It is **important** that all GNTC employees read and understand the complete GNTC Acceptable Computer Use Guidelines**.**

Here Are Some Key Points from the Guidelines

Security:

- Never allow anyone else to use a computer while logged into your account!
- Protect passwords.
- Store them on your person or in a locked and secure location.
- Do not share passwords with anyone.
- Never give out your password via email or unsolicited phone call. GNTC Technology Services personnel will never ask for your password over the phone or in email.

Access:

- Attachment of any computer to any network port at GNTC is not permitted without prior inspection by Technology Services.
- Lock your computer using [Windows Key + L] anytime you step away.

Software:

- All GNTC employees must adhere to copyright laws and license agreements.
- Requests to install software in a computer lab should be submitted through the support system a minimum of 10 days prior to the beginning of the semester.

System Integrity:

- Changing desktop computer configurations is prohibited.
- Laptop users have additional responsibilities including performing Windows Updates regularly, Updating anti-virus, anti-spyware, and other software regularly.
- Users are responsible for backing up their critical documents. The backups must be encrypted or stored in a locked and secure location.

Email:

- All employee email is archived per TCSG policy for a period of 5 years.
- GNTC distribution lists should only be used to send content directly related to GNTC college goals and mission.
- All business email correspondence with faculty, staff, and students must utilize GNTC provided email systems.

GEORGIA
NORTHWESTERN
TECHNICAL COLLEGE

Focused on **Security**
Committed to Success

GNTC Information Security Quick Reference

IT Works for You!

Strong Passwords

- Passwords Establish Identity - Passwords are crucial with information security because they establish your identity. If someone else can guess or steal your password, then they become YOU on the electronic systems! ALWAYS use the [Windows Key + L] to lock your computer every time you step away.

- Use Strong Passwords - We all know that good passwords require a mix of upper and lower case combined with numbers and symbols when possible. If you think these types of passwords are difficult to remember, then consider that you can make them easier using a few tactics. Consider using the first letters from a song verse or movie line, then add some numbers/symbols. Fmd,Idgad27 looks like a very difficult to remember password until you know the line from which it was taken: “Frankly my dear, I don’t give a darn.” The numbers added could have some other significance such as a couple of digits from your driver’s license, favorite football player number, etc.

- Password Protection - Never share your password with others. If you suspect someone else may know your password, then change your password IMMEDIATELY. Never write passwords down and try to hide them around your computer. If you write them down, then store them in a safe place such as where you keep your driver’s license or Social Security card.

Email

- GNTC Email - All emails at GNTC are scanned for viruses, spam score, and known exploits. All emails are archived per established TCSG guidelines. See the GNTC Acceptable Computer Use Guidelines

- Phishing and Social Engineering - Beware of phishing emails that try to play on your emotions, wants, or needs to trick you into either installing malicious software, or entering sensitive information such as your login credentials, SS#, credit card #, etc. Examples can be found on the Technology Services intranet site.

Malware

Def.: Malicious software or code designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems.

How Malware Gets Onto Your Computer

- Email Attachment or Link - Prevent by not opening any attachment from someone you don’t know, or from someone that you are not expecting an attachment from.

- “Free” Software - Before you download software of any type, consider the source. Is this a site you should trust? If you aren’t 100-percent certain, do some research on Google.

  Never trust a web page advertisement for free software, especially free antivirus software – it is probably spyware itself. Spyware is software that records and sends off information about you and what you’re doing on your computer.

  Avoid clicking on ads, even at trusted sites – they aren’t always safe. Often ad space is sold to one party, then resold to a second and third party. In the end, the legitimacy of a site does not vouch for the legitimacy of an ad.

- Infected Devices - Malware is commonly spread by devices you plug into your computer’s USB port. The most common culprit is thumb drives (aka flash drives or memory sticks). However other devices such as external hard disks, cameras, cell phones, etc. can also infect your computer.

  If you find a thumb drive lying around, NEVER take it back to your office computer and plug it in to see what’s on it. Go to a computer lab, unplug the network cable from the computer, then plug it in and investigate. Reboot the computer when you’re done and re-plug the network cable.