



# Continuity of Operations Plan (COOP)

**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**

Associate Vice Chancellor, UHS  
Associate Vice President, UH  
Chief Information Officer, UHS/UH

\_\_\_\_\_  
Date

\_\_\_\_\_  
**Mary Dickerson**

Assistant Vice Chancellor, UHS IT Security  
Assistant Vice President, UH IT Security  
Chief Information Security Officer, UHS/UH

\_\_\_\_\_  
Date

\_\_\_\_\_  
**David Johnson**

Assistant Vice President, UIT Technology Services and Support

\_\_\_\_\_  
Date

\_\_\_\_\_  
**Keith Martin**

Assistant Vice Chancellor, UHS Enterprise Systems  
Assistant Vice President, UH Enterprise Systems

\_\_\_\_\_  
Date

## Table of Contents

<b>SECTION 1: PLAN OVERVIEW .....</b>	<b>5</b>
1.1 Purpose.....	5
1.2 Alignment with UH Emergency Management Plan.....	5
1.3 Annual Preparedness Activities .....	5
1.4 Testing the Plan.....	6
1.5 Business Impact Analysis.....	7
1.6 Impact Assessment of Major UIT Provided Services.....	9
<b>SECTION 2: EMERGENCY DECLARATION AND RESPONSE .....</b>	<b>11</b>
2.1 Authority to Declare an Emergency.....	11
2.2 Criteria for Declaring an Emergency .....	11
2.3 Pre-Determined Criteria and Incident Levels.....	11
2.4 Emergency Response and Assessment .....	12
2.5 Travel to Campus.....	14
<b>SECTION 3: PERSONNEL AND CONTACT INFORMATION .....</b>	<b>15</b>
3.1 UIT Order of Succession.....	15
3.2 UIT Ride Out Team Assignments .....	19
3.3 UIT Incident Command Post.....	19
3.4 UH System Campus Contact Information .....	20
3.5 Supplier/Partner Contact Information.....	21
<b>APPENDIX A: COMMUNICATION STRATEGIES .....</b>	<b>22</b>
1. ITAC Network Outage Communication Plan.....	22
2. Communication Channels for UIT Service Affecting Incidents.....	24
3. External Communication .....	25
<b>APPENDIX B: TROPICAL WEATHER RESPONSE PLAN .....</b>	<b>26</b>
Action Plan – Incident Threat Level Tasks.....	26
<b>APPENDIX C: UIT EMERGENCY RESOURCE LIST .....</b>	<b>33</b>
<b>APPENDIX D: FOOD DURING AN EMERGENCY .....</b>	<b>34</b>
<b>APPENDIX E: STORM SHUTTERS FOR UHS COMPUTING CENTER .....</b>	<b>34</b>

**1. Procedures for shutter deployment ..... 34**

**APPENDIX F: COMPUTING CENTER POWER DISRUPTION RESPONSE PLAN ..... 37**

1. Computing Center on Generator Power ..... 37

2. Computing Center on UPS Power ..... 37

3. System Shutdown Priority ..... 38

**APPENDIX G: RECOVERY FROM COMPUTING CENTER DAMAGE ..... 39**

1. Assess Nature and Impact of Emergency ..... 39

2. Establish an Action Plan for Interim Operations ..... 39

3. Damage Assessment Team ..... 39

4. Recovery Team ..... 40

5. Re-establish a Full Production Schedule ..... 41

6. Restore Operations..... 41

7. Recovery Site ..... 41

8. Establish Recovery Command Center ..... 42

9. Lessons Learned Review ..... 42

**REVISION LOG ..... 44**

## 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 1<sup>st</sup> 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](http://www.uh.edu/workingoffcampus).
- UIT Ride Out Team 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 managers will review all response plans in the appendices for accuracy and completeness for their workgroups.
- The UIT Continuity plan will be reviewed to ensure it is up-to-date, tested and posted to the ITAC website at [www.uh.edu/itac](http://www.uh.edu/itac).

