Welcome to Information Security Training

Welcome to Georgia Perimeter College’s Information Security Training. Information security consists of processes, measures, and technologies employed to protect valuable GPC and student information from unauthorized modification, use, destruction, or disclosure, whether accidental or deliberate.

Information security is necessary to:

- Protect student, employee, and other valuable or sensitive College information
- Maintain customer confidence
- Protect reputation, image, and competitive advantage of the College
- Comply with regulatory and legal requirements
- Support GPC’s strategic mission and goals

As GPC employees, we are required to comply with the approved information security policies, procedures, practices, and measures. Failure to comply can result in disciplinary action up to employment termination and legal prosecution.
About This Training

The purpose of this training is to give you the information you need to learn and adhere to GPC’s information security policies, procedures, and practices. You will learn about the following elements of information security:

- Protecting Data
- Computer Security
- Password Security
- Email Security
- Internet and Web Security
- Malware Protection
- Social Engineering Security
- Physical Security

Remember - you are the key to information security. Throughout the training, you will see the icon to the left. The key indicates actions you are expected to take to comply with GPC’s information security policies.
Protecting Data

Data must be protected to prevent negative impact on GPC, our employees and students, and to comply with legal and regulatory requirements.

GPC data is classified according to level of sensitivity or confidentiality, and level of security that is required:

- **Public Data**
  Information that if made widely available inside and even outside the College, has no detrimental impact on the College. Public information has no security restrictions or markings to indicate a sensitive nature.

- **Internal Use Only**
  Data that if inappropriately disclosed or accessed could negatively impact the effectiveness of GPC’s operation, expose the College to civil liability, or result in damage to reputation and public confidence. Reasonable security must be used.

- **Restricted**
  Data that if inappropriately disclosed, accessed, or used could have substantial negative impact on the College including fines or other sanctions for non-compliance with laws and regulations, significant damage to the College’s reputation and public confidence, and critical disruption of College services. Restricted information requires the highest degree of protection.

Restricted information includes passwords and PINs, Social Security Numbers, credit card and financial account numbers, credit check information, FERPA-protected student information, individual medical information, driver’s license numbers, any personally identifiable information (any combination of data elements that allow a person to be individually identified), and any data required by law or regulation to be protected in this manner.

- Always know the classification of the data you’re handling or accessing.
- Never send Restricted data through email or any unencrypted channel.
- Do not store Restricted data on your workstation or on any mobile device (flash drive, smart phone, etc.).
- Always dispose of hard copies of Internal Use Only and Restricted information by shredding.
- Dispose of electronic copies of Restricted information by completely erasing the data with approved software (more than just deleting). Contact OIT Service Desk for assistance.
- Keep hard copies of Restricted information under lock and key.
- Do not share Restricted information with others except based strictly on need to know.
**Question:**
True or False – You are working in financial aid, reviewing a printed report containing student credit scores and Social Security Numbers. You need to break for lunch, so you put the report under some other papers where it is not readily visible. This is an acceptable way to handle the document.

**Answer:**
False. The information in the report is classified Restricted and must be locked in a cabinet or drawer when not being used.
Computer Security

Computer security refers to the protection of valuable GPC and student information that may be stored on your computer. It is your responsibility to protect this information whether you are in or out of the office, on or off campus, or at home.

While you are at the office:

- Always lock your desktop or laptop screen (Ctrl+Alt+Del) when you leave your work area.
- Lock your laptop with a cable lock when you are going to be away from your desk for an extended amount of time.

While you are away from the office:

- Never leave your laptop unattended while in public places such as a restaurant or airplane, or on the seat of a car.
- Lock up your laptop when it is not in use.

Security is set up on all GPC workstations and laptops. To ensure security is maintained:

- Do not modify any security settings on your computer.
- Contact the OIT Service Desk for assistance with all software and hardware installations.
- Do not store sensitive information on your computer unless absolutely necessary.
- Consider using encryption to protect sensitive information that you must keep on your computer (contact the OIT Service Desk for assistance).

