operations Center - www.uh.edu/oem

UH Clear Lake:	281.283.7600, EOC – 281.283.2222
UH Clear Lake – Pearland:	281.212.1700
UH Downtown:	713.221.8800, EOC – 713.221.8065
UH Northwest:	832.842.5700
UH Sugarland:	281.275.3300
UH Victoria:	361.570.4848 or 877.970.4848, EOC – 361.570.4357
UH Victoria – Katy:	281.396.3700

3.5 Supplier/Partner Contact Information

Supplier / Partner	Contact	Number
Infrastructure (HVAC, Electrical)	Facilities Mgmt	713.743.4948
IT Misc. Supplies	Graybar	Shannon Risinger – 713.423.2406
Electrical Repairs	Karl Keilbach	713.743.5606 or 832.799.9834 (cell)
Computer room raised floors maintenance	Sealco	972.234.5567 Samantha Perkins: 281.587.1100 or 405.312.7859 (cell)
Debris Removal	Facilities Mgmt	713.743.4948
Disaster Recovery Specialists	Cotton	877.511.2962 or John Neiser 281.755.1041
Electrical Power Cables	PDU Cables	Jessop Krocak: 800.336.2801 or 952.767.8763
Emergency & remedial maintenance on ERP Matrix5000 UPS, UHV UPS, PGH 116A UPS and Phone Switch DC Power Plant	Unified Power	972.524.6554 Hal Cox – 281.352.6424
Emergency & Remedial maintenance on HVAC-DX unit in Victoria	Bud Griffin / Vertiv	Clark Cooper: 713.664.5462 Chuck Haluska: 713.666.2828
Emergency & Remedial Maintenance on UPS RX	Liebert - Vertiv	800.543.2378 Chris Caldera – 281.954.1049
ERB Eaton UPS's, PDU's & Stulz CRAC Units	LC Solutions Liebert – Vertiv	Jennifer Montano 281.296.1234 or 832.714.0751 for UPS's & PDU's Chuck Haluska: 713.666.2828 for CRAC Units
Fire Suppression Systems Trane Chillers	Johnson Control	Mark Ramos: 956.708.1498 Jason McCown: 409.284.1557 (For UHV only) Wade Raymond: 210.336.4183 (C); 210.402.6311 (O)
Offsite Media Storage	Iron Mountain	800-934-3453 Customer Number A10944
Spot Coolers	Scott Maynard	Phone: 713. 910.2222 / Fax: 713. 910.7050 Email: scott@iptsupply.com
System Consulting	H/P	800.334.5144
System Components	H/P	800.334.5144
Water Removal	Cotton	877.511.2962 or John Neiser: 281.755.1041
Window Shutters	Rolltex Shutters	Elena Lopez: 281.991.9200

Cotton has been contracted as the designated vendor to respond with both personnel and equipment in the event of emergencies or catastrophic events which may affect the university. Only the IT Facilities Leader and Successors may contact Cotton or Facilities Management on behalf of UIT. The Facilities Management call center can be reached at

713.743.4948. Contact information for Facilities Management Interim Directors is: Jerry Bogna (713.743.3628), Lilianna Simmonds (713.743.4099), Mike Wheeler (713.743.5719). The Central Plant may be contacted at 713.743.5791 or through the Facilities Management call center.

Appendix A: Communication Strategies

1. ITAC Network Outage Communication Plan

Purpose

The following Network outage procedures are intended to provide communication of unplanned outages to University Information Technology (UIT) infrastructure. The procedures apply to any unplanned outage to current Network infrastructure and architecture.

Communication Process for Service Disruptions

When a UIT service experiences an outage, slowdown, or problem of any kind, our goal is to return it to regular operation quickly and to reduce the inconvenience to our customers by providing clear, concise information to the people who are affected, regular updates about the status of the service, and notification when the problem is resolved.

Our current method for notifying customers is:

- ITAC Console which sends an email to the Incident Notification ListServ and posts the information on the ITAC website.
- Posting the information Via CMS to the UIT Dashboard, which posts the information to the UIT website.

Additional methods used for buildings with network outages:

- Contact the leadership of the units affected in the building(s) such as Building Coordinator, Information Security Officer (ISO) and Technology Manager.
- Have someone physically go to the building to post signs and contact the Building Coordinator.

Initiating the Communications Process for Unplanned Outages

When a UIT service is unexpectedly disrupted, the UIT Support Center is usually made aware of the service disruption by a customer, ITAC because of service monitoring or the UIT team responsible for the service being affected. An initial Incident notification is posted within 5 minutes of the identification of a service disruption. A more substantive incident notification is posted within 20 minutes of the initial notification. A resolution Incident notification is sent once services have been restored. Regular updates will be sent throughout the event.

Technical team members' responsibilities

ITAC Responsibilities

- Once a service disruption has been identified, ITAC will provide the following information:
  - Service impacted is disrupted (i.e. network; server; application; voicemail; etc.)
  - What is being done (i.e. engineers are investigating; hardware is being replaced, etc.)
  - Who is impacted (i.e. department; building(s); district(s), campus; all campuses; etc.)
  - When service is expected to be restored, if known
- Provide status updates regularly
- If the service disruption is impacting a large portion of the university community and/or is expected to last for an extended period of time, UIT senior management will be notified using established escalation procedures.
- When services have been restored, ITAC will conduct an incident analysis, document the findings, and provide the results to UIT senior management, UIT Security and UIT Support Center using the incident analysis report template.

