OIT Desktop & Laptop Requirements

1) All university-owned machines are required to be members of the Auburn AD Domain, or authenticate against the Auburn domain, and be in compliance with the current University Computer Authentication Policy.
2) All university-owned laptops will be equipped with at-rest encryption with central key escrow. BitLocker is the preferred solution for machines equipped with Microsoft OS's, and appropriate equivalents to be determined for other platforms. A working group to find whole-disk and file/folder encryption solutions with central key escrow will be formed to include members from across the campus IT community.
3) All university-owned desktops and laptops must be backed up centrally. TSM is currently the preferred system. If TSM is not practical for all platforms, then an alternative needs to be identified and implemented. A working group to review desktop backup alternatives will be formed to include members from across the campus IT community.

Portable Device (Tablet and cell phone) Requirements

1) All portable devices that are used to access AU email should use the ActiveSync protocol.
2) ActiveSync should be used to enforce a password requirement on portable devices used to access AU email.
3) The ability to use ActiveSync to "remote wipe" lost or stolen devices should be enforced.

General

1) All OIT employees should sign the most recent version of the Confidentiality form on an annual basis. OIT Administration will manage this process. A process to notify OIT employees of relevant policy changes will be formalized.
2) Rule-based forwarding of University email to an outside account is unacceptable for OIT employees. Forwarding personal emails to a personal account is acceptable.

Updated: September 3, 2014