**Drake Technology Services**

# INFORMATION SECURITY

## POLICY STATEMENT

Drake University expects all institutional information stewards, custodians, and local support providers who have access to and responsibilities for institutional information to manage it according to University rules regarding storage, disclosure, access, classification of information, and minimum applicable privacy and security standards as set forth in this policy.

## REASON FOR POLICY

Drake takes seriously the responsibility for maintaining and protecting informational assets and complying with applicable federal and state legislation.

## ENTITIES AFFECTED BY THIS POLICY

- All units of the University

## WHO SHOULD READ THIS POLICY

- All stewards and custodians of institutional information
- Local support providers
- Unit heads

## WEBSITE ADDRESS FOR THIS POLICY

Drake University Policy Library: *drake.edu/info*
Drake Technology Services Published Policies: *confluence.drake.edu/display/SPS/Security+Policy*

**Drake Technology Services**

# INFORMATION SECURITY

## TABLE OF CONTENTS

**Drake Technology Services**

# INFORMATION SECURITY

**Drake Technology Services**

# INFORMATION SECURITY

## I. RELATED DOCUMENTS, FORMS, AND TOOLS

- DTS Data Sharing Agreement

## II. DEFINITIONS

These definitions apply to terms as they are used in this policy.
*Any item labeled as a "√* ***Best Practice Standard****" reflects a beneficial practice that might become a requirement at some future date.*

**Federal Educational Rights and Privacy Act (FERPA)**: A federal law that gives students rights to their educational records and establishes the requirement that schools must have students; consent to disclose educational records. Institutions that receive funding under a program administered by the U.S. Department of Education are required to comply.

**Information Custodian**: An individual with access to institutional information or who uses that information in the legitimate course of university business.

**Information Steward:** A University office/official with executive responsibility over certain institutional information.

**Institutional Information**: Information generated in furtherance of the University's mission, not including research data.

**Level 1 Information—Confidential Institutional Information**: Information that has been determined by institutional information stewards to require the highest level of privacy and security controls. Currently, any information that contains any of the following data elements, when appearing in conjunction with an individual's name or other identifier, is considered to be confidential (level 1) institutional information:

- Passwords
- Social Security number
- Credit card number
- Driver's license number
- Bank account number
- Protected health information, as defined by the Health Insurance Portability and Accountability Act (HIPAA)
- Student Records protected by the Federal Educational Rights and Privacy Act (FERPA ) requests for confidentiality

**NOTICE**

1. ***The data elements that comprise the category "confidential (level 1) institutional information" are reviewed regularly and are subject to change at any time based upon regulations or business needs, etc.***
2. ***A personal decision to store one's own personal information is not governed by this policy.***

**Level 2 Information—Restricted Institutional Information**: All information used in the conduct of University business, unless categorized as public (level 3) institutional information or confidential (level 1) institutional information.

**Level 3 Information—Public Institutional Information**: Information that the University has expressly made available to or published for the use of the general public.
**Legitimate Interest**: A requirement for access to institutional information to perform one's authorized duties effectively and efficiently.

**Local Support Providers:** Drake employees with responsibility for managing or maintaining information technology assets and who are employed outside of Drake Technology Services.

**Unit**: A college, department, program, research center, business service center, office, or other operating unit.

## III. RESPONSIBILITIES

Drake Technology Services

- Maintain responsibility for implementation of this policy.
- Train and educate the University community on this policy.
- Monitor technological developments, changes in the law, user behavior, and the market, and update this policy as appropriate.

Information Custodian

- Implement procedures for policy compliance.
- Execute unit's procedures for meeting minimum standards for information security according to information classification (see Procedures)
- Report all information breach incidents.

Information Steward

- Establish rules for disclosing and authorizing access to institutional information.
- Conduct annual risk assessments of privacy practices and security standards.

Local Support Providers

- Maintain overview responsibility for implementation of this policy in their unit.
- Train and educate the members of their unit on this policy.
- Monitor technological developments, changes in the law, user behavior, and the market, and suggest updates to this policy as appropriate.

