GGU Information Technology (IT) Security Policy

The purpose of this document is to describe the Information Technology policies for protecting our Students, Instructors, Employees as well as the university from problems with computer related IT security issues.

Policies

All university employees, contractors, students and affiliated employees shall adhere to the following University IT Security Policy at all times.

1.1 University IT Security Policy Owner The Chief Technology Officer (CTO) is the owner of the University IT Security Policy and is responsible for the overall enforcement of the University IT Security Policy.

1.2 Information Technology Security Officer(s) The Information Technology Security Officer (ITSO) is the person designated by the CTO to administer the Information Security program and a secondary person, if delegated by the Security Officer.

Responsibilities of the ITSO include but are not limited to the following:

• Delegate some responsibilities to other infrastructure engineers
• Monitor, audit, and test systems and networks for possible IT Security vulnerabilities
• Review IT Security Log files and investigate non-conformities
• Test and install patches and fixes for IT Security vulnerabilities in vendor systems and/or software.
• Provide investigation, coordination and follow-up of network Security Incidents.

1.3 Personnel IT Security - Review of User Access
• The university may restrict the use of its computing facilities and limit access to its networks when faced with evidence of violations of university IT policies, IT standards, IT contractual obligations or IT violations of federal state or local laws.
• Users shall be held responsible for systems and the use of information related to his or her job.
• Users may not use their computer accounts for any commercial (for profit) purpose or enterprise including advertising.
• Users may not transmit intimidating, harassing or threatening electronic communication or forge any electronic communication.
• Users may not set up unauthorized bulk or junk email or solicitations that are not business/academic related.
• Violations of IT Security requirements may be cause for disciplinary action, including termination and/or the assessment of civil damages.

The Office of Student Affairs will handle student violations. Employee violations will be handled by the Human Resource Department. Note1: In most cases GGU will attempt educational or remedial interventions prior to disciplinary actions. Note2: Access to computing facilities may be restricted or denied pending the results of the findings. Note3: Any violations may be reported to the appropriate civic authorities.

1.4 Personnel--Computer accounts (Ids and passwords)
• Users may not share their university computer accounts with any other person in, or outside the university.
• If an authorized user for valid academic and administrative reasons (i.e., someone is out sick and data needs to be retrieved) needs to access another account, then a Helpdesk lead or ETS Manager needs to approve this transaction and ensure a ticket is open to track this access.
• ETS and any department employee may not ask a user of an ETS-supported system to reveal their password.
• Any users who suspect unauthorized access of their accounts should contact ETS immediately through the Helpdesk and/or the Management of ETS.
• ETS will disable user accounts upon notification from the Human Resource Department that a faculty or staff member has terminated employment and delete the account within 30 days.
• GGU requires that passwords be changed on a regular basis:

Desktop accounts 90 days Servers 30 days Applications 90 days. NOTE: At this point the desktop accounts prompt this change but some servers and applications are left to the good faith of the personnel or the management.

• ETS shall administrate the user privilege accesses for all user and University systems:

GGUOnline (Student email) - Classroom Technology Support (CTS) Academic accounts - CTS Groupwise accounts - Helpdesk Netware accounts - Helpdesk GGU4YOU accounts - Helpdesk UNIX and PINE email accounts - Helpdesk Financial, Human Resources and Student System Accounts-Application Support (legacy) and Helpdesk - New Oracle accounts.
• Student system accounts left inactive for 180 days will be deleted.

1.5 Personnel - Electronic mail

Email messages shall include any electronic message that can be stored, attached to, or transferred with an Email message. Examples include, but are not limited to: Traditional Email messages. Voice mail. Instant message. Mobile phones, pagers, and faxes.

• Each person must take full responsibility to ensure that his or her email behavior is not prohibited under university IT Policy and standards or under federal, state or local law.

• The use of electronic mail is reserved solely for the conduct of business and instruction at GGU.

• The electronic mail system may not be used to create any offensive or disruptive messages that may include sexual implications, racial slurs, gender-specific comments or any other comments that offensively address someone's age, sexual orientation, religious or political believes, national origin or disability.

• GGU has the right to review, audit, intercept, access and disclose all messages created and received or sent over the electronic mail system of GGU.

• Any unsolicited emails that are received that violate the email policies should be reported to the Helpdesk and/or the Management of ETS.

1.6 Personnel - Internet Use

The university employees shall use the Internet consistent with the university's standards of business/academic conduct. Internet access provided to the university staff should not be used in the following ways:

• Publishing non-GGU Web pages available to the public.

• Downloading software for personal use.

• Hacking into any system without authorization from the assigned system owner.

• Accessing content of an inappropriate (e.g., pornographic) or illegal nature, or other non-work related activities.