UIT Support Center responsibilities:

- At the start of the disruption,
  - Notify ITAC, if they are not already aware
  - Gather information about the outage from ITAC and the customers
  - When necessary, gather more information from customers and provide to ITAC
  - If high call volume, update upfront message on the ACD system
  - If you haven't received an update within an hour contact ITAC
- When the issue is resolved,
  - Gather information about the resolution
  - Remove upfront message

2. Communication Channels for UIT Service Affecting Incidents

Service/ Communication Channel	Audience	Vulnerability	Notes
SendIt	UH faculty, staff, students	• Email service at UH is unavailable. • Hosted solution, therefore no access to monitor service availability.	• Could be used as a communication channel if Everbridge is down. • Can be used for creating adhoc lists using data from PeopleSoft. if Exchange services are down, this channel can be used to send to most students and faculty by using their destination email addresses; staff would be left out.
Everbridge **Email** **SMS** **Digital Signage** **Social Media**	Faculty, Staff, Students, Persons of Interest	• Hosted solution, therefore no access to monitor service availability. • All services are lost when Everbridge has a service interruption. • UH email service unavailable. • Inconsistent delivery • ROLM and/or VOIP telephony unavailable	• Can use Everbridge dynamic audience rules to send email and SMS, to employees in campus zones or building. • Can be used when email is down • Can be used when email and network services are unavailable.
UH Alerts Emergency Web Site	Automatically posts and timestamps UH Alert messages	Is hosted on Amazon Web Services Illinois data center. If that center goes down, then we lose the site.	Could be used as a 4th level failover for www.uh.edu if that service is unavailable.
Listserv email	Faculty, staff, students, external entities that are added to mailing lists	UH email service or network is unavailable; server disruptions	Listserv is the secondary academic continuity solution for UH (Primary is Blackboard). Lists are created for each course section and faculty have been educated via Education Innovation & Technology on how to use this service. http://www.uh.edu/infotech/services/e-comm/mailing-list/disaster-recovery/
Web	*.uh.edu visitors	UH network or switch instability not failing over properly to secondary data center	Failover for www.uh.edu is secondary data center, then Texas Tech. www.uh.edu could be used as a communication channel if Everbridge is unavailable.

3. External Communication

1. If the emergency is affecting the UH campus as a whole, IT Electronic Communications Center (E-Comm) will be activated by the University's Public Information Officer for emergency communications. The UH Alerts website alerts.uh.edu is used for emergency updates and inquiries.
2. The polling feature in Everbridge can be used in a recovery phase when UH leadership needs to understand the needs and status of its workforce and the student body.
3. UH Office of Emergency Management and University Marketing, Communication and Media Relations will create a message to distribute via the UH Alerts website and send the notification by email and/or SMS.

Appendix B: Tropical Weather Response Plan

UIT has pre-determined the following criteria and incident levels for responding to a Tropical Weather threat.

Scenario	Criteria	Level to Be Activated
Tropical Weather	• Threat is expected to occur within 96 hours.	5
	• Threat is expected to occur within 72 hours.	4
	• Threat is expected to occur within 48 hours.	3
	• Threat is expected to occur within 24 hours.	2
	• Threat is expected to occur within 12 hours.	1

Action Plan – Incident Threat Level Tasks

Level 5 Tasks

UIT Workgroup Leaders

All UIT Workgroup Leaders are responsible for completing the following tasks:

1. Review currently available resources and be prepared to cancel staff vacation plans as necessary to maintain appropriate incident response.
2. Verify order of succession (Section 3.1). If changes are required, notify ITAC.
3. Direct staff to review their contact information in PASS for accuracy.
4. Ensure staff have remote access capabilities to support the university from home if needed.

E-Communications

1. Ensure Everbridge system and data are ready to use.
2. Contact PIO, UHDPS and other emergency communicators.
3. Make sure data on Everbridge and SendIt is ready to use.

ITAC/IT Incident Command Post

1. Begin a mandatory monitoring schedule to remain updated with current information in regards to the threat.
2. Post status updates to the UIT ITAC website, www.uh.edu/itac.
3. Provide information to management in regards to the current threat in regular intervals.

UH Call Center

1. Double check agent access information (VPN, ACD Agent Desktop, Softphone, etc.) for remote agent group to ensure login IDs & passwords are updated.
2. Review remote call center training with remote agent group.

Web Technologies

1. Contact University Advancement.
2. Send mail to itweb@listserv.uh.edu communicating what our current level is to reinforce ITAC's messages.
3. Update the university web page as appropriate.

Level 4 Tasks

UIT Workgroup Leaders

All UIT Workgroup Leaders are responsible for completing the following tasks:

1. Review and secure all resources needed in preparation for the incident.
2. Develop Incident Action Plan for the incident and communicate plan to the Incident Command Post for inclusion into the IT Section IAP, which will be forwarded to the IC.
3. Check with customers regarding assistance with IT services and what expectations will be realized if the university was to close due to a weather event.
4. Verify/confirm Ride Out Team for this incident. Identify incident resources to remain on site to provide technical support to the IC, EOC, JIC, and ITICP or any other official designated EC as directed by the IC or ITICP. This should be the assigned ride out team.
5. Define unit coordinators, ride-out team members, and relief teams. The ITS–Incident Commander or designee will compile the list of IT personnel who are remaining on-campus in the ITICP facility, and supply this list to the UH Office of Emergency Management. A list of personnel returning after the incident to assist with assessment and restoration of IT services will also be compiled and forwarded to UH OEM. This list will be entered into the contact list of PIER and upon direction from the ITS-Incident Commander, notifications will be sent out to return to campus and check in at the IT-ICP as soon as you arrive on campus.

