6.1 Acceptable Use Policy for Technology
Sponsor: CIO
Effective Date: July 1, 2018

Objective of Policy

The purpose of this policy is to provide guidance for acceptable use of technology systems by students, faculty and staff of LETU.

Policy

Acceptable Use

LeTourneau University (LETU) relies on University-owned networks (Networks), technology systems (Systems), and the data contained within and transported over those systems (Data) to achieve its mission. This Acceptable Use Policy is to protect these Networks, Systems and Data (collectively "Technology Resources") in accordance with state and federal law and LETU guidelines and policies and to ensure that LETU can access Technology Resources to fulfill its duties and mission. All individuals granted access to Technology Resources must be familiar with and follow the acceptable use rules below.

LETU Technology Resources are provided first and foremost to facilitate the business and mission of the University. Other use of University networks and systems is permitted so long as it does not interfere with the mission-related pursuits of others and remains within applicable guidelines and policies.

Technology Resources must not be used to: engage in acts against the mission and purposes of the University, misrepresent the University, intimidate or harass, degrade performance of Technology Resources, deprive access to a University resource, obtain extra resources beyond those allocated, or to circumvent security measures.

Technology Resources must not be used for the exclusive benefit of individuals or organizations that are not part of LETU unless work for an organization is approved by the Cabinet as necessary for the completion of a strategic project.

Use of Technology Resources must conform with LETU's Statement of Faith and Community Covenant.

Intellectual Property

Faculty, staff, students, contractors, guests, or other users (collectively "Users") must not copy or reproduce any licensed software except as expressly permitted by the software license, use unauthorized copies, or use software known to cause problems on LETU computers.

The presence of illegal material such as, but not limited to, unlicensed software, audio or video recordings, or other inappropriate/illegal material is not allowed and against many state and

federal copyright laws.

Commercial Use
LETU prohibits the use of LETU Technology Systems and Data for commercial purposes unless authorized in advance by the President's Cabinet in consultation with Information Technology.

University owned and operated technology resources, including hardware, software and other resources are intended for use in University-related initiatives, including promotion, projects and fundraising unless otherwise authorized in advance by the President's Cabinet in consultation with Information Technology.

Data Protection
All critical University data and electronic files, including business process, documentation, research and other data should be backed up for disaster recovery reasons. This data should be stored on network servers approved for this purpose unless other backup arrangements have been reviewed and approved in advance by Information Technology (IT). Details about current backup procedures are available on the IT Knowledgebase. Users of data stored in locations other than those documented on the IT Knowledgebase should consult with IT on current backup practices and options.

Users of LETU Networks and Systems must not attempt to access Data or programs contained on systems for which they do not have authorization or consent. Those with access to data storage locations should use that access on an as-needed basis only for the LETU purposes for which they have been provided access.

Required Software
All computer systems accessing LETU Technology Resources from any location worldwide must have an effective and up-to-date anti-virus product installed. Computers without active and up-to-date anti-virus software may be disconnected from LETU Technology Resources.

Virus protection software must not be disabled or bypassed except as required by the temporary installation of software or for other special circumstance. Computers found to be infected with a virus or other malicious code will be disconnected from the LETU network until deemed safe IT.

Operating Systems
Computers and devices used by students, faculty, and staff on LETU networks are permitted to run most operating systems, with the exception of Microsoft Windows Server operating systems, which are restricted to use in university data centers. Some operating systems allow special programs to emulate Microsoft file sharing features. These systems must be configured to emulate the behavior of Microsoft client operating systems. For personal systems it is the responsibility of the device owner to configure systems appropriately. For LETU Systems, IT will

assist with proper configuration.

Electronic Messaging Systems

The use of Technology Resources such as (but not limited to) e-mail to communicate with another individual when they have, verbally or in writing, requested an end to such communication is not permitted.

