ISSUE: 6-9 YEAR: 2016

University Information Security Office Newsletter

Mechanization best serves mediocrity.

— Frank Lloyd Wright

Privacy

SANS Securing the Human

Technological advances have made it easier than ever before to access and share information. However, these advances have brought tremendous challenges with them. Nowhere is this more evident than in the area of individual privacy and the handling of an individual's personal information. As part of your routine work duties, you may handle personal information such as someone's Social Security number, their financial information, their education or employment records or aspects of their health or medical records.

You may not realize it, but federal, state and local laws and regulations require you to protect the privacy of personal information. More importantly, you should safeguard that information out of respect to others. Do what you can to protect their privacy, just as you would want them to protect yours. Here are some steps that you can take to help protect the privacy of others.

Authorized Systems

To protect people's privacy, you should only use authorized systems to enter, process or store their information. These systems have strong security measures in place, such as specialized security software and strict controls on how they are configured and who has access to them. Do not enter, process or store people's personal information on unauthorized systems, such as your own personal laptop or personal email accounts.

Sharing Data

Another step to protecting people's personal information is ensuring only authorized staff members have access to it. These individuals must have management's prior approval to access such data. They must also have a need to know, or in other words, they need access to the data to accomplish their job. Simple curiosity is not a sufficient need for access.

Cloud

Never store or share people's personal information on public Internet or cloud services, such as Dropbox, Apple iCloud or Google Drive, unless you have prior authorization from management.

Transferring Data

At times, you may need to transfer people's personal information to authorized individuals. There are numerous risks to transferring data, such losing it, having it stolen or even intercepted. As such, you should only use secure, authorized methods that support encryption when transferring someone's personal information. Never transfer private data using insecure means, such as using your own personal email account.

Data Destruction

A common way people's personal information is compromised is by employees improperly disposing of the information. For example, when you throw out an old USB flash drive or donate used computers, people's personal information is often still stored on those devices. To protect against this danger, all physical and electronic personal data that is no longer necessary or appropriate to store should be properly destroyed, shredded or rendered unreadable. For digital media, such as hard drives or USB flash drives, this means they should either be physically destroyed or the media should be securely wiped, ensuring the information is truly gone and cannot be recovered.

By protecting people's privacy, you help ensure our organization is compliant and demonstrate our organization's respect for others. If you have any questions about the types of information you should protect, how best to secure it or believe any of our information has been compromised, please contact the help desk or the information security team.

From the ISO's Desk

Our June Awareness topic is privacy. In this electronic age where it seems that the mantra is "Once on the Internet, Forever on the Internet" we have to be ever more careful and diligent when it comes to handling the information of the students, faculty and staff that trust that their information be kept private. Many of the topics in Loyola Aware and in past newsletters discuss things you can do to that when done together, lessen the risk of disclosure of private information.

If you would like to know more about our awareness activities, please check out Inside Loyola or go to our web page: http://www.luc.edu/uiso

Safe Computing to you all!

Jim Pardonek, Loyola's Information Security Officer

Loyola Data Classification Policy

The Loyola Data Classification Policy provides guidance on what protections need to be applied to data used and stored by all university departments.

Data Classification Types

All data covered by the policy are classified into 3 groups; Loyola Protected data, Loyola Sensitive data, or Loyola Public data.

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.

Loyola Sensitive Data is any data that is not classified as Loyola Protected data, but which is information that Loyola would not distribute to the general public. This classification is made by the department originating the data. Examples of the types of data included are: budgets, salary and raise information, and possible properties for Loyola to purchase.

Loyola Public Data is any data that Loyola is comfortable distributing to the general public. For department-specific data, this classification comes from the department. If data is created jointly by more than one department, the involved departments should jointly classify the data. If they are unable to come to a consensus, then the data must be classified as Loyola Sensitive Data. For University-wide data, this classification can only come from the Office of the President, the Office of Registration and Records, the Division of Academic Affairs, or Institutional Research. Examples of the types of data included are: department faculty lists, department addresses, press releases, and the Loyola web site. Any Loyola data that does not contain personally identifiable information concerning any individual, and that is not Loyola Protected data or Loyola Sensitive data, must be classified as Loyola Public data.

Default classification of data

Any data that contains personally identifiable information concerning any individual or that is covered by local, state, or Federal regulations, or by any voluntary industry standards concerning protection of personally identifiable information that Loyola chooses to follow, is automatically classified as Loyola Protected Data. All other data is classified as Loyola Sensitive Data by default. Online resources will be available to assist individuals in properly classifying data.

For more details about this policy, please visit http://www.luc.edu/its/itspoliciesguidelines/data_classification_policy.shtml

Technology's Impact on Privacy

The concept of privacy is not new. Organizations have collected and stored information on individuals for centuries. What has made this issue so different today is technology. Technology has not only made it possible for organizations to collect much more information on individuals, but made it easy to track specific individuals over the years as well.

In addition, technology has also made it much easier for individuals to illegally access, copy and distribute that very same information. This is why it has become so much more difficult (and important) for organizations like ours to actively identify and protect any and all private information we collect. You play a key part in protecting that private information. Only through your secure actions can we protect the privacy of others.

Loyola Aware

Our May awareness topic is " Privacy", which is available for viewing now.

Please visit: http://www.luc.edu/uiso/awareness/loyola_aware.shtml for further information.

If you have any questions in regrading to Loyola Aware, please contact the data security team by email (datasecurity@luc.edu) or call x87373 (703-508-7373)

Contact Information

University Information Security Office

Email: DataSecurity@luc.edu
Telephone: (773) 508-7373
Location: GC Room 230
Hours: M-F 8AM-5PM
Some Material © SANS Institute 2015