Today we are going to discuss protecting sensitive data. I’m sure that, for the most part, you already know what sensitive data is and why it should be protected. The main focus of this presentation is going to be giving you some tools and resources that you can use to keep that data secure.
Sensitive data means any data associated with an individual, including but not limited to social security number and data that is protected by Board policy, or state or federal law. Most of you deal with some form of sensitive data every day. This may be a piece of information widely regarded as sensitive, such as a social security number. It could also be something that you may not think of as sensitive data. Student records, grades, and student ID numbers are also considered sensitive information.
The Family Educational Rights & Protection Act of 1974 or FERPA protects student coursework, class discussions, recorded comments, and grades if they are linked to any information that would enable a member of the school community to identify the student. There are penalties for violating FERPA. These can even include schools losing federal funding if they are found negligent in the protection of student data.
There are many important reasons why sensitive data must be guarded. Some of this information can be used by criminals to steal someone’s identity. There is also a chance that data loss could result in making protected information public. In addition to that, we must be in compliance with Federal and State Laws as well as the Board of Regents and UNLV Policy. However, the most important reason for keeping sensitive information protected is that it’s the right thing to do. We have a responsibility to protect the data of our students.
I have narrowed this discussion down to four basic steps that you can take to protect your sensitive data. We will discuss each of these in more depth as we go along with some resources that will help you with accomplishing each step. The first step is to inventory your assets. This will give you a clearer picture of what needs protecting. Next, focus on disposing of data that you may have accumulated but is no longer needed. Then, look at ways of protecting the data that you do need to keep on record. Finally, if there is a loss of data, we will look at the importance of reporting it in a timely manner.
When you take an inventory of your assets, it is important to consider all mediums that may have been used in the past to store sensitive information. These could include: computers (both home & office), external hard drives, CDs or floppy disks, flash drives, or printed hard-copy files. All of these places can potentially house sensitive data that is either unprotected or no longer needed and can be destroyed.
There are a couple of tools available to help you locate sensitive data that you may not be aware of on a computer system. The first is a commercial product called Identity Finder. It is not provided by UNLV OIT so if you decide to purchase it, that would be at the discretion of your department. This is a very good product and very user-friendly. It has a high find-rate for valid information such as SSNs and credit card numbers. However, it will also find some false positives. The program does include a preview pane though so you can view each document and see if the result is really a valid result or a false positive.

The second option is a free program that was developed by Virginia Tech. It does the same thing as Identity Finder but doesn’t have the fancy user interface. It also has a lower accuracy than the commercial product. However, it may be an improvement over searching the computer manually if you don’t wish to pay for a commercial product.

(Demo Identity Finder and Find_SSNs)
After taking a thorough inventory of the sensitive data in your possession, the next step is to securely dispose of any information that is no longer needed. Digital files need to be SECURELY deleted. Simply putting them in the trash or recycle bin and emptying it does not remove them from the hard drive. Instead, the space they occupy is simply marked as “Available” until another file needs that space and overwrites them. So even after you think you have deleted a file, the free space on your hard drive may still contain many files that haven’t yet been overwritten. We are going to cover a couple of free utilities that will securely delete files so that they can’t be recovered.

Destruction of hard-copy files is much easier. They should simply be shredded in a good crosscut shredder or placed into a locked bin designated for shredding if your office has one available. Most good shredders also are able to destroy CD media as well. This is a great way to get rid of unneeded CD backups.
If you refer to your handouts, I am going to cover a few utilities that can be used to securely delete files. All of these are free to download and use. The first one for Windows users is called Eraser. After installation, the program integrates with Windows. By right-clicking on the Recycle Bin, you can securely erase the contents. If you right-click on an individual file, there will also be an “Eraser” option to securely remove that file. This program also allows you to set up tasks such as: “Securely erase all files in XYZ folder at 4am every Friday.”

In the options on all of these utilities we are going to talk about, you will see an option for “erase method” or something similar. This refers to the number of times that the program will overwrite the file with random data. A good balance between security and speed is the 3-pass option. While more passes are theoretically more secure, they also take much longer to complete. If you are wiping a large file or the free space on your hard drive, the time difference could be significant.
Not to be confused with Eraser is our next utility, EraserDrop Portable. This application is considered “portable” because it doesn’t require any installation to use. You can simply download the compressed file from the link and run it. It will create a folder that can be kept on your desktop or a flash drive and run from there.

When you run this utility, it creates a small icon on your desktop. To securely erase files, just drag them onto that icon. By right-clicking on the icon, you can also run other tasks such as: “Wipe Recycle Bin” and “Wipe Free Space”
The last tool listed on the handout is called CCleaner. It is a bit more involved because it does many other things in addition to securely deleting files. You can also use it to clear temporary files from your machine in order to keep it running at peak performance. To do a secure delete with this program, you would first move the files to the Recycle Bin. Then in the settings you choose the option for “Secure File Deletion” and check the box for “Recycle Bin”. You also have the option to wipe free space on the drive as shown in the pictures.

