Gwynedd Mercy University

Information Technology Security, Privacy and Confidentiality Agreement

(Section 2.1.4 in Gwynedd Mercy University Policy Manual)

Gwynedd Mercy University is committed to providing a secure and accessible information technology environment for teaching and learning. Security and privacy policies help Gwynedd Mercy University protect students, faculty and staff, ensure business continuity, protect the value of data usability, protect the University from lawsuits and generally avoid damage to the institution and the GMercyU brand. Many University vendors require security policies to do business. When applicable, it is necessary to comply with government regulation such as Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLB), Family Educational Rights and Privacy Act (FERPA), and other policies required by law.

Scope: The following security and privacy policy governs the use and interaction of all technology at Gwynedd Mercy University including devices, systems, networks, data centers and physical and virtual spaces. The Chief Information Officer in consultation with the Vice President for Finance and Administration is responsible for establishing, implementing and maintaining the Information Technology Security, Privacy and Confidentiality Policy.
Note: This Policy should be considered a subset of the University's various policies regarding information security, which include but not limited to the University's Student Records (FERPA), Identity Theft Protection, Information Security Program, Employee Confidentiality, and HIPAA policies.

Policy:
1. Security includes protection against unauthorized access to, use of and/or modification of information, denial of service and unauthorized access of computers, electronic devices, computer systems, networks and any and all technology.

2. Gwynedd Mercy University computers, systems and networks may be used by only individuals authorized by the University. Account creation and access to systems must be approved by an authorized University official. Inquiries regarding access, accounts, best practices, behavior and permitted uses must be referred to the Chief Information Officer or a designee.

3. Any and all attempts by an individual to gain access to accounts or systems that do not belong to that individual on any Gwynedd Mercy University system is prohibited unless approved by the Chief Information Officer.

4. Multi-use and/or shared accounts, generic accounts, test accounts or any accounts that are not directly identified with an authorized Gwynedd Mercy University individual are not permitted on any computer, device or system without prior written authorization from the Chief Information Officer.

5. Access to all data centers, processing facilities, and administrative system technology spaces are restricted to authorized Institutional Technology Services users.

6. All University computers, systems, networks, and technology space will comply with all laws without limitation including security, privacy and appropriate usage.

7. The University shall not be liable for, and users assume the risk of loss, destruction and/or interference of data, files or information resulting from the University's efforts and initiatives to maintain privacy, integrity and security of the University's computers, computer systems, networks and all associated technologies.

Responsibilities:

1. The Chief Information Officer is responsible for establishing and overseeing the implementation and enforcement of this policy.

2. Any University representative or agent who accesses or users a device or system under the authority defined in this policy must make a good faith effort to protect the integrity and privacy of data within or associated with the system.

3. The Information Security Officer is responsible for developing, implementing and enforcing this policy under the direction of the Chief Information Officer and for coordinating issues and questions with the appropriate University department including but not limited to Campus Safety, University legal Counsel, Finance and Administration, Student Services, Executive Council, and all external law enforcement and government agencies.

4. Gwynedd Mercy University computer, computer system and network users are responsible for:

a. Understanding and complying with all security and computer usage policies governing University computers, computer systems, networks and technology;

b. Put forth a good faith effort to protect the integrity and privacy of data within the University's computers, computer systems and networks;

c. Maintain and monitor the proper use of account and account activity conducted in the use of the account including creating and protecting safe passwords and ensuring local system security protection is enabled;

d. Ensure the local security of any system on the University network connected to by the user;

e. Reporting any suspected, detected or observed security lapses, issues or incidents on any University computer system or network to the University Information Security Officer;

f. Respect and maintain the physical hardware and network configuration of University networks. No system user shall modify, limit, extend the University network or network configurations on which the user's system resides without the written authorization of Institutional Technology Services;

g. No user will alter, install, modify or delete stored or executed on any computer or system without the express permission of the owner, department or office;

h. Refrain and avoid the use of University computer and technology resources for any and all unlawful purposes including without limitation infringement of intellectual property including any and all copyrighted materials.

i. Mobile devices pose an increased security risk due to their portability. Take extra care to secure mobile devices, particularly when traveling, in order to minimize the risk of theft or loss of data. If accessing University data using cell phones or Smartphones, secure such devices with a password.

5. System administrators have the same responsibilities as general users above and additional responsibilities because of their position and system privileges. System administrators including all Institutional Technology Services staff are responsible for:

a. Preparing and maintaining security procedures compliant with this policy and other applicable information security policy and procedures (i.e., Student Records (FERPA), Identity Theft Protection, Information Security Program, Employee Confidentiality, and HIPAA policies);

b. Plan and implement reasonable precaution to guard against corruption or compromise of University computers, computer systems or networks;

c. Plan appropriate measures to prevent unauthorized use of system users files or data;

d. Assure all hardware and software license are current and in force;

e. Assure all computers, computer systems and networks have appropriate backup procedures and adequate disaster recovery and business continuity plan tested and in place;

f. Limit access to privileged supervisory accounts to the administrator, except as approved by the Chief Information Officer;

g. Establish a change control process before planning any work or installing software, including patches on any information system that is in production and service users. All major changes or upgrades must be documented in writing.

