IT510 * Module 4 Reading

Please read through this PDF, as it will introduce you to some of the requirements for the Module and help guide you in completing the Assessment. The last few pages should especially be helpful if you are a career-changer.

Part 1: Different Forms of Security

Physical Security

Unfortunately, many homes and businesses are not physically secure enough and may suffer computer-related losses. Physical security includes protection from the environment, disasters, theft, and vandalism.

Good practices can take the form of workplace rules such as locking computers before walking away from them and disallowing downloads from the Internet. Security cameras, good lighting, smoke detectors, locked doors with limited access, and keeping some equipment from the public eye are also good strategies, as are monitoring temperature and humidity, backing up data in a different location, and avoiding fire and flood hazards. In the home, simply putting away a laptop when you leave is an additional safety measure. Some critical thinking can assess a situation and provide more tactics.

Logical Security

Passwords are an important first security step! You have undoubtedly encountered rules about password length and using a combination of capital and small case letters, numbers, and certain characters. It is also important not to use dictionary words or personal identification that can be easy to guess (like your birthday, favorite colors, dog's name, or address). It is also crucial not to use the same password for multiple logins, because once a hacker learned the password, they would be able to get into all of these places.

Another rule to consider is whether or not to require new passwords at regular intervals. According to many security experts, the frequent changing of passwords often results in poor practices such as creating similar ones, using patterns, reusing the same passwords for several different logins, or reverting to the use of ordinary words. These all can make it easier for a hacker to gain access.

Biometrics can add another step to authentication. These are personal physical traits (and sometimes behavioral) that make each person unique, like thumbprints or retina scans.

You might like to investigate password managers if you have not done so previously. These are software programs that will store passwords, making it easier to have many different ones and to not rely on memory or writing them down elsewhere. Far too often, computer users write lists of passwords and leave them in notebooks, on sticky notes, on scraps of paper stored in a wallet or purse, or in easily opened documents. These practices leave the user open to password theft, which can then incur identity and financial losses.

Behavioral Security

If you took IT504, you worked on an Acceptable Use Policy. Behavioral security is setting rules for human behavior, which is impossible to fully control, but with policies, training, and clear consequences outlined, problems can be minimized.

While it is clear the above information is to help you understand the three areas of security you will analyze in one of the Assessment documents, there is one more behavioral activity to consider: As you write, remember not to violate the privacy and security of your workplace by identifying it by name. Use a false name or identify it in general terms ("a financial institution," for example).

Part 2: Additional Information

Email

Email can be sent internally or to people outside of the organization. Subject lines must be descriptive of the content contained in the email. A salutation and signature are crucial elements. When creating your email for the Assessment, use the format shown below.

Subject: Descriptive of Content

Dear recipient's name,

The first paragraph is brief and explains why you are writing the email.

Keep paragraphs short and focused. Single-space them, leaving a blank line between paragraphs and sections of the email for readability.

End with a brief conclusion, which may be a thank you or an indication that you will follow up with another email or phone call soon.

Your first and last names
Job title or company (if applicable to the email)

Example:

Subject: BYOD suggestion for the Alpaca Scout leaders

Dear Ms. Chen,

In reviewing your technology needs, it was noticed that a few Alpaca Scout leaders wondered if they could use their own tablets or laptops to complete some of the necessary documentation of scouting activities.

There are inherent risks in sharing data on personal devices, but this concept may be worth reviewing, as there is also the potential for financial savings. Some restrictions on the system and other regulations may limit the risks as well.

Let me know how you feel about investigating this possibility. I will call you soon to hear your thoughts and set up a meeting to discuss it further.

Sam Wayfair
Systems Analyst

Business Letters

Business letters might be used either internally or externally; their purpose is far more formal than either memos or email. Single-space the entire letter, leaving blank lines between parts as shown below, and align all content left without indenting.

Notably, the salutation is followed by a **colon** (commas are for informal messages). The most common closures are Yours, Yours truly, Sincerely, or Regards, but others are acceptable. Do not use abbreviations.

