Computing Services Information Security Office

Security 101

Definition of Information Security

Information security is the protection of information and systems from unauthorized access, disclosure, modification, destruction or disruption.

The three objectives of information security are:

- Confidentiality
- Integrity
- Availability

Definition of Information Security

Confidentiality

Confidentiality refers to the protection of information from unauthorized access or disclosure. Ensuring confidentiality is ensuring that those who are authorized to access information are able to do so and those who are not authorized are prevented from doing so.

Definition of Information Security

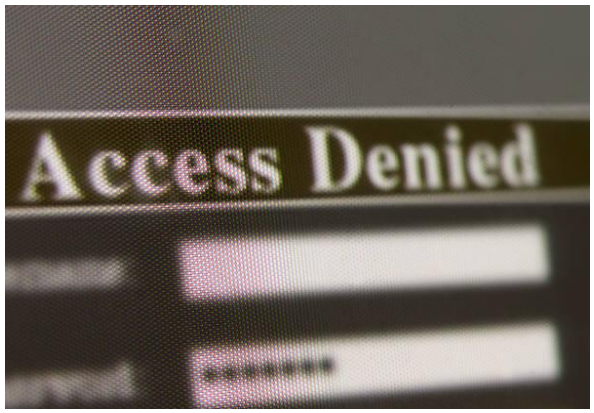
Integrity

Integrity refers to the protection of information from unauthorized modification or destruction. Ensuring integrity is ensuring that information and information systems are accurate, complete and uncorrupted.

Definition of Information Security

Availability

Availability refers to the protection of information and information systems from unauthorized disruption. Ensuring availability is ensuring timely and reliable access to and use of information and information systems.

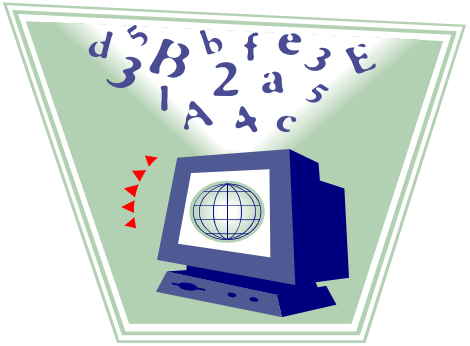


Information Security Policy

Carnegie Mellon has adopted an Information Security Policy as a measure to protect the confidentiality, integrity and availability of institutional data as well as any information systems that store, process or transmit institutional data.

Institutional data is defined as any data that is owned or licensed by the university.

Information system is defined as any electronic system that stores, processes or transmits information.



Information Security Policy

Policies

- Throughout its lifecycle, all Institutional Data shall be protected in a manner that is considered reasonable and appropriate given the level of sensitivity, value and criticality that the Institutional Data has to the University.

- Any Information System that stores, processes or transmits Institutional Data shall be secured in a manner that is considered reasonable and appropriate given the level of sensitivity, value and criticality that the Institutional Data has to the University.

- Individuals who are authorized to access Institutional Data shall adhere to the appropriate Roles and Responsibilities

Your Role in Information Security

Three primary roles have been defined in the context of information security:

- Data Steward
- Data Custodian
- **User**

A **User** is any employee, contractor or third-party affiliate of Carnegie Mellon who is authorized to access institutional data or information systems.

Users are responsible for:

- Adhering to information security policies, guidelines and procedures.
- Reporting suspected vulnerabilities, breaches and/or misuse of institutional data to a manager, IT support staff or the Information Security Office.

Your Role in Information Security

Users

- Safeguard institutional data
- Safeguard electronic communications
- Avoid risky behavior online
- Report suspected security breaches

Safeguarding Institutional Data

Know Your Data

Be mindful of what type of data you handle:

- Public
- Private
- **Restricted**

Examples of Restricted data include account passwords, drivers license numbers, education records of students, financial account information, health information and social security numbers. A more complete list of data considered to be Restricted by the institution can be found at:

http://www.cmu.edu/iso/governance/guidelines/data-classification.html#appendixa

Safeguarding Institutional Data

Protecting Electronic Data

- Avoid storing Restricted data on mobile computing devices
- Don't store institutional data on personally owned computing devices
- Don't store Restricted data on CDs, DVDs, USB thumb drives, etc.
- Don't transmit Restricted data via email and other insecure messaging solutions
- Don't use personal email for business communications
- Use strong passwords or passphrases
- Secure your computing devices

Safeguarding Institutional Data

Safeguard Your Password

- Use a strong password or passphrase
- Change your password periodically
- Avoid using the same password for multiple accounts
- Don’t write your password down or store it in an insecure manner
- Don’t share your password with anyone for any reason
- Don’t use automatic login functionality

For more information, review the Guidelines for Password Management
http://www.cmu.edu/iso/governance/guidelines/password-management.html

Safeguarding Institutional Data

Secure Your Computer

- Update and patch your operating system
- Enable automatic software updates where available
- Update and patch software applications (e.g. browsers, email clients, JAVA, etc.)
- Install and update antivirus software
- Install and configure firewall software
- Do not automatically connect to public wireless networks
- Disconnect your computer from the wireless network when it is not in use
- Use caution when enabling browser pop-ups
- Use caution when downloading and installing software
- Lock your computer when it is unattended