Unit Head

- Assume responsibility for policy compliance for the institutional information under his or her control.
- Deploy procedures to comply with the institutional information steward's rules for disclosing, categorizing, and authorizing access to institutional information.
- Deploy procedures for meeting minimum standards for institutional information security according to information classification.

## IV. PURPOSE

Privacy practices and security standards serve to preserve and protect institutional information. This policy incorporates a set of requirements for protecting the University's computers and networks as well as safeguarding the University's institutional information.

The integration of information technologies in virtually every aspect of transmission and storage of institutional information requires responsible administrative, technical, and physical security practices and standards. The focus on these procedures falls mainly on the administrative and technical aspects of privacy and security practices. All University community members are responsible for adhering to the procedures that follow.
While no one policy can absolutely ensure the protection of institutional information, this policy does provide Drake University with a coherent plan integrating state-of-the-art administrative and logical security practices based on the following principles:

- To promote an environment that fosters the availability and sharing of information.
- To ensure authenticated access and to bear responsibility for systems security.
- To strive to operate within industry standards and to adhere to all applicable laws.
- To balance the need to provide meaningful products and services against any attendant security risks to our customers and the importance of maintaining the reputation and integrity of the University.

**Drake Technology Services**

# INFORMATION SECURITY

## V. PROCEDURES

### 1. OVERVIEW

***NOTICE***

***The data elements that comprise the category "confidential (level 1) information" are reviewed regularly, and are subject to change.***

***One's personal decision to store one's own personal information is not governed by these requirements for safeguarding confidential data.***

#### 1.1 Classification of Institutional Information

Confidential (Level 1) Institutional Information
Information that has been determined by institutional information stewards to require the highest level of privacy and security controls. Currently, any information that contains any of the following data elements, when appearing in conjunction with an individual's name or other identifier, is considered to be confidential (level 1) institutional information:

- Passwords
- Social Security number
- Credit card number
- Driver's license number
- Bank account number
- Protected health information, as defined in the Health Insurance Portability and Accountability Act (HIPAA)
- Student Records protected by the Federal Educational Rights and Privacy Act (FERPA ) requests for confidentiality

Restricted (Level 2) Institutional Information
All information used in the conduct of University business, unless categorized as public (level 3) institutional information or confidential (level 1) institutional information.

Public (Level 3) Institutional Information
Information that the University has made available or published for the explicit use of the general public.

#### 1.2 Stewards, Unit Heads, and Custodians

In accordance with University IT Policy 1.7 Data Stewardship and Custodianship (*in review*), institutional information stewards assume responsibility for the management practices of information under their purviews, including a general inventory of the kind of information specific to their executive or functional roles, classification of information into one of the three categories that

this policy creates for the purposes of establishing rules for the protection of that information and, most importantly, providing up-to-date authorization for access to information. Unit heads are responsible for implementing this policy within their units. Custodians are expected to comply with the rules of this policy and the baseline standards for computer security, as well as the technical requirements for the protection of confidential (level 1) institutional information and restricted (level 2) institutional information.

### 1.3 Security of Material Documents

Anyone handling confidential (level 1) institutional information in material form should take all appropriate measures to secure it physically, which includes but is not limited to maintaining it while stored in a locked office or cabinet and, during use, under close personal supervision. Anyone in possession of institutional information should be mindful of the sensitivity of that information and use appropriate judgment about its handling and storage management. The measures outlined below are mandatory for paper documents containing confidential (level 1) institutional information. Refer to the General Records Retention Guideline determined by the Office of Business and Finance for information on retention practices.

General Requirements

Documents containing confidential (level 1) institutional information are expected to be secured so they are accessible only to authorized personnel. "Secured" means locked in a drawer; filing cabinet; or a hard-wall, private, or shared office; or containers used for easy transport or removal.

Documents containing confidential (level 1) institutional information may never be left unattended in a public area.

When no longer needed for daily operations, documents containing confidential (level 1) institutional information are expected to be destroyed or moved to a secure archive facility.

When documents containing confidential (level 1) institutional information are faxed or mailed off-campus, a signed receipt of delivery is required.

