GNTC Acceptable Computer Use Guidelines

Revision 2.1

The following serves as clarification of the Technical College System of Georgia procedure 'Acceptable Computer and Internet Use' as it applies to computer use on Georgia Northwestern Technical College campuses. GNTC does not attempt to articulate all required or unacceptable behavior by its users. Therefore, each user's judgment regarding appropriate use must be relied upon. To assist in such judgment, and assure adherence to TCSG policies as well as applicable federal and state laws, the following guidelines have been created, and must be followed by all GNTC faculty, staff, students, and guests.

General Definitions

PII – **Personally Identifiable Information** – Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, student ID number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

CUI – **Controlled Unclassified Information** – A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. (e.g., health information, student records, employment records, credit card information, etc.)

Account Credentials – Generally refers to the combination of username and password used to identify you within a computer system and gain access to permitted resources. May also include another authentication 'factor' (i.e. something you own) to increase security. This constitutes MFA, or Multifactor Authentication

DBA – **Database Administrator** – GNTC employee charged with oversight and administration of databases.

MFA – **Multifactor Authentication** – Account credentials which include another authentication "factor" besides username and password. This generally involves some other device that you own (cell phone, security token, etc.) in order to increase authentication security.

1. Account Security

1.1 Users are responsible for the proper and secure use of their accounts.

1.1.2 Proper and secure use of your account **prohibits**:

a. Providing someone else (friend, family, co-worker, student, etc.) access to, or use of, your account credentials.
b. Obtaining or using another user's account credentials for login or access.
c. Storing your username/password in an unsecure location (unlocked drawer, sticky note on desk, etc.).

d. Giving out your password via email or unsolicited phone call. GNTC faculty/staff should never ask for your username/password over the phone or via email.

1.1.3 Proper and secure use of your account **requires**:

a. That you store written passwords in a locked or otherwise secured location.
b. That you maintain backups of your data and utilize encrypted storage devices if PII/CUI is to be stored.
c. That you logoff or lock the computer you are using before leaving it unattended…even briefly.
d. That you be vigilant for possible "shoulder surfing" from bystanders who might see PII displayed on your screen.

1.2 Users must remain informed and vigilant regarding cybersecurity threats aimed at fraudulently acquiring personal information, data, or account credentials

1.2.1 Phishing attacks are generally fraudulent emails that appear to be from a reputable company, friend, or family member. However, the email's true purpose is to trick individuals into revealing personal information, account credentials, credit card numbers, etc. In many cases, the links contained in the email may look legitimate, but attempt to install malicious software code on your system, or even other systems throughout your business, college, or home.

Guidelines for recognizing phishing emails:

- Is this an email that you are expecting? If not, then be at maximum alert level!
- Inspect the 'From:' email address very carefully. Make sure the address contains the **real domain** of the company and the spelling is correct.
- Hover over any links in the email to see the actual URL to which they point. Is the URL correct and as expected?
- Do not click any links in an email unless you are 100% sure that the URL is legitimate.
- Always hover over a displayed link to make sure the actual URL matches the displayed link. Be careful of URL spelling, which may be similar, but different from the actual domain URL. (example: fristbank.com instead of firstbank.com)
- It is always safest to just open a new browser window and directly navigate to the company's website.
- If you are just not sure if an email is fraudulent, then call the person or company that the email appears to be from in order to verify they actually sent the email.

1.2.2 Similar types of fraudulent phishing activities include: Smishing – a phishing attack conducted over SMS (text messaging); and Vishing – a phishing attack conducted using voice phone calls.

2 Access

2.1 GNTC computer systems are available and accessible for use in research and education by the faculty, staff, and students of the college during normal operational hours.

2.2 The GNTC Information Security Administrator will determine authorized access levels to specific resources for GNTC employees. Access for Banner system users will be determined by the associated GNTC Banner Data Steward, and submitted to the GNTC DBA for review and implementation.

2.3 Faculty, staff, or student connection of any device to a physical network port on any GNTC campus is prohibited without prior written authorization from the GNTC Information Security Administrator

2.4 Use of classroom, lab, or lecture hall presentation (lectern) computers is limited to the following:

- GNTC employees who possess a valid login username
- Authorized guests where access has been previously requested using the GNTC support system by an employee in good standing. If approved, temporary login credentials will be provided

after the authorized guest agrees to adhere to all TCSG and GNTC Acceptable Computer Use guidelines by signing/dating the latest revision of this document.

- Instructor supervised students who use the classroom computer system for the purpose of in-class presentations. In this scenario, the following requirements must be met:
  - ✓ An account must be created for temporary student use in advance. This account must be requested using the authorized guest procedures above.
  - ✓ No removable media storage is allowed. (USB drives, external hard drives, etc.) The student must access any files required using Microsoft OneDrive cloud storage.
  - ✓ Alternatively, the student may bring their own laptop, notebook, etc., and connect only to A/V equipment in the room using supplied connectors. Any required network connectivity for the student owned device must use GNTC wireless or a cellular data network.

2.5 Perspective students, visitors, GNTC students, faculty, and staff are permitted to connect via wireless to the GNTC Guest SSID. This is an unencrypted wireless network, so it is imperative that no PII be transmitted using this network. All other wireless networks require some form of authentication in order to connect.

