This is a general awareness training presentation on information security, at the end of which you should understand the information security safeguards prescribed by the UF HSC SPICE policies so that you can do your part to secure information.

Let's start by talking about vulnerabilities. Vulnerabilities are weaknesses in our information and computing environment that could lead to a loss of confidentiality, integrity or availability of our information.

Common vulnerabilities that users contribute to are:

- Leaving offices and file drawers unlocked
- Abandoned or forgotten old and unused computer equipment
- Unprotected passwords
Unsafe storage of electronic files, especially on portable computing devices and removable media.

Practices that permit computer viruses and worms to spread; well talk more about this later.

Emailing or instant messaging unsafely

Safeguards are measures you will take to eliminate the weaknesses in our information and computing environment to preserve the confidentiality, integrity or availability of our information.

Familiarize yourself with the hours of operation of your department, noting when offices should be unlocked and when they should be locked.

Lock your office or work area if possible, when you leave it unattended.

Lock file cabinets and desk drawers over night, and during the day if you work in a shared office area.

Keep labs locked when unattended. We have much to protect in our labs.

Always wear your Gator 1 or other official department issued identification badge, in plain view. This practice makes it easier to determine if unauthorized persons are in restricted work areas.
Familiarize yourself with your visitor escort procedures. Know which areas of your work space are for authorized staff only.

Escort visitors in areas where an escort is required and don’t hesitate to question an unfamiliar person in your work area.

We work in a public institution, but not all areas are open for the public to freely roam.

Make your password strong.

A strong password is hard for hackers to guess. It should not be a predictable password like a dictionary word, names, places or dates.

It should be a minimum of 8 characters.

It should contain at least one upper case letter, one lower case letter, and one number. Add special characters to make it even stronger and harder to guess.

Keep your password secret. Don’t share it with anyone, not even a trusted co-worker, your boss, your IT support staff, or a family member.

Don’t write it down and post it in places viewable by others.

And don’t allow your computer to ‘remember’ it for you. Your computer will store it on your hard drive where it could be accessed by someone else.

A changing password is more difficult for hackers to guess with their cracking tools. For this reason, the information systems you use will periodically require you to change your password.

If you suspect someone has learned it, you should initiate the change yourself. Your logon screens offer a password change option.

When your access is no longer needed, such as if you transfer to a different college or leave the University altogether, your logon account and password must be terminated. Notify your IT support staff of the date you are leaving as soon as you know it.
### Module 4 - Safeguards

#### Safeguard Your Workstation

**Lock or logoff when you walk away**

Activate your locking screen saver or other workstation screen lock provided by your IT support staff if you are leaving your workstation unattended, even if only for a few minutes. A screen lock prevents an unauthorized person from gaining access to your computer, but it leaves your application session in tact behind the screen lock, so you don’t have to reload you application when you return.

Logoff your computer if you are leaving for longer periods. Logging off will close down the applications you have running, and prevent an unauthorized person from gaining access to your computer.

#### Workstation timeout:

- **Automatic timeout**
- **Prompt for password**

Your workstation should automatically timeout after a period of time if it is left on but not being used. When it times out, your workstation should prompt for a password to prevent just anyone from walking up and using it. This is a safeguard that helps when you forget to lock your workstation and walk away from it.

If your workstation has not been set to *automatically timeout*, contact your Unit ISM or IT Support staff to enable this feature.

#### Safeguard Data on Your Workstation

- **It is not safe to store Restricted and Critical information on workstations**

It is a bad security practice to store restricted or critical information on the local hard drive of your workstation, when a network and secure servers are available for your use. Workstations are more difficult to secure than servers.

**Save Restricted and Critical information on secured servers**

More resources have been applied to securing servers, and as a practice you should always store your data on secured servers and not on the local hard disk of your workstation.

Contact your Unit Information Security Manager to learn about storing on your Unit’s secure servers.
Safeguard Your Portable Device

Portable devices present one of the biggest challenges for information security. Portable devices present a high risk of an unauthorized disclosure because they are highly desirable for thieves, easy to steal, and easy to lose. If you store Restricted information on a portable computing device, you must maintain a heightened awareness of these risks and take extra measures to protect them. Because, away from a secure server and facility, the security of a portable device and the data stored on it become entirely your responsibility.

Your Unit Information Security Manager must approve any portable computing device before you store Restricted information on it, such as protected health information, student records or personally identifiable information. Your portable computer must be properly configured to safely store Restricted information, and protect it if your computer becomes lost or stolen. Here are some additional safeguards for portable computers...

Never leave your portable computer unattended and unlocked. In addition to locks on your office or work area doors, you should lock the physical device itself when you need to leave it unattended. You can use a Kensington lock as shown here…

Or lock the device in a locking file cabinet.

Make sure your portable device has a durable physical or electronic label on it showing current contact information. This safeguard increases the chances that the device will be returned if you lose it, and it is found by an honest person. Make sure the label is visible.
Like a workstation, your portable device must require a login with a strong password, and have the automatic timeout feature turned on.

If you must store Restricted information on your portable computer: only store what is absolutely necessary.

Ensure there is an original copy of the information backed up to a secure server. Some of the security measures on portable computers involve data destruction, so the copy of Restricted information on our portable computer must be considered a disposable copy.

Restricted information on portable computers must be encrypted.

Make sure your Unit Information Security Manager knows about your portable computer and that you store Restricted information on it. If you are unable to exercise these safeguards, then you must not put Restricted information on your portable computing device. Notify your him or her immediately if it becomes lost or stolen.

