Student and Academic Services Data Security Policy

Effective Date: December 15, 2010 *Revised: October 29, 2012*

Policy Statement

Security of confidential data is a priority for Cornell University. Employees should not store confidential university data on their work or home computers, on removable storage devices, or on cloud file storage spaces (i.e., cornell.box.com, iCloud, Google Drive, etc.). In cases where business practices require the use of confidential data, the employee is responsible for contacting tech support for assistance in securing the data.

Reason for Policy

Mishandling sensitive data can lead to Cornell suffering financial loss or damage to its reputation. The law requires Cornell to report the possible loss of certain types of data to government agencies and notify potentially affected individuals. Losing sensitive data has repercussions including: regulatory fines, loss of funding from government agencies, lawsuits, loss of donations and gifts, and loss of reputation.

Who Should Read This Policy

All employees supported by SAS-IT including all staff within the Division of Student and Academic Services, Undergraduate Admissions, Financial Aid & Student Employment, the Graduate School and the Vice Provost's Office.

Contents

Related Documents

- Using Identity Finder
- Password Guidelines

Contacts

- For questions regarding use of Identity Finder or working with confidential data securely, submit a ticket to: http://it.sas.cornell.edu/

Definitions

What is confidential data? Cornell University Policy 5.10 - *Security of Electronic University Administrative Information*, identifies the following data elements as "confidential information" when they appear in conjunction with an individual's name or other personal identifier:

- Social Security numbers
- Credit card numbers
- Driver's license numbers
- Bank account numbers
- Protected health information, as defined by HIPAA

What is a removable storage device? It is any portable device or media that is readable and/or writeable by the end user and allows you to move information wirelessly or from computer to computer without modification to the computer. This includes flash memory devices such as USB thumb drives, cell phones, cameras, MP3 players and PDAs; removable hard drives; CD and DVD disks; and floppy disks.

What is cloud file storage? It is a storage service that is delivered over the internet. Some common examples include: cornell.box.com, www.dropbox.com, iCloud, Google Drive, etc.

Roles and Responsibilities

Employees

Employees need to assume personal responsibility for university information that has been placed under their custodianship. This is no different than an employee's obligation to take appropriate care of more tangible university assets. Individual accountability is essential to good data security.

An employee's failure or refusal to comply with this policy and carry out the specified tasks should be viewed as a performance issue, to be addressed by management and local HR. Policy violations may result in disciplinary action up to and including termination.

Supervisors of student workers will take responsibility for scanning space assigned to student employees on university-owned systems, rather than having the students do this. Supervisors are responsible for ensuring that computers and assigned file server spaces of employees who have left the department are cleaned up.

Tech Support
SAS-IT Tech Support will be responsible to provide the tools to enable staff to scan their computers for confidential data as well as basic instructions. SAS-IT Tech Support can assist staff in securing and disposing of confidential data, if requested.

To enhance awareness of where confidential data is being held, and to assist both local personnel and the IT Security Office with incident response, SAS-IT must maintain a registry of any systems that continue to store confidential data. Please see Policy 5.10 for details.

Scanning File Servers and Other Storage Spaces
On a system where an employee has only a restricted account that confines him or her to assigned user space, the employee does not need to scan any other areas. The system administrator responsible for managing the system, whether single- or multi-user, is responsible for scanning the departmental spaces and providing the results of those scans to area managers so they can determine the disposition of any data found. The system administrator is exempt from scanning those spaces if he or she is sure that no user data is present.

Implementing full-disk encryption does not provide an exemption to this scanning requirement. The contents of encrypted directories/containers/volumes also need to be scanned.

Procedures: Employees

a) Acknowledge custodial responsibility for university data

All employees must acknowledge their custodial responsibility for the university information on the computer(s) and associated storage they use in the conduct of university business, whether university property or personally owned. This includes:

- The internal drives of their workstations, both laptops and desktops;
- External drives;
- Mobile devices such as smart phones;
- Portable media, such as USB flash drives, used to store or transport university data;
- Email messages and associated attachments, including copies stored on an email server;
- Network file spaces assigned for individual use, such as roaming profiles and personal folders on file servers as well as cloud-based file storage spaces (i.e., cornell.box.com, iCloud, Google Drive, etc.).

Though IT or administrative staff may assist an employee in determining what information is present on his/her computer(s) and in taking appropriate remedial actions for any data that should not reside there, this does not replace the individual's custodial responsibility.

