DISASTER RECOVERY PLAN (DRP)

Effective Date: October 18, 2002 **Revised Date: 04/2022**
Responsible Office: Information Technology Center
Division: Operations

PURPOSE

To protect Grambling State University against catastrophic equipment failures, malicious intent, disasters, data, and software loss by adequately applying recovery procedures in the Information Technology Center in accordance with the Office of Information Technology policy IT_POL_1-16.

A. Data Backups

1. All data and software essential to the continued operation of critical university functions are backed up and stored on a daily, weekly, and monthly basis using the following backup procedures. Copies of the operating system software, the database and application software are copied to backup media routinely.
2. **Incremental Backups** are processed on a nightly basis. These volumes consist of data that have been modified since the last backup. These volumes are transported and stored in the off-site storage facility on a bi-weekly basis.
3. **Complete Backups** are processed weekly. These volumes contain data processed for the entire week. These volumes are stored in the off-site facility on a bi-weekly basis.
4. **Monthly Backups** are processed monthly. These volumes consist of a complete copy of all data processed for the entire month. These volumes are stored in the off-site storage facility on a four-week basis.

B. Application Management Services

The Information Technology Center engaged in an Application Management Service contract with Ellucian to provide the following support of the Banner and Oracle environment. The AMS agreement will improve the university's business by providing additional technical support to the existing staff and technical environment. The AMS services will assist the technical staff with daily administration of key Banner and Oracle applications; maximize performance and availability of resources reducing the cost of managing resources in house. The AMS service provides 24/7 monitoring of the Banner and Oracle environment. For Backup/Recovery the Ellucian standard Remote Management software scripts will be implemented to

ensure 24/7 backups of the databases and Banner applications. The service monitors availability 24/7 and export the databases nightly for logical recovery of all objects.

C. Off-site Storage

To ensure the safety and integrity of data that is warehoused in the Information Technology Center and the recovery of all data copied/backed up in the Information Technology Center, data is transported and stored in an environmental controlled secure vault at a location approximately thirty miles from the university. The name of the company is DataBank IMX-Imaging & Information Solution in Monroe, LA.

The backup tapes are rotated off-site on a bi-weekly basis. Every other Monday, DataBank IMX Imaging & Information Solutions retrieve backups from the Information Technology Center from the previous two weeks. On a bi-weekly basis, DataBank IMX Imaging & Solutions returns backups to the department. Backups are created each day and stored in the ITC vault until they are picked up by DataBank.

D. Departmental Servers

Departments responsible for department servers must monitor backup and recovery procedures and practices to ensure compliance with this policy.

E. Backup Electrical Service

All critical systems are connected to an uninterruptible power backup unit. These units must contain enough sustainable battery power to maintain a reasonable operating/shutdown period. A large power generator supports all critical backup power units. These units must be able to sustain enough power to maintain a reasonable operating/shutdown period.

The ITC will maintain two "Head-End" sites, Jacob T. Stewart and the Telecommunications building, which are connecting points in the event that the main Information Technology Center is inoperable for any reason.

F. Testing

The Information Technology Center is required to test the recovery plan every quarter. All deficiencies must be corrected and revealed by the testing procedure.

G. Training

All training of Information Technology Center employees must consist of the following:

a. Establish an Information Technology Center Disaster Recovery Team.
b. Inform employees on the awareness of the need for a disaster recovery plan.
c. Inform employees of the existence of the plan and provide procedures to follow in the event of an emergency or disaster.
d. Train all Information Technology employees on responsibilities identified in the DRP to perform the disaster recovery procedures. (See duties of the Disaster and Recovery Team.)
e.

H. Disaster Recovery Team Emergency Plan

In the event of a major disaster or catastrophic event, the Disaster Recovery Team will hold an emergency meeting in Jacob T. Stewart (JTS) Business Building, Room 139 (Information Technology Center (ITC) Conference Room). This emergency meeting will occur no matter what time or day of the week the disaster occurs. It is the responsibility of the Disaster Recovery Coordinators to notify critical personnel. Disaster Recovery Team Members should contact the coordinators or report to JTS, Room 139 - ITC Conference Room, if they are aware of a major disaster in the area that affects computing services for the university.

In the interim between the occurrences of a disaster, each manager will inform staff members of the occurrence and determine the best course of action for each staff member.

The Disaster Recovery Coordinators will insure all members are properly notified. If necessary, the appropriate management group, administrative managers and the Office of Student Affairs will be contacted for guidance on various other priorities.

A. Establishing Communications

The Disaster Recovery Coordinator, Database Manager and Director of Network Services will have access to information technology resources that will allow the ITC recovery team to remain in constant contact with the vendor recovery team and test any applications.

Cellular phone service will be provided for critical personnel (President, University Police, Vice President of Finance, Vice President of Campus Operations/Facilities, and Director of Media Relations) to communicate with outside officials, from both state and federal agencies.

B. The Disaster Recovery Team

Information Technology Center
Disaster Recovery Team Members

1. Disaster Recovery Coordinator
2. Systems Administrator
3. Security Administrator
4. Network Services
5. Database Management/ERP
6. Desktop Support Services
7. Telecommunications Services
8. Web Administrator

Other Critical Personnel

1. Office of the President
2. Vice President for Finance
3. University Police Department
4. Director of Facilities
5. Safety/Risk Management Engineer

6. Controller
7. Accounts Payable Supervisor
8. Director of Student Accounts Receivable
9. Payroll Manager
10. Director of Media Relations
11. Director of Student Affairs

C. Duties of Disaster Recovery Team Members

1. The Disaster and Recovery Coordinator:

The Associate Vice President for Information Technology serves as the Disaster Recovery Coordinator.

