Liberal Arts Information Technology Policies

- Liberal Arts Information Resources Use and Security Policy
- Absolute Manage Usage Policy
- Backup and Retention Policy

Liberal Arts Information Resources Use and Security Policy

INTRODUCTION

In support of the educational, research, and administrative mission of the College of Liberal Arts, this policy document outlines operational requirements for successful implementation of a safe, efficient, and productive common computing environment.

These policies supplement the Information Technology policies established by the University of Texas at Austin (Information Resources Use and Security Policy), the UT System (UTS-165), and the State of Texas (Texas Administrative Code 202). In case of any conflict, those institutions’ policies take precedence over policies documented here.

Departments or research groups may implement policies that supplement this document.

INTENDED AUDIENCE

All faculty, staff, and students in the College of Liberal Arts.

IMPLEMENTATION

To relieve the burden of policy implementation, Liberal Arts ITS provides departments, staff and faculty members with tools, procedures, and other appropriate assistance to implement these policies.

ACCEPTABLE USE

Faculty, staff, and student users of IT resources benefit from regular review of the University’s Acceptable Use Policy outlined in the CW 170 - IT Security Awareness module. The University requires all faculty, staff, and student employees to review and acknowledge the Acceptable Use Policy as part of regular compliance training.

COMPUTER REGISTRATION

Register all University-owned computers that use the College’s network with Liberal Arts Desktop Support. At minimum, include the following registration information:

- Media Access Control (MAC) address of each network interface adapter on the device.
- EID of the system’s primary user. For computers or devices used by multiple users, provide the name, contact information, and email address of the person responsible for the computer.

COMPUTER CONFIGURATION AND SOFTWARE
To ensure system reliability, common access to resources, and information security, University-owned computers will be configured with a baseline operating system and software configuration that includes appropriate virus protection, firewall security, and technical support software.

To ensure data security, University Policy requires encryption of all University-owned laptops using an approved method. Liberal Arts ITS provides tools and procedures to assist staff and faculty members with laptop encryption.

For any software installed on a University-owned computer but not covered by a University- or college-wide license, the department, staff or faculty member using the computer is responsible for maintenance of installation media, proof of purchase, software keys, or installation codes.

ACCOUNTS AND AUTHENTICATION

Authentication

Liberal Arts ITS maintains a centralized computer authentication system for the college. University-owned networked computers capable of using this authentication system are configured to verify login credentials with this system.

Administrator Accounts and Position of Special Trust

Staff or faculty members who require administrator or super-user accounts on computers or server systems must complete a Position of Special Trust form.

Sharing Account Credentials

In general, user account credentials for individual computers, lab computers, or server systems should never be shared. Notify the College's designated IT Networking Custodian or IT Security Custodian if technical or procedural circumstances require credential sharing or the establishment of a role-based or group account.

Passwords

Use complex and frequently changed passwords on all accounts used to access individual computers or server systems. Please refer to these guidelines for setting a strong password.

ADMINISTRATIVE ACCESS

To deliver timely and appropriate support, Liberal Arts ITS Desktop Support staff have administrative access to University-owned computers connected to the network. Administrative access is used only:

- At the request of the primary user or administrator of the computer.
- To apply operating system or software application updates or patches to the computer.
- To investigate suspicious computer activity that could degrade the network, violate college, university or state policies, or violate local, state, or federal laws. Investigative use of administrative computer access by Desktop Support staff requires prior approval from one of the following:
  - The primary user or administrator of the computer
  - The College's designated IT Networking Custodian or IT Security Custodian
  - An associate dean of the College of Liberal Arts or the assistant dean for IT
  - The UT Information Security Office (ISO)
Liberal Arts ITS maintains a list of all authorized staff with administrative access to University-owned computers. Staff granted this level of access receive training in the proper use of sensitive and confidential information in accordance with college and University policies and applicable local, state, and federal laws.

SERVERS

Centrally supported servers offer a range of financial, technical, staff, and security benefits. In general, departments, research groups, staff and faculty members will benefit from use of college- or University-supported server resources. Staff or faculty members whose role or research requires a server should contact the College's IT Systems Custodian to help assess this need.

To safeguard the network, encourage good use of resources, and aid in technical support, servers in use by departments, research groups, staff or faculty members must be registered with the College IT Systems Custodian. For each server, provide the names and contact information of primary system administrators, a list of services the server provides, and the system's physical and network information.

All servers should meet minimum security and system hardening standards as determined by the College's IT Systems Custodian.

For mail and messaging services departments should use University resources including Austin Exchange Messaging Server (austin.utexas.edu), UMBS (mail.utexas.edu), and UT Lists. Departmental or group mail servers are not permitted.

PHYSICAL SECURITY

As the primary user of your University-provided or personal computer, it is your responsibility to prevent its theft or loss. If your computer is lost or stolen, immediately notify UTPD (471-4441) as well as the Liberal Arts ITS Desktop Support staff (471-5000). Technical support staff will report the loss to the ISO, which may be able to aid in recovery of the system.

DATA SECURITY AND STORAGE

Department staff should store all role-based data critical to their job function in the appropriate departmental folder on the 'la' file share on Austin Disk.

If your role or research requires non-centralized storage, please consult the College's IT Systems Custodian.

INFORMATION SECURITY

Category I Data

The University requires special handling of sensitive data such as Social Security numbers, student information, student grades, financial information, and sensitive research data. For a detailed list of data that falls under this designation, please refer to the Extended List of Category I Data.

If you believe that Category I data may have been compromised, follow campus procedures for reporting computer security incidents.

Sensitive Data Control Plans
Faculty members or graduate students whose research requires a sensitive data control plan as indicated by the Office of Sponsored Projects, must file this plan with the College's IT Security Custodian or the custodian’s designee.

Student Information

Student information is governed by the FERPA statute, and is typically classified as Category I data. Instructors should use appropriate learning management systems such as Canvas to store required student information and to communicate with their students.

Third Party Vendors

University business data should not be stored on third-party resources. Special rules apply to the handling of university data by vendors and contractors (see section 5.26 of the IRUSP).

EXCEPTIONS

For exceptions to these policies, contact the appropriate College IT Systems, Networking, or Security Custodian to discuss your needs.

Liberal Arts Information Resources Use and Security Policy
Document Version: Approved
Last Edited: 11/07/2013 - timf