Academic Technology and Computing Committee Report

Committee Members: Thomas Bunton, Heba Sadaka, Thomas Wallace, David Baylis, Robert Minarcin, Melissa Serfass, Rebecca Glazier, Zac Hagins, David Montague, Chris Stewart, Caleb McQuay, Rhonda Thomas, Hong Wang, & Jami Hollingsworth

Committee Activities/Meeting:

1) The committee met during the Spring 2021
2) Committee elected a new chair Spring 2021
3) Committee activities focused on
   a) Obtaining information on committee related actionable items including Post Pandemic 24 hours Blackboard Support.
   b) Obtaining IT policy documents and information from the CIO of IT Services, Tom Bunton, and Faculty Senate President, Amada Nolen.
4) Committee documents will be uploaded to committee shell in Blackboard under myOrganization.

Policies Reviewed

The committee has draft copies of amendments to these policies:

1. Security Awareness Training Policy
2. Mobile device management Policy

Timeline

The committee plans to bring policy amendments to the Faculty Senate in April 2021 for Senate action.

IT Mobile Device Management Policy

Version: 1.3
Created: 03/09/2021 - Updated: 4/12/2021
Reviewed: 4/12/2021
Approved: Pending Policy Management Board Approval – Submitted 4/19/2021

Purpose

UA Little Rock implements necessary controls, technologies, and devices to secure information systems and critical data in UA Little Rock infrastructure. However, mobile devices are an inevitable part of our daily lives, and they are used to conveniently perform UA Little Rock business-related activities and provide access to UA Little Rock data. However, mobile devices have fewer security controls to keep UA Little Rock systems and data secure. UA Little Rock developed this policy to define the principles to secure university systems and data, even on mobile devices.

Scope

This policy applies to every mobile device—university-owned or personal—accessing UA Little Rock systems and data to perform university business.

Policy

To ensure compliance with UA System policies, UA Little Rock policies, laws, and regulations, employees using mobile or personal devices to perform UA Little Rock business, functions, and tasks or accessing and processing university data must implement the following security best practices and device settings to protect the security of their mobile devices and campus data:

1.) Sensitive data must not be stored on the mobile device.
2.) If the device supports encryption, it must be enabled.
3.) All applications must be installed from official application repositories.
4.) Auto-updates must be enabled for the mobile devices operating system and all applications running on the device.
5.) Device screen must be locked with a passcode, fingerprint, face recognition, or similar method.
6.) Device auto-lock must be enabled.
7.) If the device supports "Remote Wipe", this functionality must be enabled to permit the end-user to erase a lost or stolen device.

IT Security Awareness Training Policy

Version: 1.2
Created: 03/09/2021 - Updated: 3/31/2021
Reviewed: 4/12/2021
Approved: Pending Policy Management Board Approval – Submitted 4/19/2021

Purpose

UA Little Rock recognizes the importance of information technology as part of the university's processes. Therefore, in addition to technical controls, human behavior is also a critical component of the controls and efforts to provide a secure and safe computing environment to continue to provide research and education efforts. Therefore, a policy covering information security awareness training was developed.

Scope

This policy establishes standards for information security awareness training activities. Every UA Little Rock employee is responsible for doing their part to provide a secure and safe computing environment for every member of UA Little Rock campus and community. Therefore, this policy applies to faculty and staff working for the university.

Policy

To ensure compliance with UA System policies, UA Little Rock policies, laws, and regulations, employees should complete new employee security awareness training. UA Little Rock provides the appropriate education and training necessary to comply with the policies, laws, and regulations.

Information security awareness training is part of every new employee's onboarding process, and this training should be completed within two weeks of starting employment. In addition, every employee may be required to take additional or refresher training as the security landscape and / or threats against the campus technology landscape evolves.

Additional training courses such as HIPAA, PCI, or other security training, may also be assigned based on the business functions and tasks performed by the employee.

Failure to complete mandatory training in a timely manner may result in disciplinary actions. In addition to disciplinary actions, failure to complete training in a timely manner may result in having access to UA Little Rock technology resources suspended.