Internal Control Assessment (ICA) Cycle 2 is currently in process. To help prepare for these audits, we are offering training each fall and spring semester and encourage all departments to attend. The next training session is scheduled for **February 26th from 1:30 p.m. to 2:30 p.m.**, and will be held in the Law School Room 1115. To register, please call 915-7017 or email auditing@olemiss.edu.

**Departmental Scholarship Documentation**

Departments must establish a formal process by which scholarship applicants are reviewed and selected. The formal process should include:

- Documentation as to the funding source of scholarships (i.e. grants, departmental budget, etc.). Also, please note that the retention period for documentation has recently been changed from 7 to 3 years from the end of the award year.
- Description of the application process.
- Guidelines of awarding scholarships including: minimum criteria, who determines recipient and amount of award, if a person is ineligible to receive the scholarship (i.e. family members of faculty and/or staff within the department).
- More than one individual should be involved in the selection process.
- Sufficient documentation must be maintained, especially if family members of departmental personnel are awarded scholarships.

**Anti-Virus Software**

Viruses are costly to the University in terms of data loss, staff time to recover systems, and delay of important work. Departments are responsible for purchasing virus protection software for all departmental machines. Additionally, the latest anti-virus software and operating system (OS) patches must be installed on all departmental computers and servers.

Employees are responsible for the following:

- Updating virus protection software regularly.
- Configuring machines to perform frequent (at least weekly) automatic system scans. If the Symantec software version is 12.1 or higher, an active scan is permissible; however, if the software version is lower than 12.1, a full scan is required.
- Being mindful/ careful when opening attachments.
- Reporting all significant virus incidents to the IT Helpdesk.
Inadequate scans could lead to attacks on computers and the university network through undetected viruses and malware.

*Note: The campus Security Coordinator stated that while anti-virus software has historically not been necessary for Macintosh computers, recent bulletins indicate increased instances of attacks.*

If you have any questions regarding which anti-virus software should be installed, please contact the IT Helpdesk at 5222.

---

**Segregation of Duties for Procurement Items**

Segregation of duties is one of the most effective internal controls and means that *no one person should be responsible for doing everything within a process*. For example, authorization, recording, and custody of assets should be performed by different employees. Different employees should also:

- Purchase items
- Approve purchases
- Reconcile account

In many cases, ideal segregation of duties is not possible due to the limited number of employees in a department. In such cases, compensating controls should be established, which may include more supervision, monitoring, and involvement of departmental management in the process. Additionally, someone other than the individual responsible for purchasing should be receiving Purchase Notification Reports.

---

**Information Confidentiality/Security Policy**

The [Information Confidentiality/Security Policy](#) sets standards for how confidential information maintained by the University of Mississippi (UM) is to be protected. The policy has recently been updated to include a matrix that outlines the permitted and restricted uses of data (documented below). For more detailed information, please refer to the [Information Confidentiality/Security Policy](#).
### Permitted & Restricted Uses of Data

<table>
<thead>
<tr>
<th>DATA TYPE</th>
<th>Storage Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IT Managed Computers, Servers, and Storage Devices Residing in Data Center and Approved 3rd Party Services</td>
</tr>
<tr>
<td></td>
<td>UM Google Apps ²</td>
</tr>
<tr>
<td></td>
<td>UM Box ²</td>
</tr>
<tr>
<td></td>
<td>UM Computers, Servers and Storage Devices Connected to Campus Network ³</td>
</tr>
<tr>
<td></td>
<td>Other UM Technology ⁴</td>
</tr>
<tr>
<td></td>
<td>Personally Owned / Managed Technology</td>
</tr>
<tr>
<td>Instructional Data</td>
<td>☑️</td>
</tr>
<tr>
<td>Student Educational Records (FERPA)</td>
<td>☑️</td>
</tr>
<tr>
<td>Protected Health Information (ePHI-HIPAA)</td>
<td>☑️</td>
</tr>
<tr>
<td>Mississippi State Law Notice-Triggering Information *</td>
<td>☑️</td>
</tr>
<tr>
<td>Gramm Leach Bliley (GLBA) student loans application information</td>
<td>☑️</td>
</tr>
<tr>
<td>Payment Card Information (PCI)</td>
<td>☑️</td>
</tr>
<tr>
<td>Sensitive Identifiable Human Subject Research **</td>
<td>☑️</td>
</tr>
<tr>
<td>Export Controlled Research (ITAR, EAR)</td>
<td>☑️</td>
</tr>
<tr>
<td>All Other Non-Sensitive Data</td>
<td>☑️</td>
</tr>
</tbody>
</table>

- ☑️ Permitted
- ☒️ Not Permitted
- ☞ Permitted Only with Prior Approval and Server Registry Entry

1 – Refers to systems such as SAP, Sigma ProSAM, Blackboard, Touchnet, etc. that are managed by professional IT staff with the highest security levels.
2 - Box and Google offer a certain level of protection, but each user is responsible for the management of shared access settings to prevent exposure of sensitive data.
3 - Refers to non-mobile, university-issued computers and storage devices connected to the campus network outside of Data Center or within Data Center but not behind most restrictive Data Center firewalls.
4 - Includes university-issued laptops and mobile devices. Mobile devices should not be used for temporary or permanent storage of sensitive data, although, as part of normal usage, data may be cached when it is viewed from these devices. User is responsible for securing mobile devices to ensure that transient sensitive data is not exposed.
* - Mississippi Data Breach Notification Law “Notice-Triggering Information”

An individual's first name or first initial and last name in combination with any one or more of the following data elements:

- Social security number;
- Driver's license number or state
- Identification card number
- Account number or credit or debit card

** - Requires IRB Approval in addition to IT approval.

We’d like to thank all of you who attended training in the fall. We strongly encourage all departments to send at least one departmental representative to an upcoming training session. If you have any questions, please feel free to contact us at 915-7017 or auditing@olemiss.edu.