## 1.4 Testing the Plan

UIT 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, 2017.**

### Test Exercise Procedures:

1. UIT Security will be responsible for coordinating the type of exercise and testing procedure.
2. UIT managers will execute the procedures noted in the COOP during the exercise.
3. UIT Security will coordinate a test exercise at least once a year, which could be unannounced.
4. UIT Security will conduct an After Action Review of the exercise within 48 hours of completion of the exercise.
5. 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 names, phone numbers, addresses and responsibilities. Similarly, system changes must be promptly reflected in the contingency plan. The Manager, IT Security Risk Management and Compliance will rely on the other 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](http://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 <b>Space and Facilities</b> Are Damaged or Unavailable				2. Critical <b>Equipment</b> 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	IT Security Services	2	3	1	6	2	2	1	4

Functional Area	Business Functions and Processes  (People, Property, Processes) Descriptions	3. Centrally Provided <b>Power</b> Unavailable				4. <b>Communications</b> (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	IT Security Services	2	3	1	6	2	1	1	2

(continued on page 8)

University of Houston

University Information Technology, Continuity of Operations Plan (COOP)

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	IT 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	IT Security Services	2	3	1	6	3	2	1	6

**1.6 Impact Assessment of Major UIT Provided Services**

*(May 2016 - Currently under review by UIT Senior Management)*

No.	Business Activities	Business Owner	Impact <sup>1</sup> (High=1)	Probability (High=1)	Rank (Impact * Prob)
<b>CRITICAL CORE SERVICES</b>					
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
<b>CRITICAL INFORMATION RESOURCES</b>					
1	UH/UHV Blackboard	Jeff Morgan	2	2	4
2	UH.edu Web Farm	David Johnson	2	2	4
3	Data Warehouse		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	Mike Glisson	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	Cooper	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			
	FAMIS				

*(Continued on page 10)*

<sup>1</sup> 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
6	Intranet	Charles Chambers	2	3	6
IT SECURITY CRITICAL INFORMATION RESOURCES					
1	SSL Certificates	Brian Walker	2	2	4
2	Intrusion Detection	Brian Walker	2	2	4
3	2 Factor Authentication Administration	Brian Walker	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 Levels

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

Scenario	Criteria	Appendix B. Incident Response
<b>Tropical Weather</b>	• Threat is expected to occur within 96 hours.	Level 5
	• Threat is expected to occur within 72 hours.	Level 4
	• Threat is expected to occur within 48 hours.	Level 3
	• Threat is expected to occur within 24 hours.	Level 2
	• Threat is expected to occur within 12 hours.	Level 1

Scenario	Criteria	Appendix F. Incident Response
<b>Computing Center on <u>Generator</u> Power</b>	<ul style="list-style-type: none"> <li>• Utility power lost</li> <li>• Failover to generator has occurred successfully</li> </ul>	Scenario 1
<b>Computing Center on <u>UPS</u> Power</b>	<ul style="list-style-type: none"> <li>• Utility and generator power lost</li> <li>• Power supplied solely by UPS</li> </ul>	Scenario 2

## 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 that UIT has pre-developed a response scenario for, the following steps should be incorporated into the specific response scenario 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](http://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 is a predefined trigger (such as a Tropical Weather Event or Pandemic), UIT managers should **complete** the appropriate level tasks as outlined in the appropriate Appendix for the incident.

### 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](mailto: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 email
- 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 (CC - 596)
  - General Services Building (GEN - 585)
  - Energy Research Park, Building 3 (ERP3 – 403)
  - MD Anderson Library Basement (L – 509)
  - Student Service Center 1 (SSC – 524)
  - Ezekiel W. Cullen (E – 516)
- **Determine** the impact the incident has on the UIT critical infrastructure areas:
  - Computing Center (CC - 596)
  - Cullen College of Engineering 2 (D3 – 581), room E125
  - Fred J. Heyne (H – 534), room 119
  - Philip Guthrie Hoffman Hall (PGH – 547), rooms 10, 116, & 116A
  - TDECU Stadium (STAD)
  - University of Houston Science Center (HSC – 593), 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. At all times accountability of personnel must be maintained during any incident. In the event of a university-declared incident that impacts physical security to the campus, UIT will utilize the check-in Kiosk located in the front lobby of the UHS Computing Center for accountability recording of ride-out

personnel, recovery personnel or any UIT personnel on campus. If the Kiosk is not operational or available, the IT Incident Command Post will establish and maintain a manual accountability log of personnel for the incident.

2. IT-ICP will be responsible for reporting this accountability information forward to the campus accountability center throughout the incident. This responsibility includes the initial report and any status changes, (people leaving or returning, or new personnel arriving on campus) that may take place. Currently the campus accountability center will be located in the UHPD dispatch center. It is imperative that this information be accurate, up-to-date, and reported to UHPD dispatch in a timely manner. This is a life safety issue which is top priority.

