Acceptable Use of Technology Policy

BOT Approved:

- *5/9/2010 (Approved as part of HR Manual Update)*
- *Separate Policy in new format approved by Board on January 15, 2019.*

Table of Contents

PURPOSE:

Garrett College's intentions for publishing an acceptable use policy are to ensure that all users of the Garrett College network and its related technology understand the importance of its data and systems. Garrett College is committed to protecting its employees, partners, and the organization from illegal or damaging actions by individuals, either knowingly or unknowingly. Inappropriate use exposes Garrett College to risks including virus attacks, compromise of network systems and services, and legal issues.

POLICY:

Network related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts, electronic mail, web browsing, file transfer protocol, phones, and IP telephony systems are the property of Garrett College. These systems are to be used for ***business purposes*** **only** in serving the interests of Garrett College, and of our clients in the course of normal operations. Data includes all digital data stored on Garrett College network related systems as defined above.

Effective security is a team effort involving the participation and support of every Garrett College employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and to conduct their activities accordingly.

Scope

This policy applies to **ALL** authorized users which include employees, contractors, consultants, temporary workers, and other workers at Garrett College, including all personnel affiliated with third parties. This policy applies to all equipment, software, and systems owned or leased by Garrett College and to personal equipment, software, and systems brought into Garrett College by employees or others, as above. Third parties are required to sign a third party vendor agreement of usage for Garrett College assets.

PROCEDURES:

General Use and Ownership

1. All data that is stored within the Garrett College network environment is the property of Garrett College; management has access rights and ownership of this data and the right to access and monitor this data.
2. Certain individuals within Garrett College are authorized to monitor equipment, systems, and network traffic at any time.

Security and Proprietary Information

1. Much of the data used on the network by authorized users at Garrett College is confidential. Examples of confidential information include but are not limited to: details of student or employee names, addresses, personal identifiers (social security numbers, bank account numbers, driver licenses). If you are unsure if data is confidential, the Garrett College default is that you treat it as confidential data until you can get clarification from a supervisor.

   All authorized users must comply with local, state, and federal regulations on the use and protection of data. If you are unsure, treat the information as confidential until clarification has been sought.
2. Passwords are to be kept secure at all times. Sharing passwords is a violation of this policy and users doing do are subject to disciplinary action. Under no circumstances should you ever give your password to another person. Garrett College authorized personnel will never ask for an authorized user's passwords. If you feel you are being pressured to give your password to someone, contact your supervisor immediately. User level passwords are required to be changed every ninety (90) days.
3. All desktop computers, notebook computers, and workstations will be secured with a password- protected screensaver with the automatic activation feature set at fifteen minutes.
4. Personal devices including but not limited to cell phones, tablets, personal computers, and wireless access points may not be used to access the Garrett College network unless approved by the Garrett College Information Technology Department. Failure to comply can lead to disciplinary action, including termination.
5. Authorized users must use caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
6. Authorized users should be aware of 'phishing' attempts to extract confidential

information and should report any concerns of this type of attempted security hacking to the IT department. (Phishing is the act of tricking someone into giving them confidential information or tricking them into doing something that they normally wouldn't do or shouldn't do. For example: Sending an e-mail to a user falsely claiming to be an established security expert in an attempt to scam the user into surrendering a password).

7. Garrett College is bound by its contractual and license agreements respecting certain third party resources; users are expected to comply with all such agreements when using such resources.

8. Garrett College reserves the right to access and review such information under certain conditions. These include: investigating performance deviations and system problems (with reasonable cause), determining if an individual is in violation of this policy, or, as may be necessary, to ensure that Garrett College is not subject to claims of institutional misconduct. Such access may include, but is not limited to, access to user e-mail accounts (both professional and personal), access to user social media accounts, and access to personal files that may be stored on a user's device, regardless of whether that device is owned by Garrett College or by the user. Access to files on Garrett College-owned equipment or information will only be approved by specific personnel when there is a valid reason to access those files. Authority to access user files can only come from the Chief Information Officer in conjunction with requests and/or approvals from senior members of Garrett College management. Law enforcement agencies may request access to files through valid subpoenas and other legally binding requests. Information obtained in this manner can be admissible in legal proceedings.

Unacceptable Actions

The following activities are prohibited, unless expressly exempted with written authorization obtained from the Chief Information Officer at Garrett College. The categories below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

1. Any activity that is illegal under local, state, federal, or international law while using Garrett College owned resources.
2. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Garrett College.
3. Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4. Revealing your account password to others or allowing use of your account by others.
5. Using Garrett College computers, systems, software, servers, or any other asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction. This includes sites that contain sexual content, inappropriate racial or religious material, or political materials. Garrett College may monitor internet usage for these activities.
6. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the authorized user is not an intended recipient or logging into a server or account that the authorized user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, using peer to peer software (for example, LimeWire or BitTorrents). If an authorized user has any doubts about issues of this sort, he or she should consult the Chief Information Officer.
7. Executing any form of network monitoring which will intercept data not intended for the authorized user, unless this activity is a part of the authorized user's normal job or within the scope of the authorized user's authority.
8. Providing information about, or lists of, Garrett College employees or students to parties outside Garrett College without authorization (see *Public Information Policy*).
9. Any unauthorized copying of data from the network. This is considered a security breach and Garrett College will prosecute a violation to the utmost of its organizational policies as well as local, state and federal laws.
10. Authorized users are forbidden to transmit by e-mail or other electronic means any non-public information to external sources (including cell phones and similar devices), without express permission from the responsible Dean and the Chief Information Officer. This is to ensure that security is reviewed prior to transmission in accordance with the College's approved process.

    Non-public information includes (but is not limited to) individual names, birthdates, social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers. Such information could harm an individual if it was lost or stolen. This is also a violation of a number of regulatory areas that apply to Garrett College.

    Garrett College has an encryption tool to encrypt email to outside parties. Authorized users are encouraged to use this tool for non-public information.

Enforcement

Any authorized user found to have intentionally violated the above policy and related procedures may be subject to disciplinary action, up to and including termination of employment.

Acknowledgement:

Each new employee will be required to read the Acceptable Use Policy and related procedures and sign an acknowledgement form located on the IT (Information Technology) Internal/Intranet Departmental page. For questions, please call the IT Help Desk at Ext. 3027.