E-Communications

1. Update backup of ldap databases and listserv lists.
2. Verify Everbridge contact sync data is up-to-date.
3. Change email aliases to outside email address.
4. Work with ES to back up SharePoint data offsite.
5. Make backup of feed in case connections to UH network are broken.
6. Decide if this type of emergency requires emergency updates or if it requires the University to reach out to students, faculty and staff.
7. If emergency updates only, continue to use EOC.
8. If a poll is necessary, use the poll feature in Everbridge.
9. Update uh.edu/emergency as needed.
10. Monitor inquiries with UA as primary and E-Comm as secondary.
11. Emergency Response Team (ERT) begins responding to inquiries (hopefully UA has set this team up and they call them to respond to the emergency as part of their call tree).
12. Contact UHCC and give them prepared message to respond to incoming phone calls.

IT Availability Center/IT-Incident Command Post

1. Notify the IT Incident Commander and IT Incident Leaders of the current situation of incident.
2. Begin regular 12 hour updates posted to the IT PIER Web site and ITS Incident Commander and IT Incident Leaders.
3. Review ITS Emergency site for publishing, review and update contents.
4. Request approval to stand-up the full ITS PIER emergency site.
5. Verify ITS Emergency Web pages are updated with critical information.

IT Facilities

1. Provide appropriate supplies (plastic sheeting, duct tape, etc.) for loss prevention measures in IT departments.
2. Ensure all IT vehicles are fueled.

Enterprise Systems

1. Ensure all critical servers, data and databases have a current backup.

Network Planning and Design

1. Ensure all critical routers and switches have current configuration backups.

Procurement/Contract Administration

1. Review required emergency equipment inventory, and operational status. (See Appendix C for the required emergency equipment list.)
2. Coordinate with ITAC management the status of the inventory

Telecommunications

1. Ensure all critical switches have a current backup.
2. Ensure outside conference phone facilities are in place (Customer Services).
3. Confirm alternate means of communication for key personnel – Satellite phones, varied cell providers, etc. – (Customer Services).
4. Check with customers regarding assistance with IT services and what expectations will be realized if the university was to close due to a hurricane.
5. Verify parts availability, i.e. phone, switches, A/P's, cabling.
6. Coordinate with cabling contractors for their availability

Web Technologies

1. Prepare initial notice on home page (Raise hurricane flags).
2. Scrape uh.edu site and sync it to SDC site Back-up of all important data on servers including: Production MySQL, and ITI databases.
3. Back-up of all important data on servers including:
    - Production web root (/publish/http), registration data for CAM site, all open Remedy cases and ITI
4. Backup emergency listserv for courses
5. Update contact information in the SharePoint Employee Contact Information list.
6. Delegate communication roles to maintain business continuity
7. Ensure university web page is current

Level 3 Tasks

UIT Workgroup Leaders

All UIT Workgroup Leaders are responsible for completing the following tasks:

1. Notify ride-out and return team members to check the IT-Web site for instructions.
2. Provide Situation Report (SitRep) to ITICP regarding status of loss prevention efforts every two (2) hours until loss prevention effort is complete. SitRep can be made via the IT Emergency Website.

Academic Systems

1. Ensure all critical servers, data and databases have a current backup.
2. Coordinate with customers as to the expectation of classes during this incident

Architecture & Technical Services

1. Ensure all critical servers, data and databases have a current backup.

Business Services

1. Make necessary arrangements for food, water, and necessary supplies during and after the incident.
2. Secure at least two local hotel rooms for ride out team.

Classroom Technologies

1. Ensure and assist with moving backups to a secure offsite facility.

Desk Top Technologies

1. Ensure and assist with moving backups to a secure offsite facility.

E- Communications

1. Assign all portable devices to an employee to secure during storm.
2. Provide communication support for Everbridge and EOC site uh.edu/emergency.
3. Ensure Everbridge systems and data are ready to use
4. Make backup of feed in case connections to UH network are broken
5. Engage Emergency Communicators (make sure PIO does)...distribute roles and responsibilities and make sure they have login credentials

Enterprise Systems

1. Ensure and assist with moving backups to a secure offsite facility.
2. Notify the ITICP when backups have been completed and moved to offsite.

HPC

Check for successful backup of all HPC managed systems.

IT Availability Center/IT Incident Command Post

1. Minimum 1 ITICP employee required in ITAC.
2. ITICP will increase frequency of information updates to PIER ITS emergency website in regards to the current threat. Assist in any preparations as required.
3. Establish emergency contact numbers incase internet access is disabled to allow for posting to emergency web sites.
4. Check to see if deployment of Storm Shutters is required as outlined in Appendix E or by Management.

IT Facilities Management

1. Issue hand held two way radios to critical personnel.
2. Ensure provisions are in place for IT ride-out team.

Network Planning & Development

1. Plan for alternative phone system support

Student Systems

1. Ensure all critical servers, data and databases have a current backup.

Telecommunications

1. Plan for alternative phone system support
2. Ensure outside conference phone facilities are in place (Customer Services).
3. Vary the operational state of alternate means of communication for key personnel – Satellite phones, varied cell providers, etc. – (Customer Services).
4. Collaborate with ITAC/ITICP regarding incident preparedness and status communications being posted to the IT PIER site and the University Computing Site.
5. Ensure that all tech buggies are in operational state and gas up.
6. Distribute alternate means of communication to key personnel. Ensure instruction for proper use is provided (Customer Services).
7. Plan for alternative phone system support
8. Ensure that the PGH-10,116A, UCU and ERP have been secured, i.e. sand bags, portable and building generators and UPS's

UH Call Center

1. Prepare telephone emergency announcement/front-end recordings for 31000/32255 line
2. Plan for alternative phone system support
3. Assign all portable devices/equipment to ride-out/recovery IT staff to have remote access to support the university.
4. Make arrangements for ride-out/recovery team to temporarily relocate to a non-local facility to continue communication activities

Web Technologies

1. Update backups of important data on servers including:
    - Production MySQL databases.
    - Production web root (/publish/http).
    - Production databases.
    - All open Remedy cases.
    - Development MySQL databases.
    - Development web root.
2. Change email aliases to outside email address.
3. Begin evacuation of all critical documents and systems to secure room.
4. Assign all portable devices to an employee to secure during storm.
5. Provide support for websites

Level 2 Tasks

UIT Workgroup Leaders

All UIT Workgroup Leaders are responsible for completing the following tasks:

1. Continue SitRep regarding loss prevention as indicated in L3 if not complete.
2. Ensure support personnel, who will be riding out or Incident Action Team and supporting the IC, EOC, JIC, ITICP, and any other approved EC, check-in at ITICP and obtain credentials.
3. Verify ride-out team member(s) are in place.