Removable media are things like CDs or DVDs, floppy disks, or memory sticks. These devices present a big risk if you store Restricted information on them, because they are easily lost. Also, users often forget what data they have stored on them, and lose track of them or grow complacent with securing them. Here again, security of information on removable media rests entirely in your hands.

In general, you should not store Restricted information on removable media.

Contact your Unit Information Security Manager for other alternatives, or for appropriate safeguards if it is unavoidable.
Minimum safeguards for removable media include:
Labeling your removable media with current contact information, so if it is lost it will be returned if found by an honest person. Put the word "Restricted" on the label as well so you don’t forget the importance of the data you stored on it.

And always lock up your removable media when not in use, if it contains Restricted information.

Before computers or removable media are disposed of, Restricted information must be removed in a secure manner. Information stored on computer hard drives and removable media isn’t easily deleted or erased, and proper techniques or tools must be used. Practice these safeguards:
Turn old unused computer equipment over to your IT department for proper disposal of electronic information.

Contact your Unit ISM for procedures for securely disposing of your removable media.

Don’t just throw it in the trash, even if you don’t remember storing Restricted information on them.

Malicious software consists of computer programs deposited on your computer, intent on creating problems
Two types of concern include:
Worms and viruses and Spyware
Worms and viruses causes computer outage
causes computer outage
damages data
damages data
Enables hackers to hack your computer

Spyware –
records what web sites you visit

Records private information you type (passwords, web sites) for illegitimate purposes
Malicious software comes from:

- Web sites you visit
- Software you download or install
- Email attachments you open
- A file you receive on an instant message

You play a large part in controlling malicious software in our information and computing environment. So how can you safeguard against malicious software?

<table>
<thead>
<tr>
<th>Delete email with attachments from unknown senders.</th>
<th>Even if you receive an attachment from a known sender, but didn’t expect it, call and verify before you open it. It is easy for an imposter to make an email address look like someone you know.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant messaging is a valuable communication tool, but can also be an effective avenue for viruses, worms and spyware. It is a flow of electronic information over networks, and often circumvents technical safeguards users are unaware of.</td>
<td>If you use instant messaging in the HSC computing environment, you should only use the instant messaging product recommended by your Unit Information Security Manager. If your instant messaging product requires software to be installed, you must minimally notify your Unit Information Security Manager, and ensure it is installed securely. Do not use your instant messaging service to send and receive files because viruses, worms and spyware are easily hidden in them. Always reject file transfers if they are offered while using an instant messaging service, and if possible, disable the file transfer feature altogether, in your instant messaging software.</td>
</tr>
</tbody>
</table>
Instant messaging is another way users share electronic information over network. It is sometimes set up by users on their own, and circumvents technical safeguards users are unaware of. Instant messages can easily travel over unsecured networks, and are stored unsafely on unknown servers on the internet. Careful installation and prudent use of instant messaging software avoids computer outages and unauthorized disclosure of Restricted information. If you must use Instant Messaging to share Restricted information, you are responsible to ensure the following safeguards:

You must use only the instant messaging software approved by your Unit Information Security Manager

Be wary that if you use the wrong software, or if it is not configured securely, you could be exposing Restricted information on the internet.

Instant messaging software meets our safeguard requirements for use with Restricted information, when:

It controls the flow and storage of information to known and secure servers and networks

Users are required to login with a unique and strong password, to send and receive messages

Messages are encrypted

Seek direction from your Unit Information Security Manager for the approved instant messaging product for your Unit.

You can learn more about instant messaging software requirements under the Electronic Communication section of this Safeguards module.

The internet provides very little safety from web sites with harmful intentions. Users must be cautious. At present there are no hard and fast rules for knowing which web sites are safe and which are not. When using an HSC computer to access the internet, be smart and consider these risks:

Visiting web sites you haven’t heard of and haven’t accessed in a secure manner before are risky

Permitting web sites to download software on your computer is risky

While these practices cannot be avoided 100% in our environment, be judicious when you practice them.
Antivirus software is software that runs on your computer, looks for software viruses and worms, and cleans them off. It is required to be installed and working on all workstations at the UF Health Science Center. Your antivirus software needs to be frequently updated so that it can catch the latest software viruses and worms that may be spreading around.

Your IT department will install it and ensure it is configured properly, however, you are responsible to make sure it is working on your computer, and to notify your IT department when it is not.

Learn how to check for your antivirus software.
Learn how to check the last time it scanned your computer for viruses.
Learn how to check when it was last updated to catch the latest computer viruses.

You are likely to use two types of electronic communication, both of which are very valuable tools in the UF Health Science Center, but are not secure means of transmitting Restricted information. They are:
Electronic mail
Instant messaging
Both of these electronic communication technologies have inherent security flaws and you should be very cautious about what you send in them.

If you must email Restricted information:
Minimize the Restricted content
Send to single addressees only, not to distribution lists or list serves

If encryption resources are available to you, encrypt the Restricted content, or attach a password protected file if feasible

If you are emailing protected health information, more stringent safeguards apply. See the UF Privacy policy on Email Security.
You should avoid using Instant Messaging for Restricted information. If you must use instant messaging for Restricted information:

- Use only an IM product that is approved by your Unit Information Security Manager
- Seek assistance from ISM or IT Support to install and configure IM securely

Your messages must be encrypted all the way to their destination

You must ensure the authenticity of the recipient which basically means they must have to log in to receive your messages.

Keep the amount of restricted information to an absolute minimum.

This concludes the information security general awareness training presentation on safeguards. You should be aware of the measures you must take to protect information while using the information and computing environment. You should be aware of the need for authorization and support from your Unit Information Security Manager and your IT staff, for securing technology you use. Review this training presentation regularly, and apply the safeguards to your work.