Division of Information Technology

POL-26 – Backup and Recovery Policy

Version: 1.0 Date: 2/15/2017

POLICY APPROVAL

Approved By: Ray Lefebvre (RL)
Signed on 2017/02/27 10:47:54 PST

Approved Date: 02/27/2017

PURPOSE

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

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 company. 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 and to support University business.

POLICY

- Full backups shall be performed on at least a weekly basis with backup media maintained in an environmentally secure and readily accessible library for at least four (4) weeks.
- A replica copy of production or critical data must be stored in a geographically diverse and secure location for disaster recovery and business continuity purposes and to cover in the case of the failure of the primary backup media.
- Any systems and data that needs to be backed up more frequently shall be handled on an individual basis.
- At a minimum all confidential and sensitive data shall be encrypted on backup media.
- Backup media must be completely labeled and accounted for at all times.
- Backup of non-critical data is at the discretion of the data steward or by IT Senior Leadership.
- Backup jobs shall be scheduled to run during non-business hours as not to impact application or network performance. Replication to off-site storage may occur at any time.
- 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 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 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
- This policy does NOT apply to workstations (desktops, laptops, external hard drives, etc.) or other client computing devices or hardware.

REFERENCES

Frameworks	**Name** **SANS CSC V6**	**Reference** CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps CSC 19: Incident Response and Management CSC 20: Penetration Tests and Red Team Exercises
Regulations and Requirements	**Name** **PCI DSS 3.1** **HIPAA/HITECH**	**Reference** N/A § 164.308(a)(7)(i) Contingency Plan § 164.308(a)(7)(ii)(A) Data Backup Plan § 164.308(a)(7)(ii)(B) Disaster Recovery Plan § 164.308(a)(7)(ii)(C) Emergency Mode Operation Plan § 164.308(a)(7)(ii)(D) Testing and Revision Procedure § 164.310 (d)(2)(iv) Data Backup § 164.310(a)(2)(i) Contingency Operations § 164.312(a)(2)(ii) Emergency Access Procedure
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	Name	Description
1.0	February 15, 2017	Steven Zuromski	Initial Version