E- Communications

1. Update backup of ldap databases and listserv lists.
2. Verify Everbridge contact sync data is up-to-date.
3. Change email aliases to outside email address.
4. Assign all portable devices to an employee to secure during storm.
5. Provide communication support for Everbridge and EOC site uh.edu/emergency.
6. Ensure PIER systems and data are ready to use.
7. Make backup of feed in case connections to UH network are broken.
8. Emergency Communicators begin responding to inquiries.

IT Availability Center/IT Incident Command Post

1. Minimum: 1 ITICP employees required in ITAC.
2. Update telephone emergency announcement recordings for the university switchboard x3.1000 and or One Call. If operators are not on campus ITAC will update the telephone emergency announcement recordings via an enabled Rolm phone located in ITAC when instructed.
3. Increase updates to ITS Branch Directors and Managers and send updates via Web posting, E-mail and Phone contact list as necessary before and during the incident.
4. Facilitate additional security requests from management as requested.
5. Initiate a conference bridge for use by ITS members during final preparations.
6. Five (5) hours prior to the incident, prior to nightfall, or before road closures, ITICP employees will make contact with and verify attendance of all emergency personnel. Designated Ride-out team members should be allowed to leave at **L4** activation to gather/prepare family or effects in preparation for the incident, but must return and check-in at or before the above-indicated conditions.
7. Report to UH OEM, before the incident, the list of authorized ride-out teams staying onsite for the duration of the incident, and their locations on campus.
8. Deploy UHS Data Center Storm Shutters as outlined in Appendix E or by management.

Telecommunications

1. Install voice/data emergency hardware/equipment or other related equipment required to remain operational during the incident (Technicians, Analysts, and Project Managers).
2. Update telephone emergency announcement recordings for the University Switchboard x3.1000. If operators are still in the building/on campus they will update the telephone emergency announcement recordings.

Web Technologies

1. Update backups of important data on servers including:
   - Production MySQL databases.
   - Production web root (/publish/http)
   - Production databases.
   - All open Remedy cases.
   - Development MySQL databases.
   - Development web root

UH Call Center

1. Activate telephone messaging as necessary
2. Dispatch ride-out/recovery team to temporary location

Level 1 Tasks

E-Communications

1. Create new message or use canned message if we have already created that scenario. UA creates the questions with E-Comm supporting them.
2. Send message via SMS
3. Monitor inquiries with UA as primary and E-Comm as secondary
4. Emergency Response Team begins responding to inquiries (hopefully UA has set this team up and they call them to respond to the emergency as part of their call tree)
5. E-Comm will export data daily, unless more frequent exports are needed
6. Will export: students, faculty, staff to excel
7. Will send (password protected) to DRT
8. DRT analyzes data and prepares reports for UH leadership

IT Availability Center/IT Incident Command Post

1. Minimum: 2 ITICP personnel required.
2. Monitor any available resources for up-to-date information on the incident.
3. Maintain current information on emergency website and with offsite/onsite Management, keeping them informed of conditions through Everbridge.
4. Visually inspect the CC Facility for internal damage during the incident.
5. Move to alternate planned evacuation point if necessary.

Telecommunications

1. Maintain voice/data emergency hardware/equipment and other communication equipment both established networking and installed at CSG. L4.1 to remain operational during the incident – (Technicians, Analysts, Project Managers).

Web Technologies

1. Assist JIC with updating web page and notifications

UH Call Center

1. Ride-out/recovery team continue communication activities throughout incident

Appendix C: UIT Emergency Resource List

Logistics and resources identified to support IT Incident Command Post. Number of personnel requiring support items will vary based on the incident and duration.

Items	Status
Rubber and Work Gloves Non Latex Gloves sizes (SM- 5bx, MD- 5bx, L – 10 box, XL- 5 box)	Variety in supply inventory To be ordered in box of 100 pair each
Face Masks	Face masks in supply inventory
Rubber Boots	Variety in supply inventory
Back Packs	To be ordered
Emergency Wind-up flashlights	In Stock
Flashlights – battery operated	Variety in supply inventory
Batteries	AAA – 50ea, AA – 100 ea., C – 50 ea., D- 100 ea. To be ordered
Tools	To be ordered
Braided Rope – 3/8 X 100 ft. 4 each	In Stock
Generators	Available through Facilities Management
Gasoline	Available through Facilities Management
Gasoline Cans	Available through Facilities Management
Extension Cords	Variety in supply inventory
Insect repellant small containers 300ea	To be ordered (Damaged by rodents when stored in Room 181)
Hoses – 5/8 X 100 ft. 4 each	In stock
Ice Coolers	In supply inventory
Ice	Available through Plant Ops
Water	Available per UH emergency plan

Items	Status
Toilet Paper	Facilities Management
Water Pumps	Facilities Management
Mops / Mop Buckets	Facilities Management
Wet/Dry Vacuums	Facilities Management
Brooms - Push type	Facilities Management
Plastic Coverings/Tarps	In supply inventory
Cleaning/Sanitization Products	To be ordered
First Aid Kits	In Stock
Walkie-Talkie / Hand Radios	Available through ITAC
Emergency Cell Phones / Pagers / Satellite Phones	Available through Communications Services (Sat phones to be reordered)
Face Towels 10 dz	To be ordered
Computers / Network Equipment	Available throughout IT
Inflatable Beds	In supplies inventory
Towels 5 dz	To be ordered
Extra –T- Shirts, light color/not white	10.Large, 10.X-Large, 30.2X Large To be ordered

Appendix D: Food During An Emergency

In the event members of the ride out team need meals, Dining Services may provide basic food, if it is possible for them to do so. Non-perishable food items will be stocked in the Computing Center by June 1st each year. Ride out team members with special dietary needs should include food in their ride-out team bag. UIT Business Services is responsible for coordinating the purchase of additional non-perishable food items and the delivery of hot meals prior to or after an event.