When documents containing confidential (level 1) institutional information are transmitted via campus mail, the envelope is expected to be sealed and stamped "confidential."

When documents containing confidential (level 1) institutional information need to be destroyed, an institutionally approved secure disposal service or a crosscut shredder is expected to be used.

Requirements Specific to Printers and Fax Machines

During business hours, the device should be in a location where it is accessible only to authorized personnel.

Off-hours, the device should be in a physically secure (locked) environment.

√ **BEST PRACTICE:**
If possible, periodic review of the device's record of received documents can be performed to ensure that all documents are accounted for.

***NOTICE***

***On an occasional basis, sensitive documents can be sent to an unsecured device, as long as the recipient or the recipient's authorized designee is sure to be present at the time of printing.***

## 2. BASELINE IT SECURITY REQUIREMENTS FOR ELECTRONIC INFORMATION

### 2.1 Introduction

To safeguard the University's information and information technology (IT) resources, the IT Security Office requires the following practices. These requirements apply to any system that is (a) used to conduct University business, or that is (b) connected to Drake campus networks (including non-Drake equipment).

These requirements, as well as the accompanying requirements for securing confidential (level 1) institutional information, reflect an approach referred to as "layered defense" or "defense-in-depth." As a community, we need to build defenses on multiple levels—network, system, application, and information—so if the integrity of one is weakened, another may still be able to provide sufficient protection. It is the sum of all these measures, and not reliance on

***NOTICE***

***For the purposes of this policy, "conducting university business" does not include viewing or updating your own individual university information.***

any particular aspect of security, that will move the University toward a more secure IT environment.

## 2.2 Exceptions

The following exception process is expected to be followed for all computers or other IT resources that are not able to meet these security requirements:

IT resources that cannot meet the following requirements are expected to be identified to the chief information officer (CIO) who, in consultation with DTS directors, will examine alternate methods to address the risk in question. If an alternate security solution can be found to address the specific risk, an exception is not required. If an alternate security solution cannot be found, the CIO will present the exception request to ITSA Board for review and determination of action.

***NOTICE***

***University IT Policy 1.4, The Authentication to Information Technology Resources mandates that the password associated with one's Drake ID can only be used in conjunction with the central authentication infrastructure.***

IT staff who report to University units outside of DTS may identify a local solution after consultation with the appropriate DTS director. The CIO will maintain a list of all IT resources that require an exception and review these exceptions on an annual basis in consultation with the ITSA.

## 2.3 Baseline Requirements for All Computers

1) Keep all relevant operating system, server, and application software up-to-date (patched).

   a) A local patch management process is expected to ensure that all security/critical updates are installed as soon as possible, but no later than 30 days after their release.

   b) A system that is currently not connected to the network does not need to be patched immediately. When it is brought back online, all the relevant updates are expected to be installed immediately.

2) Configure user privileges to be as low as possible while still meeting business needs. Consistent or regular use of the administrator or root account is inappropriate.

3) Ensure all accounts have strong passwords at least equivalent to the strength required for Drake ID passwords.

4) No electronic distribution of passwords in the clear, i.e., transmission is to be encrypted.

5) For any computer system that is not in a locked, private space, run a password-protected screen saver, or some other console-locking mechanism, that is triggered after 20 minutes (or less) of inactivity.

√ **BEST PRACTICE:**
Advise and instruct user to be judicious in employing automatic password selections even in cases where a computer is located in a securable, locked, private location.

6) Ensure local/personal firewalls and/or IPSec filters are installed and configured appropriately for the business need.

7) On all Windows and Macintosh systems, run anti-malware (anti-virus, etc.) software with daily updates and active protection enabled.

√ **BEST PRACTICE:**
Run an anti-malware package on Linux systems, as well.

### 2.4 Baseline Requirements Specific to Desktops, Laptops, Portable Devices, and Smart Phones

1) All local shares and other mechanisms for file access are to be password protected.

2) This requirement forbids "open shares" (unauthenticated read/write access), "drop folders" (unauthenticated write-only access), and "public folders" (unauthenticated read-only access) on an individual's system.

