New Employee Orientation

Security Awareness

August 7, 2007

Chuck Curry, Assistant Vice Chancellor for Information Security
John Gale, Security Consultant
Scott Robards, Security Consultant
Our goal is security awareness, for you to realize your responsibilities and how to protect the University and yourself.
Today’s Presentation

Inform you of your responsibilities
Empower you to support the mission of the University
(http://www.uncg.edu/cha/mission/)
Provide information so that you can help yourself

You are the individual that can protect or expose data.
A University Policy is approved at the highest levels of the University (Chancellor, the Executive Staff, Board of Trustees).

Everyone at the University is required to abide by them.
 Policies are different from procedures or standards which might be requirements set forth by your department or supervisor and will vary within the organization.
Employees need to know where policies are and spend time getting familiar with them.

A great deal of information is contained in policy and ultimately it will help you do your job effectively and safely.
List of UNCG policies:
http://www.uncg.edu/ucn/policies_procedures/

Policies cover diverse topics:
- Adverse Weather and Campus Closure
- University Colors
- Contract Review and Approval
- Sexual Harassment
- Student Disciplinary Code
- and more …
Technology-related policies:
http://its.uncg.edu/Technology_Policies/

Today we will review:
Acceptable Use of Computing and Electronic Resources Policy
Security of Networks and Networked Data Policy
Data Classification Policy
Security Breach Notification Protocol
Acceptable Use of Computing and Electronic Resources Policy:

Users of the network and computing resources must obey the law

Users should not have an expectation of privacy

Users need to know about computing activities that are **expressly prohibited** such as:

- Circumventing user authentication or security of any host, network, or account.
- Interfering or denying service to any user.
Security of Networks and Networked Data Policy:

Network operation including physical connection, workstation, and server operation
Enterprise passwords
Non-affiliate access
Remote access
Extranet (external network) connections
Data Classification Policy:

Security measures will be implemented commensurate with data value, sensitivity, and risk.

Data will be classified into one of two categories:

- **Restricted** – data whose disclosure to unauthorized persons would be a violation of law
- **Public** – data to which the general public may be granted access

Security measures for data are set by the data custodian, working in cooperation with the data stewards
The NC Identify Theft Protection Act requires State agencies to notify persons whose personal information has or may have been compromised. This protocol sets forth the circumstances and procedures under which required notifications are made. The first priority after a security breach is discovered is to contain the breach and notify supervisory personnel as quickly as possible.
How can you protect yourself?

Treat others’ confidential information the way you would like your confidential information to be treated.

Use the *Top 10 Safe Computing Practices* on the handout.
How can you protect yourself?

1. Use strong passwords
2. Protect your workstation with a firewall and anti-virus software
3. Keep workstations patched and up to date
4. Use email responsibly
5. Lock, logout of, or shut down your workstation when not in use
6. Store restricted data on University servers
7. Do not install unnecessary software
8. Back up your data
9. Securely destroy media when it reaches end-of-life
10. Physically secure the equipment in your care
How can you protect yourself?

Links from this presentation:

http://www.uncg.edu/cha/mission/
http://www.uncg.edu/ucn/policies_procedures/
http://its.uncg.edu/Technology_Policies/

Questions, please contact your IT Service Desk

Telephone: 256-TECH (8324)
Email: 6-tech@uncg.edu
Web: http://6-tech.uncg.edu