Appendix E: Storm Shutters for UHS Computing Center

Storm window shutters have been installed on all windows and doorways of the UHS Computing Center CC-596 to protect from damage by high wind projectiles, and any other threats to the building, such as a riot. When directed or if conditions warrant, ITAC personnel will deploy the storm shutters according to the procedures below. Life safety of personnel in the building is always first consideration.

1. Procedures for shutter deployment

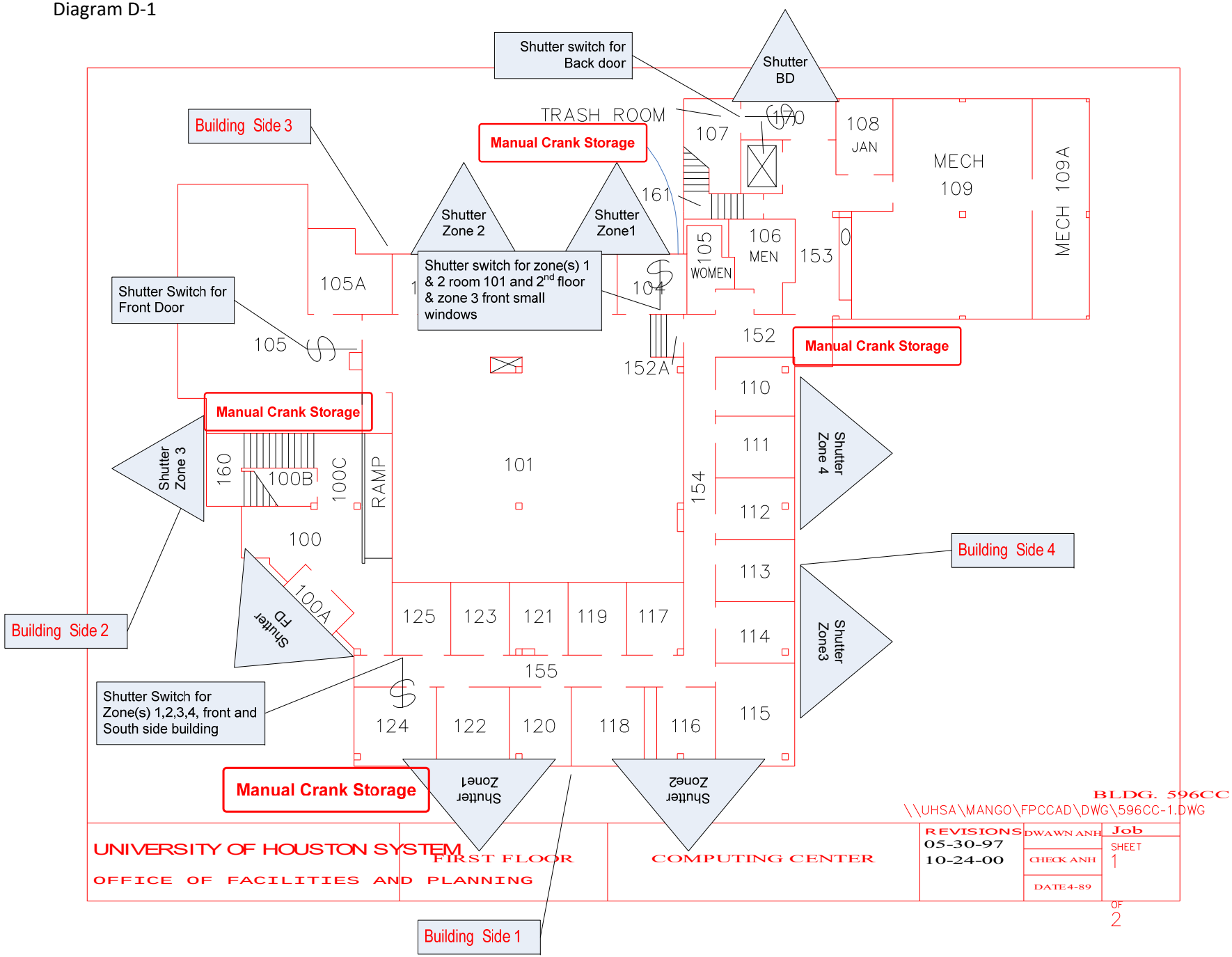
NOTE: When deploying the storm shutters until we are in a Level 1 or 2 conditions or directed differently by management, at least one personnel egression avenue (front or back door of center) will be kept open at all times.

