

# IT Security Requirements for Confidential Data

Version 1.0 – 01 Nov 07

To better safeguard the university's data, the IT Security Office requires the following practices for electronic processing and storage of Confidential Data.

The Confidential Data classification currently comprises Social Security, credit card, driver's license and bank account numbers, and patient treatment information. This set may expand based on future regulatory requirements or designations made by the appropriate university data steward (as defined in University Policy 4.12).

Please note that some data elements classified as Confidential Data are subject to legal or regulatory requirements that go beyond those given here. Such requirements for Regulated Data must be fulfilled, along with these Cornell requirements. In particular, credit card numbers and how the university handles credit card transactions are subject to the Payment Card Industry Data Security Standard (PCI DSS). For more information, see <https://www.pcisecuritystandards.org/>.

These requirements apply to Confidential Data that is under the custodianship of the university, and so do *not* pertain to your own personal information.

These requirements apply to any system that holds or processes Confidential Data, both on- and off-campus and even if not university-owned.

Here and elsewhere, a system is “holding” Confidential Data when such data is stored locally on the system or when the system is regularly used to direct mount and has access to such data stored on network volumes or file systems.

- Thus, for example, a Windows system where the primary user’s domain password is sufficient to mount a file server volume and access directories with Confidential Data would need to be secured as if such data was stored locally.
- On the other hand, a system used to access Confidential Data via an application, including database access, would not be viewed as holding such data.

Items labeled as a *Suggestion* reflect a beneficial practice that might become a requirement at some future date.

*Please note that these requirements are **in addition to** those outlined in the **Baseline IT Security Requirements**.*

## A. Exceptions

For all computers or other IT resources that are not able to meet these security requirements, the following exception process must be followed:

1. IT resources that cannot meet the requirements must be identified to the appropriate Unit Security Liaison. The Unit Security Liaison will work with the IT Security Office to determine alternate methods to remedy the specific risk being addressed.
2. If no alternative can be found, the applicable data steward will be consulted to determine appropriate course of action.
3. Both the IT Security Office and Unit Security Liaison will maintain a list of all IT resources that require an exception and review them on an annual basis.

## **B. All Computers**

1. Keep all operating system, server and application software up to date.
  - A local patch management process must ensure that all security / critical updates are installed as soon as possible, and no later than *two* business days after their release.
2. Follow hardening guidelines for the operating system and any applications or services that connect to the network.
  - Along with the software vendor, credible sources for guidelines include NIST, CIS, NSA, SANS, FIRST.
  - Disable all network services, including specific application features, that are not needed for the system to fulfill its function.
  - Change any passwords with default values set by the vendor.
3. Confidential Data and data that is being made available for public access may not be on the same system.
  - An open web site, i.e. one that does not require authentication for access, may not be run on a system holding Confidential Data.
  - Peer-to-peer (P2P) file-sharing software may not be run on a system holding Confidential Data.
  - Confidential Data and data available for public access may reside in different virtual machines running on the same system, as long as the host system and the host operating system meet all the requirements for a file or application server holding Confidential Data.
4. Activate operating system and, where possible, application logging, with logs retained for at least 90 days. At a minimum, the following must be logged:
  - Access to all audit logs;
  - Access to Confidential data;
  - Failed access attempts.
5. Maintain an inventory of all systems holding Confidential Data.
  - Review the inventory on a quarterly basis.
  - File a copy of the current inventory with the local IT head and the Unit Security Liaison.
6. On a quarterly basis, audit and verify that only currently authorized personnel have accounts that grant access Confidential Data.

*Suggestion:* Audit file, application and system privileges on a periodic basis.

## **C. Specific to Desktops and Laptops**

1. The account used for daily operations may not be configured to allow software installs.

*Suggestion:* Users are not allowed to install software themselves.

2. On any system holding Confidential Data, use a unique password, not shared with other systems, for local administrator accounts (accounts with elevated privileges).
  - In particular, the local admin password used by IT support staff must be different for each system that holds Confidential Data.
  - Such passwords can be generated algorithmically as long as the unique portion is not a string that is stored electronically on the system.
3. Confidential Data stored locally on a system must be removed when no longer needed on an operational basis.
  - Every six months, use Spider or some equivalent to review what Confidential Data is stored on the system, and where.

*Suggestion:* No storage of Confidential Data on individual staff machines.