## 2.5 Preparedness Activity Tracking

For events with pre-determined preparedness activities (such as Tropical Weather or Computing Center Power Outage), employees with assigned tasks should contact ITAC to report the completion of those tasks.

## 2.6 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 UHDPDS 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](http://www.txdot.gov/travel/road_conditions.htm). Upon receipt of information that would make travel hazardous, ITAC will work with UHDPDS 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 University Executive Management.
2. Only the University President will determine if campus operations are to be suspended. If they are to be suspended, the remainder of the UH Emergency Management Team, which includes the CIO, will be notified by UHPD and or University Communications.
3. Upon notification that the campus operations have been suspended, UIT personnel should monitor the UH Emergency Operations Center website at [alerts.uh.edu](http://alerts.uh.edu).
4. IT personnel may be asked by IT 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.
5. The ITAC shift will initiate steps to 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 the IT Staff, UH Emergency Operations Center (if stood up), Facilities Management Command Post (if stood up) and IT Incident Response Team members.
6. Once conditions have stabilized, and all hazards have been mitigated, and the President has reopened the campus, 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
<b>1st Successor</b>	David Johnson	Asst VP, UIT Tech Svcs & Suprt
<b>2nd Successor</b>	Mary Dickerson	Asst VP/VC, IT Security / CISO
	Mary Dickerson	Asst VP/VC, IT Security, CISO
<b>1st Successor</b>	Jana Chvatal	Mgr, IT Sec Risk Mgmt & Comp
<b>2nd Successor</b>	Debbie Samuels	Mgr, Enterprise App Sec & Invs
	David Johnson	Asst VP, UIT Tech Svcs & Suprt
<b>1st Successor</b>	Diane Trippel	Dir, Web & Comm
<b>2nd Successor</b>	Leroy Mays	Dir, IT Customer Services
	Keith Martin	Asst VP/VC, Enterprise Systems
<b>1st Successor</b>	Haseen Mazhar	Exec Dir, Enterprise Systems, Academic
<b>2nd Successor</b>	Charles Chambers	Mgr, Network Planning/Develop

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

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

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

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

**3.2 UIT Ride Out Team Assignments**

Name	Title	Ride Out Team Role
Bounds, Rocky	Systems Analyst 1	ITAC – Alternate
Bull, Vincent	Systems Analyst 1	ITAC – Alternate
Castillo, Matthew	Administrator, UH Web	Web Technologies
Chambers, Charles	Mgr, Network Planning/Develop	Network Planning & Development
Chance, Ron	Mgr, ITAC	ITAC – Primary
Dickerson, Mary	Assistant VP, IT Security / CISO	UH Emergency Operations Center
Ellis, George	Systems Analyst 1	ITAC – Alternate
Frankfort, David	Systems Administrator 3	Enterprise Systems - Window Systems SME
Johnson, David	Assistant VP, Tech Svcs & Support	UIT Incident Commander – Primary
Jones, Sr., Lorenzo	Telecom Tech 3	Network Operations SME
Kahanic, Mike	Systems Analyst 2	ITAC - Alternate
Longoria, Sam	Mgr, Technology Facilities	UIT Facilities
Martin, Keith	Assistant VP, Enterprise Systems	UIT Incident Commander – Secondary
Nagji, Shabnam	Systems Analyst 1	ITAC - Primary
Plant, Robert	Systems Analyst 1	ITAC - Primary
Schlicher, Tim	Systems Administrator 2	Enterprise Systems - Non-Window Systems SME
Smith, David	Systems Analyst 1	ITAC – Alternate
Stewart, William	User Services Specialist 2	ITAC – Alternate
Truong-Vu, Quy	Systems Analyst 1	ITAC – Alternate
Williams, Quinton	Analyst, Telecom 2	Network Operations SME

**3.3 UIT Incident Command Post**

Location: University of Houston  
 Computing Center (Building 596, 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](http://www.uh.edu/itac)