Safeguarding Institutional Data

Protecting Physical Data

- Close and lock your door when leaving your office unattended
- Lock file cabinets that store institutional data
- Don't leave Restricted data in plain view at your desk or on a whiteboard
- Don't leave Restricted data sitting on a printer, copier, fax machine or other peripheral device

Protecting Verbal Communication

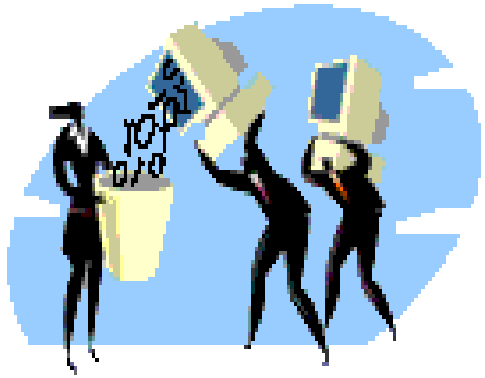
- Be mindful of your surroundings when discussing Restricted data
- Don't discuss Restricted data with individuals who do not have a need to know

Safeguarding Institutional Data

Disposing of Data

- Dispose of data when it is no longer needed for business purposes
- Use Identity Finder to securely delete files that contain Restricted data
- Use the Computer Recycling Program to dispose of electronic media
- Use a cross shredder to dispose of paper-based and written media

For more information on the Computer Recycling Program, visit:
http://www.cmu.edu/ehs/waste-environment/computers.html



Safeguarding Electronic Communications

Electronic communications can be in the form of email, instant messaging, text messaging, social network, etc.

- Avoid opening attachments from an untrusted source
- Avoid clicking on links in electronic communications from an untrusted source
- Be wary of phishing scams
- Avoid sending Restricted data through email and other electronic communications

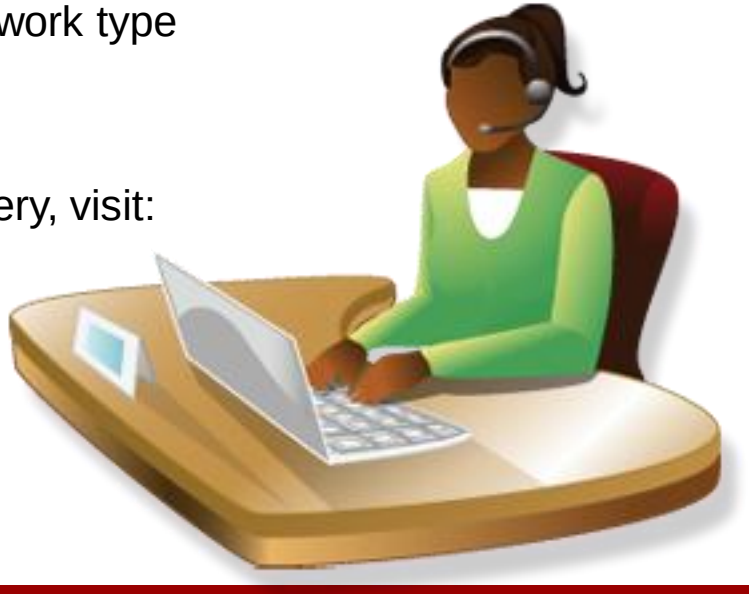
Safeguarding Electronic Communications

Safeguarding Electronic Communications

Additional Considerations

- Use an official CMU email account for all “university business”
- Avoid using personal accounts for business workflows
- Save personal communications in a designated folder
- Organize your communications by project or work type
- Save copies of important outgoing email

For more information regarding electronic discovery, visit:
http://www.cmu.edu/iso/compliance/e-discovery/



Avoid Risky Behavior Online

- Be cautious when using file sharing applications
- Be cautious when browsing the web
- Be cautious when clicking on shortened URLs
- Avoid responding to questions or clicking on links in pop-up windows

Report Any Suspected Security Breach

If you detect suspicious behavior or inappropriate use of institutional data, report your concerns to your manager or contact the Information Security Office (ISO) at iso@andrew.cmu.edu.

If you suspect your computer has been compromised, take the following steps:

1. Disconnect the computer from the network
2. Contact your department IT staff, DSP or the ISO
3. Notify users of the computer, if any, of a temporary service outage
4. Preserve any log information not resident on the compromised computer
5. Wait for further instructions from your department IT staff, DSP or the ISO

Review the Procedure for Responding to a Compromised Computer for more info:
http://www.cmu.edu/iso/governance/procedures/compromised-computer.html

Additional Information

Guidelines

- Guidelines for Bulk Email Distribution
- Guidelines for Data Classification
- Guidelines for Data Protection
- Guidelines for Data Sanitization and Disposal
- Guidelines for Instant Messaging Security and Usage
- Guidelines for Mobile Device Security and Usage
- Guidelines for Password Management

http://www.cmu.edu/iso/governance/guidelines/

Additional Information

Tools

Anti-Phishing Phil
http://www.cmu.edu/iso/aware/phil/

Anti-Phishing Phyllis
http://www.cmu.edu/iso/aware/phyllis/

Identity Finder
http://www.cmu.edu/computing/doc/security/identity/

Patch Check Tool
https://www.cmu.edu/iso/patch-check/