Checklist for Protecting Information Guideline

This document provides guidance to members of the University of Cincinnati (UC) community as a checklist for protecting information.

Checklist

Information Communicated Orally

- Make it a practice not to discuss confidential information outside of the workplace or with anyone who does not have a specific need to know.
- Be aware of the potential for others to overhear communications about sensitive information in offices, on telephones and in public places like elevators, restaurants and sidewalks.

Information Stored on Paper

Documents that include controlled or restricted information like social security numbers; student education records; an individual's medical, benefits, compensation, loan, or financial aid data; and faculty and staff evaluations need to be secured during printing, transmission (including by fax), storage and disposal.

- Do not leave paper documents containing sensitive information unattended; protect them from the view of passers-by or office visitors.
- Store paper documents containing sensitive information in locked files.
- Do not leave the keys to file drawers containing confidential information in unlocked desk drawers or other areas accessible to unauthorized personnel.
- Store paper documents that contain information that is critical to the conduct of University business in fireproof file cabinets. Keep copies in an alternate location.
- Shred confidential paper documents that are no longer needed and secure such documents until shredding occurs. If a shredding service is employed, ensure that the service provider has clearly defined procedures in the contractual agreement that protects discarded information and that the provider is legally accountable for those procedures, with penalties in place for breach of contract.

- Make arrangements to immediately retrieve or secure sensitive documents that are printed on copy machines, fax machines and printers.
- Double-check fax messages containing confidential information:
- Recheck the recipient's number before you hit 'start'.
- Verify the security arrangements for a fax's receipt prior to sending.
- Verify that you are the intended recipient of faxes received on your machine.

Information Stored Electronically

All employees and users of networked computing devices on the University of Cincinnati's (UC) network have a role in protecting the University's information assets because their machines provide potential gateways to private information stored elsewhere on the network. Therefore, whether or not you deal directly with sensitive or confidential University information, you should take the following steps to reduce risk to UC's information assets.

Educating Yourself

- Read the information security policies (www.uc.edu/infosec/policies.html) and understand their implications for the information for which you are responsible.
- Review and understand the following:
  - Data Governance & Classification Policy
  - Vulnerable Electronic Systems Policy
  - Acceptable Use of University Information Technology Resources
  - Password Policy

Know who your Department Computer Administrator is and what he can do for you.

- Immediately advise the UCIT Office of Information Security of any suspicious activity on your computer or a suspected information system security compromise.
- Be mindful of how you are sharing or transmitting sensitive information across the network.

PROTECTING E-MAIL

- Understand that email is not secure; it can be forged and it does not afford

privacy.

- Install anti-virus software on your computer and ensure that the software is set automatically to update its virus definitions at least weekly.
- UC distributes antivirus at no charge; refer to https://www.uc.edu/infosec/antivirus.html to download.
- Do not open unexpected email attachments and do not download documents or software from unknown parties.
- Clear email boxes of old messages on a regular basis by deleting unnecessary messages or archiving needed ones. Be sure to back up important email on a regular basis and secure back ups with encryption, passwords, or if in a physical form, in a locked desk or area.
- Take precautions not to send anything by email that you wouldn't want disclosed to unknown parties.
- Recipients have been known to distribute information to unauthorized recipients or store it on unsecured machines and viruses have been known to distribute archived email messages to unintended recipients.
- Learn how to encrypt email, refer to www.uc.edu/infosec/info/encryption.

RESTRICTING ACCESS TO INFORMATION ON YOUR DESKTOP

- Orient your computer screen away from the view of people passing by.
- Turn off your desktop computer at the end of the workday, unless automatic updates, backup processing and/or various other maintenance operations are scheduled during off-hours.
- Use a password-protected screen saver on your desktop computer and configure it to display after a reasonable period of non-use (1 minutes is recommended).
- Use security devices to lock down computers that are in public or otherwise unsecured spaces.
- Sanitize the hard drives of computers that you declare surplus and of those that are going out of service for other reasons to ensure that data is removed and not recoverable, Electronic Media Sanitization Standard.
- Deleting files, moving files to "trash," and emptying the "trash" file is insufficient because the files can still be recovered.
- Ensure that functions that enable data sharing on an individual workstation are either turned off or set to allow access only to authorized personnel.

