USC University of Southern California

USC OFFICE OF COMPLIANCE
Information Security Education

Information Security at USC

Introduction

Welcome to USC's course on information security.

The purpose of this course is to:

- Describe information that requires special protections by law
- Give you practical guidance on how you can better protect and secure USC information
- Tell you whom to contact in the event that you learn about a security breach

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Introduction

What do we mean when we talk about “information security”?

Although there is no standard definition, information security usually refers to the process of protecting data from accidental or intentional misuse by persons inside or outside of an organization. Information security involves technical protection (for example, network or desktop security) but also relates to physical security (locking doors and cabinets).

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Why Is Information Security Important?

The effect of unauthorized access and use of information is costly. Some of these costs include:

- Lost productivity due to unavailability of breached information resources
- Costs associated with information technology staff's detection, containment, repair, and reconstitution of information
- Loss of trust in the organization because of negative publicity
- Costs associated with notifying affected people when personal data is compromised

FYI

Businesses and universities like LexisNexis (a legal database), ChoicePoint (a risk management and fraud prevention company), and UC Berkeley have had sensitive, personal data pertaining to hundreds of thousands of people compromised by unauthorized access.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Why Is Information Security a Priority at USC?

- The University's Code of Ethics makes clear that each of us plays an important role in building an honest and ethical community – one that respects the fundamental rights and dignity of its members. Protecting sensitive information is a critical component of those rights.
- Remaining vigilant about information security upholds USC's reputation as a responsible steward of the public trust.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Information Requiring Special Protections

Beyond our ethical obligations, there are federal and state laws requiring USC to protect information from unauthorized use and disclosure. Legally protected categories of information include:

- ***Education records:*** Under the Family Educational Rights and Privacy Act of 1974, or "FERPA," USC may not disclose records relating to a student without the student's written permission.
- ***Health information:*** Under the Health Insurance Portability and Accountability Act of 1996, or "HIPAA," USC may not use or release identifiable health information without the patient's written authorization. USC must notify patients and the federal government if there is a breach of patient information.

FYI

USC FERPA Policy

USC HIPAA Policies

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Information Requiring Special Protections

Other protected categories include:

- ***Personal information:*** Under California law, USC must protect personal information including name and any of the following data:
  - Social Security number
  - Drivers license number
  - Credit card and pin number
  - Medical information
- USC must notify various state agencies and all impacted individuals in the event that personal information is breached electronically.
- ***Customer information:*** Under a federal law known as the Gramm-Leach Bliley Act, USC must protect personally identifiable financial information that it collects about an individual in connection with providing a financial product or service such as financial aid or faculty housing loans.

FIND OUT MORE

USC Privacy of Personal Information Policy

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Other Standards

Other kinds of records that are protected under federal or state law include:

- ***Personnel records:*** These records are protected under state law and include offer letters, employment records, salaries, fringe benefits, and other personnel information.
- ***Research records:*** These records may be protected by copyright, trademark, trade secret, patent, or other intellectual property laws.

FIND OUT MORE

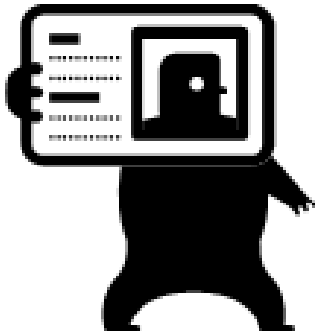
USC Information Security Policy

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Other Standards

- ***PCI compliance:*** The Payment Card Industry (PCI) Data Security Standard (DSS) is a comprehensive set of control objectives and requirements developed by the PCI Security Standards Council (SSC).
  - PCI DSS is intended to help organizations proactively protect customer account data.
  - Any organization/institution that stores, processes, or transmits credit card information must comply with PCI DSS.
- If you or your unit processes credit card transactions, you may need to comply with PCI standards. Contact the USC Treasurer's Office or Information Security Office for further assistance.



USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Other Standards

- ***FTC Red Flags:*** The Red Flags provisions of the Fair and Accurate Credit Transactions Act of 2003 are intended to help detect and prevent identity theft.
  - **Identity theft** - a fraud committed or attempted using the identifying information of another person without authority
  - **Red flag** - a pattern, practice, or specific activity that indicates the possible risk of identity theft

- Units that are covered by the Red Flags Identity Theft provisions include many departments within USC that process and maintain personal financial information.
- Covered units must develop an identity theft program.
- If you have questions about FTC Red Flags provisions, please contact the USC Office of Compliance.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Role of Information Security Office

In response to these business imperatives and legal requirements, USC established the Information Security Office, whose purpose is to assist the university's schools and departments in better protecting and securing the information they create, store, and transmit electronically and physically. It does so through:

- Providing education
- Developing and implementing policies and procedures
- Monitoring and auditing compliance with information security requirements
- Serving as a first contact in the event of information security breaches
- Working with USC's Information Technology Services (ITS) and school/unit IT administrators to address information security issues

FIND OUT MORE

Information Security Office

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

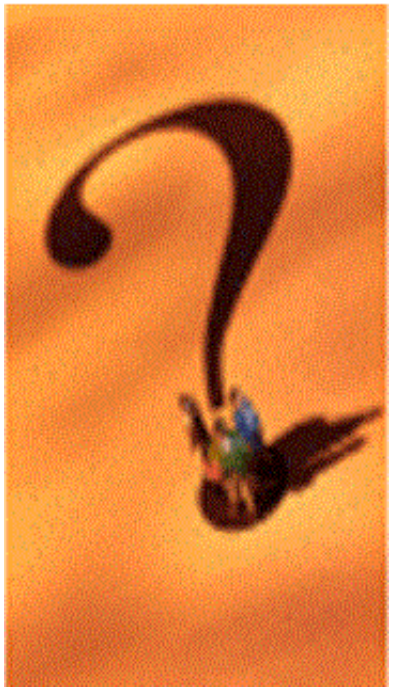
Which of the following are good reasons to protect data from accidental or intentional misuse?

A. Unauthorized access and use of information can be costly to an enterprise.

B. Many kinds of laws require USC to protect the privacy of various types of information.

C. Failing to protect the privacy of information may cause a loss of trust by the public in USC.

D. All of the above.



USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

A. Unauthorized access and use of information can be costly to an enterprise.

B. Many kinds of laws require USC to protect the privacy of various types of information.

C. Failing to protect the privacy of information may cause a loss of trust by the public in USC.

D. All of the above.

The correct answer is D. All of these reasons, among others, are good ones to protect the privacy and security of information created and/or maintained by USC.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

What are my obligations to secure USC information?

Users are responsible for utilizing appropriate measures including passwords, virus protection, patch management, and physical security to protect the security of components of the network infrastructure that they access and/or use.

Users are expected to comply with information security policies to ensure the security of the network infrastructure.

For more information, please see the USC Network Infrastructure Use policy:

http://policies.usc.edu/p5infoTech/network_use.pdf

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Security Measures – Overview

So what can you do to help protect the information you access and use every day?

The answer is several things, and most of them are simpler than you may suspect. They fall into the following areas:

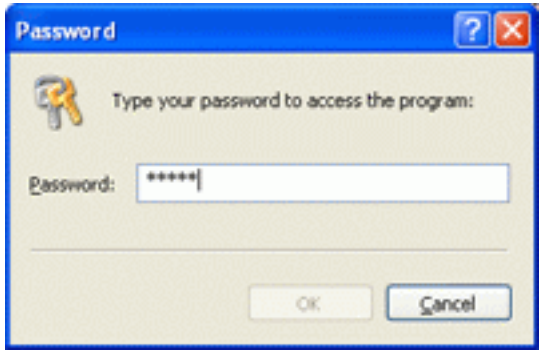
- Passwords and log-in monitoring
- Malicious software and security reminders
- Workstation security
- Data back-up
- Encryption (laptop, USB, external hard drive)
- Security incidents

We will discuss each of these measures in turn, and give you step-by-step guidance on what you can do to improve the security of the information you access and use.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Security Measures – Passwords and Log-in Monitoring



Passwords are used to authenticate, or validate, that the person using your Logon-ID is really you. However, passwords are also one of the most common targets of people trying to access information without authorization.

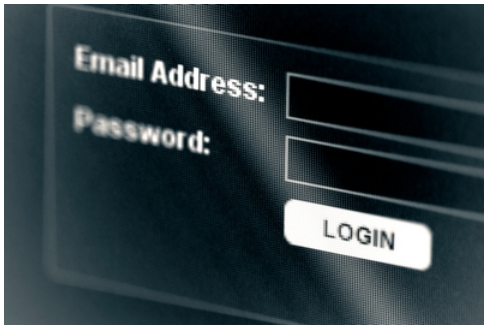
There are several methods that may be used to “break” a password. First, a hacker might just guess. This is the easiest method, because many people use personal information such as family names, birth dates, and simple number combinations like “11111.”

