Data Classification and Acceptable Use Policies
Frequently Asked Questions

With the new Data Classification and Acceptable Use Polices, there have been many questions regarding the impact to specific practices used at Union College**.** The questions below should help answer many of these questions.

Can I store confidential information on a USB drive or other removable media?

The policy states that users must not store confidential information on unencrypted removable media. What if faculty or staff currently store confidential information on USB drives or other removable media, such as a portable hard drive, as part of their functions or to support their teaching, research or administrative efforts? (For example, course evaluation data downloaded from a website, research data stored on a portable USB hard drive, committee notes, job applicants, or other documentation to be reviewed at home, etc.)

The policy applies to all confidential institutional data. Confidential information that is institutional data or stored as a part of institutional roles and functions must be stored on an encrypted device. Removable media is easily lost or stolen. To guard against confidential data being accessed by unauthorized persons, it must be encrypted. The easiest way is to encrypt the entire device itself, so that any data placed on the device is automatically encrypted. This policy does not apply to non-institutional confidential data, though we encourage the practice of encrypting ALL confidential data. If needed, ITS can work with faculty, staff and administration who are working with confidential materials to provide the necessary device and/or protections.

What about institutional laptops and desktop computers?

There is a timeline for encrypting all institutionally-owned laptop computers with full disk encryption. Until this project is completed, it is OK to store confidential institutional data on institutionally-owned desktops and laptops. All confidential institutional data should be stored on appropriate network file shares to ensure they are backed up and protected by appropriate network controls.

What about storing this data on my personal laptop, desktop or other personal device?

While we certainly understand the history and convenience of using personal devices to store confidential institutional data, like grade sheets, staff performance reviews, committee ***notes, or other things, to work on at home or while away, there is a significant risk to the institution in doing so. Personal devices can be lost, stolen or otherwise compromised and may not be up-to-date with OS and application patches or virus signatures.***

Can I email confidential institutional data?

The policy prohibits emailing confidential data to entities outside of Union College unless the data (or attachment) is encrypted. It is not difficult to encrypt and password protect attachments, like Word, Excel, PDF or other similar documents. ITS can provide you with a "Document Encryption How-To" guide to assist you in learning the process.

While the policy does not prohibit emailing confidential data to other individuals within Union College, it is not considered a best practice. This is because confidential data would now be located in the email system in addition to other applications or documents. It would be best practice to call the other person with the information or place it on a file share so they can retrieve it.

What about network file shares?

Network file shares, like the UFiles and Zeus drives are the right place to store all institutional data, whether confidential or not.

How about Cloud storage (like Google Drive or Box.com)?

Union College has approved the use of Google Apps. It is OK to store information using these approved accounts, as both the storage and transmission of everything is encrypted. Anyone using these accounts to share sensitive or confidential information is reminded that the files should remain on Google Drive and a copy should not be stored elsewhere or emailed. Please note that storing sensitive or confidential files on Google Drive is only permitted if all relevant security controls are applied as defined in Step 5 of the Procedure document for Data Classification and Handling.

Why is the Union College implementing these new policies?

Regulatory Drivers

In July 2015, the Department of Education (DOE) issued a Dear Colleague letter, with a follow-up letter in July 2016, reminding "*institutions of their legal obligation to protect student financial data under Title IV, and sets forth the new standards and methods the DOE will use when evaluating data security compliance*." This means DOE will likely be auditing institutions on their security compliance.

The specific controls identified in the Gramm-Leach Bliley Act (GLBA) of 1999 to protect student financial data include:

- Identify[ing] and assess[ing] risks to customer information;
- Develop[ing], implement[ing], and maintain[ing] a written information security program;
- Designat[ing] the employee(s) responsible for coordinating the information security program; and
- Design[ing] and implement[ing] an information safeguards program.

Additionally, the letter "*strongly encourages institutions to review and understand the standards defined in the NIST SP 800-171*". These include:

- Protect[ing] media, both paper and digital, containing sensitive information (Media Protection Requirements);
- Conduct[ing] risk assessments (Risk Assessment Requirements); and
- Assess[ing] security controls periodically and implement action plans (Security Assessment Requirements).

The letter also "*strongly encourage[s] those institutions that fall short of NIST standards to assess their current gaps and* ***immediately begin to design and implement plans in order to close those gaps using the NIST standards as a model***" [emphasis mine]. This statement makes clear that simply maintaining the status quo, or even actioning solutions too slowly, will be placing institutions at risk.

The initial risk assessment performed allowed Union College to identify any gaps in their current practice, and begin to take meaningful action to begin addressing them. As an example, the Data Classification project helped to identify what data the College had, where it was stored, and to begin to identify mechanisms (such as the Acceptable Use Policy) to better protect it. This allows the College to make the best use of limited resources since no institution can protect all of their data all of the time.

While the changes to policy will definitely require a change in culture and practice, it is not the goal of these to be heavy-handed. Additional mechanisms have been put in place to allow for exceptions when necessary, as well as other methods to ease constituents into the controls.