Coordinates the Disaster Recovery Process by notifying the recovery vendor to declare a disaster and convenes meetings with the Disaster Recovery Team and other critical groups.

Coordinates with the Director of Campus Facilities to allocate resources and implement critical operation of the Disaster Recovery Plan.

Coordinates with the Safety/Risk Management Engineer to determine safety issues, assists restoration company on any restoration issues; assesses facilities for damages.

2. Systems Administrator:

Plans hardware/software configurations, provides assistance to the recovery vendor on hardware configurations, storage issues and operating system requirements.

Provides assistance to the Network Service area on establishing network connectivity between local/remote systems and end-user work areas.

3. Security Administrator:

Serves as an Alternate Disaster Recovery Coordinator.

Coordinates with the Recovery Team, end-user access, ERP security requirements and establishes physical security requirements during the event.

4. Network Services:

The Director of Network Services serves as the Network Services Coordinator.

Establishes network services and connectivity with the Recovery Team, Database Manager and Systems Administrator.

Coordinates the establishment of Web services with the Web Administrator for outside campus connectivity and temporary connections.

5. Database Management/ERP:

The Director of Administrative Computing serves as the Database Management/ERP.

Coordinates the recovery of data between the Disaster Recovery Team, System Administrator and Security Administrator.

Verifies database integrity and coordinates with the Disaster Recovery Team establishing access to the production environment.

Retrieves database files, archived files, creates temporary test environment, and installs ERP (Enterprise Resource Planning) applications in a temporary operating environment.

6. **Desktop Support Services:**

   Coordinates with Network Services and end-users to define connectivity for each application on the network

   Provides assistance to Network Services, System Administrator and test end-users' equipment, including desktops and printers

   Provides assistance and training to end-users on use of temporary equipment

7. **Telecommunications Services:**

   Coordinates the establishment of full communicative telecommunications services with administrators, Recovery Team and Disaster Recovery Team.

   Provides assistance to the Recovery Team ensuring communication between the recovery site and the home office.

8. **Web Administrator:**

   Establishes web services and connectivity with the Recovery Team and Systems Administrator.

   Coordinates the establishment of Web services with Network Services for outside campus connectivity and temporary connections.

I. Disaster and Recovery Storage of Important Documents

1. To ensure that an updated copy of this plan is available when a disaster occurs, procedures have been established to store a copy of the plan with other important recovery documents at the off-site storage facility. Likewise, these documents are stored in the fireproof vault located in Jacob T. Stewart, Information Technology Center.

2. When changes are made, the materials are updated at both locations and stored in the proper locations. This ensures that an updated copy of the plan is available at the recovery site.

3. The following personnel have access to the vault and tape storage facility.

   a. Associate Vice President for Information Technology Center

b. Security Administrator
c. System Administrator

4. The documents stored are as follows:
   a. Complete copy of the Disaster Recovery Plan
   b. Complete copy of the Information Technology Center Office Procedures Manual
   c. Complete copy of the Information Technology Center Office Policy Manual

J. Critical Hardware/System

a. HP EVA4400 12 (1TB) – 36 (450GB)
b. (2) 8/40-Port SAN Switches
c. (2) 24-Port Ethernet Switches
d. HP DL580 Proliant G6 Server
e. (3) HP DL360 Proliant G7 Servers
f. RedHat Operating System
g. Oracle Database
h. Ellucian Higher Education Banner
i. HP Storage Works MSL2024 Library
j. HP Virtual Library System 6218
k. HP MSA1000 (4TB) – 14 300 GB
l. (6) HP BL20p G2 Blade Servers ERP (Ellucian Banner, Web Applications)
m. (8) HP BL20p G3 Blade Servers ERP (Ellucian Banner, E-Mail)
n. (2) HP BL20p G4 Blade Servers ERP (VMWare, Web Applications)
o. HP Storage Management Appliance
p. HP DL360 G4p Server
q. (3) HP DL360 G5 Server
r. HP MSA1500 (16TB) - 42 300GB
s. HP MSA30 (4TB) - 14 300GB
t. Big-IP 1600 Series F5
u. HP Bladesystem c7000
v. Fortinet FortiGate 3950B

Appendix A

Disaster Recovery Members Contact List	
Position	**Name**
President	Richard Gallot Jr.
Vice President for Finance	TBD
Chief Operating Officer	Penya Moses
Disaster Recovery Coordinator	TBD
Systems Administrator	Amila De Silva
Security Administrator	Karla Atwater
Director of Network Services	TBA
Director of Administrative Computing	Peggy Hanley
Desktop Support Services	TBA
Telecommunications Services	Stone Flemon
Web Administrator	Bruce Morgan
Associate VP for Finance & Administration	TBD
University Police Department	Quentin Holmes
Safety/Risk Management Engineer	Porcha Williams
Controller	Raymond Abraham
Accounts Payable Supervisor	Angela Harris
Student Accounts Manager	Valencia Bradley
Payroll Manager	April Henderson
Director of Media Relations	Tisha Arnold
Director of Facilities	Fredrick Carr
Vice President for Student Affairs	Rudolph Ellis

Appendix B

Information Technology Center
Schedule of Test Procedures for Emergency Notification Systems

SYSTEM	TEST DATES	PERSON RESPONSIBLE
Campus Cable TV System	**QUARTERLY** January April August December	TBD
Notification System	**QUARTERLY** January April August December	Director of Administrative Computing Peggy Hanley
Emergency Phone Towers	**MONTHLY** 2nd Friday @ 7:30 am	Telecommunications Technician Stone Flemon
University Marquee Board	**QUARTERLY** January April August December	TBD
Information Technology Center Generator	**WEEKLY/ANNUALLY** Weekly Self-Test/Annual Maintenance	Dir of Administrative Computing and System Admin Peggy Hanley