√ **BEST PRACTICE:**
Use blueSpace shared file storage instead of local shares.

3) If multiple individuals use a system, each should have his or her own login account, or the system should be restored to a known, clean state prior to each individual use. This also applies to "loaner" systems.

4) A desktop, laptop, netbook, or tablet that is left unattended in a public or otherwise insecure location is expected to be physically secured.

√ **BEST PRACTICE:**
Provide locking cables to staff members who travel with such mobile devices.

### 2.5 Baseline Requirements Specific to Application and File Servers

1) Follow hardening requirements for the operating system and any applications or services that connect to the network.

- Along with the software vendor, credible sources for guidelines may include NIST, CIS, NSA, SANS, and 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. See University IT Policy 1.4 Authentication to Information Technology Resources.

2) Shared accounts are prohibited, except where it is not technically possible to provision individual accounts.

- Where a shared account is necessary, maintain a local inventory of who has access to the account.

- Change the password for any shared account when there is any change in personnel or access requirements.

√ **BEST PRACTICE:**
Keep servers, especially those that are open to users outside of the local workgroup, on a segregated network.

**Drake Technology Services**

# INFORMATION SECURITY

## 2.6 Baseline Requirements Specific to Public Workstations and Kiosks

1) Such systems are expected to display an appropriate login banner, splash screen, or bear signage with the following information:

- A statement about responsible use. See University IT Policy 1.2 Responsible Use.
- A warning about using the system for personal or sensitive information
- A reminder to logout and/or clear any active credentials

2) No local file shares permitted.

3) If a user needs system privileges (ability to write files), then the computer is expected to be restored to a known, clean state between individual sessions.

4) Visually inspect such systems regularly, at the very least on a quarterly basis, to see if physical security has been compromised.

## 2.7 Network Security

1) The primary goal is to limit network access to servers and other critical resources. Consider to what extent you might want to filter traffic to and from individual computers.

- When designing a rule set, make sure you thoroughly understand the services required for a given network, taking into account the needs of your unit and of others who might use it. The director of communication and network services can assist in developing a rule set.
- Ensure host firewalls and similar measures are used to supplement network ACL/firewall rules.

2) All systems are expected to be registered by MAC address and assigned to a user or network administrator, including any unit

wireless networks and wireless access points. No unregistered systems should be on any Drake network. This requirement is detailed in University IT Policy 1.5 Network Registry.

## 2.8 Reviews and Assessments

The unit is responsible, at least annually, for assessing the local infrastructure and environment. This assessment should include the following:

1) Review edge ACLs and other network security mechanisms.

2) Run a vulnerability scanner and remediate high-risk vulnerabilities.

3) Review the security of all file and application servers.

- Check for vulnerabilities in Web sites, databases, etc.

- Use an approved DTS tool to scan file servers for confidential (level 1) institutional information. (This requirement does not apply to databases or other structured data repositories.)

4) For a sample set of staff computers, conduct content inventories using an DTS approved data discovery tool to ensure no improper instances of confidential (level 1) institutional information.

√ **BEST PRACTICE:**
Run annual, or more frequent, content scans of all systems.

5) Audit account distribution to ensure that only current, authorized personnel have access to departmental systems.

**Drake Technology Services**

# INFORMATION SECURITY

## 3. IT SECURITY REQUIREMENTS FOR CONFIDENTIAL (LEVEL 1) INSTITUTIONAL INFORMATION

***NOTICE***

***These requirements are in addition to those outlined in the "Procedures — Baseline IT Security" Requirements" section of this policy.***

### 3.1. Introduction

To better safeguard the University's institutional information, the Information Technology Security Advisory Committee requires the following practices for electronic transmission and storage of confidential (level 1) institutional information. The following sections of this policy outline classifications of institutional information, and, for information that is classified at the highest level (level 1), its encryption requirements, scanning requirements, and other measures.

### 3.2 Information Classification

This policy establishes three institutional information security classifications:

1) Confidential (level 1) Institutional Information
2) Restricted (level 2) Institutional Information
3) Public (level 3) Institutional Information

Unless otherwise classified, all information used in the conduct of University business is restricted (level 2) institutional information. Institutional information that has been explicitly made available to the public, with no authentication required for network access, is public (level 3) institutional information.

