Security Requirements for Using Approved Cloud Storage Solutions and for Emailing Confidential Information

University Personnel* who maintain any information that is protected under applicable federal or state law or regulations, including, but not limited to, FERPA, HIPAA, PCI, or GLBA, or under terms of a University contract (“Confidential Information”) are required to protect that information by ensuring the information is stored only on secure devices or servers or in secure storage. Legal actions and fines may result from violations of contracts or federal or state law or regulations, including but not limited to, HIPAA, FERPA, PCI and GLBA.

University Personnel must set strong passwords, as defined in the University’s Password and Account Policy, and must encrypt emails that contain Confidential Information, as described below. Before storing any Confidential Information on a portable device, desktop computer, or other electronic device, University Personnel must encrypt the device or equipment or contact 405-325-HELP to have the device or equipment encrypted. The device or equipment must also be registered with IT Security. Instructions for encrypting your devices and emails and registering devices with IT Security can be found below.

* University Personnel: Faculty, staff, volunteers, students and trainees, and other persons whose conduct, in the performance of work for the University, is under the direct control of the University, whether or not they are paid by the University (also referred to as “Workforce Members”). 45 C.F.R. § 160.103

Encrypting Your Computer’s Hard Drive

Encryption requires more than using a password. University Personnel who store Confidential Information on electronic devices must submit an email request to security@ou.edu for encryption of those devices. The request must include machine type and Operating System (OS) version. OU Information Technology will provide an encryption enrollment client for the user to install on the device. Following installation, the client will report to IT that the machine remains encrypted, when queried. The client also allows the encryption key to be stored and backed-up in case it is lost or forgotten.

**WARNING**: Users must follow these steps completely. Losing your encryption key can render a machine unusable, preventing retrieval of any data from the drive.

**BitLocker for Windows Devices**

1. Click Start, click or search for Control Panel, then click BitLocker Drive Encryption.
2. On the BitLocker Drive Encryption page, click Turn On BitLocker next to the primary disk volume (C:\). **NOTE**: An administrator or administrator account will be required to complete this step.
3. If the TPM module is not initialized, you will see the Initialize TPM Security Hardware wizard. Follow the directions to initialize the TPM and restart your computer.
4. On the Save the recovery password page, you will see the following options:
   a. Save the password on a USB drive.
   b. Save the password in a folder.
   c. Print the password.
5. Use one or more of these options to preserve the recovery password.
6. Drive encryption will take time to complete (several hours to a day or more). You should be able to restart your computer as needed. It will pick up encrypting again automatically until complete.
7. That’s it! Ensure you record / remember your passphrase or key. You will need it to boot your machine.
8. Email security@ou.edu with your machine type and OS version to receive instructions for enrolling your machine and backing up your encryption key.
FileVault for OSX devices

1. Open System Preferences.
2. Click the Security & Privacy icon in the System Preferences window.
3. Click the FileVault tab.
4. Click the lock icon and enter an administrator name and password.
5. Click the “Turn on FileVault” button.
6. If you enable FileVault on a Mac with more than one user account, you’ll be asked to identify which users can unlock the startup disk as part of setup. Click enable next to a user name to let that user log in to your Mac at Startup. Then, enter the password for that account.
7. Choose a recovery option:
   a. In OS X Yosemite and later, you can store your key in iCloud. You can use your iCloud account name and password to unlock your startup drive or reset your password.
   b. In OS X Mavericks, you can share your FileVault key with Apple by answering a set of security questions. You can then contact Apple Support if you forget your login password and need to decrypt your startup drive.
   c. You can also create a recovery key that consists of a combination of numbers and letters. You can use this key to unlock your drive or disable FileVault. Keep a copy of this key somewhere other than your encrypted disk.
8. Restart your Mac. When FileVault is enabled, you can’t log in automatically. A password is always required when you start up your Mac.
9. Encryption of the hard disk will take time (several hours to over a day). You can continue to use the Mac as normal. You should be able to restart your computer as needed. It will pick up encrypting again automatically until complete.
10. That’s it! Ensure you remember your passphrase or key. You will need it to boot your machine.
11. Email security@ou.edu with your machine type and OS version to receive instructions for enrolling your machine and backing up your encryption key.

Using Email Encryption OU IT offers message encryption that allows University Personnel to send secure emails. Message encryption must be used when sending Confidential Information or sensitive data via email. Message encryption is available only to ou.edu and ouhsc.edu email account holders.

- Messages between ou.edu and ouhsc.edu email addresses are automatically encrypted.
- To send an encrypted email message from an ou.edu address to a non-OU email address, type [ouencrypt] in the subject line, using the brackets.
- To send an encrypted email message from an ouhsc.edu account to a non-OU email address, type [secure] in the subject line, using the brackets.
When an encrypted email is received the recipient may open the email by clicking on the attachment:

[OUENCRIPT] Test of Encrypted Email

Thursday,
To:

message.html (135.3 KB) [Preview]

You have received a secure message from the University of Oklahoma. Please click on the links below to view the contents of this message.

To view your message
Save and open the attachment (message.html), and follow the instructions.
Sign in using the following email address: recipient's name@ou.edu

CONFIDENTIALITY NOTICE: This e-mail communication and any attachments may contain confidential and privileged information for the use of the designated recipients named above. If you are not the intended recipient, you are hereby notified that you have received this communication in error and that any review, disclosure, dissemination, distribution or copying of it or its contents is prohibited. If you have received this communication in error, please destroy all copies of this communication and any attachments.

Message encryption by Microsoft Office 365

INFORMATION TECHNOLOGY

Once the attachment is opened the recipient will be prompted to sign in or use a one-time passcode to view the email. To sign in, use your OU email alias:
Once you’re signed in, you should be able to view the email.

To use a one-time passcode, click on Use a one-time passcode.

Then you will receive a message that a passcode has been sent.
We sent a one-time passcode to recipient@email.com.

Please check your email, enter the one-time passcode that corresponds with the reference code and click continue. The one-time passcode will expire in 15 minutes.

Reference code: 6224
One-time passcode

[ ] This is a private computer. Keep me signed in for 12 hours.

Continue

Didn’t receive the one-time passcode? Check your spam folder or get another one-time passcode.

Check your email for the passcode, and enter it into the site. The passcode expires 15 minutes after it is requested.

Your one-time passcode to view the message

Office 365

Here is your one-time passcode

88509013

To view your message, enter the code in the web page where you requested it. This one-time passcode matches reference code 6224.

NOTE: This one-time passcode expires 15 minutes after it was requested.

Don’t want to use one-time passcode every time you get a protected message? Use your email address to create a Microsoft account

Click continue and the message will be displayed.