Agenda

- 1400 Series Policies
  - IT Governance
  - Information Security
  - User Identity and Access Control
- Risk Management
### 1400 Series Policies - CARMC

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1400.1</td>
<td>Information Technology Governance</td>
</tr>
<tr>
<td>1400.2</td>
<td>Information Security Governance</td>
</tr>
<tr>
<td>1400.3</td>
<td>User Identity and Access Control</td>
</tr>
</tbody>
</table>

“Periodic consideration of information technology matters by the audit/compliance/risk management committee of the institution’s board”

“Demonstration of a comprehensive information technology governance program that encompasses both centralized IT and distributed IT”
Information Technology Governance

• Refers to the framework, policies, rules, standards, structures, and processes

• Supports the missions, goals, and objectives of the UNC System and each constituent institution

• Manages information technology resources in accordance with rules and policies

• Identifies and addresses risks and threats to information technology and information resources

• Encompasses the planning, prioritization, funding, evaluation, auditing, and security of information technology and information resources
IT Governance Campus Feedback

Leadership
- Comprehensive view of campus IT services/groups
- Support Data Management activities
- Support interconnections between systems
- Prioritize project work, services, and rate of change for users
- Guidance on risk & compliance

Provost Direct Reports
- Understand entire IT portfolio
- Need for flexibility in some areas
- Data management

ITAC
- Data management
- Interconnectedness of systems
- Realize effectiveness/efficiencies in services
- Holistic view of services and needs
“Information security program” means policies, assessments, protocols, and trainings designed to govern the storage, accessibility, and security of information resources.

IT Security 300 series policies – Effective July 2021

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>07.300.00</td>
<td>Information Security</td>
</tr>
<tr>
<td>07.300.01</td>
<td>Identity and Access Controls</td>
</tr>
<tr>
<td>07.300.02</td>
<td>Operational Security</td>
</tr>
<tr>
<td>07.300.03</td>
<td>Physical and Environmental Security</td>
</tr>
<tr>
<td>07.300.04</td>
<td>Cryptographic Security</td>
</tr>
</tbody>
</table>
Information Security

• Information Security Program published July 2021

• Information Security Awareness training became mandatory for faculty and staff

• Hired two Information Security Analysts

• Multi-factor authentication

• State Audit of UNCW Cybersecurity Controls

• MCNC Assessment completed

• Conducted Executive Incident Response Tabletop

• Formalized Vulnerability Management Team
User Identity and Access Control

- A risk-based implementation of appropriate identity confirmation and access control techniques, such as multi-factor authentication, to control access to University data.

- Each institution’s user identification and access control measures must sufficiently control access to sensitive University data such as personally identifiable information, personal health information, and information subject to state or federal laws or regulations.
User Identity and Access Control

• Require two-factor authentication for all students, faculty, and staff to access many campus resources

• Federal requirements to protect student data have increased

• Distributed Systems Administrators

• Secure data sharing solutions for research collaborations

• Greater need for Data Governance
  • Data Governance Policy
  • Data Governance Program
  • Data Governance Committee
  • Data Classification Matrix
  • Data Handling Standards
## Top Critical IT Risks

<table>
<thead>
<tr>
<th>Research Cybersecurity Requirements</th>
<th>Recruitment/Retention of IT Staff</th>
<th>Incomplete Data/System Inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td>University Systems/Data in the Cloud</td>
<td>Network Segmentation/Research</td>
<td>Vendor Management</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>Information Security Awareness Training Compliance</td>
<td>Missing Security Requirements on Some Systems</td>
</tr>
<tr>
<td>Proliferation of Systems/Integrations</td>
<td>Storing Sensitive Data in Unmanaged Locations</td>
<td>Compliance with Increased Federal Requirements to Protect Student Data</td>
</tr>
</tbody>
</table>
## Mitigations for Risks

<table>
<thead>
<tr>
<th>Data Security Training</th>
<th>Complete Data/Systems Inventory</th>
<th>Endpoint Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement Network Segmentation</td>
<td>Vendor Risk Management</td>
<td>Expanded Vulnerability Scanning</td>
</tr>
<tr>
<td>Information Security Awareness Training</td>
<td>Multi-Factor Authentication</td>
<td>Data Governance</td>
</tr>
</tbody>
</table>
Thank you!