Working Remotely and FERPA/HIPAA

Overview

It is always critical to comply with FERPA and HIPAA regulations when handling LETU data. However it is particularly vital to be aware of these regulations when working away from the LETU campus to ensure that data does not end up unprotected on systems which LETU cannot proactively manage and secure.

The following is not an exhaustive guide to FERPA or HIPAA compliance - please consult your supervisor or area leadership for specific guidance in your department for FERPA and HIPAA compliance. If questions remain at this point please contact IT for assistance determining the best way for your department to securely handle data.

If you experience uncertainty about the proper way to secure data when working remotely, please limit remote access to Confidential data to LETU's Remote Desktop Services until you are comfortable your questions about how to handle Confidential data in other environments have been answered.

Requirements for Personal Systems (including desktops and mobile devices) when remotely connecting to LETU data or systems

Any personal system used to connect to LETU OneDrive or LETU VPN services must meet the following requirements at all times:

- The system must be configured to automatically install security updates as they are released
- The system must be configured with an up-to-date antivirus/antimalware program (Windows 10's built-in Defender program is acceptable and strongly recommended for Windows 10 systems)
- The system must be configured with a password of no less than 15 characters
- The system must lock on inactivity
- No non-LETU users (including other household members) may use the login account configured with local OneDrive sync or VPN access. Secondary (non-administrator) accounts may be created for other household users on that same machine if needed.

Any personal system used to connect to LETU Remote Desktop Services must meet the following requirements at all times:

- The system must be configured to automatically install security updates for the operating system as they are released
- The system must be configured with an up-to-date antivirus/antimalware program (Windows 10's built-in Defender program is acceptable and strongly recommended for this purpose)
- LETU Remote Desktop Services must be disconnected when the Faculty/Staff member is away from the desktop. As an alternative, the Faculty /Staff member may leave their session connected when away from their computer if:
    - their computer is setup with a password 15 characters or greater
    - their computer is configured to lock on inactivity
    - no other household users have access to the user account

Data Classification

- The LETU Data Classification Policy Classifies data as ***Restricted***, ***Confidential*** and ***Unrestricted***. Definitions of those terms are in the LETU Faculty/Staff Policy handbook under *Policy 6.2 Data Classification* which all LETU Faculty/Staff are responsible for being familiar with.
  For convenience - a summary of these data classifications is below, however for complete guidance faculty and staff must consult the entirety of policy 6.2.

	Restricted	Confidential	Unrestricted
Guideline	Data protected specifically by federal or state law or university or system rules and regulations (e.g. HIPAA, FERPA, Sarbanes-Oxley, Gramm-Leach-Bliley, Texas Identity Theft Enforcement and Protect Act). Also includes data that is not protected by a known civil statute or regulation, but which must be protected due to contractual agreements requiring confidentiality considerations.	Data not otherwise identified as Restricted data, but which are releasable in accordance with the Texas Public Information Act (e.g. contents of specific e-mail, data or birth, salary, etc.). Such data must be appropriately protected to ensure a controlled and lawful release.	University data not otherwise identified as Restricted or Confidential data (e.g., publicly available). Such data has no requirement for confidentiality, integrity, or availability.
Common Data Elements	Social Security Numbers Credit Card Numbers Banking Account Numbers Driver's License Numbers (See Appendix A)	Information protected by HIPAA (see Appendix A) Information protected by FERPA (see Appendix A)	

Restricted data is prohibited from being stored anywhere except on LETU-managed databases, servers and back-end systems. You should never have a reason to store ***Restricted*** data in personal storage, even in LETU-provided personal storage such as OneDrive or MyDocuments. If you are uncertain how to correctly handle the need to work with ***Restricted*** data as part of your job responsibilities, please first consult your supervisor and then if necessary IT for further guidance.

Confidential data includes data where every effort should be made to store the data on approved systems instead of personal storage, but where it is acceptable to store copies of ***Confidential*** data in approved, secured storage locations as long as specific guidance is followed. Please see **OneDrive and FERPA/HIPAA** for more information. You **must** ensure you are familiar with the requirements for correctly configuring OneDrive folder sync settings before storing ***Confidential*** data on OneDrive.

Wherever possible, items like grades, addresses and other ***Confidential*** data should reside in CX, Canvas or other LETU-managed servers and systems. Please make every effort to minimize the storage of this data outside those locations. For cases where ***Confidential*** data may need to be securely used outside these back-end systems, all Faculty/Staff are responsible for following the guidance at **OneDrive and FERPA/HIPAA** if they choose to store ***Confidential*** data outside of LETU back-end servers and systems.

OneDrive and FERPA/HIPAA

Consult **OneDrive and FERPA/HIPAA** for guidance on secure storage of LETU data on LETU OneDrive.

Other Cloud Services

LETU's internal policies as well as compliance requirements with federal and state regulations such as but not limited to FERPA/HIPAA prohibit the storage of LETU-related data (whether Confidential or Unrestricted) or discussion/exchange of such data on any non-LETU-managed cloud services including all personal cloud storage and collaboration services. This includes but is not limited to such services as Box, Slack, Zoom, or other technology services.

If you are uncertain how best to utilize OneDrive, Teams, LETU local file services and other technology resources to manage data exchange and collaboration needs, please contact IT.

Remote Access Methods

LETU's **Remote Desktop** services are the only method which should be used for access to desktop resources from outside LETU's campus. Typically Remote Desktop services are provided through our TS1 Remote Desktop solution. In some cases, secure access to other resources on campus is available through remote desktop upon request to IT.

LETU's *Faculty/Staff Policy Handbook 6.1 Acceptable Use of Technology* prohibits the use of remote access methods other than those directly supported by LETU in order to avoid the risk of unintended compromise of LETU technology resources through personal computing systems and technology.

If **Remote Desktop** services are not meeting your need for remote work or instruction, please contact your supervisor, and if needed IT for assistance with unmet needs.