The use of unsolicited mass mailings to contact large quantities of people, whether associated with LETU or not, is prohibited. If someone has not consented to be part of a group email then you are not permitted to include them in a group mailing. Emails to small groups you are a member of (e.g. classes, clubs, friends) are acceptable as long members continue to consent to communications.

All e-mails sent from any LETU Technology Resource to an e-mail address not owned by LETU, or e-mails sent on behalf of LETU by third parties, must comply with the CAN-SPAM Act of 2003. (https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business) These e-mails and business processes must adhere to the following guidelines:

- The e-mails should have accurate header information. The "To:," "From:," and "Reply-To:" fields must be clearly identifiable as LETU addresses.
- The e-mails should have an accurate subject line.
- The e-mail should be clear as to its purpose.
- The e-mails must contain LETU's physical address.
- The e-mails must contain clear instructions on how the recipient can opt out of receiving future e-mails from LETU.
- LETU must honor the opt out request in a timely manner.

IT does not provide inclusive lists of student e-mail addresses to third parties. In addition, directory services which provide access to such information are designed to discourage or prevent the retrieval of large quantities of information. Users are prohibited from attempting to manually assemble such limited information into a broader database of any kind. As part of our services, IT may distribute official communication on behalf of LETU via e-mail or other method to all users as necessary to communicate critical or timely information on issues affecting our user community, but such opportunities are not provided to any third parties not involved with assisting LETU with its mission.

The following electronic messaging (including email) activities are prohibited:

- Posing as anyone other than oneself when sending messages, except when authorized to do so by the owner of the messaging account.
- Use of messaging software that poses a significant security risk to other Users on the LETU network.

- Sending or forwarding "chain" messages or any other message asking the recipient to forward a message to multiple additional recipients whose content is not related to LETU business process or academic activities.
- Sending unsolicited messages to large groups except as required to conduct University business in an approved manner.
- Sending or forwarding messages that are likely to contain computer viruses.
- Using LETU messaging systems for purposes of political lobbying or campaigning except as permitted by LETU policy.

Due to the design of the e-mail standard, delivery and timeliness of delivery of e-mail is not guaranteed and should not be used as an official transmission method for internal business processes, or between LETU and external organizations, or as a storage mechanism for critical Data.

Confidential or Protected Information
Users shall not disclose confidential or protected information except to authorized users as required to accomplish authorized business functions in support of the institutional mission.

All transmission or storage of confidential or protected data must be in accordance with the Data Classification Policy.

Incidental Use of Information Resources
Incidental personal use of electronic mail, internet access and other information resources by an employee is permitted by University policy subject to individual department guidelines but is restricted to employees (it does not extend to family members or other acquaintances). It must not interfere with normal performance of an employee's duties, must not result in direct costs to LETU and must not expose the University to unnecessary risks.

Internet Use
Access to the Internet is provided to authorized users for business, education, research, and patient care purposes. Authorized users include LETU faculty, staff, students and approved guests.

To facilitate network maintenance, performance monitoring and security requirements and to ensure compliance with applicable laws and policies, all user activity may be subject to logging and review.

Remote Computing
All devices accessing LETU data or technology systems must be protected with a strong password or complex, non-trivial unlock sequence to prevent access by unauthorized parties. Passwords or unlock sequences must be changed immediately if there is suspicion that the

password has been compromised.

Due to abuse of anonymizing services by phishing and other malware agents, access to LETU resources should not be made from services that mask source IP addresses or otherwise provide anonymous access to internet resources (e.g. anonymizing VPN agents or similar). Such connection attempts may be restricted.

Employees accessing LETU Technology Resources from a remote device must adhere to all policies that apply to access from within local campus networks. Remote devices configured to access LETU Technology Resources are subject to the same rules and security requirements that apply to University-owned computers.

Supervisors of employees who have been approved to work primarily or exclusively from home or from another non-LETU campus or site location must consult with Information Technology for guidance on required Remote Office technology.