More automated methods (that are easy to do) include using software that can decrypt passwords within minutes.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Security Measures – Passwords and Log-in Monitoring



Here are some common mistakes to avoid when choosing a password:

- **Obvious passwords**: Avoid passwords with obvious personal meaning like your first or last name, or default passwords like “password” or “administrator.”
- **Short passwords**: Any password less than six characters simply won’t hold up under attack for very long. Many systems require passwords at least eight characters in length.
- **Common dictionary words**: Some software programs use searches of all words found in the dictionary as the basis for their attack and can complete such an attack within minutes.
- **Using the same password over and over**: Passwords should be changed frequently and a different password used each time.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Security Measures – Passwords and Log-in Monitoring

Here are some tips on how to create effective passwords:

- **Use a combination of upper case, lower case, numbers, and special characters**: On systems that support them, passwords should contain at least one of each of the following – uppercase letters, lowercase letters, numbers, and punctuation marks (!@#$^&*()+=-)
- **Use misspelled words**: By using a misspelled word, you avoid many dictionary-based attacks.
- **Numeric substitutions**: By using a combination of letters and numbers, a phrase can be spelled out without using complete words.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Security Measures – Passwords and Log-in Monitoring

Some examples of good passwords using these methods include:

- “2L8again” (“Too Late Again”)
- “rokiTshiP” (“Rocket Ship”)
- “Jak8&tiE” (“Jacket and Tie”)
- “WayteTilL8r” (“Wait Until Later”)

Effective passwords help ensure that unauthorized persons are unable to access information stored on your computer.

FYI

In addition to choosing an effective password, it is also important to safeguard the password. If, for example, you write down a password on a piece of paper, do not leave the paper in a place where other people can see it or use it.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Security Measures – Passwords and Log-in Monitoring

Another effective security measure is to make sure your computer automatically logs off when you are away from it for any length of time.

If a computer is not configured to log off automatically after it is not used for a specified length of time (for example, 10 minutes), then you may be away from your computer for hours and have no idea whether an unauthorized user has accessed private information you store on or access from your computer.

Configuring your system to log off automatically is a relatively simple task, but depends on what kind of operating system you use. Contact your IT administrator if you need additional assistance.

FIND OUT MORE

Contact your system administrator or the Information Security Office for assistance on passwords and log-in monitoring.

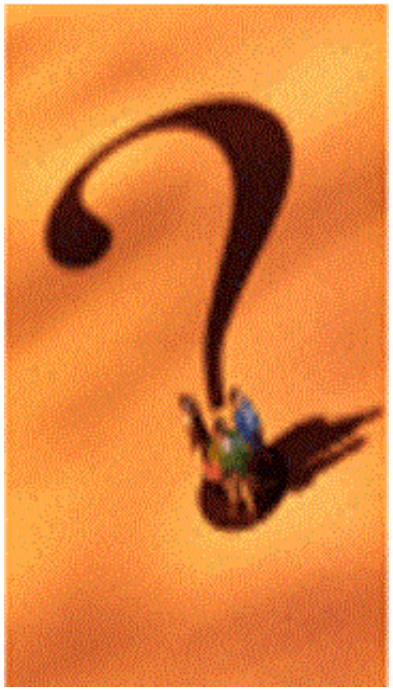
USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Security Measures – Passwords and Log-in Monitoring

Laura Harris is a new employee at USC and is trying to think of a password to protect her computer against unauthorized access. She decides to use “lharris” since it is short and easy to remember.

Is this a strong password?



USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Security Measures – Passwords and Log-in Monitoring

The correct answer is “No.”

Avoid using short, obvious passwords that are all in lowercase like this one. Instead, choose passwords that are not obvious; use a combination of upper case, lower case, numbers, and special characters; use misspelled words; and insert numeric substitutions. In this case, an example of a stronger password would be “1LoraHar%.”

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Malicious Software and Activities

Malicious software are programs that cause undesired actions in information systems. Some of the most common examples include:

- **Viruses**: Viruses are programs that spread to other software of the system. Viruses can weaken the availability, integrity, and confidentiality of data by destroying, changing, or altering it. Almost all viruses are attached to an executable file, which appears as an attachment to an e-mail that must be opened in order for the virus to spread.
- **Worms**: Worms are programs which often reproduce automatically and which can make use of the host computer's files. Unlike a virus, a worm does not need a computer user to open an attachment containing an executable file in order to spread.

