

You Are Responsible For...

installing anti-virus software
and scanning your University
systems

Choosing “hard to guess”
passwords for the applications
and systems you access

Applying “patches” and up-
dates to University systems you
use or manage on a frequent and
consistent basis

Using screen-saver locks or
shutting your systems down when
you are away for extended time
periods



**Security Awareness
and
Incident Prevention**

Copyright @Georgia State University, 2002

Tammy L. Clark
Information Security Officer
Georgia State University
Classroom South, CS573/506
Email: tlclark@gsu.edu
Phone: 404-463-9612
<http://www.gsu.edu/security>

**The
Gramm-Leach-Bliley
Act:
Information Security
Awareness Training**



*Protecting
Customer
Information From
Harm...*

Guidelines for GSU Employees

Did You Know...

- **That a single compromised system on your campus can:**
 - allow someone to steal SSN's and sensitive info
 - result in identity theft, crimes and fraud
 - give someone access to accounts and/or passwords
 - expose sensitive or confidential information
 - cause your internet and email access to be halted
 - attack other systems over the internet
 - cause your computer to be compromised!
- **That a single security "unaware" University computer user can**
 - open a virus attachment in an email and unknowingly infect any unprotected systems on your campus
 - implement file sharing and as a result, allow anyone over the internet to see and delete the entire contents of their "C" drives
 - unknowingly execute a Trojan Horse program that will allow a complete stranger to have remote control of their computer
 - use weak passwords that can be "cracked" to allow someone access to University systems, applications, and databases of sensitive customer information!

GSU Employee Guidelines

1. Keep viruses off of your computer! Install antivirus software and scan your files on a regular basis. Never click on emailed links or attachments from "strangers."
2. Back up financial/sensitive data to your network directory, not to your computer's hard drive. Set a password on these files to keep unauthorized persons from being able to view or access this information, and don't leave printouts sitting around.
3. Use "hard to guess" passwords for all of your University accounts. Try to use a pass phrase that you can remember with a mixture of lowercase and uppercase letters, numbers or symbols. An example might be 2LuVm31s2N0M3 (to love me is to know me).
4. If you have a laptop that you use to dial into your campus network remotely, install a personal firewall to add another important layer of security and connect over your campus's VPN if that service is available.
5. Don't attach an external modem to your campus system (and leave it set on auto answer).



6. Update and apply patches to your University systems on a regular and consistent basis! Microsoft comes out with new security patches all the time and if you fail to install them, your system can become vulnerable to attacks and intrusions. Unix and Mac OSX users must be very vigilant in installing necessary patches as well.
7. Don't expose your accounts and passwords by writing them on "post it" notes that are stuck on your desk or computer monitor.
8. If you are going to be away from your computer for periods of time, turn on a password-protected screensaver, log off the network, "lock" your workstation, or shut your system down.
9. Lock rooms and file cabinets where paper records are kept.
10. Encrypt sensitive customer information when it is transmitted electronically over networks or stored online.
11. Recognize fraudulent attempts to obtain customer information
12. Keep customer information secure and confidential. Report any suspected instances of fraud or negligence to your supervisor!