Your Name
Your Street Address
Your City, State, ZIP
Contact information (email and/or phone)

Date in a recognizable format

Recipient
Recipient's Company if applicable
Recipient's Street Address
Recipient's City, State, ZIP

< usually two blank lines before the salutation

Dear Recipient:

The first paragraph should get to the point of the letter quickly and clearly. Single-space paragraphs, and leave a blank line between them. Do not indent the first line of the paragraphs.

Start new paragraphs for new ideas. Keep paragraphs relatively short so they can be read quickly and efficiently.

In the last paragraph, thank the recipient for their consideration or at least for reading your message. If you need a response, request it here and include contact preference.

Closure line,

Your Name
Your Title (optional unless required by assignment instructions)

Example:

Kirsten Jones
111 Green Street
Springfield, AK 20998
mjones@WYK.com

August 2, 2021

Ruben Martinez
CEO, CQTR Industries
5000 Athens Drive
Springfield, AK 20996

Dear Mr. Martinez:

I would like to inquire if your newly designed modems are available for bulk purchase at this time. I am currently serving as a systems analyst for several companies, and have three clients in particular who may be interested.

Your modems were demonstrated at the recent device conference in Springfield. These devices are quite extraordinary in range, power, and longevity.

Thank you in advance for any information you can share. I can be reached at the above email address or at 888-441-2345 weekdays.

Respectfully yours,

Kirsten Jones
Systems Analyst for WYK, Inc.

Quiz

You are encouraged to take the non-graded quiz. In this module, the quiz covers testing, maintenance, auditing, and conversion concepts. The questions are all multiple choice (with just one potential answer) and true-false.

Getting Help

To find the Academic Success Center, look for My Studies > Academic Success Center from your home page (where your courses are listed, not inside this classroom). There you will find a plethora of information for writing, math, science, business, and technology. You can also connect with tutors. This is a free service for Purdue Global students; if you have not investigated it prior to this term, it is a good idea to check it out and see what great help is available.

* * * * *

If You Are New to IT

This section is presented for those who are new to the field or just wish to solidify understanding of computer concepts relevant to the module or the course. It is a good idea for seasoned professionals to scan this information, too, in case there is something new to learn.

More About Security

The ebooks listed below are in the course's Library list as "optional." Click on More Tools > Library to look for these items.

Meyers, M., Jernigan, A., & Lachance, D. (2019). *CompTIA IT fundamentals+ all-in-one exam guide (exam fc0-u61)* (2nd ed.). McGraw Hill. https://libauth.purdueglobal.edu/sso/skillport?context=144895

- *Chapter 4: "Data Storage and Sharing" (review)*
- *Chapter 11: "IT Security Threat Mitigation"*

Meyers, M. (2019). *CompTIA A+ certification all-in-one exam guide (exams 220-1001 & 220-1002)* (10th ed.). McGraw Hill. https://libauth.purdueglobal.edu/sso/skillport?context=144455

- *Chapter 13: "Users, Groups, and Permissions"*
- *Chapter 21: "The Internet"*
- *Chapter 27: "Securing Computers"*

System Backups

Backing up a company's data is of utmost importance, because loss of data affects the ability to do business. There are also records that must be kept for financial, tax, compliance, and other reasons. There are several methods used for database backups:

A **full** backup is when an entire database is copied and stored elsewhere. Typically, this is done on weekend nights when there is little business activity, as it may slow down the system during the backup process.

A **differential** backup copies and stores all content that changed since the last full backup. This will not take as long as a full backup and could be done nightly.

An **incremental** backup copies and stores the content that was changed since the last backup, whether it was a full or differential one. Should there be data loss, the information saved in this kind of backup will need to be "stitched" into a copy of the full backup.

There are other kinds of backups, including a full-computer backup, which records the structure of all software and inner hardware. A mirror backup copies but does not compress the files, so it tends to be faster; it needs more space and may not be secure, however. **RAID** — Redundant Array of Independent (or Inexpensive) Disks — technology can also provide necessary redundancy and protection against hard drive failure and subsequent loss of data.

Backing up data in the cloud or elsewhere **off-site** is recommended. Should a company's servers be destroyed by a fire or tornado, for example, the data would still be saved if the backups were stored off-site. Similarly, should a hacker infect a database with a virus, a fresh start would be possible if everything were saved elsewhere.