**Question:**
True or False – If you work in an office that has several GPC employees in close proximity, you can leave your desktop or laptop screen unlocked while you attend a short meeting in a conference room around the corner.

**Answer:**
False. You should always lock the screen on your workstation, using Ctrl+Alt+Del, when you leave your work area.
Password Security

Passwords are used to authenticate the identity of an individual. You are responsible for all activity performed on GPC computers and networks under your login ID and password.

- Never share your password or ID.
- Change your password at least every 90 days, more often if you deal with sensitive information.
- Choose a strong, secure password.

Keep the following in mind while creating your password:

- Passwords must be at least eight characters long.
- Passwords must be a combination of alphabetic and numeric characters:
  - Upper case letters (A-Z)
  - Lower case letters (a-z)
  - Numbers (0-9)
- Special characters should be used whenever possible (for example*&^$#@!)

Do not create a password that can be easily guessed. The following should not be used:

- Names of pets
- Words directly out of the dictionary
- Familiar names (sport teams, fictional characters, product names)
- Your login name in any form (as is, reversed, capitalized, etc.)
- Any part or variation of your name, including initials, aliases, or nicknames
- Anything with dates (birthday month and year, anniversaries, relatives' birthdates)

What should I do if someone asks for my password?
Immediately report the incident to your manager or the OIT Service Desk.

Question:
Which of the following would be considered acceptable passwords for Joseph Smith?
SmithJ22
Cs042201
Goheels41
c2J6*45b

Answer:
C2J6*45b is an acceptable password. It is a random combination of alphabetic and numeric characters and includes special characters.
SmithJ22 is not an acceptable password because it is a variation of the employee's name.
Cs042201 is not an acceptable password because it includes a date.
Goheels41 is not acceptable because it includes a familiar name.
Email Security

GPC’s email system provides effective communication for its employees. Using it correctly is important to maintaining appropriate protection of our data and network.

GPC’s email system is the official means for the College to communicate with faculty and staff for everything except highly confidential data. Similarly, the GPC-provided email system for students is the official means to communicate with students for everything except highly confidential data.

Unless you arrange with GPC’s OIT group to implement encryption on all your email, it is not secure enough to send highly sensitive information. Highly sensitive information includes legally-protected student information, personally identifiable information (e.g., SSN, driver’s license numbers, financial account numbers), passwords or PINs, credit card numbers, and protected health information.

You should not expect privacy in emails. All information stored, processed, or transmitted using GPC’s email system is subject to inspection or monitoring as needed to address any security or technical issues.

- Do not modify the security setting within your Outlook profile.
- Do not send any highly sensitive GPC information via email.
- Do not transmit or receive statements that contain any material that is offensive, slanderous, or threatening.
- Do not use the email system as a record retention vehicle.
- Do not open suspicious email.
- Do not reply to unsolicited emails.

What should I do if I think a security violation involving my email account has occurred?
If you find evidence regarding a security violation involving your email account, report the security problem immediately to your manager or the OIT Service Desk.
Internet/Web Security

The Internet/Web is another area of information security risk. You should always be aware of protecting sensitive GPC information while working on the Web.

Security risks on the Internet include malware, identity theft, theft of other sensitive data, and phishing and fraud scams.

GPC employees must ensure that any Internet surfing or activities in which they engage do not interfere with their job responsibilities.

- Do not post any sensitive GPC information on any Web site, mailing list, news group, blog, or social networking site.
- Do not give the impression of representing GPC in any Internet communications (e.g., blogs, social networking sites) unless you are authorized to do so.
- Never respond to spam or unauthorized requests for sensitive information.
- Do not download software or freeware (contact the OIT Service Desk for assistance).
- Avoid use of peer-to-peer file sharing (or use it very carefully) to not violate copyright laws.
Malware Protection

Malware refers to several types of malicious software which usually have destructive or criminal intent. Malware today can be used in identity theft, theft of any sensitive or valuable information, keystroke logging, uploading/downloading/deletion/insertion of files, interruption of service, and to spy on users. McAfee is GPC's anti-malware solution for desktops and laptops.

