Policies & Rules Update

Key with new policy is Data Steward or their Designated Trustee approve data use for specific purpose.

<table>
<thead>
<tr>
<th>Effective 2017</th>
<th>Planned for 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Acceptable Use Policy (Updated)</td>
<td>• Access and Authentication Policy</td>
</tr>
<tr>
<td>• Data Access Policy (New)</td>
<td>• Access Management Rule</td>
</tr>
<tr>
<td>• Minimum Security for Computing Devices Rule</td>
<td></td>
</tr>
</tbody>
</table>

UAB Information Security
Standards set for Minimum Security

- One of the provisions (4.2) in the Minimum Security for Computing Devices Rule is “current, vendor-supported operating systems”
  - Windows 7 SP1
    - January 14, 2020
  - Windows Server 2008 R2
    - January 14, 2020
  - Windows 10 – Version 1511
    - April 10, 2018
  - Windows 10 – Version 1607
    - October 9, 2018
  - OS X El Capitan (10.11)
    - Late 2018
  - Red Hat Enterprise Linux 6.7
    - December 2018
  - Ubuntu 17.10
    - July 2018
  - Ubuntu 14.04 LTS
    - April 2019
Annual Board Report

• The UA System Board of Trustees requests an annual reporting of centralized and decentralized servers with sensitive records counts

• Using the IP Address Management System to provide the report this year so please make sure information is current and accurate

Update on DDI:
- DNS cutover – Summer
- DNS rollout for distributed management – Summer/Fall
- DHCP begin rollout for VOIP – Spring
- DHCP begin rollout for distributed networks - Summer
New Alabama Breach Notification Law

• Signed into law March 28, 2018 and effective June 1, 2018
  • Specifically defines what information is considered sensitive PII governed by the Act - such as a social security number, driver’s license number, etc
  • Must implement and maintain “reasonable security measures” to protect sensitive PII from a potential breach
  • If a breach has occurred or is suspected to have occurred, “a good faith and prompt investigation” must occur
  • If there is a notification requirement, the Act sets forth certain mandatory obligations with deadlines and exceptions for notification
  • Requires “reasonable measures” to dispose of records containing sensitive PII when the records are no longer required to be retained pursuant to applicable law.
Data Reduction & Handling

Delete
- If you don’t need it, delete it.

Redact
- De-Identify
- Remove the restricted elements.

Tokenize
- Use an alternate identifier
- UABID

Secure
- If you need it, secure it.
UAB is establishing NIST 800-171 as the baseline for system security for Compliance requirements.

<table>
<thead>
<tr>
<th>Control Family</th>
<th>Control Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>Media protection</td>
</tr>
<tr>
<td>Awareness and training</td>
<td>Personnel security</td>
</tr>
<tr>
<td>Audit and accountability</td>
<td>Physical protection</td>
</tr>
<tr>
<td>Configuration management</td>
<td>Risk assessment</td>
</tr>
<tr>
<td>Identification and authentication</td>
<td>Security assessment</td>
</tr>
<tr>
<td>Incident response</td>
<td>System and communications protection</td>
</tr>
<tr>
<td>Maintenance</td>
<td>System and information security</td>
</tr>
</tbody>
</table>
Two Factor Authentication

Growth since go-live Jan 8th

- 40.8% Faculty/Staff
- 59.2% Students

Next phase is risk based expansion to systems with Restricted data and users that handle Restricted data.
Email Data Loss Prevention

• Protection of SSNs and CCNs within email
  • 1,651 alerts in March alone – average of 54 per day

• Examples
  • A UAB organization was submitting students’ credit card information for payment processing via unencrypted email on a regular basis, multiple times during the week.
  • A user tried to email PII that included the SSNs of 500 different UAB constituents.
  • PHI tied to patients’ upcoming doctor’s appointments were being sent on a daily basis. Each instance could include PHI of 10 or more patients. Each email was sent to multiple UAB recipients, which meant PHI was piling up in more than a dozen UAB Inboxes on a daily basis.

An added benefit is that we are able to detect scams in which the bad guys offer a debit or credit cards (with the full number) that supposedly are pre-loaded with cash or access to credit lines. When the UAB user receives such a scam email, an automated email warning also is sent to the user’s Inbox that addresses such scams.
Information Security Exception Request

• ~1500 exception requests in various categories:
  • Do Not Scan
  • End of Life OS
  • PGP Encryption Waiver
  • Open Email Relay
  • World Accessible RDP or other Vulnerability

• Current Average age: > 5 Years
Vulnerability Management & Pen Testing

• Vulnerability Management Program
  • Currently scanning 98.4% of UAB Campus Network
  • Targeting all Critical and High Severity be addressed by mid summer
  • Authenticated Scanning for IT Desktop Customers in upcoming months
  • Plan for Fall 2018 – more widespread authenticated scanning of campus

• Penetration Testing Program
  • Focus: Enterprise Systems and systems with restricted data attestation
  • Conducted tests of IRAP, IDM, Banner, Oracle and ancillary systems
  • Upcoming Trustwave PT of systems associated with PCI
Blazer for Life

UAB IT is advertising the Blazer for Life email service to students and employees.
Blazer for Life

When a student leaves the University his or her @UAB.edu mailbox is retained for one year.

When a graduate sets up email forwarding, their @UAB.edu address stays active (although their mailbox content is deleted after a year).
Email encryption will soon be available using two methods.

**BUTTON**
Clicking a custom button in Outlook will encrypt the message for the recipient.

**SUBJECT LINE**
Including the word [Encrypt] in the subject line will encrypt the message for the recipient.
Office 365 Groups

UAB units will be able to request an Office 365 Group as a replacement for distribution lists. Groups offer more functionality:

- Email address
- Calendar
- Planner
- SharePoint site
Legacy DLs

• If units want to keep legacy distribution lists, they will be able to edit the membership list.

• If admins do not request to keep the DL, they will expire in one year.

• DLs should not be simultaneously used as permission lists.
UABMC collaboration

Those with UABMC email addresses have three ways to collaborate with those on the campus side:

1. Sign up for free Box account
2. Use OneDrive
3. Request exception for Box account

Note: Restricted/PHI data is not permitted in the cloud.
TLS changes for Box and Office 365

Box and Office 365 are deprecating their support for certain types of encryption so that old browsers will not be able to access the services.

Deprecation: June 15
Deprecation: Oct. 31
12 bad enterprise security habits to break

<table>
<thead>
<tr>
<th>Habit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delayed patching</td>
</tr>
<tr>
<td>Treating security like a black box</td>
</tr>
<tr>
<td>Thinking basic solutions will be enough</td>
</tr>
<tr>
<td>Lack of security automation</td>
</tr>
<tr>
<td>Lack of fire drills</td>
</tr>
<tr>
<td>Failure to protect users from themselves</td>
</tr>
<tr>
<td>Reviewing security at the end of the app dev process</td>
</tr>
<tr>
<td>Just saying “no”</td>
</tr>
<tr>
<td>Turning a blind eye to shadow IT</td>
</tr>
<tr>
<td>Forgetting the end-user</td>
</tr>
<tr>
<td>Adding weak links via the Internet of Things</td>
</tr>
<tr>
<td>Poor password hygiene</td>
</tr>
</tbody>
</table>

UAB Information Security
Questions