1. Storm shutters can be deployed and retracted by either the remotes located in ITAC or by wall mounted controls located throughout the building. Manual cranks are also located throughout the building in the event there is a total power failure. Manual cranks are also located outside the building in controlled 911 boxes for use by emergency personnel in case emergency entrance is needed. (See diagram E-1 below).
2. Storm shutters will be deployed in a protective mode when:
   - Wind speeds reach or exceed a sustained speed of 45 mph or guests exceed 65 mph.
   - Hail larger than a quarter is being experienced.
   - Or any other threat to the building that may sustain damage to the windows is evident.
3. Storm shutters for room 101A can be controlled by either a remote control unit located in ITAC or by wall switch located on the wall within room 101A. (See diagram E-1 below for location of switches and window Zone #'s). To deploy the storm shutters for room 101A you will:
   a. Locate remote control marked for room 101A shutters (ITAC#3). Select zone 1 on the remote by depressing and release the button at the bottom of the control. Once depressed and released a LED should illuminate and flash this indicated you have selected Zone 1. Depress the button with the down arrow and the Room 101A; Zone 1 storm shutters will close protecting the windows. To open the shutters follow the same instructions above but depress the button with the up arrow.
   b. Wall switches are located in Room 101A (See diagram E-1 for locations) for building side 3 (back of building). Bottom set of controls are for Room 101A and the windows in the stair well on side 2 of the building. Zone 1= SE windows in Room 101A, Zone 2= NE windows in Room 101A, and Zone 3 = Windows in stair well East side of building. Wall controls work similar to remote controls. Depress button at bottom of switch to select zone, once zone is selected, depress either the down arrow or up arrow button to control the shutters.
   c. Controls for storm shutters for 2nd floor side 3(Rear of building) are also located in Room 101A just above the controls for the 1st floor. These controls operate just like the controls for room 101A controlling the storm shutters on the 2nd floor. There are only two (2) zones; Zone 1=2nd floor side 3 SE shutters, Zone 2=2nd floor side 3 NE shutters.
4. Storm shutters for windows in front and SW front side of UHS Data Center building. Front shutters are divided into four (4) zones. Zone1=Front windows, Zone 2= Second section of front windows, Zone 3=Front side windows, Zone 4=Front side windows second section. Control is operated in the same fashion as outlined above. By depressing the zone button you can

select any of the four zones to control. The Wall switch is located just inside the doorway to building area 100A. This switch controls the four (4) zone storm shutters for this first floor area. Manual emergency cranks are located throughout the area see diagram J-1 for more information.

5. Front and Rear doors: Each door has its own remote control and manual control. (Remember one door way must remain open at all times unless conditions prevail or instructed by management to secure) Remote Controls are located in ITAC for both front and rear doors. Manual switch for the rear door is located next to the rear door with up and down buttons. Shutters must be fully in the up position for the door to open. Emergency manual cranks are wall mounted next to the door. Front door wall switch is located in ITAC; Emergency manual crank is located in the front foyer.

Diagram D-1


Shutter switch for Back door
Shutter BD
Building Side 3
TRASH ROOM
Manual Crank Storage
107
170
108 JAN
MECH 109
MECH 109A
161
Shutter Zone 2
Shutter Zone1
105 WOMEN
106 MEN
153
Shutter Switch for Front Door
105A
Shutter switch for zone(s) 1 & 2 room 101 and 2nd floor & zone 3 front small windows
104
105
152
152A
Manual Crank Storage
110
Manual Crank Storage
111
Shutter Zone 3
160
100B
100C
RAMP
101
154
Shutter Zone 4
112
100
Building Side 4
113
Building Side 2
100A
Shutter FD
125
123
121
119
117
114
Shutter Zone3
155
Shutter Switch for Zone(s) 1,2,3,4, front and South side building
124
122
120
118
116
115
Manual Crank Storage
Shutter Zone1
Shutter Zone2
Building Side 1
BLDG. 596CC
\\UHSA\MANGO\FPCCAD\DWG\596CC-1.DWG
UNIVERSITY OF HOUSTON SYSTEM
OFFICE OF FACILITIES AND PLANNING
FIRST FLOOR
COMPUTING CENTER
REVISIONS
05-30-97
10-24-00
DWAWN ANH
CHECK ANH
DATE 4-89
Job
SHEET 1
OF 2

Appendix F: Computing Center Power Disruption Response Plan

UIT has pre-determined the following response plan to a Computing Center Power Disruption.

Scenario 1 - Computing Center on Generator Power

When utility power is interrupted or lost, the power will failover to the generator within 20 seconds, and an alarm will sound to notify ITAC that the generator has started. A generator failover will be assigned an impact of MEDIUM, and ITAC will take the following steps:

1. Establish a Technical Bridge.
    - The preset bridge is 713.743.6112, conference ID 4178349.
    - The bridge will remain open until the disruption event has been resolved.
2. Send out Technical Bridge notification. Prewritten notification located in PIER:
    - *Incident Action Plans > Computing Center > Power Disruption > On Generator*
    - Everbridge contact group *Tech Bridge – Computing Center Disruptions*
3. Send out incident notification. Prewritten notification located in PIER:
    - *Incident Action Plans > Computing Center > Power Disruption > On Generator*
    - Everbridge contact group *Tech Bridge – Computing Center Disruptions*
4. Provide additional communications as necessary using normal ITAC communication procedures.

Scenario 2 - Computing Center on UPS Power

If neither utility power nor generator power is available, power will be supplied solely through the UPS that provides 30 minutes of power to ensure proper shutdown of systems. Another audible alarm will sound to indicate UPS power only, and text messages will be sent to UIT senior management and a select group of SME's instructing them to call a pre-defined technical bridge. The UPS will continually announce the amount of battery time available via text messages.