Emergency Radio  
 Frequency: 452.20000 and 457.20000

### 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](http://www.uh.edu/oem)

UH Clear Lake: 281.283.7600, EOC – 281.283.2222

UH Downtown: 713.221.8800, EOC – 713.221.8065

UH Northwest: 832.842.5700

UH Sugarland/Cinco Ranch: 281.275.3300

UH Victoria: 361.570.4848 or 877.970.4848, EOC – 361.570.4357

### 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
Computer room raised floors maintenance	Sealco	972.234.5567
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 and Associates	713.664.5462
Emergency & Remedial Maintenance on UPS RX	Liebert	800.543.2378 Chris Caldera – 281.954.1049
Fire Suppression Systems	Simplex Grinnell	Chad Stein: 281.814.4645 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
Spot Coolers	Scott Maynard	Phone: 713. 910.2222 / Fax: 713. 910.7050 Email: <a href="mailto:scott@iptsupply.com">scott@iptsupply.com</a>
System Consulting	H/P	800.334.5144
System Components	H/P	800.334.5144
TDECU Stadium Eaton UPS & CRAC Unit Emergency & Remedial Management	Evolve	832.375.0099
Water Removal	Facilities Mgmt	713.743.4948
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 Incident notification is posted within 5 minutes of the start of a service disruption and a resolution Incident notification is sent when service has been restored. Regular updates will be sent throughout the event.

#### Technical team members' responsibilities

##### ITAC Responsibilities

- At the start of the disruption, 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); campus; all campuses; etc.)
  - When service is expected to be restored, if known
- Provide status updates regularly
- When the issue is resolved, provide the UIT Support Center the following information:
  - Description of the problem and how it was fixed
  - Who was impacted (i.e. department, building(s), campus, all campuses, etc.)
  - If additional work will be done, explanation of when and the impact (i.e. weekend maintenance to replace a part, etc.)
- If the outage is impacting the entire university and/or is expected to last for an extended period of time, escalate to appropriate UIT management.

**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**

<b>RightNow</b>	UHS faculty, staff, students	<ul style="list-style-type: none"> <li>Email service at UH is unavailable.</li> <li>Hosted solution, therefore no access to monitor service availability.</li> </ul>	<ul style="list-style-type: none"> <li>Could be used as a communication channel if Everbridge is down.</li> <li>Also use RightNow for creating adhoc lists using data from PeopleSoft: if Exchange services are down, we can use this channel to send to most students and faculty by using their destination email addresses; staff would be left out.</li> </ul>
<b>Everbridge</b>  <b>Email</b>  <b>SMS</b>  <b>Digital Signage</b>  <b>Social Media</b>	Faculty, Staff, Students, Persons of Interest	<ul style="list-style-type: none"> <li>Hosted solution, therefore no access to monitor service availability.</li> <li>All services are lost when Everbridge has a service interruption.</li> <li>UH email service unavailable.</li> <li>Inconsistent delivery</li> <li>ROLM and/or VOIP telephony unavailable</li> </ul>	<ul style="list-style-type: none"> <li>Can use Everbridge dynamic audience rules to send email and SMS, to persons in campus zones or building.</li> <li>Can be used when email is down</li> <li>Can be used when email and network services are unavailable.</li> </ul>
<b>UH Alerts Emergency Web Site</b>	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 4 <sup>th</sup> level failover for <a href="http://www.uh.edu">www.uh.edu</a> if that service is unavailable.
<b>Listserv email</b>	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 ETO on how to use this service.
<b>Web</b>	*.uh.edu visitors	UH network or switch instability not failing over properly to secondary data center	Failover for <a href="http://www.uh.edu">www.uh.edu</a> is secondary data center, then Texas Tech. <a href="http://www.uh.edu">www.uh.edu</a> 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 <http://uh.edu/emergency> is used for emergency updates and inquiries.
2. We are able to use the polling feature in Everbridge in a recovery phase when UH leadership needs to understand the needs and status of its workforce and the student body.
3. UHDPS and University Advancement will create a message to distribute via the EOC web site 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. Verify staff access to Emergency Email. All staff members should log on to the Emergency Email system at <https://mail.emergency.uh.edu> using their CougarNet ID and password.
4. Direct staff to review their contact information in PASS for accuracy.
5. 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 RightNow is ready to use.

