Catastrophic Events Procedure

Continuity of Operations for Jarvis Christian University

Jarvis Christian University Catastrophic Events Procedure

Purpose

The purpose of this procedure is to establish a clear framework for ensuring the continuity of operations at Jarvis Christian University in the event of catastrophic incidents. This procedure sets forth the University's intent to safeguard its community, maintain essential functions, and provide financial and operational support during and after disruptive events.

Scope

This procedure applies to all departments, offices, and personnel of Jarvis Christian University, including faculty, staff, administrators, and contractors engaged in university operations. It covers all catastrophic events that significantly impact the University's ability to deliver academic, administrative, or support services.

Definition

For the purposes of this procedure, a catastrophic event is defined as any incident—natural or man-made—that causes severe disruption or poses a substantial threat to the normal operations of Jarvis Christian University. This includes, but is not limited to, natural disasters (such as hurricanes, tornadoes, floods, earthquakes), major fires, pandemics, acts of terrorism, or other emergencies resulting in widespread impact on campus facilities, personnel, or resources.

Procedure Statement

Jarvis Christian University is committed to protecting its students, employees, and assets during catastrophic events. The University will take all reasonable measures to ensure the safety of its community, minimize operational disruptions, and facilitate timely recovery. The institution pledges to maintain transparency, communicate effectively, and provide necessary support to affected individuals and departments throughout the duration of such events.

Guidelines

1. Preparedness: All departments must maintain updated continuity plans, including procedures for remote work, alternative facilities, and communication protocols.
2. Response: Upon declaration of a catastrophic event, the University Emergency Management Team will coordinate the immediate response, activate emergency protocols, and disseminate instructions to all stakeholders.
3. Roles and Responsibilities:
4. University President: Provides overall leadership and direction.
5. Emergency Management Team: Coordinates operations, communication, and recovery efforts.
6. Human Resources: Administers compensation plans and employee support.
7. Finance Office: Oversees budget allocations and financial disbursements.
8. Department Heads: Ensure departmental continuity and report status.
9. Communication: Timely and accurate information will be provided through official University channels, including email, website updates, and emergency notification systems.
10. Recovery: The University will assess damages, restore services, and support the community in returning to normal operations as swiftly as possible.
11. Review and Improvement: After each event, the University will conduct a thorough review of its response and update this procedure and related procedures as necessary.

Contact Information

For questions regarding this procedure or for assistance during a catastrophic event, please contact the Office of Emergency Management or Human Resources at Jarvis Christian University.

Recommended Technology Resources for Catastrophic Events

Based on the Catastrophic Events Procedure and recent technology upgrades at Jarvis Christian University, the following resources are essential for ensuring operational continuity, safety, and rapid recovery during and after a catastrophic event:

1. Campus-Wide Broadband and Network Infrastructure

- **Upgraded CAT 6 Wiring:** All major campus buildings (Chapel, People Dixon, Meyers) have been upgraded to CAT 6 wiring, ensuring high-speed, reliable connectivity even during emergencies.

- **Redundant Internet Connections:** Multiple internet service providers or backup lines should be maintained to prevent total loss of connectivity.

2. Personal Devices and Hotspots

- **Laptops with Built-In Hotspots:** Over 200 laptops with built-in hotspots have been distributed to students, allowing remote access to university resources if campus facilities are inaccessible.
- **Free Tablets for Students and Community Members:** Tablets with activated data plans provide alternative access points for communication and online learning.

3. Emergency Communication Systems

- **Mass Notification Platforms:** Systems for sending alerts via email, SMS, and app notifications to all students, staff, and faculty.
- **Smartboards and Collaboration Tools:** These support virtual meetings and remote instruction, ensuring academic continuity.

4. Workforce and Community Technology Labs

5. IT Support and Network Specialists

- **On-Site and Remote IT Support:** A network specialist has been hired to maintain and troubleshoot technology infrastructure, especially during crisis situations.

6. Cloud-Based Services and Data Backup

- **Cloud Storage for Critical Data:** Ensure all essential university data is regularly backed up to secure cloud platforms, enabling rapid restoration after an incident.
- **Remote Access to Academic and Administrative Systems:** Faculty, staff, and students should be able to access learning management systems, payroll, HR, and other critical applications from any location.

7. Cybersecurity and Ransomware Protection

- **Cybersecurity Training and Awareness:** Regular workshops for students and staff on best practices for digital safety, especially relevant during periods of increased vulnerability.
- **Robust Firewalls and Endpoint Protection:** To safeguard university assets from cyber threats during and after a catastrophic event.

8. Laptop Checkout and Device Lending Programs

- **Library Device Lending:** Students can check out laptops for study and collaboration, ensuring access to technology even if personal devices are lost or damaged.

9. Remote Work and Learning Capabilities

- **Virtual Meeting Platforms:** Zoom, Teams, and other platforms should be available for remote instruction, meetings, and emergency coordination.
- **Online Training and Support:** Ongoing training for faculty and staff to adapt to remote work and teaching environments.

Significance:
These technology resources are critical for maintaining communication, supporting remote work and learning, protecting university data, and ensuring that students, faculty, and staff can continue essential functions during and after a catastrophic event. They align with the university's commitment to safety, operational continuity, and rapid recovery as outlined in the Catastrophic Events Procedure.

Cloud Backup and Remote Access Procedure

Purpose:
To ensure the protection, availability, and rapid restoration of critical university data and systems during and after a catastrophic event, Jarvis Christian University will maintain robust cloud backup and remote access capabilities.

Cloud Backup

- **Scope:**
  All essential academic, administrative, and operational data must be regularly backed up to secure cloud platforms.
- **Implementation:**
  - Use object storage solutions with geographic redundancy to safeguard data against local disruptions.
  - Schedule backups at regular intervals, with automated snapshots and replication to multiple regions.

    - Deploy a centralized backup management system to monitor, verify, and restore backups as needed.
    - Control access to backup data with encryption and regular audits to ensure compliance and security.
    - Provide ongoing training for IT staff in backup and recovery procedures; test disaster recovery plans annually.
- **Review:**
  Backup policies and procedures will be reviewed after each catastrophic event and updated as necessary.

Remote Access

- **Scope:**
  All faculty, staff, and students must be able to access university systems and resources remotely during a catastrophic event.
- **Implementation:**
    - Maintain and upgrade campus network infrastructure to support secure, high-bandwidth remote connections.
    - Provide secure VPN access, with multi-factor authentication required for all remote logins.
    - Migrate essential applications (learning management, payroll, HR, etc.) to cloud platforms for universal accessibility.
    - Distribute laptops, tablets, and mobile hotspots as needed to ensure all community members can connect remotely.
    - Offer IT support both on-site and remotely to assist with access issues and device setup.
    - Conduct regular training on remote access tools and cybersecurity best practices.
- **Communication:**
  Procedures for remote access will be communicated through official university channels, including email, website updates, and emergency notifications.