ISSUE: 9-11 YEAR: 2014

University Information Security Office Newsletter

One machine can do the work of fifty ordinary men, No machine can do the work of one extraordinary man.

-Elbert Hubbard

From the ISO's Desk

There are many ways which we get and use data. From the start of the university's relationship with a student, employee, or contractor, we often require information from them that, although necessary for the business of the university, can also be used to steal or compromise someone's identity or financial information. This month's newsletter highlights personal data and how we, as good stewards of this data, must protect it. There are several university policies mentioned in this month's articles. Please take the time to look them over and put them into practice. As always, if you have any questions please don't' hesitate to contact me or my staff.

Jim Pardonek

Information Security Officer

University Information Security Office

Email: DataSecurity@luc.edu
Telephone: (773) 508-7373
Location: GC Room 230
Hours: M-F 8AM-5PM

Safety with Portable Storage Devices

Created by Jim Pardonek

Portable media storage such as CDs, SD cards, and USB drives changed how people share files. Even in this era of fast Internet connections where online file storage is available, many individuals still use CDs and USB drives to quickly transfer files from a computer and or to share files with one or more people. With USB drives, in particular, the small form factor makes it convenient to keep in your pocket so that you can take your work with you without the hassle of lugging a laptop between your office and home. This small form factor, however, makes it easy to steal, lose, or inadvertently leave it in a computer.

Because of these risks, one should be careful with the type of data that is stored on portable media. For example, the Loyola University Policy on Electronic Storage of data states: “No Loyola Protected Data may be stored on workstations, desktops, computers, laptops, thumb drives, mobile phones, or mobile devices. Loyola Protected Data may only be stored on ITS managed information resources, such as file servers, application servers or databases.” Loyola Protected Data is any data that contains personally identifiable information concerning any individual and is regulated by local, state, or Federal privacy regulations, or by any voluntary industry standards or best practices concerning protection of personally identifiable information that Loyola chooses to follow. Some brief examples are; Social Security Number and Credit Card Number.

A full list is located in the Loyola Data Classification Policy http://www.luc.edu/its/itspoliciesguidelines/data_classification_policy.shtml.
USB drives can also be used maliciously. An example I like to use is one where someone walks into an office reception area and tells the receptionist that they have a presentation and left their notes on their printer. They then ask if the receptionist will print them a copy off of their flash drive. The receptionist complies and puts the drive in their computer. While they are printing out the notes, a program on the USB device is installing malware or a key logger on the computer. These days malware can be disguised as a PDF, word, excel, or other file, which will infect a computer when it is opened. Additionally, many computers are set to automatically load or launch USB devices and CDs when they are inserted into a computer. This could be potentially dangerous as a malicious file can be automatically loaded without knowledge of the user. To keep your information and the information of others safe, follow these 3 steps:

1. Make sure that you are not storing protected data on your portable storage device
2. Don't leave your device where it can easily be stolen
3. Never insert a strangers CD or USB device into your computer

The full policy on Electronic Security of Protected Data is located at: http://www.luc.edu/its/itspoliciesguidelines/Electronic_Security_of_Loyola_Protected-_Sensitive_Data.shtml

Data Disposal

Created by Cai Wang

Companies will always have some old data in the forms of paper and electronic that will neither be used any more nor need to be kept in the archive. However, this data could be either protected by law or too sensitive to let people outside of the company see it. All protected and sensitive data that exists in paper document form should be disposed of by shredding, and electronic documents should be securely deleted. It is a great way to protect company information. At Loyola, we have a policy that specifically states how to dispose all Loyola Protected and sensitive data. It applies to both paper documents and electronic documents. All documents should be dropped off in designated containers that will be shredded by a licensed and bonded document destruction company. All electronic media containing Loyola Protected data should be sent to the ITS Information Security team for secure deletion. The ITS Information Security team will delete the Loyola Protected data from the media in accordance with the current ITS Secure Deletion procedure. Any media which cannot be processed according to this standard will be destroyed by the ITS Information Security team.

Data disposal not only applies to company information, but personal documents in our daily lives. We are receiving emails like bank statements, utility bills, loan payment notifications, etc. These documents contains a large amount of your personal information, such as name, address, phone number, account Number, etc. Documents like your previous year's tax return file even have your social security number, ID number, etc. Properly shredding these documents is necessary.

Loyola Data Disposal Policy: http://www.luc.edu/its/itspoliciesguidelines/DisposalofLoyolaProtected-SensitiveData.shtml

Loyola Data Classification Policy: http://www.luc.edu/its/itspoliciesguidelines/

Clean Desk Practices

Created by Brett Weston

Take a look around your workspace. How many sheets of paper contain potential sensitive information? Social Security Numbers, student grades, credit card numbers, employee health information. All of the above are just examples of information that is protected by local, State, and Federal laws and disclosure of this information, even if unintentional, to unnecessary or unauthorized parties carries serious punishments.

For some, working with sensitive information is a job requirement. As such, it is important to practice a "clean desk" when leaving your workspace. Here are some tips to get you started:

- Store anything containing sensitive information in a locked cabinet or drawer when leaving at the end of the day
- Keep an empty folder handy to cover sensitive information when stepping away from your desk for short periods of time
- Minimize the amount of sensitive information in plain sight to avoid accidental disclosure to passersby
- Lock your computer when leaving your desk to prevent unauthorized access to sensitive electronic data Install screen privacy filters on computer monitors in pubic, high traffic areas
- Limit printing sensitive information and never leave copies in fax machines, printers, or copiers
- Always shred sensitive information with cross-cut shredders instead of placing it directly in recycle or trash bins

Physical Security Tips

Created by Yuan Liu

1) Lock the door of your office room or study room in Library when leaving
2) Label your device in case it is lost
3) Consider a lock or alarm for your device
4) Don't leave your device unattended in the classroom, library or any public places
5) Don't write down your password and leave it in public place, and don't save your password in your phone or computers without encryption
6) Physical PC Securities:

- Lock your PC when walking away
- Store paper copies of files in a safe, locked location
- Treat laptops like cash
- Always keep your devices with you when leaving a public area