In general, data important to or required for LETU operations must not be stored on end-user computing devices unless approved. Where approved, such data must be compliant with LETU's Data Classification Policy and backed up to an approved location for recovery in the event of a disaster or loss of information. This includes but is not limited to a local desktop "C drive."

Requesting Computer Accounts

All employees are granted university computer accounts. These are initiated by Human Resources (HR) when one is first employed and end when one ceases employment. Upon being notified of a new employee, IT obtains information to determine which Technology Resources are needed.

On occasion, someone who is not a university employee will need a computer account. Computer accounts may be provided to non-employees who need e-mail or other system access in their work with the University. Authorization for such accounts must come from those in the Executive, Administrative or Academic Administrative classifications.

On occasion, a former employee may need access to LETU Technology Resources after their employment is terminated. Such needs must be coordinated directly with HR in advance of the employee's separation in order for continued access to Technology Resources to be possible.

Wireless

- Wireless access points not owned by the University may not be connected to LETU networks and may not be configured to broadcast settings which imitate LETU wireless networks or in any other way interfere with the normal and secure operation of the LETU campus wireless network.

- The LETU wireless network is provided for use on personal devices by students, faculty and staff as long as such personal use adheres to LETU policy.
- The wired network is considered the primary supported campus network for LETU business processes.
- Use of the wireless network as the primary network on a device for business process or other official LETU purposes must be approved by Information Technology. Depending on the nature of such use, there may be cost associated with use of the wireless network as a primary network for a business process device as there is with the wired network.
- Occasional use of the wireless network by LETU-owned portable devices (such as laptops or tablets) is allowed when mobility is required but wireless devices may not be part of a critical LETU business process unless support for such a setup is approved in advance.
- University laptops should be plugged into a wired jack when serving as a primary office computer.

Decentralized Technology Resources

- To provide specialized capabilities and services quickly and conveniently, some technical resources at LETU may be operated and maintained by individual schools or departments where approved by the CIO or designee, such resources are referred to as decentralized technology resources.
- Decentralized technology resources may be connected to the University network if they are approved by the CIO or designee, are administered by qualified technical staff, and adhere to established policies.
- Decentralized technology resources may only be used for their approved purposes and may not offer services not already approved. In general, services which require access to the internet will require hosting in a University Data Center.
- Faculty, students or staff who are designated administrators of decentralized technology resources are responsible for maintaining the appropriate security environment on their systems, including current virus scanning software and operating system security updates.
- To protect LETU data and technology resources, decentralized computers or servers will be disconnected from the University network if a threat is posed from that system by a virus, cyber-attack or other means. The affected system may be reconnected once it has been restored to a safe condition.

Credentials and Passwords

- LETU computer/network accounts, passwords, personal identification numbers (PIN), digital certificates, security tokens (i.e. Proximity Card or Smartcard), or any other similar credential or device used for identification and authorization purposes must not be shared under any circumstances. Each user of LETU resources is responsible for all activities conducted using his or her account(s). Perceived needs for account or

credential sharing should be submitted to Information Technology via the IT Helpdesk so that an appropriate solution to the need may be created.
- Faculty/Staff passwords must be changed annually unless secured by LETU Multifactor Authentication (MFA).
- The password used for LETU must be unique to LETU and not used on non-LETU systems or services.

IP Addressing

- For student, faculty, staff and guest-owned personal devices, the option for "DHCP" or "Automatically obtain IP information" should always be used unless otherwise instructed by Information Technology. All other TCP/IP information including Gateways, DNS/Name Servers, WINS, etc. should be blank.
- Static IP Addresses are not permitted on LETU networks unless approved in advance by IT.

Network Extension

- **Switches:** Students are allowed to connect Ethernet switches to residential network jacks. Ethernet switches may not be connected to jacks in administrative or academic buildings without prior approval of IT.
- **Other Devices:** With the exception of the residential switch accommodation above, no network devices or software which extend the network beyond the LETU-provided jack or which connect other networks to LETU networks are allowed (including but not limited to wireless access points, VPN or other software solutions, or multi-homed computers used as bridges or routers).

