Limestone College Backup and Recovery Policy

PURPOSE

The purpose of this policy is to define the criteria for the backup, archival storage and restoration of critical data and systems at Limestone College.

Backup data is defined as information that can be restored to a point in time in the event of a disruption of business, and then used in the daily operations of the college. This policy outlines the minimum requirements for the creation and retention of backups. Special backup needs which exceed these minimum requirements, should be accommodated on an individual basis.

SCOPE

The scope of this policy includes all data and systems required to conduct college business and to support college functions and mission.

POLICY

- Data and systems to be backed up and archived will be identified by Limestone College Information Technology Leadership and Legal Counsel based on college need and on legal, regulatory, and business requirements to determine content and time frames for retention.
- At a minimum all cloud systems and data are required to be backed up on a nightly (at least incremental or differential) basis.
- At a minimum all on-premise systems and data are required to be backed up on a weekly (at least incremental or differential) basis.
- College Information Technology Leadership will identify any systems and data that needs to be backed up more frequently for approval by College Leadership.
- Full backups shall be performed on at least a monthly basis with backup media maintained on disk securely and readily accessible for at least one (1) month.
- At a minimum all confidential and sensitive data shall be encrypted on backup media.
- Backup media catalog must be labeled and accounted for at all times.
- Backup of non-critical data is at the discretion of the College leadership.
- Recovery procedures must be tested at least every six (6) months to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.
- Backup and recovery documentation must be reviewed and updated at a minimum on an annual basis to account for new technology, business process changes, and migration of applications to alternative platforms.
- Backups and archives will be treated with the same level of criticality and sensitivity as the data and applications stored on them.
- The backup system(s) cannot recover modifications to a file made between the last successful backup and the point of failure (point in time in which the file becomes deleted, corrupted, lost, etc.).
- Rare recovery problems do exist that are beyond IT's ability to control and may result in the file being unrecoverable, or may affect the time required to recover a file including:
    - Incomplete backup
    - File was "open" or "in use" during the backup
    - Errors writing to the media during the backup

- Corrupt file prior to backup
- Network errors during recovery
- Disk errors during recovery

RELATED REGULATIONS

This policy is a component of Limestone College information security program that is intended to comply with the PCI-DSS, FERPA, Gramm Leach Bliley Act and other regulations.

EXCEPTIONS

Only the Chief Information Officer (CIO) or a designated appointee is authorized to make exceptions to this policy with approval of the Provost. Any requests for exceptions shall be made using the "Request for Policy Exception" form and a copy maintained by the CIO. The Request for Policy Exception Form is attached for your convenience.

VIOLATIONS

Any user found to have violated this policy may be subject to disciplinary action, up to and including notifying the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity

A Supervisor, Department Manager, Dean, or Vice President will address violations of this policy by staff members and have full authority to sanction an immediate stop to the actions in question. Appeals from any formal disciplinary action taken against a unit professional staff member will be governed by their specific contractual grievance procedure. The Complaint Procedure of the Board of Higher Education Non-Unit Professionals Personnel Policies will govern non-unit staff. The Vice President of Enrollment Management and Student Affairs will address violations of this policy by students.

DISCLAIMER

The College makes no warranties of any kind, whether expressed or implied, with respect to the information technology services it provides. The College will not be responsible for damages resulting from the use of communication facilities and services, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions caused by the negligence of a College employee, or by the user's error or omissions. Use of any information obtained via the Internet is at the user's risk. The College specifically denies any responsibility for the accuracy or quality of information obtained through its electronic communication facilities and services, except material represented as an official College record. The College also does not accept responsibility for removing material that some users may consider defamatory or otherwise offensive. Users should be advised, however, that dissemination of such material may subject them to liability in other forums.

Role	Responsibility
IT System Administrators	Define data and systems to be backed up including the content, frequency, and retention time. Define data to be archived for legal and/or regulatory purposes in conjunction with the Information Security Officer.
Legal Counsel	Define data to be archived for legal and/or regulatory purposes in conjunction with the Business Management. Ensure new legal and/or regulatory requirements concerning the archival of information is communicated to Business Management and changes are implemented.
Staff	Ensure that any critical data residing on their workstations or portable media are backed up in accordance with this policy.

Information Security Officer	Provide mechanisms to ensure backup and archival process are implemented following the guidelines of Business Management and Legal Counsel. Perform reviews to ensure compliance with this policy.

REFERENCES

Frameworks	NIST 800-53 (CP-9, CP-9-1, CP-10), NIST 800-171 (3.8.9)
Regulations and Requirements	
Supporting Standards and Procedures	

REVISION HISTORY

This section contains comments on any revisions that were made to this document and the date they were made.

Revision Number	Date and Time	Name	Description
1.0	1/19/2019	BS	Initial Version

Limestone College Request for Policy Exception Form

Name of Requester _____

Title _____

Department _____

Date _____

Signature _____

Please state your policy exception request and reason for the exception below. If you need more space you may attach additional pages and/or documentation.

_____

_____

_____

_____

_____

Chief Information Officer/Provost Section

_____ Denied

_____ Approved as requested

_____ Approved with the following changes:

_____

_____

_____

_____

Chief Information Officer

_____

Print Name

_____

Signature

_____

Date

Provost

_____

Print Name

_____

Signature

_____

Date