##### ITAC/IT Incident Command Post

1. Begin a mandatory monitoring schedule to become and remain updated with current information in regards to the threat.
2. Post status updates to the UIT ITAC website, [www.uh.edu/itac](http://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](mailto:itweb@listserv.uh.edu) communicating what our current level is to reinforce ITAC's messages.
3. Update the universities 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 tropical storm or hurricane.
4. Back up important documents from staff workstations to media that can be taken to an off-site location (CDs, DVDs, and external hard drives).
5. 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.
6. 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 UHPD dispatch. A list of personnel returning after the incident to assist with assessment and restoration of IT services will also be compiled and forwarded to UHPD-dispatch. 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 ITICP 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](http://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. Obtain 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 the 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:
  - o 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. Notify Marc Mullen, VP Customer Support PIER Systems of activation of Emergency sites. (360)756.8080 or (360) 303 1527. 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:
  - o Production MySQL databases.
  - o Production web root (/publish/http).
  - o Production databases.
  - o All open Remedy cases.
  - o Development MySQL databases.
  - o 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 Pier 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. The bridge information will be published on the PIER ITICC emergency Web site.
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 Police through PIER, 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. When Operators are not in the building/off campus, ITAC will update the telephone emergency announcement recordings via an enabled Rolm phone located in ITAC.

#### Web Technologies

1. Update backups of important data on servers including:
  - o Production MySQL databases.
  - o 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 PIER.
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 repellent 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

Eating Utensils (plates, cups, knives forks, etc.)	To be ordered
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 (Damaged by rodents when stored in Room 181)
First Aid Kits	To be ordered (Damaged by rodents when stored in Room 181)
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 food supplies, University Dining Services will provide basic food. Ride out team members with special dietary needs should include food in their ride-out team bag.

## 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

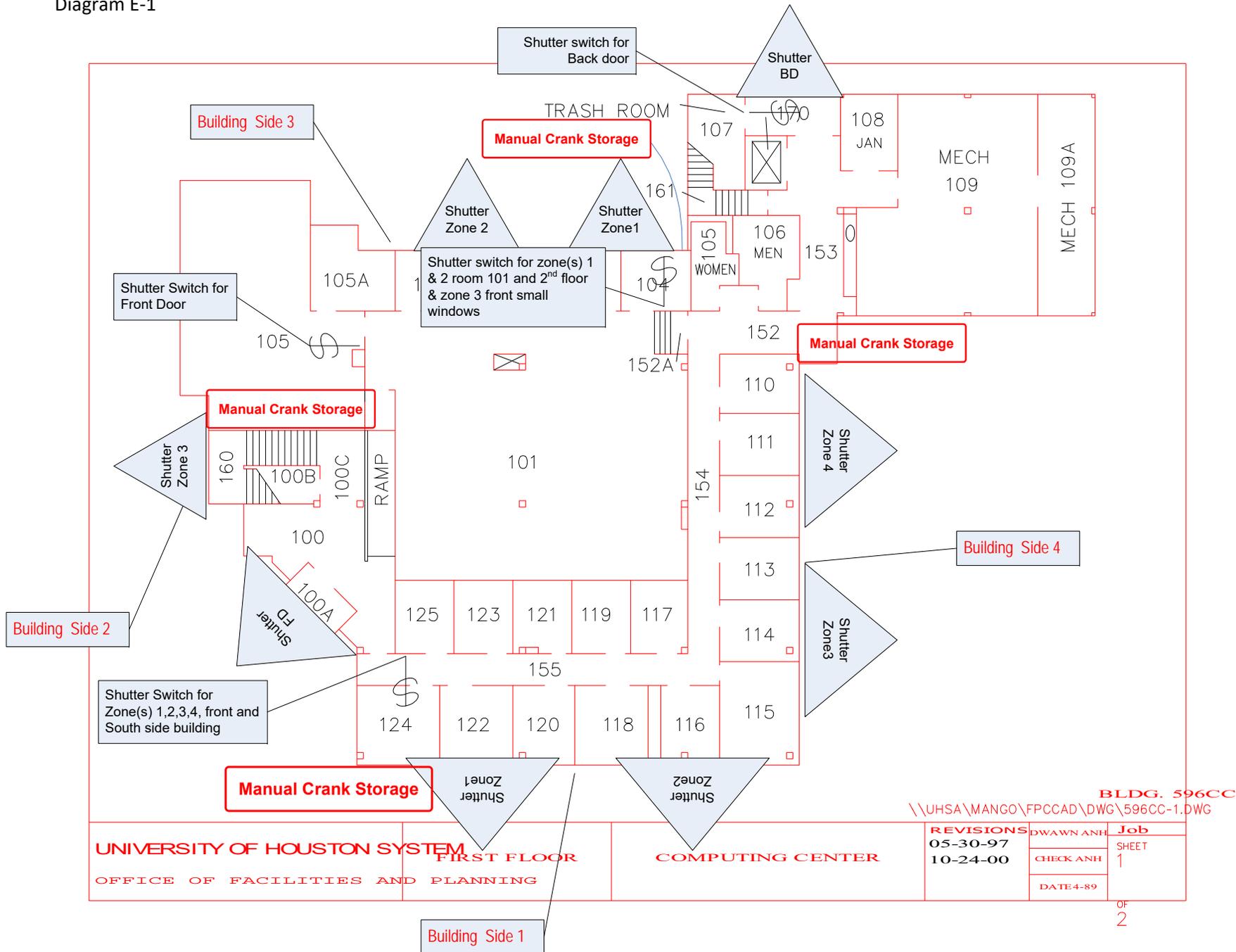
**NOTE: When deploying the storm shutters until we are in a Level 1 or 2 conditions or directed differently by management, at least one personnel egression avenue (front or back door of center) will be kept open at all times.**