The confidential (level 1) institutional information classification currently comprises the following data elements, when they appear in conjunction with an individual's name or other identifier:

- Passwords
- Social Security number
- Credit card number
- Driver's license number
- Bank account number
- Protected health information, as defined in the Health Insurance Portability and Accountability Act (HIPAA)
- Student Records protected by the Federal Educational Rights and Privacy Act (FERPA) requests for confidentiality

This set may expand based on future regulatory requirements or designations made by the appropriate institutional information steward and with appropriate review.

These requirements apply to confidential (level 1) institutional information that is under the custodianship of the University, so they do not pertain to your own personal information you may have stored on a computer or device.

Please note that some data elements classified as confidential (level 1) institutional information are subject to legal or regulatory requirements that go beyond those given here. Such requirements for regulated information are expected to be fulfilled, along with these Drake 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).

### 3.3 Systems Subject to These Requirements

These requirements apply to any system that holds confidential (level 1) institutional information, both on- or off-campus, even if system is not University-owned.

For the purposes of this policy, a system is considered to be "holding" confidential (level 1) institutional information when such information is stored locally on the system or when the system is used regularly to direct mount and has access to such information 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 (Level 1) institutional information would need to be secured as if such information was stored locally.

On the other hand, a system used to access confidential (level 1) institutional information via an application, including database access, would not be viewed as holding such information.

### 3.4 Encryption Standards

In several places, these requirements specify a need to encrypt information, either for storage or for transmission. Some examples are given of viable encryption implementations but no comprehensive list is provided here.

The CIO will approve a given method of encryption for use with confidential (level 1) institutional information if it both (a) employs a contemporary algorithm, and (b) is effectively implemented by the product in question.

### 3.5 Exceptions

The following exception process is expected to be followed for all computers or other IT resources that are not able to meet the security requirements stated in this policy:

1) IT resources that cannot meet the following requirements are expected to be identified to the CIO who, in consultation with DTS Directors, will examine alternate methods to address the risk in question. If an alternate security solution can be found to address the specific risk, an exception is not required. If an alternate security solution cannot be found, the CIO will present the exception request to the Information Technology Security Advisory Board for review and determination of action.

2) IT staff who report to University units outside of Drake Technology Services may identify a local solution or consult with the appropriate DTS Director.

3) The CIO will maintain a list of all IT resources that require an exception, and review these exceptions on an annual basis in consultation with the Information Technology Security Advisory Board.

### 3.6 Confidential (Level 1) Institutional Information—Requirements for All Computers

1) Keep all relevant operating system, server, and application software up to date.

- A local patch management process is expected to ensure that all security updates are installed as soon as possible and no later than 30 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 guidelines, 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 (level 1) institutional information and information 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 (level 1) institutional information

- Peer-to-peer (P2P) file-sharing software may not be run on a system holding confidential (level 1) institutional information

- Confidential (level 1) institutional information and information 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 (level 1) institutional information

4) On a quarterly basis, audit and verify only currently authorized personnel have accounts that grant access to confidential (level 1) institutional information.

√ **BEST PRACTICE:**
Audit file, application, and system privileges on a periodic basis.

### 3.7 Confidential (Level 1) Institutional Information—Requirements Specific to Desktops and Laptops

1) The account used for daily operations is expected to be configured not to allow software installs or is expected to require the account password for an install.

√ **BEST PRACTICE:**
Where feasible, do not give end users any accounts that permit software installation.

2) On any system holding confidential (level 1) institutional information, use a unique password, not shared with other systems, for local administrator accounts (accounts with elevated privileges).

   In particular, the local administrator password used by IT support staff members is expected to be different for each system that holds confidential (level 1) institutional information.

   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 (level 1) institutional information stored locally on a system is expected to be removed when no longer needed for an operational reason.

√ **BEST PRACTICE:**
Do not permit storage of confidential (level 1) institutional information on individual staff member machines.

