▶ Cloud Storage 1
▶ Online Harassment 1
▶ Use of Electronic Mail Systems 2
▶ Student Worker Access to LOCUS 2

ISSUE: 1 January/February YEAR: 2015

University Information Security Office Newsletter

Technological Progress has merely provided us with more efficient means for going backwards.

-Aldous Huxley

From the ISO's Desk

Welcome Back Everyone! Hope the holiday season was happy and healthy for all of you.

This month's issue continues our overview of university policies and how they pertain to each of us. Our first article explains what cloud storage is and gives guidance on what is appropriate to store using this resource.

We follow this with an overview of the policies on Online Harassment and Proper use of University Email.

Finally, many departments that employ student workers should read and understand the article on student worker access to LOCUS.

We hope you find this month's issue enlightening and informative.

As always, if you have any questions about information security please contact anyone in the University Information Security Office

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

How to Use Cloud Storage

In computer-speak, the term cloud has worn many hats from the use of "dumb terminals" connected to mainframes, CPU time sharing, and Remote Job Entry in the 1950's to virtual circuits in the 1990's to what we know of today as services provided by an entity other than ourselves. Examples of this are Google Mail, Box for file storage, and Office 365 for our students.

Cloud storage is a useful, convenient and cost effective way to keep your files handy or to share them with collaborators. Files stored in the cloud can usually be accessed from anywhere, anytime and in most cases, a smartphone or other mobile device can be used. Although cloud storage companies make for convenient access to files, there is a responsibility that we, as end users, have when using these services.

First, we should separate our personal files from university-related files. Just as many of us may have a file folder in our desk marked personal, we generally don't sprinkle the contents amongst the other file folders in the drawer that contain our work.

Second, we need to make sure that we only use approved providers for Loyola information. Currently the only university approved cloud storage provider is BOX. There are however, 2 versions of BOX as they provide free space for any individual as well as the purchased separate space for Loyola University Chicago use. For university files, we need to make sure that we are using the Loyola BOX. (https://luc.box.com)

Third, we need to make sure that we look at the files that we want to store in the cloud and decide which classification type they fall under, be *See Cloud on Pg 2*

Online Harassment

While many online interactions appear to provide a certain degree of anonymity, your actions can always be traced back to you. Unfortunately, some see this apparent anonymity as an excuse to harass others. Loyola University does not tolerate cyberbullying or any other type of online harassment, and neither should you.

What You Can Do

Clearly tell them to stop: While it may appear basic, this is an important first step in dealing with any type of harassment. Making it known that the interaction is unwanted as early as possible helps to protect you, especially in the event that the harasser decides to continue.

Avoid escalating the situation: While responding with anger or hostility can be a natural reaction to harassment, this is likely to provoke the individual and escalate the situation. Although difficult at times, consider simply not responding at all. Bullies are known to thrive on the reactions of their victims.

Save everything: Keep digital as well as printed copies of any activity that is related to the harassment. You should also avoid deleting the original communications if at all possible. These records, combined with accurate dates and times, can provide a strong case if there is ever a need for any involvement or legal action by the appropriate authorities.

Report online harassment: If you or anyone you know experiences online harassment, report the interaction to the appropriate parties. If the harassment or threatening behavior continues after attempting to cease the communication, report the activity to the Department of Campus Safety or local authorities.

Adjust your privacy and security settings: Limit how and where you share information. Wherever available, make sure to locate and review all privacy and security-related settings to ensure you are comfortable with the level of information sharing. The less personal information about you that is publicly available, the better.

Follow the Golden Rule: Even when online, always remember to treat others as you would want to be treated. It can be all too easy to hastily send a message or post something without taking any time to cool off or think about what you really want to say. Practicing good online habits benefits not only yourself, but the digital community as a whole.

