

Desktop and Laptop Security Policy

Effective Date: November 1, 2007

Policy Statement

Columbia University requires that all individuals utilizing University Electronic Information Resources abide by the desktop and laptop security standards described by this policy.

Reason for the Policy

With the prevalent use of personal computing in the University, there is the risk that if computing system security vulnerabilities are left unsecured, then the information and data stored in personal computers are susceptible to theft and/or exploitation. This policy defines a number of safe computing standards to provide data protection on desktops and laptops.

Primary Guidance to Which This Policy Responds

This policy is established under the provisions of Columbia University's Information Technology Security and Policy Program.

Responsible University Office & Officer

The office of Columbia University Information Technology Security is responsible for the maintenance of this policy, and for responding to questions regarding this policy. The Chief Information Security Officer (CISO) is the responsible officer.

Revision History

This policy was established in October 2007.

Who is Governed by This Policy

This policy applies to all individuals who access, use, or control University Electronic Information Resources. The individuals required to adhere to this policy include, but are not limited to faculty, staff, students, those working on behalf of the University, guests, tenants, contractors, consultants, visitors and/or individuals authorized by affiliated institutions and organizations.

Who Should Know This Policy

Anyone who accesses, uses, or controls University Electronic Information Resources should be familiar with this policy.

Exclusions & Special Situations

None

Policy Text

Computing technology is constantly evolving and new vulnerabilities are discovered everyday; therefore, no system is completely immune to exploitation. Applying layered security controls will better protect University computers from hackers. This policy outlines Columbia University's multi-layer security strategy for defense against unauthorized access to University

desktops and laptops. The following steps must be adhered to by the User and/or the System Administrator (SA) indicated in parenthesis following each of the items below.

1. *Implement credible and reputable anti-virus software, perform continuous and/or scheduled scanning, and keep it up-to-date. An anti-virus program will protect your computer from malicious programs. (User and SA)*
2. *Implement anti-spyware to protect your private information. Spyware is a class of programs designed to steal personal information.(User and SA)*
3. *Enable the built-in firewall that is included in major operating systems and/or install a firewall application. A firewall is an application to restrict others from connecting to your computer. (SA)*
4. *Regularly check for vendor security updates and apply them. Periodically, security weaknesses in the operating system and/or application are discovered and the vendor will then provide security updates to remediate such security exposures. (SA)*
5. *Establish strong password(s) syntax and protect your password(s). A password is used to provide authentication to an application and/or system. (User and SA)*
6. *If you are logged into a session, remember to log out after you are finished. Also, enable a password-protected screen saver when leaving your computer temporarily. (User)*
7. *Keep your machine, especially laptops, physically secured. (User and SA)*
8. *Confidential and sensitive information must be safeguarded. Take appropriate measures (e.g., encryption for electronic information, physically secure physical media) to prevent unauthorized disclosure. (User and SA)*
9. *Scan all email attachments before opening them. Email is a method to spread malicious program via email attachments. (User)*
10. *Refrain from using the save password feature applications because others who have access to your computer will also have access to your account.(User)*
11. *Disable accounts which are not used and always change default passwords. Some operating systems come with predefined user accounts. These accounts are active by default. (SA)*
12. *Disable service which is not needed. Operating systems are packaged with services that are used by specific applications, such as ftp (for file transfer) or SMTP (for email). (SA)*
13. *Create regular backups of your data and files. Computers are like any machinery and can fail, and may result in the data and files that are corrupted or unrecoverable. (User and SA)*

14. *Be alert and aware of information stealing methods such as: social engineering, phishing scams, and shoulder surfing to obtain personal and sensitive information about you.(User)*

15. *Sanitize your computer before donating or disposal. (User and SA)*

Examples to assist with interpretation and administration of this policy are provided in the *Appendix A – “Examples of Desktop and Laptop standards and guidelines”* at the end of this document.

Responsibilities

Implementing these security standards and guidelines provide you with added protection from malicious programs and unauthorized access. Failure to implement these security controls may result in your machine being infected. If it is connected to Columbia University’s network and if it is infected, Columbia University will immediately prohibit your connection until your machine has been sanitized.

Definitions

Data is a stored collection of information that may include alphanumeric, words, sounds, symbols, or images.

Electronic Information Resources include data, networks, computers, and other devices that store or display data, communications devices, and software used on such devices.

Contacts

For questions or comments:

Columbia University Information Technology

Web: <http://www.columbia.edu/cuit/support/>

Email: security@columbia.edu

Telephone: 212-854-1919

Cross References to Related Policies

For related CUIT Security Policies, see the University Administrative Policy Library, CU Information Technology section on the website -

http://www.columbia.edu/cu/administration/policylibrary/responsible_office/cuit.html

For additional policy relating to computing use, see the Accept Use of IT Resources policy.

For additional policies relating to confidential and sensitive information controls, see the following policies:

- Social Security Number (SSN) and Unique Person Number (UPN) Usage,
- Data Classification, and
- Use of Encryption.