FYI

Executable files usually have the file extension ".exe" or ".zip" at the end of the file name. Never double click on an attachment from a sender you do not know, especially if the attachment has an ".exe" or ".zip" file extension at the end of the file name.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Malicious Software and Activities

Other forms of malicious software include:

- **Spyware**: Spyware are programs that explore the files in a computer and then forward the information to its maker or others. Spyware can be used for investigation of software users, for advertising purposes, or for preparation of an attack.
- **Trojan Horse:** includes harmful features of which the user is not aware. An example of such a feature is a so-called “back door,” which enables intrusion through bypassing user authentication methods. The Trojan Horse may appear to be useful software but will actually do damage once installed or run on your computer.

FYI

U.S. consumers lost $7 billion over the last two years to viruses, spyware, and phishing schemes, according to Consumer Report’s State of the Net survey.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Malicious Software and Activities

Other forms of malicious activities include:

- **Social engineering: t**he act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information. Social engineering is successful because its victims innately want to trust other people and are naturally helpful. The victims of social engineering are tricked into releasing information that they do not realize will be used to attack a computer network.
- **Phishing:** The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The email directs the user to visit a website, where s/he is asked to update personal information (such as passwords and credit card, Social Security, and bank account numbers) that the legitimate organization already has. The website is bogus and set up only to steal the user's information.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Malicious Software and Activities

How to detect phishing techniques

- The communication may include some threat or request for information. Some common phrases are “verify your account,” “you have won the lottery,” and “if you don’t respond within 48 hours, your account will be closed.” These messages convey a sense of urgency so that you’ll respond immediately without thinking. If you are urged to “verify” sensitive account information, contact the company directly instead.
- Phishing attempts from foreign countries may use poor grammar and spelling.
- Hovering over the link shows a URL that differs from the intended organization. Here is an example:

- Never trust links that point you to URLs that only show numbers in an IP address and no other registered domain name.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Malicious Software and Activities

Additional tips on how to detect phishing techniques

- Phishing emails use generic greetings in their emails. Emails from banks and credit card companies will usually include partial account numbers. Therefore, one should always be suspicious if the message does not contain specific personal information.
- Always look for “https” on any site you use to enter sensitive information. This includes login pages, online shopping sites, and bank web sites.
- In some cases, phishing attempts will slightly alter the domain:
  - www.micosoft.com
  - www.mircosoft.com
  - www.verify-microsoft.com

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Malicious Software and Activities

Possible consequences of complying with a phishing attempt

- Providing a username and password can allow access to your bank, email, or any other online account.
- Clicking on a link can download some malware, thereby turning your computer into a spamming station that further proliferates the phishing attempt. Key logger software can also be installed that records everything you type and then sends that information to scammers.
- Contact your IT support or Information Security Office when you suspect phishing activities.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Malicious Software and Activities

How do you protect yourself from malicious software?

The good news is that you can install anti-virus software on your computer that will improve your computer's chances of resisting a malicious software attack. Click on the link on the right-hand side of the page to obtain the latest antivirus software for your operating system.

Many operating systems may also be configured to update your computer automatically to make sure it has the latest protections and to scan the computer for viruses. Also, makers of many popular software programs publish free updates, which provide additional protection.

FIND OUT MORE

Instructions for Downloading Antivirus Software

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Malicious Software and Activities

The following is a useful checklist to help determine if you are taking the necessary steps to protect against malicious software on your computer:

- Make sure your computer contains anti-virus software.
- Make sure your anti-virus software is configured to apply updates automatically.
- Make sure your computer scans for viruses automatically.
- Enable all anti-virus protection features.

Contact your IT support or Information Security Office for assistance.

