Responsible College Official: Director of Information Technology

Responsible Office: Division of Information Technology

Email as a Secure Means of Internal Communication

Table of Contents

Policy Statement

Email is a primary method for internal communication on campus. Unfortunately, the underlying technology used during the transporting of email is not secure. This is because email moving between two providers, such as Google and Microsoft, is sent in clear text. However, email that is sent between Cornell users only reside on servers from a single provider and thus can be considered secure. To assure that email meant to be internal does not leave the College's email system, Cornell employees must not forward/send email containing confidential information to non-Cornell email accounts. Violations of this policy may result in disciplinary action up to and including termination or expulsion.

Who Needs to Know This Policy

Faculty, staff and student workers

Policy/Procedures

Cornell employees must not forward emails containing confidential information to non-Cornell email accounts.

- Employees may not configure their Cornell College email account to automatically forward to a non-Cornell email account.
- Employees may not manually forward individual emails containing confidential information to a non-Cornell email account.
- Emeriti email accounts must be treated as a non-Cornell account. Do not send confidential information to Emeriti accounts.
- If email must be used to communicate confidential information to a non-Cornell account, the confidential information should be sent as an attached encrypted/password protected file, or using a third party secure email application.
    - MS Word and Excel can create encrypted/password protected files. How to protect your MS Office file.

- ZixMail is an example of a third part secure email application. Please contact Information Technology with questions or for ordering information.

Definitions

Confidential Data: Confidential Data is information protected by statutes, regulations, college policies or contractual language. Managers may also designate data as Confidential. By way of illustration only, some examples of Confidential Data include: • Social Security Numbers • Medical records • Bank account numbers • Student records and other non-public student data (For detailed information regarding student privacy please visit http://www.cornellcollege.edu/student-affairs/compass/student-policies-information/communications-confidentiality-of-student-records.shtml)

If you have questions regarding whether a specific piece of information is considered confidential, please contact the college office that is responsible for that data.

Website Addresses for This Policy

http://www.cornellcollege.edu/information-technology/policies/technology-policies/index.shtml

Related Information

Student Records Privacy Options (FERPA)
http://www.cornellcollege.edu/registrar/ferpa/index.shtml
Confidentiality of Student Records (FERPA) http://www.cornellcollege.edu/student-affairs/compass/student-policies-information/communications-confidentiality-of-student-records.shtml

Who Approved This Policy

Technology Policy Advisory Committee (TPAC) - Nov 2014
President's Council - January 2015

History/Revision Dates

Origination Date: Nov 2014
Last Amended Date: NA
Next Review Date: 2017 or as needed