Banking Encryption
Sensitive Data – Banking Information

Internal Control Guidance

• Sensitive data should be stored in SharePoint or OneDrive
  • Note: OneDrive is stored in SharePoint but provides a personal drive
  • Google drives are not secure and should NOT be used for sensitive data
• Do not electronically forward banking information unless using email encryption
  • Outlook – Options – Encrypt – “Oregon State University – Confidential”
    • If sending outside OSU: Outlook – Options – Encrypt – “Encrypt Only”
    • Do NOT send banking data through Teams

UIT is exploring utilizing a blanket rule in Microsoft to automatically encrypt messages that are marked/determined to be sensitive data, but this does not work for shared email accounts – and you should not wait for this solution to be fully deployed.
Microsoft Outlook Steps

Before sending a message that contains banking information – select Options in the top ribbon
Choose the level of Encryption

When the encryption is selected, a message will appear defining each level.

- **Encrypt-Only** - This message is encrypted. Recipients can’t remove encryption. Permission granted by: heather.hesano@oregonstate.edu

- **Do Not Forward** - Recipients can read this message, but cannot forward, print, or copy content. The conversation owner has full permission to their message and all replies. Permission granted by: heather.hesano@oregonstate.edu

- **Oregon State University - Confidential** - This content is proprietary information intended for internal users only. This content can be modified but cannot be copied and printed. Permission granted by: heather.hesano@oregonstate.edu

- **Oregon State University - Confidential View Only** - This content is proprietary information intended for internal users only. This content cannot be modified. Permission granted by: heather.hesano@oregonstate.edu