**1. What is data management?**

[**Data management**](https://www1.udel.edu/data) is the responsible stewardship of data throughout its lifecycle.

There are five components to data management:

* **Acquisition**—What data is acquired, how, and why?
* **Utilization**—How is the data used? Does the use support an institutional need or University activity?
* **Maintenance**—For how long is data retained? What are the data management rules?
* **Access**—Who is authorized to access, under what requirements, and under whose approval?
* **Protection**—How are the [**confidentiality, integrity, and availability**](https://www1.udel.edu/security/data/) of data maintained?

Effective data management requires appropriate acquisition, utilization, maintenance, access, and protection of data. Data management depends on information [**confidentiality**](https://www1.udel.edu/security/data/confidentiality.html) and [**criticality**](https://www1.udel.edu/security/data/criticality.html).

**2. How does proper data management help me?**

Proper [**data management**](https://www1.udel.edu/data) is a responsibility of every University employee; you are responsible for any University information to which you have access. Properly managing the data in your care will help protect you, the University, and the community from data-related harm.

Improper data management can lead to [**IT security incidents**](https://www1.udel.edu/report), which are a cause of identity theft, reputational harm, lawsuits, and extremely expensive damages. The goal of data management is to appropriately manage these risks without impairing University operations.

**3. How can I manage data safely?**

The best way to manage data safely is to recognize that it's an integral part of your job responsibilities and to incorporate it into your workplace routine. Turn safe computing and information behavior into [**new habits**](https://www1.udel.edu/security/bestpractices), and be mindful of how your actions affect the security of your data and devices.

Knowing what kinds of data you use, as well as how and where you use them, is the first step. This knowledge will help you maintain a cleaner system and respond more quickly to possible IT security incidents.

Review the [**Secure UD Essentials**](https://www1.udel.edu/essentials.html) and [**best practices**](https://www1.udel.edu/bestpractices) for information security and take note of opportunities for you to improve the way you manage the data in your care. Be aware of and understand your responsibility to support unit security efforts. Your unit will have an information security plan that describes the requirements and processes for protecting IT resources.

IT provides [**tools and services**](https://www1.udel.edu/resources) to help you manage the data in your care and meet information security standards. Some of these tools and services may also be offered locally through your unit.

**4. How do I know whether I have sensitive data?**

In many cases, sensitive data is hidden in larger data sets or files. To [**find sensitive data**](https://www1.udel.edu/security/bestpractices/inventory.html) on your computer, download a program to detect sensitive data and use it to scan your computer. Upon completing a scan, it will generate a report that will assist you in finding and protecting any unencrypted sensitive information, including Social Security numbers, on your computer or drives.

**5. How do I protect the data I have?**

Once you determine what data you have and where it's stored, you can protect it by [**archiving, encrypting, or erasing it**](https://www1.udel.edu/security/bestpractices/inventory.html) as appropriate.

For sensitive University information:

* If you still need the information, but don't need to store it on your device, archive it on a network drive or by contacting [**University Archives and Records Management**](http://www.udel.edu/Archives/).
* If you need the information and it must be stored locally on your device, [**encrypt it**](https://www1.udel.edu/security/bestpractices/encryption.html).
* If you no longer need the information to fulfill an operational requirement, [**securely erase it**](https://www1.udel.edu/security/bestpractices/disposal.html) from your device.

You can apply the same principles to your personal information. If you don't need to store records like old tax returns, bank statements, or other records on your computer or other device, you can store them on an encrypted flash drive or external hard drive and then securely delete them from your device. You should also encrypt any files that you choose to keep on your device (and encrypt the device itself with [**whole disk encryption**](https://www1.udel.edu/security/bestpractices/remoteprotection.html)).

**6. What is a backup?**

A backup is a copy of the data stored on a device. It's useful for restoring data if your device crashes or continuing work if your device is lost or stolen.

When you [**back up your data**](https://www1.udel.edu/security/bestpractices/backups.html), you create a copy of some or all of the files on your device and store them in a separate location (which is usually either on a flash drive, removable hard drive, or in the cloud). Some kinds of backups even store your device configurations. Backup and recovery software can automate the backup process by performing backups based on a set schedule.

To restore data from a backup, you use either recovery software (to restore full backups of a device's data and configurations) or manually replace files with copies from the backup (usually to restore lost or corrupted files).

**7. How often should I back up my data?**

It depends on how [**critical**](https://www1.udel.edu/security/data/criticality.html) that data is. If it's important that your data be accurate and available (to you or others), you should consider backing it up often. For example, you may want to back up critical project data at the end of each day or week.

You can use backup and recovery software to automate the backup process and remove much of the effort involved in performing backups.

**8. What is encryption?**

[**Encryption**](https://www1.udel.edu/security/bestpractices/backups.html) is a means of protecting files and devices. When you encrypt a file, you "lock" it with an encryption key or password. The file itself is scrambled and becomes unreadable without the appropriate key or password.

Faculty and staff are required to encrypt [**portable devices**](https://www1.udel.edu/security/bestpractices/remoteprotection.html) (laptops, tablets, smartphones, and removable storage media) and sensitive University information.

IT recommends that all members of the University community also encrypt their personal devices and sensitive files to protect them from misuse. Don't leave your data defenseless against thieves and hackers!

**9. Can I just erase sensitive data?**

No. Sensitive data needs to be [**securely erased**](https://www1.udel.edu/security/framework/program/index.html) to ensure that it can't be recovered.

When you delete a file using your computer's Recycling Bin (Windows) or Trash (Mac) feature, what you're actually doing is telling your computer to forget where that file is located. The file itself—and all the data it contains—is still on your computer, and hackers can still find it if they search your device's memory. In order to prevent a file from being recovered, you must securely erase it. When you securely erase a file, your computer overwrites it with randomly generated data to destroy its original contents, ensuring they can't be recovered.

Always securely erase sensitive files to prevent them from being recovered and compromised.

**10. Can I use email to send sensitive data?**

You shouldn't use email to send or receive sensitive data. If an email account is hacked or if the email is forwarded, that sensitive information could easily be exposed to someone other than the original, intended recipient. Instead, use a secure file transfer service like [**UD Dropbox**](https://www.udel.edu/it/help/dropbox/) or a secure Web form.

If, for some reason, alternatives are not available and you must use email to transmit sensitive information, that information must be encrypted. Encrypt the file first, then send the encrypted file as an attachment. Contact the recipient separately to provide the encryption password. **Never send sensitive information in clear text.**