Your Responsibility for Electronic Data and it's Retention at CSU

The responsibility for data and its security is governed by several different University Policies.

How long do I have to keep Electronic Data around?

- How long you keep data is governed by the University's Records Retention Policy located at: http://www.csuohio.edu/offices/recordsretention/. This policy will inform you of the procedures surrounding electronic records and how long the various records are to be retained.

How long do I have to keep email?

- Email retention is also governed by the University's Records Retention Policy located at: http://www.csuohio.edu/offices/recordsretention/. This policy informs you of what categories of email must be retained and in what form. By default, all CSU email is backed up nightly but deleted emails are not retained beyond 30 days. It is your responsibility to read the Records Retention Policy and act accordingly with your emails.

How do I deal with Administrative Data?

- The use of Administrative Data is governed by the University Administrative Data Policy located at: http://www.csuohio.edu/offices/ist/technologypolices/UniversityAdministrativeDataPolicy.pdf. This policy informs you that official Administrative Data (Student, HR, and Financial data) is backed up by IS&T as part of its nightly backup process. Proper authorization is required to view and use, and there are rules surrounding its use. There are three categories of Administrative Data: General Access Data, Limited Access Data, and Sensitive Data. At no point is Sensitive Data (data containing specific and protected information about students, faculty and staff) to be stored locally on a computer's hard drive or any media (CD, thumb drive, etc.). Sensitive Data may only be stored on secured storage in the University's Data Center.

How do I secure working data located on my PC or local server?

- Securing working data is done according to University Policy (University Information and Technology Resources General Policy and University Hardware Policy). Technology Policies are located at: http://www.csuohio.edu/offices/ist/technologypolices/index.html. You are responsible for securing and backing up data stored on your PC or local server. This involves ensuring that your machine is kept up-to-date with operating system and application patches, that your machine is using the University's licensed malware tools that are kept up-to-date, that you practice safe web browsing and computer use, that you follow secure password guidelines (University Password Policy) and that you keep your working data backed up on a regular basis.

How do I backup data on my PC or local server?

- There are several options available to you:

1. Your department can purchase networked storage from IS&T ($6.00 per Gigabyte per year). This is IS&T's preferred method for you to backup your working data. This storage is automatically backed up nightly and allows you to recover your data directly. This storage also can be shared by different users based on rules defined by the department.
2. You can backup your data (but not sensitive data) to an Optical Drive such as a CD drive or DVD drive. It is, however, your responsibility to secure these disks properly.
3. You can backup your data (but not sensitive data) to a removable drive such as a USB Thumb Drive or a removable or USB hard drive. Again, it is your responsibility to secure these drives properly.
4. You can backup your data (but not sensitive data) to a tape drive. Again, it is your responsibility to secure these tapes properly.

There are legal reasons why you should not use off-campus, publicly available storage to store or backup University data (i.e. publically available backup sites or data storage sites).