Jarvis Christian University

Disaster Recovery Procedure

Purpose

The purpose of this Disaster Recovery Procedure (DRP) is to ensure that Jarvis Christian University (JCU) can prepare for, respond to, and recover from disruptive incidents that impact university operations, technology services, facilities, or critical functions. This plan establishes structured procedures to minimize downtime, protect university assets, and maintain continuity of instruction and student services.

Scope

This Disaster Recovery Procedure applies to the following:

- All university departments, academic units, and administrative offices
- All campus locations and remote sites
- All information systems, communication services, and critical infrastructure
- All JCU employees, contractors, vendors, and emergency partners

Objectives

- Protect life, safety, and well-being of students, faculty, and staff.
- Maintain or quickly restore mission-critical operations.
- Protect sensitive data and IT systems.
- Ensure accurate, timely communication during and after a disaster.
- Minimize financial, academic, and operational losses.
- Provide a structured recovery and return-to-normal operations.

Disaster Types

Jarvis Christian University recognizes the following categories for disasters.

I. **Natural Disasters**
   - Hurricanes
   - Tornadoes
   - Flooding
   - Severe Storms
   - Extreme heat or power failures
   - Pandemic Outbreaks

II. **Technological/Infrastructure Disasters**
   - Network outages
   - Server failure or data corruption

- Cyberattacks (ransomware, DDoS, intrusion)
- Utility failures (power, water, HVAC)

III. Human-Caused Incidents

- Fire
- Active threat situation
- Vandalism
- Hazardous materials spill

Roles & Responsibilities

The Disaster Response Team for Jarvis Christian University consists of representatives from:

- **President's Office**
- **Information Technology**
- **Facilities Management**
- **Public Relations**
- **Student Affairs**
- **Human Resources**
- **Finance & Administration**
- **Campus Security**

I. Key Responsibilities

Role	Responsibilities
Disaster Response Team Leader	Directs response, declares severity level, approves recovery steps
Information Technology Director	Restores technology systems, ensures cybersecurity protection
Facilities Director	Evaluates structural damage, make repairs where needed
Public Relations	Issues Alerts, updates website, social media, and press
Student Affairs	Help evacuate residential halls, securing residential hall once evacuated, evaluate the on-campus student count, and notifying students and parents of procedures and next steps
HR Director	Staff accountability, remote work procedures
Finance Office	Tracks costs, manages vendor contracts and insurance claims
Campus Safety	Manages safety, evacuation, and coordination with public agencies

Emergency Response Levels

Level I Minor Disruption

1. Localized outage or small system failure
2. Recovery expected in < 8 hours
3. Disaster Response Team notified but not fully activated

Level II – Major Disruption

1. Multiple systems or buildings affected
2. Recovery expected in < 16 hours
3. Disaster Response Team notified bit not fully activated

Level III – Campus Wide Disaster

1. Full shutdown or campus operations
2. Potential long-term recovery required
3. Disaster Response Team fully activated with Executive Leadership Team

Disaster Response Procedures

I. Immediate Actions (First 30 Minutes)

A. Ensure safety first. (Evacuate if needed)
B. Executive Leadership Team and Disaster Response Team Leader assess the immediate hazards
C. Executive Leadership Team and Disaster Response Leader declares the emergency level
D. Activate the Jarvis Christian University Alert System (texts, email, phone calls, and social media sites)
E. Disaster Response Leader, Student Affairs, and Campus Security begin emergency management plan
F. Begin incident documentation once the incident has come to a close

Stabilization Phase

1. Information Technology Director shuts down systems to prevent further damage (cut network and isolate servers)
2. Student Affairs secures residential halls
3. Facilities secure administration and academic buildings, utilities, and any equipment
4. Establish an Incident Command System (ICS) - (physical or virtual)
5. Public Relations Officer prepares updates for social media and press release

Technology Disaster Recovery

Data and System Prioritization

I. Tier 1 – Mission Critical (Restore within 24 Hours)

A. Jarvis Christian University website & emergency communication
B. Student Information System
C. Email and authentication (Microsoft 365)
D. Server infrastructure and virtual machine hosts

II. Tier 2 – Essential (Restore within 3-5 days)

A. Finance and Human resource systems

B. Library systems
C. Research servers

III. Standard (Restore in > 5 days)

A. Departmental applications
B. Non-critical workstations

Communication Plan

I. Internal Communication

A. Jarvis Christian University Alert System (SMS, email, text message, and phone call)
B. University email
C. Microsoft Teams or Zoom

II. External Communication

A. Jarvis Christian University website
B. Social media updates
C. Press releases
D. Student, parent, and alumni notifications

Communication Requirements

Jarvis Christian University messaging should be:

A. Clear
B. Accurate
C. Timely
D. Approved by Executive Leadership Team

Academic Continuity

To continue to provide our students with their academic needs, Jarvis Christian University will:

A. Shift to online learning if campus facilities are inaccessible.
B. Students will be informed of remote class instructions
C. Academic leadership may adjust academic calendars, deadlines, and exam formats.

Recovery

I. Facilities

A. Conduct structural inspections.
B. Secure hazardous areas.
C. Coordinate repairs with outside contractors if needed.
D. Restore water and HVAC.
E. Evaluate residential halls and essential student facilities first.

II. Recovery and Return-to-Normal Operations

A. Restore essential services and administrative operations.

B. Reopen residential halls, dining, and classrooms when safe.
C. Conduct damage assessments.
D. File insurance claims and track financial impacts

III. After Action Review (within 2 weeks of recovery)

A. Conduct a Disaster Recovery Team debrief.
B. Document lessons learned from the disaster and the response efforts.
C. Update any policies and procedures that may need to be updated from the learning phase of the recovery.
D. Create training sessions to help keep the institution prepared for incidents.
E. Train staff at least twice a year on emergency procedures
F. Decide on a plan maintenance for disasters.
    A. Review the Disaster Response Plan annually or after any major disaster.
    B. Updates should be approved by the President or designee.
    C. Revised copies should be distributed to all departments.