Malware generally consists of the following types:

- **Virus**
  A virus is unauthorized software usually disguised as something else that causes an unexpected and undesirable event, and often automatically spreads to other computers.

- **Worm**
  A worm is a self-replicating virus that usually resides in active memory and duplicates itself. Worms use parts of operating systems that are automatic and invisible to the user.

- **Trojan**
  A trojan is malware that appears to perform a desirable function but in fact performs undisclosed malicious functions, allowing hackers unauthorized access to the computer.

- **Spyware**
  Spyware is a program that monitors and gathers information about a system, a user, or the user’s actions, including logging or capturing the user’s keystrokes.

Malware can enter computers from many different points:

- Infected email attachments and links
- Peer-to-peer file sharing
- Internet downloads
- Free and shared software
- Instant messaging

Symptoms of a virus include:

- Odd behavior, frequent crashes
- Sluggish system performance
- Browser and system preferences changed to settings you didn't select
- Pop-ups that are unrelated to the sites you normally visit
- Applications on your machine that you did not install yourself
- Additional browser toolbars appear

- Run a scheduled anti-virus scan at least once a week.
- Don't open suspicious emails.
- Don't open attachments if you don't know the sender.
What should I do if I think my computer is infected with a virus?
Don't panic. Immediately call the OIT Service Desk for assistance. Don't shut down your system and don't delete any files or programs.
Social Engineering Security

Social engineering is the method of obtaining unauthorized access to information or a system by deceiving someone.

Social engineering can be orchestrated using many different approaches:

- Impersonating or imitating someone of authority.
- Requesting confidential or personal information on-line.
- Using flattery (ingratiation).
- Befriending people. This approach is used most often.

Phishing, requesting confidential or personal information on-line while impersonating someone of authority, is one of the most common types of social engineering being used today. Emails containing official-looking forms and documents are often used to convince users that the request for confidential information is legitimate (e.g., from sources claiming to be a bank).

What should I do if I think an inappropriate request for sensitive information has been made?
These requests may be made in person, by telephone, email, or the Web. Immediately report any such incident to your manager or the OIT Service Desk.

**Question:**
You are attending the Educause annual convention and are talking to a potential vendor. He explains that in order for him to better answer your questions, he needs to know more details about how you store student data. How should you respond to his request?

**Answer:**
Explain to the vendor that you are not at liberty to discuss confidential GPC information. If he needs additional information, you would be happy to give him the name of an appropriate GPC contact.
Physical Security

While on GPC campuses and office locations, be aware of the people around you and your environment. The following terms relate to physical security as it pertains to protecting information:

- **Tailgating**
  Occurs when an individual follows an employee into a secure location.

- **Office Creepers**
  Individuals who try to blend into the office environment in order to obtain information or goods.

- **Shoulder Surfing**
  Occurs when an individual looks over your shoulder while you enter your password. Be aware of who is in your area while typing in your password.

- **Dumpster Diving**
  Snooping through your trash. An person dumpster dives to obtain confidential information. Shred all confidential documents before discarding them.

- Shred all confidential documents before throwing them away.
- Do not write your password down. Individuals will rummage through your desk to obtain information, including your password.
- Be aware of your surroundings and the people around you.
- Challenge people you don't recognize in your area and ask if you can be of assistance.

**Question:**
You are on your way out to lunch when a gentleman in a maintenance uniform tells you he needs to do some repairs in the men's restroom on the second floor, inside a secure area. You should:

A. Open the secure door for him and then leave for lunch.
B. Escort him to the men's restroom, watch him change the light bulb, then escort him out of the building.
C. Refer him to building security for access.

**Answer:**
C. Refer him to building security for access. Although the gentleman may look official, he may be using a blend of tailgating and office creeping to gain access to secure information.