A total power loss will be assigned an impact of HIGH, and ITAC/SME's will take the following steps:

1. SME's will execute ready/tested scripts to shutdown systems.
    - No approval needed.
    - See details in System Shutdown Priority section
2. ITAC will establish the Technical Bridge.
    - The preset bridge is 713.743.6112, conference ID 4178349.
    - The bridge will remain open until the disruption event has been resolved.
3. ITAC will send out Technical Bridge notification. Prewritten notification located in PIER:
    - *Incident Action Plans > Computing Center > Power Disruption > Total Power Loss*
    - Everbridge contact group *Tech Bridge – Computing Center Disruptions*
4. ITAC will send out incident notification. Prewritten notification located in PIER:
    - *Incident Action Plans > Computing Center > Power Disruption > Total Power Loss*
    - Everbridge contact group *Tech Bridge – Computing Center Disruptions*

System Shutdown Priority

Upon receipt of a text message that the Computing Center is on UPS power, the SME's will execute ready/tested scripts in the following areas to shut down the systems without any further approval.

Table 1: System Shutdown Priority

Priority	Task	Systems	When Performed	Order Performed within Systems	Time to Perform	Comments
1.1	Shutdown TSM Services	TSM, ProtecTier, Compellent 1	SME receipt of UPS text message		10 min	Shutdown the Talos 1/2 servers and Compellent1
1.2	Shutdown Storage Arrays	Compellent 2, 3, and P2000	SME receipt of UPS text message		10 min	
2.1	Shutdown Critical DB Servers	Oracle Prod RAC 1, 2, & 3; 5 Oracle GP Database Servers	Upon generator failure	Simultaneously	10 min	
2.2	Shutdown Critical Apps	Exchange Lync DC's		Simultaneously	10 min 2 min 2 min	Lync Dial Tone will remain Up
3	Shutdown VMs		After Critical Apps shutdown completed			

Table 2: System Shutdown Contact Information

Task	Manager	Primary SME Systems	Secondary SME
Shutdown TSM Services: TSM, ProtecTier, Compellent 1	Reggie Beavers	Jerry Raschke	Reggie Beavers
Shutdown Storage Arrays: Compellent 2, 3 and P2000	Howard Jares	Howard Jares	David Frankfort
Shutdown Critical DB Servers: Oracle Prod RAC 1, 2, & 3; 5 Oracle GP Database Servers	Jitender Kumar	DBA on call: http://www.uh.edu/infotech/services/computing/people-soft-admin/dba-on-call/	DBA on call: http://www.uh.edu/infotech/services/computing/people-soft-admin/dba-on-call/
Shutdown Critical Applications: Exchange, Lync, DC's	Shivi Pawa	Exchange & Lync : Anshul Singla DC's: Michael Keo	Exchange & Lync : Shivi Pawa & Tim Schlicher DC's: Anshul Singla
Shutdown Virtual Machines	Howard Jares	David Frankfort	Tilak Brahmbhatt

Appendix G: Recovery from Computing Center Damage

1. Assess Nature and Impact of Emergency

- **Within the first 2 hours** after notification, the UIT Recovery Manager will:
  1. Obtain initial damage assessment report from assessment team(s)
  2. Develop Action Plan (determine if recovery is feasible in place, at the affected location, or if the alternative site must be mobilized as the back-up)
  3. Provide briefings to staff on damage assessment and the Operation Period Action Plan.
  4. Coordinate with team managers to notify the vendors that have agreements to initiate replacements equipment shipments to the affected site, if possible, or the alternate site, as circumstances dictate.
- **Within 3 hours**, the UIT Recovery Manager will:
  1. Coordinate with Team Managers to ensure maintenance contact with vendors to alert them of the situation and the anticipated Action Plan for equipment replacement.
  2. Contact off-site storage provider as needed.
  3. Obtain Situation Reports from operations, applications and DBA team to develop Operation Period Action Plan.
  4. Obtain Situation Reports from the infrastructure and telecommunications managers to develop Operation Period Action Plan for site readiness for replacement equipment and rerouting of telecommunications links as needed.
- **Within 4 hours**, the UIT Recovery Manager will:
  1. Provide management with an updated Situation Report including an estimated recovery schedule.
  2. Meet with Business Services to arrange for travel, if needed, and any other extra expenses necessary to deal with the event.
  3. Instruct operations, applications and DBA teams to proceed with retrieval/recovery of backup tapes.
  4. Instruct the infrastructure recovery team to coordinate restoration at the alternate site as appropriate.

2. Establish an Action Plan for Interim Operations

- **Within 12 hours**, if replacement equipment is not yet available, the UIT Recovery Manager, in concert with operations, telecommunications, applications and DBA recovery managers will:

  1. Initiate a new Operation Period Action Plan to show alternative schedule to share the resources of the remaining site to support operational requirements.
  2. Hold Operation Period Action Plan briefings with teams.
  3. Test and verify communications capabilities.

- **Within 24 hours, the UIT Recovery Manager will**:
  1. Provide Situation Report to management every 24 hr. Operational Period.
  2. Create new Operational Period Action Plan and hold briefings with teams.
  3. Post alternate/interim production schedules on Everbridge.

3. Damage Assessment Team

Primary: UIT Incident Commander
Alternate: Manager - IT Facilities & Environmental

The DAMAGE ASSESSMENT TEAM Manager's primary responsibilities are:

1) Provide Situation Report to UIT Recovery Manager to assist with the decision of the recovery site.
2) Provide Situation Report of salvageable hardware components.

