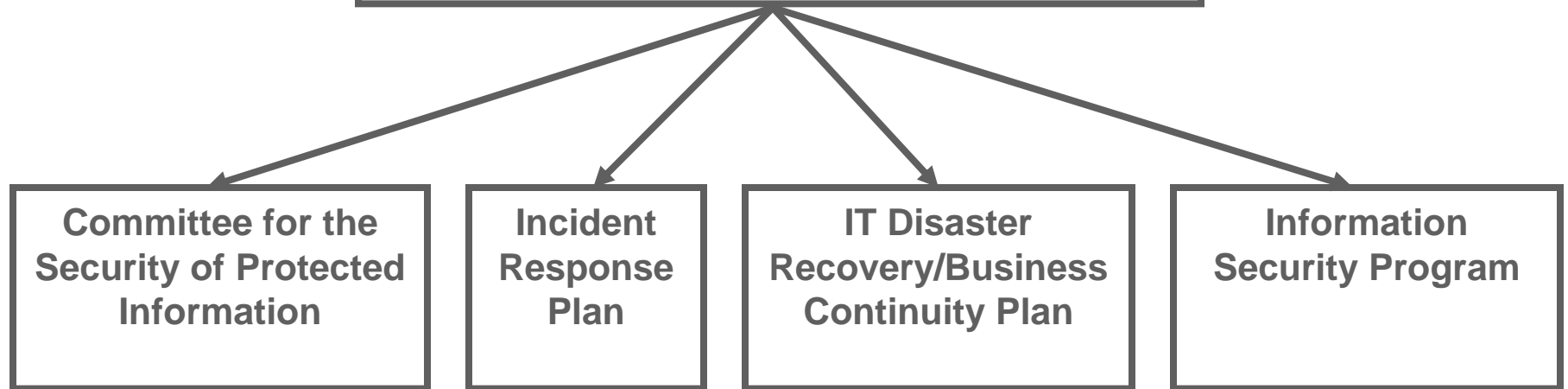


# **Information Security Overview**

**Presented to  
Deans, Directors, and Department Heads**

**March 18, 2008**

Information Security Policy – [OP 01.10](#)



◆ [www.infosecurity.msstate.edu](http://www.infosecurity.msstate.edu)

# Committee for the Security of Protected Information

- ◆ Reports to the President
- ◆ Serves in an oversight role for all issues related to information security
- ◆ Coordinates the Incident Response Plan, the IT Disaster Recovery/Business Continuity Plan, and the Information Security Program
- ◆ Reviews all significant security incidents and recommends appropriate action and remediation

<b>Name</b>	<b>Title/Dept.</b>	<b>Position</b>
Bell, Ann	Director, Human Resources Management	
Bland, Wayne	Associate VP for Finance & Administration	
Boles, Dave	Associate Director, Athletics	
Brown, Vickie	Director, Advancement Information Technology	
Fulgham, Julie	Interim Director, Institutional Research	
Geuder, Maridith	Director, University Relations	
Gilbert, Jerry	Assoc Provost & Assoc VP for Academic Affairs	Co-Chair
Guest, Charles	General Counsel	
Harpole, Sandra	Associate VP for Research	
Harris, Lisa	Associate VP for Student Affairs	
Johnson, Jeremy	President, Student Association	
Lewis, Neil	Facility Security Officer for the Office of Research	Ex-Officio
Mixon, Melissa	Associate VP for Ag, Forestry, and Vet Medicine	
Odom, Joy	Chair, Prof & Support Staff Advisory Council	
Rackley, Mike	Head, Information Technology Services	Co-Chair
Ritter, Tom	Security and Compliance Officer, ITS	Ex-Officio
Stokes, Butch	Registrar	
Vaughn, Ray	Director, Center for Computer Security Research	Ex-Officio
Wolverton, Bob	President, Faculty Senate	
Zant, Don	Director, Internal Audit	

# Incident Response Plan

- ◆ Outlines procedures to effect a timely and appropriate response in the event of an information security breach
- ◆ Key elements include:
  - Incident Reporting
  - Investigation
  - Communication including media relations
  - Forensic Analysis
  - Post Mortem

# Disaster Recovery-Business Continuity Plan

- ◆ Mandates procedures to effect the timely and orderly restoration of information technology resources and services in the event of a significant interruption
- ◆ Key elements include:
  - Organizational Preparedness
  - Continuity of Critical Applications
  - Restoration of Normal Operation

# Information Security Program

- ◆ Identifies technologies, procedures, and best practices to ensure ongoing institutional focus on the protection of information
- ◆ Key elements include:
  - Data Classifications & Individual Responsibilities
  - Risk Assessment & Safeguards
  - Training & Awareness
  - Monitoring
  - Audit and Compliance
- ◆ Covers all forms of data - electronic, paper, etc.

# Data Classifications

- ◆ Category I – Most sensitive -  
compromise would result in significant harm to the institution
- ◆ Category II – Less sensitive –  
compromise would result in some harm to the institution
- ◆ Category III – Public information

# Risk Assessment & Safeguards

- ◆ What are threats to the data?
- ◆ What measures are in place to protect the data?
- ◆ Are measures commensurate with data classification?
- ◆ Are new or improved safeguards called for?

# Information Security Training

- ◆ Required of faculty, staff, and student workers with access to sensitive information
- ◆ Unit heads responsible for ensuring compliance – Banner report being developed to assist
- ◆ Available online via onCampus portal
- ◆ In-person training available first Friday of each month in ITS McArthur training lab

# Training continued

- ◆ Current employees have until July 30<sup>th</sup> to complete training
- ◆ New employees required to complete within 30 days of employment
- ◆ Must retake every four years
- ◆ 1,725 have completed training so far

# Monitoring

- ◆ Requires continuous vigilance on the part of data holders, data stewards, and system administrators to thwart attempts to compromise protected information
- ◆ Includes computer, network, physical, operational, and procedural security
- ◆ System admins must ensure appropriate tools and procedures are in place to detect and deter electronic attacks and compromises

# Audit and Compliance

- ◆ Periodic audits will confirm compliance with information security policy and program
- ◆ Coordinated by Office of Internal Audit

# Other Highlights

- ◆ Minimum Security Standards for Computer Systems
- ◆ End User Best Practices
- ◆ System Administration Best Practices
- ◆ Property Control will coordinate with departments to ensure removal of sensitive information prior to disposal of electronic equipment

# Related Policies

- ◆ Access to Computing Resources [OP 01.11](#)
- ◆ Use of Computing and Network Resources [OP 01.12](#)
- ◆ World Wide Web Pages and other Electronic Publications [OP 01.13](#)
- ◆ Misuse of University Assets [OP 01.19](#)
- ◆ Social Security Number Usage [OP 01.23](#)
- ◆ Buckley Amendment [AOP 10.06](#)
- ◆ Electronic Communications Infrastructure [AOP 30.04](#)
- ◆ Records Management and Security [OP 60-109](#)
- ◆ Credit/Debit Card Processing [OP 62.08](#)
- ◆ Student Use of Computing Resources [OP 91.117](#)

# Online Training Demo

- ◆ Point web browser to <http://oncampus.msstate.edu>
- ◆ Login with NetID/NetPassword
- ◆ Click on “Office” tab
- ◆ “Information Security Certification” channel in upper left corner

**Questions?**