THE UNIVERSITY of MISSISSIPPI
OFFICE OF INTERNAL AUDIT

January 2017 Newsletter

The Audit Perspective

In This Issue

Password Managers

You should never use the same password for more than one system (i.e. SAP, myOleMiss). You should also never use anything in your password that someone could easily guess such as any part of your name or anything related to your job (i.e. Rebels, Ole Miss, 1848, etc.). The Office of Information Technology posted an article on TECHNews that explains the importance of a strong password. Consider using a password manager! See the IT Security website for more information and password manager recommendations.

Remember to ***never*** share or write down your passwords!

Anti-Virus Protection for UM Computers Policy

Viruses, malware, and spyware are costly to the University in terms of data loss, staff time to recover systems, and delay of important work. Inadequate virus protection and inadequate scans could lead to attacks on computers and the university network through undetected viruses and malware.

Anti-virus software is an important tool to help safeguard your data. Symantec Antivirus can be purchased from the Faculty Technology Development Center's website.

According to the Anti-Virus Protection for UM Computers Policy, it is the **department's responsibility** to:

- Purchase and install virus protection software for ***all*** UM owned computers (PCs and Macs) and ***all*** servers through the IT recommended solution.

- Designate a local (departmental) contact for departmental virus protection. The contact will assist in installation of software, education of the user community, and incident response.

According to the Anti-Virus Protection for UM Computers Policy it is each **employee's responsibility** to:

- Configure the software to check for updates daily and also configure in an active scan or real time scan mode.
- Exercise extreme caution when opening attachments.
- When a virus is detected, ***immediately*** disconnect the infected machine(s) from all networks. Report all virus incidents to the IT Helpdesk.
- Perform regular backups of data on individual computer systems (daily recommended).

Need an IT Security Refresher?

The Office of Information Technology provides security awareness training at no-charge to all employees. There are classroom and online options. All employees are encouraged to complete the online training periodically. Those with SAP GUI access are required to complete this training every two years.

Information Confidentiality/Security Policy

The Information Confidentiality/Security Policy has recently been updated. Employees should be aware of the following:

Screensaver Lock

Employees must use session/screensaver lock to prevent access of data after a certain period. Session lock is recommended after 15 minutes of inactivity.

Backups

- Daily backups should be used for critical systems.
- Full backups of all systems should be performed weekly.

Sensitive Data

- Sensitive data should not be stored on externally hosted systems, including cloud-based storage systems, without a contract that is fully vetted for compliance with University policies.
- Email is **NOT** a permitted medium for storing, processing, transmitting, or receiving any un-encrypted sensitive UM data.
- The University provides Secure Document Exchange via portal for sharing sensitive data within the University.

- For more information on acceptable storage methods, please review this helpful chart, which can also be found at the end of the Information Confidentiality/Security Policy.

Computer & Server Registry
All UM owned computers or servers, which are used to store, process, or transmit sensitive information, must be registered so they can be periodically scanned for vulnerabilities. To register a server or computer, go to the Campus Server Registry. The associated department must provide an active contact for each machine and ensure that registered information is kept current.

Copier/Scanner/Printer Security

Copier/scanner/printer devices may include the capability of storing documents. Whether owned or leased, the University requires these devices be configured and maintained. Specifically:

- Unnecessary services must be disabled on printers.
- Local storage of documents should be disabled.
- Email capabilities on printers can lead to data exposure and is discouraged. Additional caution must be taken by the department to mitigate the risks if email is necessary. In these cases, the device must be configured to use UM email servers, and transport-layer security should be enabled. Additionally, the printer should require a code to be entered for usage.
- When a device is taken out of service, the internal storage component must be overwritten to render data inaccessible. If this cannot be accomplished, the internal storage component must be removed and delivered to Procurement Services for destruction.

New or Updated Policies

The University of Mississippi Policy Directory is a central location for accessing and posting University policies. Over the past 30 days the following policies have been updated:

- Employee Responsibilities – *Employees should refrain from excessively using social media outlets. When there is an appreciable amount of time unoccupied by office duties, the position should be reduced to part time or the incumbent should be made available to give assistance to other departments.*
- Use of Novel Compounds Policy
- Background Checks

Self-Assessment

Self-assessment is a valuable tool to help identify internal control deficiencies and assist in departmental management and audit preparation. The self-assessment consists of a series of "yes" or "no" questions. "Yes" indicates adequate controls in an area, while "no" indicates control deficiencies. Additional control related information is provided below each question to aid in resolving control deficiencies. Links to relevant policies are also included for each section.

The self-assessment can be accessed here. For questions not addressed in the self-assessment, please feel free to contact us at 662-915-7017 or auditing@olemiss.edu.

Thanks

We hope you find the information in our newsletters useful. If you have any suggestions, questions, or feedback, please contact us at 662-915-7017 or auditing@olemiss.edu. Feel free to share our newsletters with those in your department you feel would benefit. You can also visit our website for more helpful information.