A note about access to confidential data: Only those who need access to confidential data to perform their job duties should have access. Access privileges should be reviewed periodically. If your job duties have changed and you no longer need access to confidential data, contact your IT staff to have your access privileges removed.

b) Inspect for confidential data

To assist in understanding what information one is holding, all employees are required to run a tool that can scan for confidential data regularly*, such as Identity Finder to scan the internal and external drives of their workstations (laptops and desktops) as well as network file spaces assigned for their use. Additionally employees should visually inspect files in storage spaces where a tool can't be used (i.e., cloud file storage) or the tool can't identify the type of confidential data (i.e., HIPAA protected data).

As a general rule, if you can write to a space (a folder on a file server or cloud file storage for instance), then you need to inspect it. Any virtual machines on a workstation, including instances of Windows running on a Macintosh, also need to be scanned, in accordance with the above guidelines.

*The required frequency for running a tool such as Identity Finder will differ depending on the department and the role of the individual and will be determined by local management in consultation with SAS-IT.

c) Understand the information under one's care

We expect employees to take reasonable measures to understand what information is in their care, especially confidential data, and to safeguard that information as specified by university and divisional policy.

d) Take action when confidential data found

When an employee finds confidential data, through the scanning process or by other means, he or she is obligated to take appropriate action. Our divisional practice is that no confidential data should be stored on local workstations or in cloud file storage spaces.

- If the data is no longer needed it should be securely deleted (the Identity Finder software has a "shred" function that provides this feature). If you are unsure of how to securely delete data from your computer, please contact SAS-IT Tech Support.
- If the data needs to be kept, but is no longer used, contact your local tech support to determine the appropriate way to archive it.
- If, after review, it is determined that the employee needs to have access to the data to perform their job, they are required to contact local tech support to determine the best way to secure the data.

e) Accept personal responsibility / Biannual attestation

All users with access to confidential information must attest twice a year to their awareness of the relevant policies, use of available protective measures, and their active compliance with data security policies.

General Data Security Requirements

- All accounts must have strong passwords at least equivalent to the strength required for NetID passwords. No electronic distribution of passwords in the clear, i.e., transmission must be encrypted. See Password Guidelines.
- All local file shares and folders on file servers must be password protected. If multiple individuals use a system, each should have his/her own login account.
- Never send confidential data via email. Use the Cornell DropBox (http://dropbox.cornell.edu) if you need to share confidential data.
- Keep all relevant operating system, server, and application software up-to-date (patched).
- User privileges will be configured as low as possible while still meeting business needs.
- Any computer not in a secure, private space, will run a password-protected screen saver that is triggered after 15 minutes or less of activity.
- Ensure local/personal firewalls and/or IPSec filters are installed and running.
- Run anti-malware (anti-virus, etc.) software with daily updates and active protection enabled.
- Always report virus alerts or other unusual system behavior to SAS-IT Tech Support as soon as possible.

Security for Removable Storage Devices

All business practices that require you to store confidential data on a removable storage device must be examined to ensure that the most secure storage or transfer method is used. Use of an alternative transfer method, such as the Cornell DropBox (http://dropbox.cornell.edu) should be strongly considered over use of removable storage devices. Cornel DropBox cannot be used for data storage as all files expire after a maximum of 21 days.

If it is determined that business procedures require the use of a removable storage device to store confidential data, employees are required to contact SAS-IT Tech Support for assistance. The employee must also agree to fully comply with the security guidelines outlined below for protecting and storing confidential data on removable storage devices.

Guidelines for storing confidential data on a removable storage device:

- The removable device must always be physically secured.
- The removable device must be regularly scanned for any malicious software using the latest version of Symantec anti-virus software.
- When the removable device is no longer needed, proper disposal techniques must be employed.
- Confidential data stored on removable devices must be encrypted.

Additional Information

What is encryption? Encryption is a procedure used to convert data from its original form to a format that is unreadable and/or unusable by anyone without the tools/information needed to reverse the encryption process. Contact tech support for assistance and security tools.

What are alternative ways to securely transfer confidential data? Use the Cornell DropBox (http://dropbox.cornell.edu) or other secure transfer methods (i.e., SFTP) to securely transfer confidential data between computers, users, or vendors.

How can I ensure my confidential data cannot be retrieved after I have deleted it from the removable storage device? Deleting a file from the removable device does not ensure that it cannot be retrieved. Formatting the device, then throwing it in the trash is not the proper disposal method! Contact tech support for guidance and assistance with proper disposal techniques.

Is the data secure if I put a password on the file? Password solutions within applications may or may not secure the data. For example, while Microsoft Office 2007 includes a facility for appropriately strong encryption of documents, the password-protection feature found in older versions of Word and Excel is not sufficient.