**Rose State College I.T. Disaster Recovery Plan**

Rose State College has instituted a disaster recovery (DR) plan for the institution’s information technology infrastructure based upon the availability of funding. The college’s DR plan is reviewed annually by appropriate Information Technology Services staff, after which recommended inclusions, modifications, or deletions are approved by the Vice President for Information Technology. Careful attention is given to meeting institutional, state of Oklahoma, and federal mandates to further shape the functionality of recovery procedures or plan structure, though the ability to either fulfill or mitigate changes are limited by available resources and funding.

**SECTION 1 – Scope of Services Provided in Event of Disaster**

In the event of the primary campus data center in Administration room 205G being rendered non-functional, the backup data center located in the Learning Resources Center, room 210 is activated. The following information technology services are available via the backup data center:

1) Access to the current version of the PeopleSoft ERP databases and software. This supports basic functionality of the Financials, Human Resources, Student Administration, and Payroll components within PeopleSoft.

2) A limited number of PC workstations for access to the PeopleSoft system. The total number of workstations is less than ten.

3) A viable laser printer for printing PeopleSoft reports.

4) Tape drives and cd-writers for data archival or data transport to off-site recipients (such as the Oklahoma Office of Management and Enterprise Services, or OMES).

5) Cisco Voice Over IP (VOIP) telephone server, including voicemail. This will permit basic operation of the campus VOIP phone system.
   a. Mobile cellular phones and campus radios are also readily available for point-to-point communications.

6) Internet access through OneNet.

7) Primary file storage services utilized by central college offices with the exception of the Application Extender archive.

8) Domain controller servers for internal DNS services.

Within 48 hours of activating the backup data center, the following services can be activated and operational.

1) Microsoft Exchange email services.

2) External domain controller services for external DNS services.

The following services are currently **NOT** available via the backup data center.

- File server or print server network services for either administrative or academic areas.
- Campus video surveillance system.
Despite a potential failure of the campus primary data center, the following services are readily available to campus users, including faculty and students, via cloud-hosted providers.

1) Desire2Learn (D2L) learning management system
2) Google Gmail (for students and faculty)
3) Campus external website (www.rose.edu)
4) OCLC Worldshare Management Services supporting the college’s library circulation database.
SECTION 2 – Procedures for Activation of Backup Data Center

1) Contact the college’s Vice President, Information Technology immediately. Other participants or campus I.T. Services support personnel will then be activated in accordance with the campus emergency response plan and procedures. (See the Rose State College Policies and Procedures Manual, Section 3-37, for further details.)

2) Designated representatives from key campus offices are contacted to ensure immediate access to critical campus services. These include, but are not limited to, representatives from: Information Technology Services, President’s Office, Administrative Services and Payroll, Human Resources, Admissions, Financial Aids, and Enrollment Services.

3) Secondary systems that require up to 48 hours to be brought online (see page 2) are mobilized for startup and operation.

4) Critical campus operations resume at minimal operating levels until the primary campus data center is returned to an online state.

5) Backups are performed regularly to ensure continued data integrity and continued disaster recovery mitigation.

6) Preparations are made to institute repairs to the primary data center to bring it online as soon as possible. In addition, secondary plans are made for activation of additional IT-related services in the event the primary data center cannot be brought online in a timely fashion, as determined by the Vice President of Information Technology.

[This space intentionally left blank.]
SECTION 3 – Primary Contacts

The primary contact for the IT Services disaster recovery plan is the Vice President, Information Technology. The secondary contacts are the Director, Information Systems and Director, Information Technology. Current contact information for those positions is listed below. Of the following information, the mobile phone numbers contained in section 3 are considered operationally sensitive and confidential, and will not be publicly disseminated or posted in a publicly accessible venue.

Vice President, Information Technology: John Primo  
I.T. Services Department – ADM 200A  
Voice: (405) 733-7354  
Fax: (405) 736-0339  
Mobile: {Redacted}  
E-Mail: jprimo@rose.edu

Director, Information Systems: David Swingle  
I.T. Services Department – ADM 200B  
Voice: (405) 733-7908  
Fax: (405) 736-0339  
Mobile: {Redacted}  
E-Mail: dswingle@rose.edu

Director, Information Technology: James Johnston  
I.T. Services Department – ADM 205  
Voice: (405) 733-7356  
Fax: (405) 736-0339  
Mobile: {Redacted}  
E-Mail: jjohnston@rose.edu