Based on Situation Report the Recovery Management Team will acquire replacement equipment for the recovery. Additional duties include:

1) Focus on recovery team's needs, identify and account for all personnel.
2) The UH Department of Public Safety will be notified to assist if evacuation is required.
3) Identify the extent of damage to the facility and evaluate in one of the following levels of damage:
    a. Destroyed
    b. Minor Damage
    c. Major Damage
    d. Affected but Habitable
    e. Inaccessible
4) Identify the extent of damage to major hardware components(servers, network, HVAC, fire system, PDU's, UPS's and power)
5) Identify salvageable hardware components(servers, network, HVAC, fire system, PDU's, UPS's and power)
6) Provide Situation Reports to the Recovery Manager

4. Recovery Team

The UIT Recovery Manager will:

- Execute the Service Continuity Plan based on declaration from the UH-CIO
- Conduct the recovery operation activation briefing(s)
- Establish and maintain the Recovery Action Plan for the Operational Period(s). Normal duration of an Operational Period is 24 hours, unless designated otherwise
- Coordinate and provide Situation Reports at the end of each Operational Period with/to executive management and posting on Everbridge throughout the recovery operation
- Manage all recovery operations
- Select the Recovery Site and direct activities to activate the site
- Direct notification of vendors found in Section 7.12
- Have E-Communications Team report to the JIC

Initiate the recovery of the systems by the various teams specified below:

- Applications Recovery Team
- Operations Recovery Team
- Operating Systems Recovery Team
- DBA Recovery Team
- Telecommunications Recovery Team (Data & Voice)
- Infrastructure Recovery Team
- Damage Assessment Team
- Disaster Site Recovery Team
- Recovery Site Team
- Lodging and Transportation Support Team

- Internet Support Team (Web Technologies)
- IT Technology Support Services Team

5. Re-establish a Full Production Schedule

Upon delivery of replacement equipment, Operations, Telecommunications, Applications and DBAs teams will:

- Develop Action Plan for re-establishment of full production
- Hold briefings with teams regarding new Action Plan
- Install and test all applications software on replacement hardware
- Restore data on replacement equipment
- Monitor restored operations to verify continuity, data integrity, etc.
- Resume full production schedules
- Provide Situation Report to Recovery Manager on re-establishment of full production

Within 3 to 4 days the UIT Recovery Manager will:

- Provide Situation Report to management every 2 hr. Operational Period.
- Hold briefings with teams and management regarding the resumption of full production schedules
- Maintain the disaster recovery logs documenting restoration of operations

6. Restore Operations

If the above steps resulted in restoration of operations at the affected site:

- Re-assess status of equipment (necessity of bidding permanent replacement equipment)
- Re-assess any other physical/facilities requirements before considering restoration complete
- Confirm status of hardware/software with vendors/service providers

If the above steps resulted in restoration of operations at the alternative site:

- Work with Facilities Management and other groups to restore original site
- Work with purchasing and other groups to purchase permanent replacement equipment
- Install permanent replacement hardware
- Transport backup tapes to restored site
- Reinstall all operating systems, applications software, data, etc.
- Test and verify all systems are operational
- Re-route and test communications to restored site
- Announce restoration and re-scheduling of operations from restored site
- Resume all production operations, and then recover other environments such as test and dev.

7. Recovery Site

If an event has disabled or will disable, partially or completely, the University UHS Data Center and/or the communication network for a period greater than 3 days, ERP building 3 has been identified as the recovery site location. This site contains sufficient floor space for the operation of an equivalent configuration, but may require the installation of power and HVAC before computing equipment can be installed.

To activate ERP as the recovery site, computer hardware must be procured from the university's hardware vendors after a disaster has been declared. Agreements have been secured from the various vendors to supply needed equipment in the event of a disaster. These agreements are located in the ES Operating System manager's office. The PeopleSoft platforms are all standard commercially available equipment.

Recovery Facility

UH Technology Bridge
Building 3, 2nd floor, Room 244
5000 Gulf Freeway
Houston, Texas 77204

Secondary Data Center

University of Houston – Victoria
3007 Ben Wilson Room 204b
Victoria, TX 77901
(361) 570.4848 – main switch board

8. Establish Recovery Command Center

The Recovery Center's location will be determined by the magnitude of the event. The General Services Business (GEN) building will be used if available, if not the Recovery Manager will determine the location.

Primary Recovery Command Center
General Services Building
4211 Elgin St.
Room 111

Houston, Texas 77204

Alternate Site 1
Leroy and Lucile Melcher Center for Public Broadcasting
4343 Elgin St.
Houston, Texas 77204

Alternate Site 2
UH Technology Bridge
5000 Gulf Freeway
Building 3, Room 145
Houston, Texas 77204

9. Lessons Learned Review

Within 48 hours after stand-down a Lessons Learned Review will be conducted. The Manager, IT Security Compliance will schedule and conduct a Lessons Learned Review of the Incident. A lessons learned review (LLR) is a structured review or de-brief process for analyzing *what* happened, *why* it happened, and *how* it can be done better, by the participants and those responsible for the incident.

- A LLR is distinct from a de-brief in that it begins with a clear comparison of intended vs. actual results achieved.
- A LLR is distinct from a post-mortem in its tight focus on participant's own action - learning from the review is taken forward by the participants.

Within 3 business days following the Lessons Learned Review, ITSC will publish the findings, recommendations and action items drawn from the participants of the incident and LLR.

Revision Log

Date of Change	Revision	Made By	Description
5/24/2017	4.9	J.Chvatal	• Updated Approval and Implementation with correct names and titles • Section 1.2 – added MAPP 06.01.02 • Section 3.1 – updated information • Section 3.2 – updated information • Appendix A: Communication Strategies – Updated with current practices
6/21/2017	4.10	J. Chvatal	• Updated PIER with Everbridge • Section 3.1 – updated information
8/24/2017	4.11	J. Chvatal	• Section 3.1 –updated with new succession information • Section 3.2 – removed Virtual ride out team members • Section 3.3 – updated Briefing Conference Bridge number • Removed references to www.uh.edu/checkin
9/4/2018	4.12	J. Chvatal	• Section 1.3 – added activities • Section 2.4 (B) and (C) – updated lists • Section 2.4 (D) – added additional items • Section 3.1 – updated with new succession information • Section 3.2 – updated with new ride out team member information • Section 3.3 – removed emergency radio frequency • Appendix A – updated with current process