Data Protection Policy		*Department:* **Information Technology Services** *APP No.*	
Department Vice President: **Vice President for Finance & Administration/CFO**	*Revised:*	*Original Effective Date:* November 16, 2020	**Page 1**
Subject: The Linfield University Data Protection Policy addresses the actions required for data security when working off-campus, to protect the university's information, resources, computing and network infrastructure.		*Applicable Divisions:* **All**	

PURPOSE

These guidelines describe actions you can take to protect University information and resources when working outside the on-campus computing and network infrastructure and when using personal devices.

By reviewing these Guidelines, you will become familiar with best practices and the University's expectations when using or accessing computing resources and/or University data from "off-campus" and when using personal devices. These Guidelines include expectations for the use of both University provided and managed devices and personally owned devices when working off-campus and for the use of personally owned devices when working on-campus or off-campus.

RESPONSIBILITIES

When working remotely with University information or resources or when using a personally owned device, you are responsible for your working environment. You are responsible for protecting Linfield data and systems and for complying with all related laws and regulations and University policies, guidelines, licenses, and agreements.

POLICIES

- Policies and Handbooks
- Acceptable Use Policy

PASSWORD AND ACCOUNT BEST PRACTICES

- Maintain different account names and passwords across platforms and applications. Do not use the same password for personal accounts as you do for Linfield related accounts. Try to keep personal account names from matching your login name for public sites like Gmail, NetFlix, and Facebook.

- Use long passwords, utilizing phrases or sentences. The password "SheSellsSeaShellsByTheSeaSh0re" is extremely more difficult to hack than "F%Gih^&40!" and yet easier to remember.
- Never give your password to anybody.
- Always manually log out of anything you logged in to when you are finished.
- Read more on creating a secure password

DATA STORAGE

While working remote do not store confidential data on any unencrypted laptop or device. For confidential data users can VPN into the campus and work directly from Winfiles/Pyramid or other approved applications. Visit the Data Storage page on the ITS site to learn about the storage options. Visit the Data Classification Chart to understand which data is confidential, restricted, or unrestricted.

VIRTUAL PRIVATE NETWORK (VPN)

Linfield University uses the Cisco Anyconnect client for secure connectivity. The client is available for MACs and PCs. This client should only be installed on Linfield assets, or as instructed by ITS.

- VPN is required when accessing Colleague, network file shares, and other applications hosting confidential data. View the ITS Data Classification Chart. VPN is not required to submit grades, access Blackboard, email, Microsoft Teams, OneDrive, Office 365, or Zoom.
- Always disconnect from VPN before walking away from computer

PHYSICAL SECURITY

- If you access confidential or restricted data, you will want to make sure this information is for your eyes only. Do not position your screen so it can be viewed by others. This includes having your screen facing a window.
- When devices are not in use make sure they are stored in a secure location.
- Lock Screens - When you are away from your computer you should manually lock the screen or log out of your account. This is best practice for on campus and remote work.
- If you setup your phone to access Linfield email, or other resources, make sure to lock the screen when you walk away from your device. Do not share your code to access your phone. If you need to share the device remove access to any Linfield resources.
- Make sure you pay attention to shoulder surfing. If you access confidential or restricted data, you will want to make sure this information is for your eyes only. Do not position your screen so it can be viewed by others. This includes having your screen facing a window.

Wi-Fi

- Avoid using public “free Wi-Fi” with assets that are used to VPN or attach to Linfield’s Network.
- Never join “ad-hoc” networks
- Use only secure Wi-fi - Use WPA2 or WPA3 for wireless encryption; avoid using the older WEP security standard because it can be easily hacked.
- Make sure your home Wi-Fi is setup with a strong password.

SOFTWARE

- Only install trusted software
- If you are unsure if you should install a piece of software contact the ITS Service Desk.

DEVICE SHARING

- Linfield owned computer/tablet should only be used for work related business, and not used by anyone except the employee.
- It is important to keep your child’s digital curriculum separate from your work device. Both are huge targets for threat actors.

EMAIL

- Do NOT send confidential or restricted information (SSN, Banking info, health records, credit card numbers, etc.) over unencrypted email. There is an encryption feature in Outlook if you are required to email confidential or restricted information.
    - After sending encrypted email, the original message is stored in your Outlook “Sent Items” folder and not encrypted. This means that the information in the email message could become compromised if someone other than you gain access to your account. Deleting these messages from your “Sent Items” helps protect the privacy of your recipient. To ensure that the message is permanently deleted from your email account you also need to delete the messages from the "deleted items" folder. This two-step deletion provides you with a means to recover emails just in case you accidentally delete something.
- Ultimately, confidential data should be stored on Winfiles. You can reference the location of a file in an email instead of attaching the file. Data Classification Chart
- Do not send work-related emails from your private email address and vice versa.

PATCHES AND ANTI-VIRUS

- All operating systems, including Windows and Mac OS, should be set to auto update. If prompted to update, follow the instructions to complete the update.
- For Windows Clients, Defender Firewall should be set to on for Domain, Private, and Public networks always.
- For Apple Mac OS Clients, the Mac Application Firewall should always be on.
- More virus information

PERSONAL DEVICES

If you access Linfield resources on your person computer, tablet, or phone you will need to make sure you are securing your device.

- Require password on device.
- Require a passcode on Phone
- When possible create a separate work account on your personal device.
- Do not share your password for a computer/laptop and do not share your passcode for mobile devices.

BEWARE OF PHISHING, SCAMS AND FRAUD

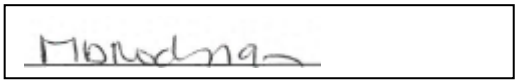
- Do not click on links received in emails from unsolicited or untrusted sources. Best to type in the URL (address) or visit the site directly.
- Do not open unsolicited on unexpected, shared documents and email attachments.
- More information on phishing

LINFIELD SUPPORT SOFTWARE

- **Microsoft 365**
  Microsoft 365 includes: Outlook, Teams, Word, Excel, PowerPoint, and a variety of other solutions. These applications are part of a suite of tools that enhance your remote work experience. Visit http://portal.office.com/ or https://myapplications.microsoft.com/.
- **Outlook**
  Linfield hosts email with Microsoft as part of the Microsoft 365 product line.
- **Microsoft Teams**
  Microsoft Teams is a secure chat and collaboration solution. Microsoft Teams is part of the Microsoft 365 suite of tools.

- **Zoom**
  Zoom is a video conferencing tool used for meetings, classes, and campus events. Zoom has a chat feature that provides a communication channel for Linfield users. Zoom can be used for HIPPA related meetings or conversations, that feature does require setup. Contact ITS to setup your account.

Date Issued: November 16, 2020
Date Last Revised:
Responsible Executive: Vice President for Finance and Administration
Responsible Office: CIO/Information Technology Services



Vice President, Finance and Administration/CFO Date: November 16, 2020