Disaster Recovery Policy	BOT Approved: January 15, 2019

Table of Contents

POLICY STATEMENT:

This Policy addresses the requirements for the continuation of information security controls in the event of a disaster scenario. Failure to include security controls during such an operational challenge would leave Garrett College ("Garrett") non-public data at risk of compromise, destruction, and/or non-availability.

PROCEDURES:

Planning information security continuity

- Information security requirements must be included in any impact analyses and overall planning for business continuity and disaster recovery programs.

- Response and recovery procedures must address how Garrett will manage a disruptive event and will maintain its information security to a predetermined level, based on administration-approved information security continuity objectives.

- The Information Technology ("IT") Department shall establish alternative command center location(s) that provide secure facilities for management of recovery activities.

- Garrett third parties and contractors involved in providing services that support business continuity and disaster recovery will be contractually required to support Garrett business continuity and disaster recovery requirements. These contractual obligations may involve service level agreements, recovery time objectives (RTOs), recovery point objectives (RPOs), annual tests, special access for Garrett personnel during emergency mode operations, as well as other Garrett business continuity and disaster recovery requirements.

- The IT Department shall establish the management structure required to prepare for, mitigate and respond to a disruptive event using personnel with the necessary authority, experience and competence.

- A list of disaster recover responsibilities will be developed, maintained, and communicated to all members of the IT Department and senior administration officials.

Implementing information security continuity

- Garrett will develop, maintain and implement procedures and technologies to enable the continuation of critical functionality required to protect the confidentiality, integrity and availability of Garrett non-public data. These procedures and technologies must include operating system, application and data backups for critical processes, assigned responsibilities for Garrett personnel, third party providers and contractors, and emergency mode operations.

- Backups will be taken or replicated off-site in accordance with the following backup strategy:
    - Backup and recovery procedures must be documented, available to operators, and reviewed by the administration to ensure recoverability of key student and financial data.
    - All permanent changes to backup procedures must obtain administrative approval.
    - All restore operations will be managed by the IT Department. Any requests for non-scheduled restore operations will be assessed by the administration.

- All backups will be monitored for successful completion.

Verify, review and evaluate information security continuity

- All Garrett disaster recovery policies, processes and procedures will be reviewed and approved on an annual basis.

- Garrett will periodically conduct disaster recovery tests, which will include the testing of security controls within the disaster recovery program.

- Disaster recovery tests must involve the Garrett administration and IT Department personnel assigned disaster recovery responsibilities.