4) In areas where confidential (level 1) institutional information is handled on a regular basis, run a data discovery tool on all systems every six months.

5) Confidential (level 1) institutional information is expected to be encrypted on all of the following:

- Any system that, even on a temporary basis, is not located on one of the Drake campuses or some other formal University location

- Any laptop, netbook, tablet, smart phone, PDA, or other mobile device

√ **BEST PRACTICE:**
Where feasible, use full-disk encryption on such devices.

- 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, ensuring that the encryption does not interfere with the ability to create and retrieve backups.

Protect encryption keys against disclosure, misuse, and loss

Examples of portable media include external hard drives, USB drives, CDs, DVDs, tapes, and diskettes.

Acceptable encryption solutions should be identified in consultation with the Director of Computer Network Services.

√ **BEST PRACTICE:**
Encrypt all instances of confidential (level 1) institutional information under the custodianship of individual staff members.

***NOTICE***

***Video monitoring is an acceptable solution to this requirement. Visitors are not permitted except under escort.***

### 3.8 Confidential (Level 1) Institutional Information—Requirements Specific to Application and File Servers

1) All application servers and file servers are expected to be housed in a physically secure computer room or data center. Entry is expected to be logged and the logs retained for at least five days.

√ **BEST PRACTICE:**
Where feasible, log exits as well.

2) An individual's access to a store of confidential (level 1) institutional information 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.

3) Confidential (level 1) institutional information should be removed from file servers when it is no longer needed on an operational basis. To the extent feasible, this also applies to confidential (level 1) institutional information stored in databases and other application frameworks.

√ **BEST PRACTICE:**
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.)

4) Any confidential (level 1) institutional information on development and test systems is expected to be masked or redacted.

### 3.9 Confidential (Level 1) Institutional Information—Requirements Specific to Public Workstations and Kiosks

Such systems may never be used for administrative processing of confidential (level 1) institutional information.

### 3.10 Confidential (Level 1) Institutional Information—Network Security

1) The edge ACL or other packet-filtering mechanism on any subnet with systems housing confidential (level 1) institutional information is expected to employ a default-deny strategy that prohibits unnecessary inbound, internal and external connections and that strictly limits access to the systems with confidential (level 1) institutional information.

√ **BEST PRACTICE:**
Where off-campus connectivity is not needed, put the system into a non-routable space.

2) Any system holding or accessing confidential (level 1) institutional information that uses a campus wireless connection

is expected to be authenticated and encrypted using a DTS approved standard.

3) Any remote, off-campus access to a system containing confidential (level 1) institutional information is expected to use an encrypted communication. Examples of encrypted network transport include ssh/sftp, SSL/TLS, and VPN with encryption enabled.

4) Fully document the list of services, protocols, and systems permitted access into such subnets.

5) 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 CIO.

### 3.11 Additional Confidential (Level 1) Institutional Information—Encryption Requirements

1) Confidential (level 1) institutional information is expected to be encrypted when it is transmitted via email.

***NOTICE***

***Drake's email system provides a secure, Web-based vehicle for exchanging files with other people holding Drake IDs.***

This applies to such information either in the body text or in an attachment.

√ **BEST PRACTICE**
Use email that uses HTTPS 128-bit SSL-enabled connection and encrypted transmission protocols (POP-S/IMAP-S/SMTP-S).

1) Confidential (level 1) institutional information may not be transmitted via instant messaging (AIM, etc.) or text messaging (SMS).

2) Confidential (level 1) institutional information is expected to be encrypted when it is accessed via the Web.

3) Confidential (level 1) institutional information is expected to be encrypted when it is transmitted over non-Drake networks.

***NOTICE***

***IM or SMS would be permissible if the transmission was encrypted, but encryption is not available with the standard, commercial IM and SMS offerings.***

√ **BEST PRACTICE:**
Whenever feasible, it should also be encrypted when transmitted within Drake networks. Use a Virtual Private Network (VPN) when transmitting over a non-Drake network,

4) If passwords that grant access to confidential (level 1) information are stored on a networked device, they are expected to be encrypted. While Microsoft Office 2007 includes a facility for appropriately strong encryption, the password-protection feature found in older versions of Word and Excel is not sufficient. Similar facilities in other applications may not fulfill this requirement.