More information concerning Loyola's Online Harassment Policy and applicable state laws can be found at: http://www.luc.edu/its/itspoliciesguidelines/policy_onlineharassment.shtml

Chris Campbell

Use of Electronic Mail Systems

Loyola's e-mail usage policy has been in place since 1997 to ensure the integrity of the electronic mail communication, guide users to use this communication method with Loyola's values in mind, and to remind users that their e-mails do not disappear once they hit the "Send" or "Delete" button. The electronic mail policy covers all users who can access or use the university's e-mail system. This includes students, faculty, staff, contractors, and any other person who has access to the e-mail system, whether it is on- or off-site.
The policy is broken down into basic guidelines, but is not limited to:

Respect the rights and personhood of others. Simply put, do not send abusive, harassing, intimidating, insulting, hostile, or threatening messages. Keep in mind the University policies on harassment, racial discrimination, and abuse. Users are encouraged to keep controversial conversations limited, unless it advances learning and mutual understanding. Do not access someone else's e-mail files, unless you have authorization or proxy rights of access. Refrain from forwarding messages without a legitimate business purpose, especially to embarrass any user or in the case where the sender requests limited viewing of the message.

Identify yourself clearly and accurately. Altering your name or source of the e-mail is unethical and may be illegal. Identifying yourself clearly is also a professional gesture.

Confidentiality is not guaranteed. Although the University has no interest in regulating the content of e-mail, it cannot guarantee the privacy and confidentiality of electronic. However, the University reserves the right to inspect, access, view, read and/or disclose an individual's computer files and e-mail that may be stored or archived on University computing networks or systems, for purposes it deems appropriate.

Send efficiently. Promote the efficient use of e-mail by refraining from sending spam e-mails, chain messages, junk mail, and other broadcast messages that are unneeded. These e-mails can interfere with work, and can be a waste of time for users who did not need to see the e-mail. Also, do not send or distribute any material that violates copyright laws or any other illegal or irrelevant material.

Conserve e-mail system resources. Check your e-mail frequently, delete unwanted messages, and do not use your University e-mail for commercial or financial gain without the University's permission. Limit your use of electronic discussion lists, and unsubscribe from unused mailing lists.

Failure to comply with this policy may result in the denial or removal of access privileges, disciplinary actions, or criminal prosecution. Employees can have network access denied, and can be suspended, or even terminated, depending on the case.
This policy is a general guideline for all electronic communication within Loyola's network, and relates to other policies regarding acceptable conduct.

Suggestions and comments concerning the Policy Regarding Access and Responsible Use of University Electronic Mail Systems can be directed to the University Information Security Office at datasecurity@luc.edu.

Jacob Schuldt

Cloud from Pg 1.

it Protected, Sensitive, or Public.

Per the Loyola University Chicago Cloud Computing Policy: (http://www.luc.edu/its/itspoliciesguidelines/cloud_computing_policy.shtml), it is never acceptable to store Loyola Protected data on any cloud service. This includes data such as grades, social security numbers, private correspondence, classified research, etc. These should be stored on internal central or departmental servers. Putting protected information in cloud storage could place you and the university in a position where state or federal laws and regulations are violated.

If there is ever a doubt whether a file should be saved in the cloud, you can always contact the University Information Security Office for guidance. *Jim Pardonek*

Student Worker Access to Locus

There is a lot of sensitive data in LOCUS, including personal information and academic records. It is important to assign all users an appropriate level of access to the PeopleSoft system.
Student workers who are required to access the PeopleSoft system as a part of their job need to be limited to certain pages and data. Undergraduate student workers and graduate assistants will have different levels of access based on their job responsibilities and the approval of the Registration & Records department.

We ensure that student workers have the right access and that activities performed by a graduate student worker can be tied back to an ID that is only used by that graduate student worker. We also ensure that restrictions are in place around times a student worker can access the PeopleSoft system, and that access is removed at the end of each term. If the student worker will need continued access to the system, their supervisor needs to submit a new access request before the end of each semester.

Separate ID types
All student workers will receive an additional ID in our eDirectory system. The ID will be in the format $UVID. The "$" character will indicate to system administrators that this ID
belongs to a student worker with access to the PeopleSoft
system. This ID will not have access to any systems other than PeopleSoft. Password resets for these IDs will be performed
by the Technology Support Center.

Time-based restrictions
To prevent students from accessing the system outside of their working hours, the PeopleSoft administrators will set time-based restrictions for when student workers are allowed to access the system. Every student worker can be set up for different days and working hours.

Periodic access removal
At the end of each term, all student worker accounts will have their access removed.

Functional areas that require their student workers to retain access will need to send a new LOCUS student worker Access Request form to the PeopleSoft administrator in the UISO.

Any accounts that have had their access removed will be deleted within 30 days if no form was submitted on behalf of that ID.

Yuan Liu