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 gusts 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 2<sup>nd</sup> floor side 3(Rear of building) are also located in Room 101A just above the controls for the 1<sup>st</sup> floor. These controls operate just like the controls for room 101A controlling the storm shutters on the 2<sup>nd</sup> floor. There are only two (2) zones; Zone 1=2<sup>nd</sup> floor side 3 SE shutters, Zone 2=2<sup>nd</sup> 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 E-1



UNIVERSITY OF HOUSTON SYSTEM  
OFFICE OF FACILITIES AND PLANNING

FIRST FLOOR COMPUTING CENTER

REVISIONS	DRAWN ANH	Job
05-30-97		SHEET
10-24-00	CHECK ANH	1
	DATE 4-89	

REVISIONS	DRAWN ANH	Job
05-30-97		SHEET
10-24-00	CHECK ANH	1
	DATE 4-89	

BLDG. 596CC  
\\UHSA\MANGO\FPCAD\DWG\596CC-1.DWG

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*
  - PIER 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*
  - PIER 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*
  - PIER 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*
  - PIER 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: <a href="http://www.uh.edu/infotech/services/computing/people-soft-admin/dba-on-call/">http://www.uh.edu/infotech/services/computing/people-soft-admin/dba-on-call/</a>	DBA on call: <a href="http://www.uh.edu/infotech/services/computing/people-soft-admin/dba-on-call/">http://www.uh.edu/infotech/services/computing/people-soft-admin/dba-on-call/</a>
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 Brahmabhatt

## 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 PIER.

### 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 PIER 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**

Energy Research Park (ERP)  
Building 3, 2<sup>nd</sup> 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 (GEN)  
Room 111  
Building 585, Entrance 17 off Elgin  
Houston, Texas 77024

**Alternate Site 1**

Leroy and Lucile Melcher Center for Public Broadcasting  
CPB- Building 536

**Alternate Site 2**

Energy Research Park  
Building 3 Room 145

**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 debrief 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
6/19/2009	3.2.2	Savage	Update UH Contact Center task in levels 5 – 1 per Kelli Gipson PIER Inquiry # 143243
6/22/2009	3.2.2	Savage	Update Appendix "C" per Bill Spindler
7/28/2009	3.2.3	Savage	Insert Signature Page, update title, incorporate IT Service Continuity plan into Incident Action plan. Change title from Information Technology Section (ITS) Incident Action, Emergency Response and Service Continuity Plan to Information Technology Incident Action, Business and Service Continuity Plan.
9/1/2009	3.2.4	Savage	Insert Appendix R – Technique for Working from Home. Corrections to supplies Ride-out team food provisions. Corrections to DR org chart
12/14/2009	3.2.6	Savage	Change Mission Critical Resources to Critical Information Resources. Changed Impact Classification levels for BIA to conform with UH Standard
1/4/2010	3.2.7	Savage	Corrected spelling errors in document. Revised revision notes.
3/3/2010	1.7	Savage	Corrected revision number Corrected spelling errors Removed references to Sara Baber
5/14/2010	1.9	Savage	Removed references to Reatha Brown. Corrected building designations
6/2/2010	1.10	J. Savage	Inserted BCP and Cotton Contacts. Remove Enterprise Production Section
6/3/2010	2.0	J. Savage	Corrections to tables, Insertion and renaming of departments Insertion of Telephone Bomb Check List in Appendix S
6/3/2010	2.1	J. Savage	Removed IT Communications & Training Changed Academic Technologies to Instructional TV Replaced all references to TAC with TPPS. Removed Organizational Development sections. Corrected Page Footer to update correctly throughout entire document. Sorted IT-ICP Organization chart.
6/4/2010	2.2	J Savage	Revised Recovery Org Chart Aligned Departments in order Corrected overrun of contact chart Corrected format errors
6/8/2010	2.3	J Savage	Updated Section 6, Center of Attention Tornado procedures.
6/14/2010	2.4	J. Savage	Updated Web Technologies