3 Protection of PII/CUI

3.1 Information meeting the definition of PII or CUI must always be kept private and secure.

3.2 PII or CUI must never be transmitted electronically between GNTC and external entities without the use of industry standard encryption techniques. If you have any doubts regarding how to safely transmit protected information, please contact Technology Services.

3.3 GNTC owned data should never be sent and/or stored on any cloud-based or physical system (email, Dropbox, laptop, etc.) not owned and/or managed by GNTC or TCSG.

3.4 Information not intended for public dissemination (includes, but not limited to PII/CUI) that is stored on any type of portable media or computing device at a minimum must be encrypted using a current industry standard encryption algorithm. This includes, but is not limited to, information stored on laptops, notebooks, disk drives, smartphones, DVDs, USB drives, etc.

3.5 PII/CUI must always be encrypted when emailing to a non-GNTC or TCSG email address. For GNTC employees, this can be done from the GNTC email system by using the [encrypt] keyword in the subject of the email.

3.6 Text messaging (SMS) of PII or CUI is prohibited.

4 Software and Copyrighted Material

4.1 All users of GNTC computer systems are required to follow established and applicable copyright laws. Unauthorized downloading, reproduction, and/or distribution of licensed materials is prohibited without proper authorization from the author or creator. Downloading or uploading substantial parts of a copyrighted work without authorization may constitute a violation of U.S. copyright laws.

4.2 GNTC blocks Peer-to-Peer file sharing on the web content filter in compliance with the Higher Education Opportunity Act. (HEOA) and TCSG Security Guidelines.

4.3 Any software being considered for purchase by any department, division, or GNTC employee must be evaluated by Technology Services for resources required, security ramifications, potential impacts, etc. **prior** to submission of a request for purchase (RFP). This software evaluation process must be initiated by a support request using the GNTC support system.

4.4 For the installation and configuration of GNTC purchased software, faculty/staff must submit a request using the GNTC support system. Software install requests must be submitted at least 10 working days prior to the date the software is needed. The Department of Technology Services may also work with faculty/staff regarding emergency installations. However, such accommodations may not be possible due to previous commitments and priorities.

4.5 Use of, and/or installation of, any personally owned or acquired software on GNTC computers is prohibited.

5 Computer System Integrity

5.1 GNTC faculty, staff, students, or guests must not install or otherwise modify device hardware and related configurations on any GNTC owned compute device. (e.g.; desktops, laptops, tablets, etc.)

5.2 Food or drink may be restricted in student lab areas. Specific lab policies will apply. Check the specific policies posted in the lab area.

5.3 GNTC Technology Services must initially configure all GNTC owned laptop/notebook and similar devices in order to meet appropriate technical and security specifications.

5.4 Assigned users of GNTC laptops/notebooks must schedule a support session (using the GNTC support system) every 90 days in order to scan and update the device's security configuration.

6 Internet Access

6.1 Internet access is available for all GNTC employees and students for instructional and other uses consistent with the GNTC mission statement.

6.2 Occasional personal use of Internet connectivity and/or email is permitted. Such use should be brief, infrequent, and shall not interfere with the user's performance, duties, or responsibilities.

6.3 For security purposes, all Internet access from GNTC is subject to various access rules and restrictions. These restrictions protect the security and integrity of GNTC data and systems. If a user at GNTC is denied access to a vital Internet site or service due to these access restrictions, the GNTC Information Security Administrator or designee will evaluate the access requested and make every effort to allow the access. However, if the Information Security Administrator determines that the requested access poses a significant risk to resources, security, or the integrity of GNTC systems or users, then the access request will be denied.

6.4 Internet information accessed from GNTC campuses is filtered for content based on TCSG guidelines. GNTC is not responsible for discriminatory, offensive, sexually explicit, or other material which may circumvent filter settings. If filter rules block legitimate, necessary content from entering the campus, the department of Technology Services will make every effort to allow the needed content without compromising overall filter functionality and GNTC resources, security, or integrity of GNTC systems or users.

7 Email and O365 Guidelines

7.1 GNTC (per TCSG requirements) archives all employee email for a period of 5 years.

7.2 Employees of GNTC are not to use wide scale distribution lists such as ALL_GNTC, WCC_GNTC, FCC_GNTC, etc. to send emails containing any information, pictures, or other content not **directly** related to GNTC college goals or mission statements.

7.3 The appropriateness of '**Reply All**' when responding to an email must be considered **carefully** on a case-by-case basis. 'Reply All' can interrupt the workflow for unnecessary recipients, and more importantly, possibly expose PII, CUI, or other private information to unintended recipients!

7.4 All college business and instructional email correspondence must utilize GNTC provided email systems.

7.5 The use of Microsoft OneDrive is encouraged for all faculty, staff, and students. However, security of all information on OneDrive is the responsibility of the user. Please see the 'GNTC OneDrive Security Recommendations' link below for further information and guidance.

8 Additional Computer Security Policy and User Resources:

- Technical College System of Georgia Acceptable Computer and Internet Use Procedure
- GNTC OneDrive Security Recommendations

Important: If you are viewing a printed copy of these guidelines, it may not be the most current version. The most current revision can be found on the GNTC website.

GNTC does not discriminate on the basis of race, color, creed, national or ethnic origin, gender, religion, disability, age, political affiliation or belief, veteran status, or citizenship status (except in those special circumstances permitted or mandated by law).