Georgia Tech Information Security Policy Update – Fall 2009
Computer & Network Usage and Security Policy (CNUSP)

• Last updated July 2005

• The landscape has changed over the years

• CNUSP helps to protect campus and guides technology use
CNUSP – Guiding Principles

• Users of Georgia Tech IT resources and data will be good stewards of the resources to which they have access and will act in a responsible manner.

• The Institute is bound by federal, state, and local laws as well as contractual and regulatory obligations to protect access to Georgia Tech IT resources and data.
CNUSP – Areas to note

• Usage of IT Resources (scholarly/business purposes/consulting)

• Integrity of IT Resources and Protection of Data (student data/research data/export control)

• Intellectual Property (licensing/fair use/export control)
CNUSP – Approval

• Policy Committee – Faculty & Staff (1/09-7/09)

Next Steps:
• Awareness/Solicit input – SGA & General Faculty
• Review with Associate Deans and Staff AVPs
• Finalize and Publish in Spring 2010
Our Collective Efforts have Reduced the Number of Incidents and Their Impact to Our Mission

The CNUSP is a Policy within the Institute’s Information Security Plan – the plan’s goals are to:

• Support the Institute’s academic and research goals
• Ensure seamless and secure access to teaching, research and administrative resources
• Protect Institute users, IT resources, and data
• Ensure compliance with various regulatory and legal bodies

Office of Information Technology
http://www.oit.gatech.edu
GT’s Security Program Impact

- Average attacks per week:
  - 2 million
  - 2.5 million
  - 3.75 Million
  - 5.5 million
  - 6+ million
  - 10+ million
  - +110 million
  - 150+ million

- Incidents per Year:
  - 5500
  - 2875
  - 2463
  - 1662
  - 556
  - 81
  - 172
  - 118

- Timeline:
  - 2001: Intrusion Detection
  - 2002: Started unit-level Firewall program
  - 2003: Defense in depth GT InfoSec Guidelines
  - 2004: DeskTop AV and ResNet/EastNet Network Admission
  - 2005: Executive risk management seminar
  - 2006: Anti-Spam/Virus E-mail Gateway
  - 2007: Campus-wide Data Cleanup
  - 2008: T4/Sakia – facility to house student info

- Malware:
  - Nimda
  - Klez
  - Blaster
  - Mydoom
  - Bagel
  - Sasser
  - Botnets
  - Mydoom.ax
  - Worms
  - Phishing
  - BotNets
  - Conficker
  - Fake AV

- Repositories:
  - Office of Information Technology
  - Student Information Exposure
  - Laptops / Unit Repositories

Office of Information Technology
http://www.oit.gatech.edu