5) Any confidential (level 1) institutional information on a storage device used to transport data physically is expected to be encrypted.

- This does not apply to media that is used exclusively to store data and is kept in a secure location. For example, CDs, DVDs, or tapes kept under lock and key.

- Where this is not feasible, compensatory measures, such as increased physical security, are expected to be taken.

### 3.12 Inventory of Confidential Institutional Information

1) Maintain an inventory of all systems holding confidential (level 1) institutional information. Review the inventory every six months.

2) File a copy of the current inventory with the local IT staff and the CIO, DTS.

3) Both workstations (laptop and desktop) and servers (file, application, and database) need to be included in the inventory. Out of scope are mobile/smart phones, PDAs, USB drives, and removable media (DVDs, CDs, diskettes, and tapes).

4) The required information, detailed below, is expected to be recorded explicitly for each system holding confidential (level 1) institutional information. However, not all of this information

needs to be in the inventory itself, as long as the rest of the required elements can all be retrieved on short notice. The inventory does need to contain sufficient detail, so the mapping to the balance of the requested information is unambiguous.

Information required for workstations:

- Date of entry into inventory
- Date of last review or update
- Assigned user (or, if not for use by a single individual, the administrator)
- Role of the individual/function of system
- Whether a desktop or a laptop
- OS platform (Win, Mac, *nix, etc.)
- Primary hostname
- As applicable, assigned IP(s) for wired interface(s)
- MAC address(es) of Ethernet and Wi-Fi interfaces
- Make, model, and serial number
- Inventory tag (optional)
- Number of associated external hard drives, if any
- Backup (none, local, departmental, or Retrospect)

Information required for servers:

- Date of entry into inventory
- Date of last review or update
- Primary administrator
- Function(s)
- Type of service (dev, test, or prod)
- OS platform (Win, Mac, *nix, etc.)
- As applicable, DB platform (Oracle, MS SQL, FileMaker, etc.)
- Primary hostname
- Physical location
- Assigned IP address(es)
- MAC address(es) (optional)
- Make and serial number
- Inventory tag (optional)
- Data storage (internal, external, or both)
- Backup (none, local, departmental, or Retrospect)

5) Any of the following that are specific to the department or unit are expected to be listed in the inventory:

- Email servers (detail required for other types of servers does not need to be given)
- Outsourced applications that process confidential institutional information.
- Outsourced data repositories that hold confidential institutional information.

### 3.13 Additional Process and Documentation Requirements

Drake Technology Services will provide templates and specific guidelines for fulfilling items listed here.

1) Define and document incident response and escalation procedures for a potential loss of confidential (level 1) institutional information. Review these processes on a semiannual basis.

2) Document how confidential (level 1) institutional information 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 staff and CIO.

The relevant central unit will be responsible for fulfilling this requirement for any campus-wide application or service that handles confidential (level 1) institutional information.

3) When a unit grants any non-governmental external entity access to confidential (level 1) institutional information, that entity is expected to provide documentation of the following:

- How this information will be transmitted, processed, stored, and secured.
- How such information is monitored and what incident response mechanisms are in place.

- A Data Sharing Agreement. Contact the director of computer information services to obtain a Data Sharing Agreement template.

4) Review this documentation on an annual basis.

- Follow a documented process for disposing of confidential (level 1) institutional information when it is no longer needed for legal, regulatory, or business purposes.
- Ensure that local and University information retention guidelines are met.
- Review this documentation on an annual basis.
- File a copy of the current documentation with the Chief Information Officer.

5) All users with access to confidential (level 1) institutional information are expected to execute a yearly attestation of the awareness of the relevant policies, risk, and protective measures. An individual's electronic access to confidential (level 1) institutional information does not convey any right to share that information with unauthorized personnel.

Adapted from: Cornell University,
http://www.dfa.cornell.edu/dfa/treasurer/policyoffice/policies/volumes/informationtech/infosecurity.cfm