FIND OUT MORE

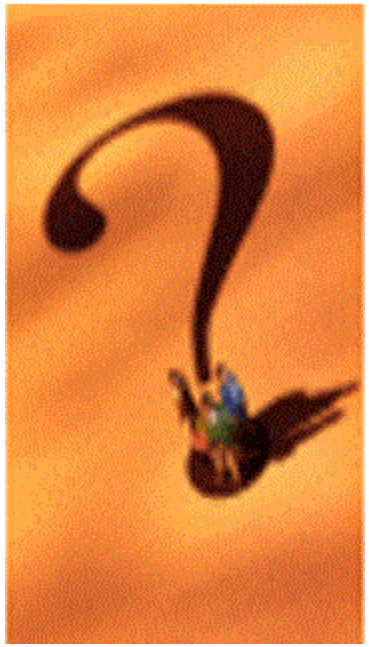
Information Security Office

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

University Policies

- For additional information on how to safeguard your workstation and data, please refer to the USC Network Infrastructure Use policy and the USC Information Security policy:
  - USC Network Infrastructure Use Policy
  - USC Information Security Policy



USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Physical Security

Protecting the security of information is not just a technical issue. Physical security is one of the most often overlooked aspects of information security.

Physical security measures should be designed with two goals in mind: to offer protection from intruders (even casual or accidental ones) and to provide protection and recovery from major disasters.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Physical Security

Physical security consists of the same systems and routines you would often find in your home, such as:

- Door locks
- Safes and lockable filing systems
- Security alarm systems
- Document disposal processes such as shredding

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Physical Security

What do these routines mean in the workplace? Some good measures include:

- **Control access to your office**:
  Don't allow vendors and other visitors to wander around your office. A good practice is to have visitors wait in the front lobby. They should be escorted when accessing other areas.
- **Secure your workspace**: When leaving your work area, be sure to lock away any loose papers or documents that may contain sensitive and/or confidential information.
- **Lock down your workstation**:
  Because PC's are smaller and lighter than ever, they are more vulnerable to theft. As a deterrent, PC's can be locked to a desk with computer lockdown plates.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Physical Security

Other steps you can take are:

- **Door locks and keys**: Some basic access questions you need to be able to answer about your keys include:
  - Do you know who has keys to your building, department, or office?
  - Are there master keys to your area, and if so, who controls them?
  - Are keys collected from terminated employees?
  - How many keys in your area have been distributed over time?
- **Locked cabinets**: You should store as much information as possible (documents, reports, etc.) in a locked cabinet when you are away from your desk. And because USB flash drives, CDs, and DVDs can fit into someone's pocket or bag, they should be secured in a locked desk or cabinet when not being used.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Physical Security

Some more important physical security issues include:

- **Laptop security**: Laptops and smartphones are very portable and easy to take, so pay special attention to them.
  - Most laptops are equipped with a universal security slot that allows them to attach to a cable lock or laptop alarm.
  - Remove any USB devices from the laptop when not in use, and put them in a safe place.
- **Mobile device**: Use passcodes on iPads and other tablet computers to block unauthorized access to your apps and information.
  - Keeping the device under your physical control is the most effective way to protect your data

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Physical Security

Workstation security issues even apply when you are no longer using documents or electronic media.

Be sure to have everything properly erased or shredded before disposing of it. This includes documents as well as hard-drives and CDs. Many people are unaware that an erased file on a diskette or hard-drive can be easily recovered.

Contact your IT support or Information Security Office on how to properly erase data.

- http://www.dban.org/

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Physical Security

Copier models from as early as 2002 are equipped with hard drives that may have sensitive information stored on them.

- http://www.cbsnews.com/video/watch/?id=6412572n&tag=mg;mostpopvideo

Copiers should be equipped with an encryption or overwriting function to erase and delete any data being stored on the hard drive to prevent a breac of sensitive information.

Depending upon the information your unit stores, transmits, or receives, you may have specific compliance obligations. For example, if you receive employee background screens, you may be required to follow the FACTA Disposal Rule, which requires the proper disposal of any such information stored on a copier just as would be required of paper information or information stored on computers.

If you are the office manager or administrator of a unit and do not know if the office's copier/s are equipped with hard drives, please contact the USC Information Security Office for further assistance.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Physical Security

The following tips will help you protect USC information assets:

- Off and shut down your workstation at the end of the day.
- Shred all sensitive and confidential documents that are to be disposed of.
- Don’t post your password where others can find it.
- Lock your office door when you leave for extended periods and at the end of the day.
- Lock cabinets, desk drawers, and other storage containers that contain sensitive information.
- Don’t leave sensitive information in view.
- Don’t leave computer resources such as USB drives, laptops, or mobile devices unattended.