University of Houston

University Information Technology, Continuity of Operations Plan (COOP)

			Updated E-Communications Removed Charter School
6/22/2010	2.4.1	J. Savage	Updated Appendix H
6/25/2010	2.4.2	J. Savage	Removed Jim Bradley Update Plan Distribution
9/17/2010	2.4.3	J. Savage	Updated Secondary Data Center Location. Changed Plan title from "Incident Action, Business and Service Continuity Plan" to Continuity of Operations Plan (COOP). Updated plan to reflect new title. Removed Webinar section no longer has service.
9/30/2010	2.4.4	J. Savage	Updated Appendix –R with Cotton information
01/21/2011	2.5	J. Savage	Inserted Risk Cost Assessment, Added IT Security office to approval and implementation page. Inserted Appendix –U- Mission Critical Information Backup Schedule
2/3/2011	2.5.1	J. Savage	Added Snow and Ice procedures section 3.3.3. Removed Mike Alleman and replaced with Eric Block. Added David Johnson to plan.
2/7/2011	2.5.2	J. Savage	Corrected OSG to ES, Updated Organization Chart, Corrected addresses on Cotton contact sheet, modified Table of Contents to show Activation levels
4/28/2011	3.0	J. Savage	Modified plan to reflect new National Terrorism Advisory System triggers. Removed Courtney from ride out team list. Corrected spelling errors in document. Inserted Emergency Radio Frequency into plan, Inserted Director, Emergency Management into plan.
5/2/2011	3.1	J. Savage	Added accountability section 1.9 to plan. Updated Appendix I with regard to accountability reporting. Included in IT-ICP task for level-4 responsibility of accountability log and reporting upward to command.
5/3/2011	3.2	J. Savage	Updated Business Owner names in section 2.3.2 Impact Assessment. Added Senior IT Management to the Approval and Implementation page, Changed section 1.2 heading from Applicability and Scope to Alignment with UH Emergency Management, Removed or designated assistant and replaced with IT Senior Management, re-ordered section 2.2 Scenarios – to reflect order of Rank, Reworked Hurricane Tracking Map and changed title to Hurricane Threat Level, Entered paragraph to describe the UHIT Emergency Response Tracking system, Changed title of section 3.3.3 from Snow, Ice, or Flooding to Travel to Campus, removed snow, ice or flooding and inserted Various Weather Conditions, Removed Mike Kahanic from Deputy Branch Manager for IT-ICC and inserted Dave Johnson .
5//2011	3.3.2	J. Savage	This update includes updates from V-3.3 and 3.3.1. Reference now have contact information located on the page, IT-ICP members roster now shows Order of Succession for each area

University Information Technology, Continuity of Operations Plan (COOP)