Systems and Security

- Attempting to circumvent existing security measures or the spirit of such measures as deployed by LETU or by the owner of individual technology resources is prohibited.
- Attempting to disrupt service to any computer or computing resource is prohibited.
- The University makes common services available via server systems. Services to other users may only be provided from systems approved by LETU IT to provide such services. Systems other than approved LETU servers should not be configured to be reachable outside LETU's network.
- In general, connectivity to other computers should be limited to University servers (for the specific purposes for which they are made available) and to student computers with information sharing points which the user has been explicitly granted permission to access. Where it is obvious that information is available that another individual did not mean to make publicly available, it is the responsibility of the user making such a discovery to inform the other individual or IT as soon as possible and to avoid using the information in any way.
- Distribution of account information for any LETU Technology Resource to anyone other than the intended account holder is prohibited.

- With the exception of University-owned Terminal and Remote Access servers, remote access to a computer you do not own is prohibited (whether or not such access is authorized by the computer's owner). Students are allowed to remote control only computers they legally own that are connected to the LETU network and registered to their username. Remote control of student computers is permitted only to/from campus-based wired or wireless student networks (i.e. not from Faculty/Staff or off-campus locations). Remote control of Faculty/Staff workstations is not permitted unless authorized for business reasons. Contact Information Technology for more information on remote access to Faculty/Staff resources and best practices.
- End-user use or distribution of tools which provide packet sniffing, spoofing, port or service scanning or indexing, or other tracing functionality is prohibited on LETU networks.
- Users may not run DNS, DHCP, WINS, or MS Domain Server Services. Users are permitted to run the client versions of these services.
- Undue use of network resources (usage which is unusually intense and/or disruptive) even when otherwise engaged in acceptable activities is prohibited.
- Security programs or utilities that reveal or exploit weaknesses in the security of a system or that reveal data by circumventing established authorization procedures and systems should not be downloaded, distributed and/or used, except as authorized by IT. For example, password cracking programs, packet sniffers, or port scanners on University information resources are not permitted. Users must report any identified weaknesses in LETU computer security and any incidents of possible misuse or violation of this agreement to IT or an immediate supervisor or department head as applicable.
- Where technically feasible, all personal technology devices which access LETU technology systems (including PC's, laptops, tablets, and other devices) should be configured with a lock screen and automatic activation set at a short interval to prevent unauthorized access to the device. For LETU-owned devices, Information Technology will automate the configuration of local workstations in accordance with current University guidelines.

Policy Enforcement

- Devices or users not abiding by the LETU Policy may be disconnected from University technology systems at the earliest possible opportunity without prior notification.
- The Student Handbook details the various actions and restorations for our students under Technology Guidelines and Policies.
- Use of LETU Technology must also follow other polices published in the LETU Policy index.
- Policy enforcement action is never taken lightly, and policy enforcement decisions may be appealed through the standard appeals process outlined for all LETU users in the Student or Faculty/Staff Handbooks.

Definitions

Network: The collective entity formed by technology that secures access to and connects technology systems for the purpose of transporting, sharing and securing data.

Systems: University servers and all other technology owned or managed by LETU for the purpose of accomplishing its mission.

Data: Data contained within or transported across LETU Networks and Systems.

Technology Resources: Collective term for Network, Systems and Data

Certification Statement

This policy has been approved by the following and represents LeTourneau University policy and procedure from the date of this document until superseded.

President and Cabinet

The following individual is the policy's Senior Reviewer and is responsible for being the most knowledgeable about the policy, as well as supporting the execution of the policy.

Director, Network and Telecommunications Services

Policy History

Approved Policy Revision, February 3, 2010
Approved Policy Revision, September 21, 2011
Approved Policy Revision, June 18, 2018