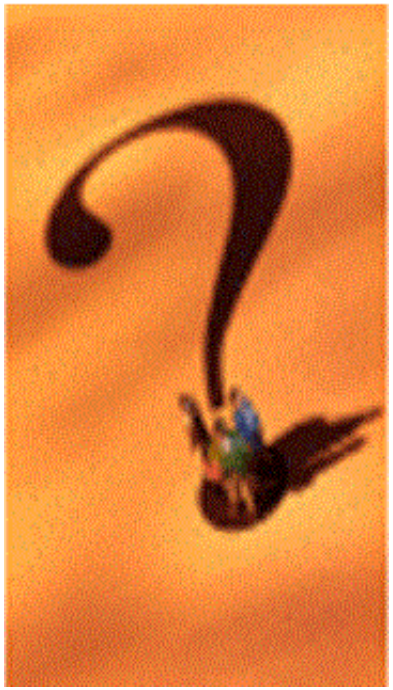
USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Physical Security

Dr. Robert Wong is a new supervisor in a laboratory at USC. Several people in this facility have been issued keys to access a file and storage room where significant amounts of personal information are kept. Dr. Wong is not entirely sure which employees currently have keys or whether additional people who are no longer employed by the lab still have keys. On his second day in the lab, a technician tells Dr. Wong he is leaving to pursue another job opportunity.

If Dr. Wong collects the technician's key on his last day of work, has he done enough to ensure that the file room is secure?



USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Physical Security

The correct answer is “No.”

Although it is important for Dr. Wong to collect keys to the room when employees leave, he should also try to assess who has been issued a key to date and whether all employees who no longer work in the lab have returned any keys they were issued. If he cannot determine who was issued a key or who may still have one, it may be a good idea to change the door lock.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Data Backup

Most computer users need to access data for a period of time after they create it in order to perform their job duties. In addition, many laws require USC and its employees to keep information for varying lengths of time before destroying it.

Therefore, it is critical to make sure that data you need or are required to keep is retrievable in the event that it is inadvertently lost.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Data Backup

The Information Technology Services (ITS) at USC makes nightly backups of files on the major timesharing systems and departmental machines that are under its support.

However, if your computer is not supported by ITS, there are a few ways to back up data:

- A full, or archival, backup backs up all files on a computer.
- An incremental or differential backup only backs up those files that have changed since the time of the last full backup.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Data Backup

After you have decided which type of backup to do, the next step is to decide how frequently backup should occur.

The best way to decide how frequently data backup should occur is to ask yourself how critical the data is.

For example, if you can still perform your job if you lost a week's worth of data, but not if you lost two weeks' worth, then you should back up your data once a week.

If possible, encrypt your backup data to enhance security.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Data Backup

Data that is backed up should be stored somewhere off-site. Setting up a data storage arrangement with a records and storage management company is one way, but there are some monthly costs involved.

Making a storage agreement with a remote department or school is another way to store data off-site. This can be especially cost effective if each department agrees to store the other's data.

It is, however, important that each partner in such an arrangement takes the storage requirement seriously and creates a secure environment for the data being stored.

Contact your IT support for assistance on how to back up your data.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Encryption

In order to ensure the integrity of university data, USC requires all laptops and mobile storages that are paid for with university funds and/or used for university business purposes to be purchased with an encryption solution.

This applies to laptops and mobile storage devices purchased from all sources of university funds, including sponsored project accounts.

It also applies to devices used for business purposes but purchased with personal money.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

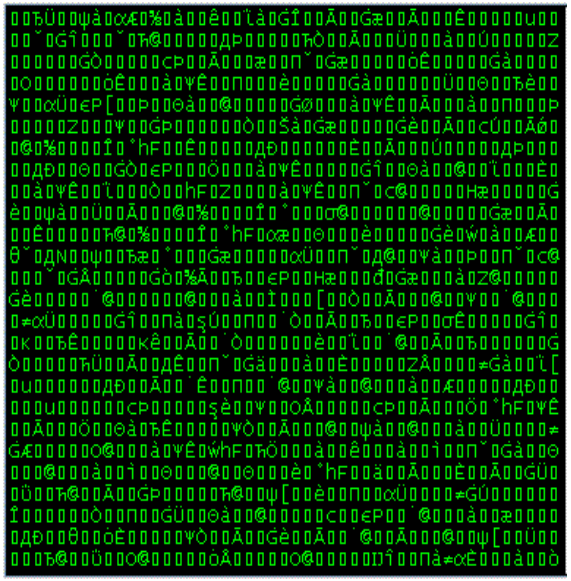
Information Security at USC

Encryption

To be in compliance with this policy, laptops and mobile storage devices must be either:

- Delivered with built-in encryption
- Accompanied by a software-based encryption solution for subsequent installation

Note that, even if the instrument is encrypted, the best practice is to avoid storing any sensitive data on any laptop or mobile storage device.



USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Encryption

To facilitate compliance with this policy, USC's contract suppliers have agreed to sell only laptops and mobile storage devices with encryption solutions when the instrument is paid on a university purchase order.

The list of contract suppliers of laptops and mobile storage devices is posted on the following web page:

- http://fbs.usc.edu/depts/purchasing/page/4101/computer-contract-supplier-home-page/

FIND OUT MORE

Purchasing policy regarding encrypted laptops and mobile storage devices

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

What Is Cloud Computing?

Cloud computing enables convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Users access the applications, infrastructure, or platforms they need via a web browser or other simple front-end interface, grabbing and releasing them at will and paying only for what they use.

- NATIONAL INSTUTUTE OF STANDARDS AND TECHNOLOGY (NIST)

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Cloud Computing

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Cloud Storage Concerns

Being able to access your files from anywhere, and from any computer, is one of the Internet's great conveniences. However, the associated security concerns should not be forgotten.

The two biggest concerns about cloud storage are reliability and security. You should not entrust your data to another company without a guarantee that you will be able to access it whenever you want -- and that no one else will be able to get at it.

You should not store any sensitive or protected information in non USC-sanctioned or commercial cloud storage services since cloud storage is a shared environment.

The USC Digital Repository provides cloud-computing services for USC communities. For more information, please go to http://repository.usc.edu/

FIND OUT MORE

Storing USC Materials in the Cloud

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Cloud Storage Concerns

When selecting a cloud storage vendor, ensure that the company uses a combination of techniques to secure data:

- Encryption at-rest – using AES/algorithm to encode information stored in the cloud system.
- Encryption in-transit – using AES/algorithm to encode the information while uploading and downloading from the cloud system.
- Proper Key management – Only you or the authorized user have the key to decrypt the information stored on the cloud system.
  - If the cloud vendor manages the key, there should be contractual obligations to safeguard the key.
  - If you manage the key(s), appropriate safeguards should be applied.

Contact your IT support or Information Security Office for assistance.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Security Breaches

One way you might lose data would be if a security breach occurred. A "security breach" means an unauthorized acquisition of data that compromises the security, confidentiality, or integrity of information maintained by USC. This includes breaches of physical security as well as of computer or information systems security.

All university employees who become aware of a security breach must report the breach immediately to their supervisor and to the USC Information Security Office at infosec@usc.edu or (213) 821-2614 for review.

FYI

As we discussed earlier, state laws require USC to notify any potential affected individual of any computer security breach that allows an unauthorized person to acquire certain personal information (such as Social Security numbers, drivers license information, and/or credit card information) about that resident.

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Security Breaches

There are some signs you can look out for that might indicate a security breach has occurred. These include:

- A sudden, unexplained loss of hard disk or storage space
- A new or unexpected user or administrator ID on the system
- A sudden, unexplained performance degradation of your computer or network connections
- Unexpected service or icons on the desktop

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

Information Security at USC

Security Breaches

If you suspect that a security breach has occurred, contact your supervisor and the Information Security Office immediately.

The USC Information Security Office verifies the incident and contacts the appropriate staff for investigation and resolution. The Information Security Office will work with you and your department to prevent the incident from reoccurring and to try to reduce any impact on your information systems as a result of the breach.

FIND OUT MORE

Information Security Office

USC Office of Compliance
University Gardens, Suite 105
Los Angeles, CA 90089-8007
complian@usc.edu

What Can You Do?

Everyone has a Role in Securing USC Information

- Read and follow USC's Information Security and Network Infrastructure Use policies.
- Password protect your workstation, laptop, and mobile device.
- Use strong passwords, and don't share them with other people.
- Confirm that you have anti-virus protection and current updates on your workstation and laptop, or call your IT support for assistance.
- Don't respond to suspicious emails, and don't open attachments from unknown senders. If you are unsure about the origins of an email or attachment, contact your IT administrator for guidance.
- Lock your doors when you leave the office for any length of time.
- Use a screensaver, preferably one that is password protected.
- Encrypt sensitive data or password protect documents that contain sensitive data.
- Don't send sensitive data via email unless it is protected by encryption, passwords, or some other secure method.
- Call the Information Security Office immediately if you suspect or become aware of a security breach!