			with contact information. Incorporated ITAC escalation and notification procedures into manual.
7/6/2011	3.3.3	J. Savage	Removed Aaron Wilson from ride-out team, inserted Tesfaye Kumbi into recovery team. Inserted Critical Core and Information Services for IT Security and Telecommunications in risk analysis.
08/01/2011	3.4	J. Savage	<ul style="list-style-type: none"> <li>• Updated all hurricane Level 5 pages to reflect task to verify emergency email.</li> <li>• Updated all hurricane General tasks for all levels to verify emergency email.</li> <li>• Moved reserve hotel rooms in hurricane procurement section from L-5 to L-3</li> <li>• Updated section 3.1.7 with new pass code for Conference Bridge.</li> <li>• Updated section 5 to reflect new HLS Cyber alert levels</li> <li>• Modified section 2.3.2 Impact Assessment of Major IT Servers chart by adding two columns for A/B utilities.</li> <li>• Hurricane L-4 – Web Technologies, removed task “Begin coordination to procure temporary storage space in a secure room” per D. Trippel</li> <li>• Added Appendix – V – UIT order of succession.</li> <li>• Added Office of Computer Information Officer hurricane L-5</li> </ul>
10/26/2011	3.4.1	J. Chvatal	<ul style="list-style-type: none"> <li>• Reformatted to decrease number of pages</li> <li>• Updated Section 3.1.5 UIT Order of Succession for IT-ICS due to recent organizational changes.</li> <li>• Removed Appendix V. UIT Order of Succession (duplicate information)</li> </ul>
6/21/2012	4.0	J. Chvatal	<ul style="list-style-type: none"> <li>• Major revisions and restructuring from previous version.</li> </ul>
5/21/2013	4.1	J. Chvatal	<ul style="list-style-type: none"> <li>• Minor updates to personnel names.</li> </ul>
6/18/2013	4.2	J. Chvatal	<ul style="list-style-type: none"> <li>• Updated authority to declare an emergency based on pre-determined criteria</li> </ul>
7/29/2013	4.3	J. Chvatal	<ul style="list-style-type: none"> <li>• Updated Section 4.1, UIT Order of Succession</li> </ul>
5/27/2014	4.4	J. Chvatal	<ul style="list-style-type: none"> <li>• Removed Sections: <ul style="list-style-type: none"> <li>○ 1.3 Goal</li> <li>○ 1.4 Assumptions</li> <li>○ 1.5 Objectives</li> <li>○ 1.8 Concept of Operations</li> </ul> </li> <li>• Section 1.3 – updated to include staff being prepared to work remotely.</li> <li>• Section 2.4 (B)(1) - updated Applications Currently Available in Secondary Data Center</li> <li>• Section 2.4 (D) – updated with UIT Check-In System.</li> </ul>

University Information Technology, Continuity of Operations Plan (COOP)

			<ul style="list-style-type: none"> <li>Moved Section 3: Assessment and Recovery to Appendix G: Recovery from Data Center Damage.</li> <li>Updated Section 3: Personnel and Contact Information with current names and information.</li> <li>Appendix A: Communication Strategies – removed Table 1.</li> <li>Appendix A: Added ITAC Network Outage Communication Plan.</li> <li>Appendix C: UIT Emergency Resource List – updated with current supplies.</li> <li>Appendix D: Food During An Emergency – updated with current process.</li> <li>Removed Appendix G: Cyber Terrorism</li> </ul>
7/16/2014	4.5	J. Chvatal	<ul style="list-style-type: none"> <li>Section 3.1 &amp; 3.2 – added job titles to charts</li> </ul>
6/15/2015	4.6	J. Chvatal	<ul style="list-style-type: none"> <li>Updated personnel and other contact information</li> </ul>
9/22/2015	4.7	J. Chvatal	<ul style="list-style-type: none"> <li>Section 1.6 - Removed (<i>May 2014 – list currently under review</i>)</li> </ul>
6/2/2016	4.8	J. Chvatal	<ul style="list-style-type: none"> <li>Updated Section 1.6</li> <li>Section 2.3: Pre-Determined Criteria and Incident Levels - Updated Tropical Weather criteria, deleted Pandemic scenario table, added Computing Center Power Disruption scenario table</li> <li>Section 2.4 (C)(1) – removed Philip Guthrie Hoffman Hall (PGH – 547)</li> <li>Section 2.5: UIT Emergency Response Plan Tracking System – Deleted</li> <li>Section 3.1: Updated information as necessary to be current</li> <li>Appendix B: Tropical Weather Response Plan – Updated B.1. Tropical Weather criteria, removed B.2. Hurricane Tracking Chart</li> <li>Added Appendix F: Computing Center Power Disruption Response Plan</li> </ul>
5/24/2017	4.9	J.Chvatal	<ul style="list-style-type: none"> <li>Updated Approval and Implementation with correct names and titles</li> <li>Section 1.2 – added MAPP 06.01.02</li> <li>Section 3.1 – updated information</li> <li>Section 3.2 – updated information</li> <li>Appendix A: Communication Strategies – Updated with current practices</li> </ul>
6/21/2017	4.10	J. Chvatal	<ul style="list-style-type: none"> <li>Updated PIER with Everbridge</li> <li>Section 3.1 – updated information</li> </ul>
8/24/2017	4.11	J. Chvatal	<ul style="list-style-type: none"> <li>Section 3.1 – updated with new succession information</li> <li>Section 3.2 – removed Virtual ride out team members</li> </ul>

			<ul style="list-style-type: none"><li>• Section 3.3 – updated Briefing Conference Bridge number</li><li>• Removed references to <a href="http://www.uh.edu/checkin">www.uh.edu/checkin</a></li></ul>
--	--	--	--