H-190 COMPUTER, NETWORKING, AND INFORMATION RESOURCES

INTRODUCTION

1. The H-190 policy set constitutes Gateway Technical College's (Gateway or College) policy for the management of the College's computing, networking, and information resources. These resources include, but are not limited to, the central computing facilities, District-wide network, campus local area networks, email, nodal labs, classroom multimedia equipment, video conferencing equipment, access to the Internet, wireless access, voice mail, departmental and public computing facilities, scanners, printers, My Gateway, Self-Service, the learning management system (LMS), software, data, and related equipment and services.
2. Your use of Gateway computing and networking resources and information systems is governed by federal and state law; all Gateway policies; and the Employee and/or Student Handbook.
3. **Your use of any of the College's computing, networking, and information resources constitutes your acceptance of this policy set.**

POLICY STATEMENT

1. Gateway provides computing and networking facilities and information resources to support its mission. These facilities include computer labs, communications networks, information systems and associated software, files, and data. Your access to and use of Gateway computing and network resources is a privilege that depends on your using the resources appropriately. In general, appropriate use means respecting the rights of other users, the integrity of the physical equipment and systems, and following all pertinent license and contractual agreements.
2. Users do not own their college-provided accounts, including, but not limited to accounts in the following types of systems: email, Learning Management System (LMS), data-storage, student information systems. Users are provided temporary access/use of these systems for College purposes only.
3. Faculty, staff, and students may use the College's computing and networking resources for College purposes related to their studies, their responsibilities for providing instruction and performing research, the discharge of their duties as employees, their official business with the College, and other Gateway-sanctioned or authorized activities. In addition, residents of the District who have library cards may use computers in the public areas of Gateway libraries subject to compliance with all other rules and policies. The use of College computing and networking resources and information systems for any sort of solicitation is prohibited, absent prior written permission of a current officer of the College.
4. Computing resources may be used only for legal purposes and may not be used for any of the following purposes or any other purpose which is illegal, immoral, unethical, dishonest, damaging to the reputation of the College, inconsistent with the mission of the College, or likely to subject the College to liability. Impermissible uses (some of which may also constitute illegal uses) include, but are not limited to, the following:
    a. sending messages with the intent to frighten, intimidate, threaten, abuse or harass another person;
    b. intentionally and without authorization:
        1) accessing, modifying, destroying, taking possession of, distributing, or copying data, computer programs or supporting documentation;
        2) disclosing restricted access codes or other restricted access information to unauthorized persons;
        3) modifying computer equipment;
        4) destroying or damaging a computer, computer system, or computer network;
    c. disruption or unauthorized monitoring of electronic communications;

d. unauthorized copying or transmission of copyright protected material;
e. unauthorized attempts to break into Gateway systems, networks, accounts or uncover security loopholes. This includes creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data.
f. using Gateway systems or networks as any part of an attempt to break into or attempt to break into other systems or networks;
g. Installing unauthorized software of any kind.
h. use of identification numbers, user names, and/or authentication assigned to others;
i. use which constitutes academic dishonesty;
j. violation of software license agreements, network usage policies, and regulations;
k. accessing, displaying, storing or sending obscene, pornographic, sexually explicit, or offensive material;
l. using any obscene, lewd or profane language or suggesting any lewd or lascivious act;
m. intentional or negligent distribution of destructive programs such as computer viruses;
n. use that is deemed unnecessary or excessive; use which facilitates violating other Gateway policies; and use which interferes or disrupts Gateway employees from performing their jobs.

ACCOUNT GUIDELINES

1. Once you are given access to computing resources at Gateway, you are responsible for any and all use made of those resources with your user identification. The following responsibilities apply to users accessing any of the College's computer and networking resources and information systems. The user is responsible for correct and sufficient use of the tools available for maintaining the security of information stored on each computer system.
   a. Computer accounts, usernames, passwords, and other types of authorization that are assigned to individual users may not be shared with others.
   b. The user should assign an obscure account password.
   c. No unauthorized persons may use Gateway computer and network resources. Authorized users include only Gateway employees, currently enrolled students, and residents of the District who have obtained library cards.
2. Be sensitive to the needs of others, and use only your fair share of computing resources. Collegiality requires:
   a. regular deletion of unneeded files from one's accounts on shared computing resources;
   b. refraining from overuse of information storage space, printing facilities, or network services;
   c. refraining from use of sounds and visuals which might be disruptive to others in the area;
   d. refraining from use of computing resources in an irresponsible manner
3. All employees who become aware of or suspect a data breach or other misuse of protected College data must immediately report this to the CIRT (Cyber Incident Response Team), Tech Central, or Human Resources.