The CCleaner tool is also available for Apple OSX users. It will work with OSX 10.5 and newer. There is a separate link on the handout for the OSX version, but the user interface is generally the same as the Windows one. For this reason, we will not cover it separately in the OSX section.
Now here is a chance for you Apple people to profess superiority over Windows. Since version 10.3 of OSX, Apple has included the Secure Empty Trash in their operating system. You don’t need a separate utility. You can simply place the files in the Trash and then go to Finder>Secure Empty Trash. This will wipe the files from the hard drive so that they can’t be recovered. This is a great feature to be included in the operating system and hopefully Windows will catch up soon.
If you are running a slightly older version of OSX that doesn’t have the Secure Empty Trash feature, you can download a utility called Permanent Eraser. This program works with OSX 10.1 and newer. It will either sit on your dock or integrate into Finder. Either way, you can simply drag a file onto the icon and it will be securely deleted. Worth noting with this utility is that it automatically uses a 35-pass deletion method, so it will considerably slower than the other methods.
The next step of the process is protecting the data that can’t be destroyed. This can be either active data that you are currently using or information that needs to be archived for some purpose. A minimum level of security would be protecting your Excel sheets with a password. (Live demo of protecting Excel sheet) This is not going to deter an attacker that has stolen the information and wants to access it. However, it will stop someone from casually making a change to something on the sheet.

There are also several utilities that will allow you to encrypt data on removable media, such as a flash drive or CD. These utilities can be either software or hardware based and we will discuss several that are listed on your handout. It is a very good idea to get in the habit of encrypting sensitive data when storing it on removable media. Since it is much easier to lose a flash drive or CD than to lose a laptop, these devices are more susceptible to compromise.

It is also vital that you think about physical security when protecting data. Keep archived hard-copies in a locked file cabinet or drawer. Lock your laptop to a desk or table with a security cable. Don’t leave laptops unattended in vehicles in plain view. All of these steps will help to avoid a possible loss of
data.

In the near future, there will be provisions available to allow you to encrypt your entire hard drive. At this time, OIT does not support this because we don’t yet have a key store set up that would allow you to decrypt the drive if you forget the password. However, this is in the works and it will help to keep the data on your laptop or desktop secure in the event of theft or loss.
The handout shows a couple of utilities that can be used to protect data on removable media devices. The first for Windows users is called BitLocker ToGo. This is built into Windows 7, but only on the Enterprise and Ultimate versions. To encrypt a drive, you simply insert it into the computer and then right-click on the drive and select “Turn on BitLocker...”. The downside to this utility is that it is only available in certain versions of Windows 7. You also need a separate utility to read an encrypted drive on older Windows OSes, such as Windows XP.

The second utility I have listed is called TrueCrypt. This is an excellent free encryption utility that is available for both Windows and Apple OSX users. It is very secure and can be used in a portable mode, meaning that the encrypted files can be read on any machine in which you use your flash drive. The only downside to this one is that it is slightly more complicated to set up. For this reason, I have available a handout showing you how to make a portable drive that is encrypted with TrueCrypt.
For the Apple OSX users, we already mentioned that Truecrypt will work with OSX as well as Windows. There is also a built-in option on OSX 10.7 and newer. Apple’s FileVault2 will encrypt portable drives in addition to the local hard drive. From the FileVault2 utility, you can just click on your removable drive and create a new encrypted partition.
Another option for encrypting removable storage is to buy a drive that includes hardware encryption on it. These drives are always encrypted and the data can only be viewed after entering some sort of authentication mechanism. Different types of drives may use passwords, a keypad pin, or even a fingerprint scan to authenticate you.

Some of the best of these drives are the IronKey line by Imation and the Aegis line by Apricorn. The only real downside to these drives is the price. A 16GB Aegis SecureKey costs about $125 and a 16GB IronKey is about $200. When you compare this to approx $20 for a normal 16GB flash drive, it does seem expensive. However, you need to consider the benefits of securing your data and the ease of use that these drives provide.
The final step to our process of protecting sensitive information takes place in the event that, despite our best efforts, a loss or breach does occur. In this case, it is important to report the incident as soon as possible. The more quickly that OIT can begin looking into what occurred, the better chance we have of protecting any data that may have been compromised.

Often you can recognize signs of malware or viruses on your machine. These can include: constant hard drive activity when you are doing very little on the machine, pop-up windows or unrecognized icons on your desktop, or your web browser taking you to a different site than you expected. If you suspect that your computer has been breached by malware or a virus, you should disconnect the computer from the network and immediately report the breach. Although it may seem like an inconvenience to have to disconnect now, it could save you from a longer period of downtime in the future. It also helps to keep the incident contained rather than allowing it to spread across the network.
At this time, are there any questions on anything we covered today? Or anything I overlooked that I might be able to answer for you?
Contact Information

Vito Rocco – OIT Information Security Specialist
vito.rocco@unlv.edu
x50400

Here is my contact information. If you have a question about keeping your data secure or anything else we talked about today, please don’t hesitate to contact me. Thank you!