Rules:

1. <u>Authorized Users</u>:

a. Authorized users include full-time and part-time workers who have been approved by Information Technology Services department and have read and understand the Computer

Usage Policy, this Information System Security, Privacy and Confidentiality Policy, and signed the Security, Privacy, and Confidentiality Agreement Form (see Appendix 5). No other individuals in any capacity may access systems unless otherwise approved in writing by the Chief Information Officer;

b. Generally, Gwynedd Mercy University students, temporary workers, vendors and visitors are not permitted access to systems that contain student records, financial information, business intelligence, strategic data, or other confidential University information. If granted access, such individuals are obligated to comply with all University policies, including but not limited to the University's Confidentiality related policies. Moreover, when appropriate, contractual arrangements with service providers, including service providers that are entities outsourced for the provision of hosting services, should specifically require the service provider to maintain its own identity theft prevention program. Generic or group accounts are strictly prohibited and can never be created for these groups. All University accounts must be associated with an individual;

c. No individual, office or department may make exception to this rule by creating a temporary or generic account, allowing others to login with their account or otherwise allowing access to unauthorized individuals;

d. It is the responsibility of the Gwynedd Mercy University community to notify the Information Security Officer of violations to protect Gwynedd Mercy University.

2. University Network:

a. The office of Institutional Technology Services is responsible for configuring and managing the network as well as all wired and wireless connectivity to the University network;
b. All remote access to any University system is subject to monitoring by Institutional Technology Services;

c. All access to restricted systems requires authentication (name and password). University printers, print servers, copiers, faxes, storage and other systems shall not be access able from the Internet without the written approval of the Information Security Officer;

d. All IP –capable devices installed on the University network must have an IP address issued by Institutional Technology Services;

e. Institutional Technology Services may filter network traffic to exclude malicious traffic on both an incoming or outgoing basis. Malicious traffic can include viruses, and unsolicited e-mail;

f. All wireless communication on the University network and authenticated access to the University network systems and servers must follow the Institutional Technology Services standard encryption protocol.

3. Security Protection:

a. Security patches will be applied within 30 days of vendor release unless otherwise approved by the Information Security Officer;

b. All IP addresses assigned to computer equipment by Institutional Technology Services will be protected by the University's approved antivirus protector, which is regularly maintained and updated.

4. Privacy, Security and Confidentiality:

a. The privacy and security of files, electronic communication, and other information belonging to individual University users shall be protected to the extent reasonably possible. However, computers, computer systems and networks, specifically Gwynedd Mercy University networks should never be considered fully private particularly because of the open nature of the Internet and related technology and the ease in which files and data can be accessed, copied and distributed. Users should take all appropriate precautions to protect sensitive and confidential information stored on their systems;

b. All students, faculty, staff, vendors, visitors and users are required to adhere to the Security, Privacy, and Confidentiality Policy. Failure to comply with this policy may lead to denial of service, account locking or account removal. Security violations and non-compliant behavior is not tolerated and can lead to termination and/or expulsion for employees and students. Gwynedd Mercy University will investigate and prosecute violators to the fullest extent of the law including but not limited to The Computer Fraud and Abuse Act (Title 18, 1030);

c. To support privacy and secure data authority to log, intercept, inspect, copy, remove or otherwise alter data, file or system resource on Gwynedd Mercy University's network rests with the Chief Information Officer. The Chief Information Officer, at his or her sole discretion, may take action when he/she determines there is a potential or actual threat to the security or integrity of University computers, computer systems, networks or non-standard or unauthorized use. All requests for such actions must be made to the office of the Chief Information Officer;

d. Without limiting its right in any way the University specifically reserves the right, in its sole discretion to limit, restrict of suspend or terminate any user's account or use of the University network or use of any computer or computer system at any time for any reason. The accounts of persons leaving the University or no longer requiring access will be disabled;

e. All computers removed from service shall be purged of all information stored in the system;

f. All media returning from back up storage to be passed to a different end-user or taken out of usage altogether shall be purged of all information contained therein;

g. The purchase of anti-virus software for purposes of installation on any University computer must be pre-approved by the Chief Information Officer. The purchase and use of Information Security tools including firewalls, intrusion detection systems and hacking tools, must be pre-approved in writing by the Information Security Officer.

h. CONFIDENTIALITY STATEMENT: The information contained in any Gwynedd Mercy University e-mail, system, report, account, repository, hard copy, wireless device, PDA, including attachments and verbal explanation, is the confidential information of, and/or is the property of, Gwynedd Mercy University. The information is intended for use solely by the authorized individual or entity and may not be shared, discussed or translated with any other entity or individual. All Gwynedd Mercy University system users must adhere to the Gwynedd Mercy University computer usage and e-mail policy. If you are not an intended user of any Gwynedd Mercy University system, then any review, printing, copying, discussion or distribution of any such information is prohibited