# Encryption Policy

**Effective Date: December 1, 2007**

**Policy Statement**
This policy defines the encryption guidelines and standards for Columbia University.

**Reason for the Policy**
This policy provides guidelines to situations for encryption usage. It also provides guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.

**Primary Guidance to Which This Policy Responds**
This policy responds to the Data Classification Policy, which stipulates sensitive and confidential data are required to be encrypted. This policy also responds to all applicable federal and state statutes pertaining to protection of sensitive and confidential information that require encryption, including, but are not limited to Payment Card Industry Data Security Standard (PCI DSS).

**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 December 2007.

**Who is Governed by This Policy**
This policy applies to all individuals who access, use, or control University electronic information resources. Those individuals covered include, but are not limited to faculty, staff, students, those working on behalf of the University, and 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**
Existing systems and applications containing sensitive and confidential information which cannot use encryption because of technology limitation but have compensating controls may be granted special waiver. However, these systems and applications must still be thoroughly risk assessed to ensure that major risks are addressed via compensating controls to protect the data in lieu of not using encryption.

**Policy Text**
Access controls are the first line of defense in protecting data. Access controls are built into every file system, operating system and many major applications (such as databases), and they

are effective at controlling who can access and manipulate the data. Use encryption to enhance security control by providing an additional layer security.

Encryption may not be applicable in all situations. Therefore, use encryption on data that is deemed sensitive and confidential in accordance with the "Data Classification Policy" and under the following circumstances:

*1) Encrypt Data That Moves (Physically or Virtually),*

*2) Encrypt for Separation of Duties When Access Controls Aren't Granular Enough, or*

*3) When encryption is mandated.*

Use appendix A "Situations for applying Encryption" at the end of this document to determine when encryption is applicable.

Use only encryption technologies which are based on standard algorithms (e.g., DES, RSA, and IDEA). These algorithms represent the actual cipher used for an approved application. For example, Secure Socket Layer (SSL) uses RSA encryption.

At a minimum, use a 128 bit encryption cipher key.

**Responsibilities**
The following roles and responsibilities are established for carrying out this policy:

*Data Trustee / Owner:*
Data Trustee / Owners are senior University officials (e.g., Provosts, Deans, VPs, AVPs, or their designees) within each businesses and/or operational units within the University. Data Trustee / Owner responsibilities include: assigning data stewards, establishing departmental data protection policy and procedures for data encryption.

*Data Steward:*
Data Stewards are University officials (e.g., Directors, Managers, or their designees) having direct operational level responsibility for information management. Data stewards are responsible for: working with Data Trustee / Owner to classify data, implementing and enforcing departmental data encryption policy and procedures, and custodian of the encryption key.

*Data Administrator:*
The Data Administrator is responsible for providing infrastructure support of the data, including coordinating with the data stewards to implement optimal encryption software solution for the business.

Encryption software typically utilizes a password or pass phrase to both encrypt and decrypt the information / data. If the encryption password or pass phrase is lost, then the encrypted information / data cannot be decrypted rendering the data unusable. To handle such a situation,

the department must create an 'encryption password escrow procedure' specifying the terms and conditions for which the procedure will be executed to recover the loss password / pass phrase.

**Definitions**
An *algorithm* is a procedure or formula for solving a problem. A computer program can be viewed as an elaborate algorithm.

A *cipher* is any method of encrypting data (concealing its readability and meaning).

*Data* is defined as any information within the University's purview, including student record data, personnel data, financial data (budget and payroll), student life data, departmental administrative data, legal files, research data, proprietary data, and all other data that pertains to, or supports the administration of the University.

*Data Encryption Standard (DES)* is a widely-used method of data encryption using a private (secret) key.

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

*International Data Encryption Algorithm (IDEA)* is an encryption algorithm developed at ETH in Zurich, Switzerland. It uses a block cipher with a 128-bit key, and is generally considered to be very secure. It is considered among the best publicly known algorithms.

Rivest-Shamir-Adleman (*RSA)* is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers.

**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 CUIT Security Policies, see the University Administrative Policy Library, CU Information Technology section:

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

The "Data Classification Policy"

Applicable Acts, Regulations, and Laws:

- Payment Card Industry Data Security Standard (PCI DSS)
  https://www.pcisecuritystandards.org/tech/