



NORTH CAROLINA AGRICULTURAL
AND TECHNICAL STATE UNIVERSITY

INFORMATION TECHNOLOGY DEVELOPMENT INITIATIVE

Tom Jackson

Vice Chancellor of Information Technology Services and Chief Information Officer

April 27, 2018

BOT Risk Management, Audit and Compliance Committee

AGGIES **DO**

IT Development Initiative

- ISO Standard
 - » Policies, Operating Standards and Baseline Procedures
- Information Security Management
 - » Several projects related to IT security
- Compliance
 - » Information Security Assessments
- Organization
 - » Filling IT leadership positions and consolidation of technology and staff

ISO Standard Status

- Governance
 - » Information Security Advisory Committee formed
 - » Information Security Incident Response Team formed
- Policies
 - » Information Security Policy pending Broad of Trustees approval
 - » Acceptable Use, Data Stewardship and Email polices under development
- Operating Standards
 - » Seven (7) standards under development

Information Security Management Status

- Initial Projects
 - » Fourteen (14) projects underway
- Vulnerability Scanning
 - » Third scan underway
 - » Reviewing results to identify remediation projects
- Remediation Projects
 - » First remediation project underway

Compliance

- Information Security Assessments
 - » Performed annually on each unit that manages technology
 - » Information Technology Services assessment will occur first, in summer 2018
 - » Assessment will lead into Information Security Program
- Information Technology Risk Assessment
 - » Will occur late fall 2018

Organization Status

- Search Firm
 - » Deputy CIO
 - » Associate VC Data Governance
 - » Director, Enterprise Applications
- Interviews
 - » Director, Network and Systems
- Filled
 - » Director, Client Technology
 - » Director, IT Project Management and Business Operations
 - » Interim Director, Network and Systems

UNC Policy 1400.2

- Establish an information security program
 - » Preserve security, confidentiality, accessibility and integrity of information resources
 - » Comply with ISO 27002 standard
- Designate a senior officer responsible for information security
 - » Accountable to Chancellor
 - » Report to Board of Trustees (BOT) on information security upon request
 - » Annual report to BOT Risk Management, Audit and Compliance (RAC) Committee
- Oversight of information security by BOT
 - » Include information security in Internal Auditor annual audit planning and risk assessments
 - » Include emerging information security matters as regular RAC agenda item

Information Security Program Elements

- Policies on storage, use and accessibility of information resources
- Regular risk assessments of existing information resources
- Strategy statement setting forth priorities for managing identified risks
- Incident response planning and notification procedures

Information Security Policy

- Based on ISO 27002 standard
- Includes requirements from UNC Policy 1400.2

Questions?