Information Security - Backup, Archive, and Restore

- GGU will ensure that University data is adequately backed up per business/academic requirements.

- Plans must be developed to recover from losses that range from minor losses or temporary outages to comprehensive disasters.

- The IT Data Archive Policy of the Technical Operations Infrastructure group specifies the details for each academic or administrative area.

NOTE: This IT Policy does not apply to the backup of hand-held devices, e.g. palm tops, telephones, pagers, two-way pagers, and other wireless hand-held devices.

Information Security - Secure Disposal of Equipment and Media

All items of equipment containing storage media (e.g. fixed hard disks) shall be checked to ensure that all sensitive data and licensed software have been removed or overwritten prior to disposal or reassignment.

Adherence to University IT Security Policy

All university employees, contractors, and affiliated employees are required to adhere to the University IT Security Policy as a condition of employment. Any failure to comply with this IT Policy may result in disciplinary action, up to and including termination of employment.

Enforcement of IT Policy

All the university employees shall advise the Information Technology Security Officer of any observed breach of the following University IT Security Policy immediately. No employee shall be punished, reprimanded, demoted, dismissed, or otherwise impacted for contributing to the enforcement of IT Security Policy. This will remain true regardless of the position of any individual responsible for the reported breach in IT Security.
Process

The processes used to implement the Policies stated above contain information that is too sensitive to release to all Staff Members. These Processes are included in a separate Controlled Document that has restricted access. This document will be the Internal ETS IT Security Policies Document.

Record Keeping and Retention

IT Security documentation and all related articles will be securely stored and will be under document control and archived for a period of two years.

Public Distribution of Confidential Information

All the university documentation, electronic and printed will be handled as sensitive information. This includes, but is not limited to: memos, agendas, calendars, proposals, financial statements, interoffice mail, customer information, personal planners, resumes, faxes, e-mails, and notes. All the university documents should be guarded to ensure confidentiality; documents that reach their end of life should be destroyed (e.g. shredded).