SECURING MOBILE DEVICES

Information stored on laptop computers, tablets and other mobile devices are susceptible to equipment failure, damage, or theft. Information transmitted via wireless connection is not always secure.

- Protect and secure mobile devices from theft at all times.
- Use internal firewalls and strong authentication when transmitting information via wireless technologies.
- Use personal firewalls on laptops that will access the UC Network from a remote location.
- Back up the data on your mobile devices on a regular basis.
- Change batteries on mobile devices as soon as the "low battery" prompt appears to avoid losing information, configurations and settings.
- Enable encryption on mobile devices.

PROTECTING PASSWORDS

- Employ passwords that are easy for you to remember but impossible for someone else to guess:
- Passwords should not consist of a word that can be found in a dictionary.
- Passwords should be at least 8 characters in length and consist of a combination of numeric characters, mixed upper and lower case alpha characters and at least one special character.
- Consider using the first letter of each word in a phrase or sentence that you can easily remember. For example, "pSi#1ime" is derived from "Professor Smith is #1 in my eyes."
- Secure your passwords and restrict access to them. Passwords written on a post-it in a work area, placed under a keyboard, or stored in an unlocked desk drawer are not safe from unauthorized access.
- Never share your passwords or accounts.
- Change your passwords at least every 180 days. The more sensitive the information being protected, the more frequently you should change your passwords.
- Understand how to properly restrict file sharing on your computer to mitigate the risk of unintentionally granting access to unknown parties.

SAFEGUARDING THE INTEGRITY OF INFORMATION

- Apply system updates for your desktop systems and department servers' operating systems and their integrated network services (e.g., e-mail and web browsers) in a timely manner.
- Keep local applications updated and patched. Configure your computer to automatically download and install the latest patches.
- Install a personal firewall and keep it set to automatically or regularly download and install updates.
- Password protect documents containing sensitive information.
- Refer to the documentation on how to encrypt Microsoft Office documents.
- Store all confidential data on a centrally managed server and not on individual workstations or laptops whenever possible.
- Do not place any sensitive information in an unsecured online location.
- Secure local servers in a locked room and limit the access to the room to system administrators only.
- Ensure that remote access (from off campus) connections are done securely using SSH or VPN.

BACKING UP INFORMATION

- Know the back-up and recovery strategies for the information for which you are responsible.
- Know whether your data is backed up centrally and/or locally.
- Know the frequency with which the back-ups occur.
- Know who is responsible for backing up your information.
- Make sure that the recovery procedures for your information have been tested.
- Know where your back-ups are stored. Store back-ups of critical information in an alternate location, preferably in another building across campus or off-site.
- Make sure that private information stored on back-ups in alternate locations is protected from unauthorized access.
- Know how you will recover critical data and resume related business operations in the event of loss of power, disruption of network services, theft of your computing device, or inability to access your office or building.
- Destroy CDs and delete unneeded files containing sensitive information on a

regular basis.

DEPARTMENTAL CHECKLIST

- Review the list of individuals who have access to shared drives used by the department at least annually.
- Do not allow shared user ID's.
- Remove authorization for access to systems (for individuals who have left the department or no longer require access) in a timely manner.
- Designate a locked cabinet for back-up data and a procedure that includes access to media (who has keys) and procedures for clearly labeling all backup data.
- On shared workstations, establish individual accounts for everyone who will use the device.

Related links

Policies
Security Standards
Data Governance & Classification
Vulnerable Electronic Systems Policy
Acceptable Use of University Information Technology Resources Policy
Password Policy
Antivirus
Encryption
Electronic Media Sanitization Standard
Encrypt Microsoft Office Documents

Phone Contacts:

IT@UC Office of Information Security 513-558-ISEC (4732) infosec@uc.edu

History:
Effective Date: 4/15/2015
Revised Date: 5/26/2017