ROLE OF THE LEARNING INNOVATION DIVISION

1. Responsible system maintenance may require that files be backed up, data cached, activity logs kept, and overall system activity monitored. In the process of these activities, Gateway staff may see your digital activities and files. The College may also have access to and may

monitor non-Gateway computer and network activity when used by Gateway employees in the course of their official duties.

2. An account may also be inspected or monitored when:
   a. Activity from an account prevents access to the College's computing or networking resources by others.
   b. Activity from an account is disrupting or threatening the integrity and/or security of the network or network systems.
   c. General usage patterns indicate that an account may be responsible for illegal activity.
   d. LID receives reports of alleged law or policy violations.
   e. It appears necessary to do so to protect Gateway from possible legal liability.
   f. It is required by and consistent with law.
3. Whenever evidence of criminal activity is discovered, Gateway will provide the evidence of such activity to law enforcement officials in accordance with state and federal statutes.

SANCTIONS FOR TECHNOLOGY POLICY VIOLATIONS

Sanctions apply to the following computer and network use policies:

a. D-110 - Telephone Usage
b. H-190 - Computer, Networking & Information Resources
c. H-190a - Learning Innovation Division: Information Security & Confidentiality Policy
d. H-190b - Digital Communications
e. H-190c - Technology Procurement
f. H-190d - Data Security Policy
g. H-190e - System Access, Identification, and Authentication Policy
h. H-190f - Local and Remote Systems Protection Policy
i. H-190g - Information Security Incident Management
j. H-199 - Printing and Photocopying Policy

1. Violations of Gateway technology or security policy may result in disciplinary actions or the loss of privileges, including but not limited to, loss of access to computing resources as well as to Gateway disciplinary action up to and including termination and/or legal action.
2. Any offense that violates federal, state and/or local laws may result in the immediate loss of all Gateway computing privileges and will be referred to appropriate Gateway administrators and/or law enforcement authorities.
3. If Gateway Learning Innovation Division staff has evidence of misuse of technology systems, resources, or policy violations through a specific account, they will take the following steps to protect the systems, networks, and the user community:
   a. The suspected accounts will be suspended immediately pending the outcome of any investigation.
   b. The user's account files, digital storage, and/or other data and computer accessible storage media associated with the account will be inspected for evidence.
   c. Investigation of a student will be reported to the Student Success Division, and investigation of a faculty or staff member will be reported to that individual's supervisor when appropriate.

d. Any violation will be reported to the appropriate authorities:
    1. Policy violations by a faculty or staff member will be reported to the individual's supervisor and to the Human Resources Department.
    2. Policy violations by a student will be reported to the campus dean and the executive vice-president/provost.
    3. Policy violations by any other user will be reported to the campus dean and the executive vice president/provost.
    4. Illegal activity by a faculty or staff member, student, or District resident will be reported to the police and other appropriate law enforcement officials.

DATA SECURITY AND INTEGRITY

1. Gateway provides reasonable security against intrusion and damage to files stored on college-provided storage services. In the event that data have been corrupted as a result of suspected intrusion or malicious action, you must contact the Cyber Incident Response Team (CIRT) immediately at CIRT@gtc.edu.
2. Gateway provides limited backups for approved college-provided network/cloud storage options and may attempt to retrieve files specified by users and recover files after accidental loss of data on its storage services. However, Gateway cannot be held accountable for unauthorized access by other users and is not liable for the inadvertent or unavoidable loss or disclosure of the contents of stored files.
3. Gateway requires the use of college-provided network/cloud storage options for files typically stored on a laptop, desktop, or other mobile device. Users are responsible for storing data in the appropriate location.
    - Gateway recommends that students back up their own data on a regular basis
    - Gateway is not responsible for backup or any lost student data.

4. Employees must store important data on Gateway-provided storage services. Backups are not performed on Gateway endpoints/computers provided to faculty and staff.