AUBURN

UNIVERSITY

Technology and Data Security Policy Update

February 19, 2018

Policy Why's

- Security
- Accessibility
- Privacy
- Compliance with State Law

Policy How's

- Working Group
  - Office of the CIO (ISO, OIT)
  - Distributed IT
  - Legal
  - Audit, Compliance & Privacy
  - Other stakeholders
- Review Process
  - Stakeholders
  - Executive
  - Legal

Software Acquisition Process

- Security
- Accessibility
- Privacy
- Compliance with State Law
- Contract T’s & C’s

Software Acquisition Process - 2

- Integration
  - Will it require integration with existing systems?
    - Banner?
    - Canvas?
- Cost/Value to the University
  - Do we already have a license for this?
  - Do we already own a similar product?
  - Have we evaluated the total cost of ownership?

So How Do I Buy Software??

- Distributed IT Provider
- AU Software (Part of OIT)
  - Barbara Cosby & Dudley Dent
  - ausoftware@auburn.edu
- It does take time
  - (Don’t wait until the last minute and send a requisition straight to PPS).

Policies Update

- Social Security Number Protection Policy (January 11, 2017)
- Information Security Incident Employee Reporting (January 11, 2017)
- Cardholder Data Environment Policies (Office of Cash Management) (March 21, 2017)
- Information Security Policy (May 31, 2017)
- Authentication Policy (May 15, 2017)

Policies

- Core Administrative Systems (Replace Banner) (August 31, 2017)
- Operating System Current Version Policy (October 1, 2017)
- Wireless Networking Policy (October 1, 2017)
- **Software and IT Services Approval Policy (November 10, 2017)**
- Endpoint Protection Policy (November 15, 2017)

Policies

- Electronic Data Disposal Policy (April 30, 2016)
- Computer Authentication (April 30, 2016)
- Email Policy (Combined three existing policies) – (October 31, 2016)
- Eligibility for Auburn University Computing Accounts – (October 31, 2016)
- Appropriate Use Of AU IT Resources Policy – (October 31, 2016)

Policies in process of review

- Data Classification Policy (1/1/2015)
  - Updating NOW
- Mobile Encryption Policy (10/01/15)
- Data Storage Policy (NEW)

NEW SECURITY STANDARD

- Government unclassified data required by law and statutes requiring protection standards for disclosure and dissemination.
- CUI data includes 115 categories and sub-categories. Some examples include:
  - **Export Control: Research**
  - Privacy: Student Records: Financial Aid
  - Information Systems Vulnerability Information
  - Procurement and Acquisition
  - Patents
  - Law Enforcement
  - Proprietary Business Information

WHEN

- DOD:
  - Implement NIST 800-171 requirements prior to December 31, 2017
- Other Government Agencies
  - Awaiting implementation dates from various agencies, expecting details in 2018

NIST 800-171

- A higher education institution must review its contracts with federal agencies carefully. There must be a document (contract/agreement) referencing both (1) the data the federal agency is sharing that it has specifically identified as CUI, and (2) that the institution must follow the terms of NIST 800-171.
- Depending on the type of data received from the federal government, CUI could include data received as part of a research grant or data received to conduct business **(e.g., student financial aid information).**

NIST 800-171: Impact to Auburn

- Actions Taken:
  - Work group established
  - Segmented Network
  - Template Developed
- Next Steps:
  - Review new contracts carefully
  - Determine Security Steps Needed based on Contract Language
  - The Information Security Office and the Research Security Office can assist and or advise, but cannot implement or attest.

QUESTIONS?