• Using chat rooms and bulletin boards (not directly related to business needs)

• Using file-sharing software for music and other non-business needs.

1.7 Personnel - Screen Savers and Screen Locks

• The university Employees are asked to lock their personal computer screens via the standard Operating System (OS) locking mechanism when leaving their computers unattended.

1.8 Personnel - Copyright

• Users may not distribute or duplicate copyrighted software without appropriate licensing agreements and use must be consistent with licenses.
• For GGU copyright policies please go to the following link:
http://internet.ggu.edu/university_library/ggucopyright.html

1.9 Personnel-Privacy
• GGU may examine material stored on or transmitted through its electronic
environment. The university will examine files only when reasonable
business/academic needs require official intervention for the protection of
the university assets, its employees or systems.
• All GGU employees must keep confidential student, faculty and employee
and business/academic data and must comply with the FERPA (Family
Educational Rights and Privacy Act) regulations by filling out and filing with
the Registrar the FERPA form.

• Monitoring of university computers, networks, databases and websites will
be done on a regular basis by ETS and will be done to discover or investigate
IT Security violations. Generally this is reviewed at the Daily Operations
Meeting.
• ETS employees may not intentionally access, view, use or change any
confidential business/academic data.

1.10 Network Security - User Remote Access
• Remote access connectivity to the university systems, network
infrastructure, and applications shall be adequately secured to minimize IT
Security risk.
• Remote access connectivity shall be a monitored service that will be
granted based upon approved requests. Any third-party or consultant who
requires remote access will be granted only temporary access. Access will
immediately be revoked after their work is complete. A ticket will be opened
to track the access user, plus their start and end time.
• Authorized internal users may access the university’s network via setting
up a Citrix account with ETS or via the Checkpoint VPN client requested
through ETS process.

1.11 Lab access
• Users must sign in to enter the computer drop-in lab. Student Ids must be
checked and students need to sign-in.
• NOTE: For IT Security reasons, student ID numbers will not be logged.
• Users must use the lab machines for academic or administrative use only
and my not install any software on the lab machines.

1.12 Network Security - General
• The production and University network infrastructures shall be monitored
and protected at all times.
• Modems shall not generally be installed in, or attached to, the university office desktop PCs. Exceptions are for some financial applications needed for financial transactions with banks or other known academic vendors.
• Modems may be installed in laptop or notebook PCs. They may not be used to connect to any outside network while the computer is connected to University or production networks.
• Connections to the Internet, remote systems, and networks shall be routed through the university Internet firewall.

1.13 Physical IT Security and Configuration Management - Equipment Rooms
Physical access to the following shall be restricted to prevent theft, loss, and damage of equipment or disruption of service:
• All equipment rooms at local facilities.
• All equipment rooms and/or cages at remote facilities.
• Maintenance and repair people may enter after notifying ETS.

1.14 Physical IT Security and Configuration Management - Incident Response
Users shall report to their immediate Supervisor or the University IT Security Officer any observed or suspected IT Security breaches, threats, weaknesses, or malfunctions that may have an impact on the IT Security of the university assets.

1.15 Network Security - Virus Prevention
• Virus detection software shall be installed, regularly updated, and used to scan computers and media for known viruses.
• Removable media for internal usage shall be checked for viruses before use on the university systems.
• Students need to be encouraged to have anti-virus software on their laptops prior to connecting to the Academic network.

1.16 Network Security - Non University Equipment
• No non-university computer equipment shall generally be connected to the university network at any time, with the exception of monitored vendor demonstrations or consultants performing agreed upon tasks or students/faculty /employees connecting via the university-approved wireless connections after their MAC address has been registered into the GGU process. Go to this link: www.ggu.edu/wireless
• The key example of the exception to this policy is a laptop used by the students especially in the Law school. This exception is allowed in good faith and as such the student would be solely responsible for any damage incurred to the university resources following the use of his/her laptop on the university network.
• ETS technical operations and Law School technical support requests to
these student that proper precautions be taken for virus checking, malicious software, Trojans, back doors and so on, before using the university network.

1.17 Network Security - Redeployment of Equipment and Software
• No user not specifically authorized by the ETS shall move any device to a different network port.
• No user not specifically authorized by ETS-Technical Operations shall reconfigure any device, nor add any new equipment to the network. No user not specifically authorized by the ETS-Technical Operations shall move, unplug, or otherwise disturb any network cable, hub, switch, router, or other networking device.
• No user not specifically authorized by ETS-Technical Operations shall install any software or software updates on any PC or Server.
• NOTE: Exceptions are designated tech support personnel, who have some privileges to perform certain jobs.

1.18 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.

1.19 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.

2. 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.

3. 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.
4. 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.

5. 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.

6. 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).