4. Confidential Data must be encrypted on:
  - (a) any system that, even on a temporary basis, is not located on one of the Cornell campuses or some other formal university location; and
  - (b) any laptop or other portable device, including portable media, that ever leaves a secure location accessible only to authorized university personnel; and
  - (c) any other system that is not physically secured or in a secure location accessible only to authorized university personnel.
    - If full-volume encryption is used, the volume should be mounted only when the system is in active use. (Make sure that the encryption does not interfere with your ability to create and retrieve backups.)
    - Protect encryption keys against disclosure, misuse and loss. See University Policy 5.3, Use of Escrowed Encryption Keys.
    - Examples of portable media include: external hard drives, USB thumb drives, CDs DVDs, tapes, diskettes.
    - Use of the password-protection feature found in Microsoft Word, Microsoft Excel and similar applications does not fulfill this requirement.
    - Acceptable encryption solutions include but are not limited to EFS under Windows 2000 and later, BitLocker under Windows Vista and Server 2008, FileVault under Mac OS X, CyberAngel, TrueCrypt.

*Suggestion:* Encrypt all instances of Confidential Data under the custodianship of individual staff members.

5. Unless the Confidential Data is protected by encryption, only authorized university personnel may have access to the system.

#### **D. Specific to Application and File Servers**

1. Must be housed in a physically secure computer room or data center.
  - Entry must be logged and the logs retained for at least five days.

*Suggestion:* Where feasible, log exits as well.

- Video monitoring is an acceptable solution to this requirement.
  - Visitors not permitted except under escort.
2. An individual's access to a store of Confidential Data should be via an account assigned for the sole use of that individual.
    - This requirement is not to be interpreted as disallowing access to an encrypted dataset via a shared encryption key.

*Suggestion:* Use dual-factor authentication for root/administrator access to these systems. (When campus-wide mechanisms are in place for dual-factor authentication on all standard platforms, this will become a requirement.)

*Suggestion:* Implement a formal change control process.

### **E. Specific to Public Workstations and Kiosks**

1. Such systems may never be used for administrative processing of Confidential Data.

### **F. Network Security**

1. The edge ACL or other packet-filtering mechanism on any subnet with systems housing Confidential Data must employ a default-deny strategy that prohibits unnecessary inbound internal and external connections and that strictly limits access to the systems with Confidential Data.

*Suggestion:* Where off-campus connectivity is not needed, put the system into a non-routable space (10 space).

2. Any system holding or accessing Confidential Data that is on a wireless connection must use RedRover-Secure, or a departmental wireless network with equivalent or stronger security.
3. Any remote, off-campus access to a system containing Confidential Data must use an encrypted connection.
  - Examples of encrypted network transport include: ssh/sftp, SSL/TLS, a VPN with encryption enabled.
4. Fully document the list of services, protocols and systems permitted access into such subnets.
  - A subnet's ACL list or firewall rule set suffices to fulfill this requirement.
  - Review this documentation on a semiannual basis.
  - File a copy of the current documentation with the local IT head and the Unit Security Liaison.

### **G. Additional Encryption Requirements**

1. Confidential Data must be encrypted when it is transmitted via e-mail.
  - This applies to such data either in the body text or in an attachment.

- Use of the password-protection feature found in Microsoft Word, Microsoft Excel and similar applications is not sufficient to fulfill the requirement of encrypting e-mail attachments that contain Confidential Data.
2. Confidential Data must be encrypted when it is accessed via the web.
  3. Confidential Data must be encrypted when it is transmitted over non-Cornell networks.  
*Suggestion:* Whenever feasible, it should also be encrypted when transmitted within Cornell networks.
  4. If passwords that grant access to Confidential Data are stored on a networked device, they must be encrypted.
    - Use of the password-protection feature found in Microsoft Word, Microsoft Excel and similar applications does not fulfill this requirement.

## **H. Additional Process and Documentation Requirements**

*The IT Security Office will provide templates and/or more specific guidelines for fulfilling items listed here.*

1. Define and document incident response and escalation procedures for a potential loss of Confidential Data.
  - Review these processes on a semiannual basis.
2. Document how Confidential Data flows into and out of the local business unit and local applications.
  - Review this documentation on a semiannual basis.
  - File a copy of the current documentation with the local IT head and the Unit Security Liaison.
  - The relevant central unit will be responsible for fulfilling this requirement for any campus-wide application or service that handles Confidential Data.
3. When a unit grants any non-governmental external entity access to Confidential Data, that entity must provide documentation of:
  - (a) how this data will be transmitted, processed, stored and secured; and
  - (b) how such data is monitored and what incident response mechanisms are in place.
    - Review this documentation on an annual basis.
4. Follow a documented process for disposal of Confidential Data when no longer needed for legal, regulatory or business needs.
  - Ensure that local and university data retention guidelines are met.
  - This process needs to include an approach to data / media destruction.
  - Review this documentation on an annual basis.

- File a copy of the current documentation with the local IT head and the Unit Security Liaison.
5. All users with access to Confidential Data must execute a yearly attestation of the awareness of the relevant policies, risk and protective measures.
- An individual's electronic access to Confidential Data does not convey any right to share that data with unauthorized personnel.