

*For student workers*

introducing INFOSEC

Introducing INFOSEC

*For student workers*

**MALWARE PROTECTION**



Awareness

IT policies

Expectations

Training

Be suspicious of all links, attachments or downloads that accompany e-mails or other electronic messages.

Be aware that websites may be infected with malware.

Report to your supervisor any University computer behaving irregularly which you believe may be the result of malware.

**wireless**

Use wired access as opposed to wireless access when possible. This will ensure better speed, reliability, and security.

Careful what you click. This is not really

an email from Longwood & downloads malware.

Hover over links to check the full url.

**INTELLECTUAL**

**PROPERTY RIGHTS**

Music, movie, and software trade associations do contact the University regarding copyright violations, and we do follow up.

http://anrom.edurm.ru/administrator/components/com\_massmail/owa.longwood.edu.htm

Not
Longwood

Pretending to be
Longwood

*but*

A communication from

infosec@longwood.edu

 LongwoodInfosec

This page is intentionally left blank.

**Information Security**

**Awareness Agreement**

***Return this completed form to the Department Supervisor with the required hiring documents.***

Student Name:

Lancer Net ID:

Supervisor Name:

Department:

By signing and returning this form, you are acknowledging that you agree to follow the guidance provided in each of these documents.

**Student Signature**

**Date**

Information Security Awareness

“Security is everyone’s responsibility”

We challenge all members of the Longwood community

to always take a second to be secure.

*Tips to make your information more secure*

**PASSWORDS**

![C:\Users\goldchainam\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\QRZ40J4M\MC900325662[1].wmf]()

Avoid writing down your password. If you do write it down, keep it in a secure place.

Never use auto-logon or save password features on websites or in programs.

No request for your password is legitimate, not from your bank, not from your supervisor, not from ITS..

*

*

*

**HANDLE DATA SECURELY**

(www.longwood.edu/infosec/39078.htm)

Data is restricted because it’s “personally identifiable” or an unauthorized disclosure of it will cost the University. Do not share:

 Name + Social Security #

 Driver’s License #

State ID #

 Financial Acct.

Credit/Debit Card #

**ASK YOUR SUPERVISOR:**

*

*

*

How the data may be transmitted.

How data storage media should be used, such as hard drives, USB’s or CD’s.

Know the procedures of disposing of sensitive information.

Maintain the confidentiality of information that you have access or exposure to in the course of your work.

View only the information you are asked to view. Make only the changes you are authorized by your supervisor to make.



**REPORT SUSPICIOUS ACTIVITY TO YOUR SUPERVISOR**

You are accountable for all activity originating from your Lancer Net ID and any other account issued to you for your use.

**THESE INCLUDE UNAUTHORIZED ACCESS TO A SYSTEM, UNAUTHORIZED MODIFICATIONS TO DATA, OR MISUSE OF IT SYSTEMS.**

Read more about the Policy 6104 on www.longwood.edu/policies/6104.htm