The Cost of a Security Breach

There are currently no laws requiring Universities to publish all details about breaches or the fines or fees associated with these. Ergo determining the specific costs of security breaches at Universities is not a science. "*The actual cost of a security breach may be a heavy hit to a university. According to the Ponemon the education sector has one of the highest per capita data breach costs, at $259 [though again, not a hard and fast number] for each lost or stolen record containing sensitive information. This amount exceeds the per capita cost of data breach suffered by companies in the energy, financial services, communications, and pharmaceutical sectors*." Some recent examples of breaches include:

- 2015: Security breaches reported at Universities such Pennsylvania State University (PSU), Washington State University, Harvard University, Johns Hopkins University, the University of Virginia (UVA) the University of Connecticut, Princeton UCHV, University of Maryland, the University of Delhi, Algonquin College, and the University of Baltimore are among those that have sustained damaging cyberattacks this year. (https://edtechmagazine.com/higher/article/2015/09/putting-2015-s-higher-education-cyberattacks-perspective)

- 2016 & 2017 (So far): Security breaches have been reported at 24 US universities and 10 in the UK by one hacker alone. (http://www.computerworld.com/article/3170724/security/hacker-breached-

63-universities-and-government-agencies.html) Additional breaches have been reported at University of Central Florida, UC Berkeley, Tidewater Community College, University of Oklahoma, Washington State University, https://www.identityforce.com/blog/2016-data-breaches and https://www.identityforce.com/blog/2017-data-breaches

We know that change is not easy, and we do not advocate "Security for security's" sake. We take a very practical approach to security, understanding that it must support the goals of the institution. The best security is not heavy-handed, but a balance of function and control.

Real-world Incidents

Regulatory drivers are only a part of the motivation incentive by higher education to look at their security policies and controls. Many Universities and Colleges have increasingly been victims of data breaches and theft, with peak years of ~2007 and ~2012 (https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-analyzing-breaches-by-industry.pdf) .

From 2006 to 2013, 550 universities reported some kind of data breach, though these usually receive far less media attention than financial or entertainment organizations. (http://www.nbcnews.com/tech/security/universities-become-targets-hackers-n429821)

- 2013: Universities Face a Rising Barrage of Cyberattacks (New York Times)
  Notable quotes: "University officials concede that some of the hacking attempts have succeeded. But they have declined to reveal specifics, other than those involving the theft of personal data like Social Security numbers." "Universities and their professors are awarded thousands of patents each year, some with vast potential value, in fields as disparate as prescription drugs, computer chips, fuel cells, aircraft and medical devices.
  (http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?pagewanted=all&_r=2&)

- 2014: Student and staff data was breached at 30 educational institutions last year, and five of the leaks were bigger than the Sony attack.
  (https://www.eab.com/daily-briefing/2015/01/20/five-higher-ed-data-breaches-worse-than-sonys)

- 2015: Security breaches reported at Universities such Pennsylvania State University (PSU), Washington State University, Harvard University, Johns Hopkins University, the University of Virginia (UVA) and the University of Connecticut, Princeton UCHV, University of Maryland, and the University of Delhi, Algonquin College, University of Baltimore are among those that have sustained damaging cyberattacks this year. (https://edtechmagazine.com/higher/article/2015/09/putting-2015-s-higher-education-cyberattacks-perspective)

- 2016 & 2017 (So far): Security breaches have been reported at 24 US universities and 10 in the UK by one hacker alone. (http://www.computerworld.com/article/3170724/security/hacker-breached-63-universities-and-government-agencies.html) and additional reports of breaches at University of Central Florida, UC Berkeley, Tidewater Community College, University of Oklahoma, Washington State University, https://www.identityforce.com/blog/2016-data-breaches and https://www.identityforce.com/blog/2017-data-breaches

While we cannot discuss each breach individually, below is some data related to higher education breaches:

Specific Examples:

1.) University of Maryland
In March 2014, more than 300,000 student, faculty and staff records were compromised at University of Maryland. Though no financial, medical or academic records were compromised, the breach did include names, birth dates, university ID numbers and even Social Security numbers. According to University of Maryland's student newspaper, *The Diamondback*," the database that was accessed contained information from everyone who has received a university ID from the College Park or Shady Grove campuses since 1998."

2.) North Dakota University
In February, 2014, a server at the North Dakota University System storing personal information of nearly 300,000 past and present students was hacked. Such personal information included names and social security numbers.

3.) Butler University
The third largest data breach in 2014 among colleges happened at Butler University. According to the University Herald, hackers got access to the school's network, exposing personal information of nearly 200,000 people. Personal information exposed included names, birth dates, driver's licenses, social security numbers, and bank account information.

4.) Indiana University
The fourth largest in 2014 among colleges happened at Indiana University, where data breach left more than 146,000 current and former students had their personal information exposed. This included names, addresses, and social security numbers of students. IU's response to the data breach ended up costing the school about $130,000.

5.) Arkansas State University
About 50,000 people were impacted by a data breach at Arkansas State University. According to University Business, full and partial social security numbers were leaked.
http://www.huffingtonpost.com/kyle-mccarthy/five-colleges-with-data-b_b_6474800.html

The Cost of a Security Breach

"The actual cost of a security breach may be a heavy hit to a university. "The list of potential expenses is long. It includes forensic consultants, lawyers, call centers, websites, mailings, identity-protection and credit-check services, and litigation." According to the Ponemon Institute, the education sector has one of the highest per capita data breach costs, at $259 for each lost or stolen record containing sensitive information. This amount exceeds the per capita cost of data breach suffered by companies in the energy, financial services, communications, and pharmaceutical sectors. As seen with many of the recent breaches that have involved the personal information of hundreds of thousands (if not millions) of individuals, the total cost of a breach suffered by an educational institution may be in the multi-million-dollar range. (https://www.universitybusiness.com/article/1015-jwd)

References

Dept. of Education letters:
https://ifap.ed.gov/dpcletters/GEN1612.html

Legal obligation to protect:
http://www.higheredlawreport.com/2016/07/recent-u-s-department-of-education-dear-colleague-letter-raises-the-bar-on-standards-for-protecting-federal-financial-aid-data/)

FTC Recommendations:
https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying