Responsible College Official: Director of Information Technology in consultation with the FERPA Administrator/Registrar, and the Director of Financial Assistance.

Responsible Office: Division of Information Technology

INFORMATION SECURITY POLICY

Table of Contents

Policy Statement

Information is a vital college asset and requires protection from unauthorized access, modification, disclosure or destruction. Maintaining the security, confidentiality, integrity, and availability of information stored in the college's electronic systems and in paper form is a responsibility shared by all users. 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

Users of college systems, both electronic and physical, are responsible for protecting the information processed, stored or transmitted using these resources, and for incorporating the following industry standard best practices into their daily activities. In addition, administrative departments maintaining and or disposing of confidential information are required to update an information security worksheet annually.

A. Protecting Confidential Information

1. DO NOT store confidential data in any college system, both electronic and physical, unless the persons who have access to that system have a legitimate need to know the information involved.
2. DO NOT distribute confidential or sensitive data to external entities unless approved by the appropriate Cornell authority.
3. Only distribute confidential information to internal entities on a need to know basis.
4. Assume all student information is private unless the student has signed a FERPA release form (except for directory information as defined by the Cornell College Compass at

http://www.cornellcollege.edu/student-affairs/compass/student-policies-information/communications-confidentiality-of-student-records.shtml).

5. Use secure means to transmit confidential data.
    - Email sent outside the Cornell College domain is not secure. All employees must adhere to the "Email as a Secure Means of Internal Communication" policy. http://www.cornellcollege.edu/information-technology/policies/technology-policies/Email-as-Secure-Communication.pdf.

B. Securing Physical Space/Data

6. Physical spaces such as filing cabinets, offices and workrooms containing protected college information shall remain locked when unsupervised.

C. Securing Information on Workstations and Other Electronic Systems

7. Utilize strong passwords to minimize the risk of a password being compromised and data being lost due to unauthorized access. All user network/email passwords must meet the requirements outlined in the Password Requirements policy http://www.cornellcollege.edu/information-technology/policies/technology-policies/Cornell-College-Password-Requirements.pdf.
8. Do not share account names and passwords if the account was not configured to be a shared account.
9. DO NOT open attachments and links embedded in emails unless you are confident the email is from a reliable source and intended to be sent from that source.
10. DO NOT enter your username and password into an Internet form to "Verify" your credentials. Information Technology, or any other legitimate organization, will never ask you to verify your username and password in that manner.
11. Log out of public systems when finished working.
12. Log out or lock college assigned systems when finished working.
13. DO NOT save passwords in web browsers or e-mail clients when using a public computer system.
14. DO NOT post college material on any publicly-accessible computer or website unless first approved by the appropriate Cornell authority.
15. DO NOT intentionally damage, alter, or misuse any college-owned or maintained hardware, software, or information.
16. DO NOT test security controls in place at the college or any other location (including ethical hacking) without authorization from the Director of Information Technology.
17. Secure devices by requiring a password when the device is turned on and when the screen saver is deactivated as outlined in the Requiring Password Protected Screen Saver policy http://www.cornellcollege.edu/information-technology/policies/technology-policies/Requiring-Password-Protected-Screen-Savers.pdf and the Mobile Device Security policy http://www.cornellcollege.edu/information-technology/policies/technology-

policies/Mobile%20devices%20must%20be%20password%20protected.pdf (public computers with no critical or sensitive information may be excluded).

18. All computers (desktops/laptops) accessing Cornell electronic data must run up-to-date anti-virus/malware software.
    - Exception may be made with approval from the Director of Information Technology.
19. All mobile devices (smart phones/tablets) must adhere to the Mobile Device Security policy http://www.cornellcollege.edu/information-technology/policies/technology-policies/Mobile%20devices%20must%20be%20password%20protected.pdf
20. Keep all computer systems up to date with the latest software maintenance releases.
    - IT pushes out critical updates to college owned Windows computers. Users are responsible to apply awaiting updates when they are available. A reboot once a week will meet this requirement unless notified otherwise. Apple users and users of non-Cornell owned devices are responsible for their own updates.

D. Communicating Security and Confidentiality Issues

21. Notify the Director of Information Technology immediately if passwords or other system access control mechanisms are lost, stolen or disclosed, or are suspected of being lost, stolen or disclosed.
22. Notify the Director of Information Technology if sensitive or critical college information is lost or disclosed to unauthorized parties, if any unauthorized use of college systems has taken place, or if there is suspicion of such loss, disclosure or unauthorized use.
23. Forward information pertaining to security-related problems to the Director of Information Technology immediately. DO NOT further distribute this information.
24. DO NOT discuss information security-related incidents with individuals outside of the college, or with those inside the college who do not have a need to know.

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