CORNELL UNIVERSITY
POLICY LIBRARY

Use of Escrowed Encryption Keys

POLICY 5.3

Volume 5, Information Technologies
Chapter 3, Use of Escrowed Encryption Keys
Responsible Executives: Chief Information Officer and Vice President for Information Technologies/University Counsel
Responsible Offices: Office of Information Technologies/University Counsel
Originally Issued: January 8, 2003

POLICY STATEMENT

Cornell University expects stewards, custodians, and users of institutional administrative data who deploy software or algorithmic programs for encryption to establish procedures ensuring that the university has access to all such records and data.

REASON FOR POLICY

In furtherance of its missions and to comply with federal, state, and local regulation and law, the university must maintain access to all institutional administrative data transmitted or stored on computers owned by the university or used for university business.

ENTITIES AFFECTED BY THIS POLICY

All units of the university (excluding the Weill Cornell Medical College)

WHO SHOULD READ THIS POLICY

- Anyone who creates, encrypts, or has custodial use of institutional administrative data
- Anyone who operates computers that store institutional administrative data

WEB ADDRESS FOR THIS POLICY

www.dfa.cornell.edu/treasurer/policyoffice/policies/volumes/informationtech/encryption.cfm

Policy 5.3
Use of Escrowed Encryption Keys

RELATED DOCUMENTS

University Documents
University Policy 4.12, Data Stewardship and Custodianship
University Policy 5.1, Responsible Use of Information Technology Resources
Cornell University's Policy on Abuse of Computers and Network Systems

CONTACTS

If you have questions about specific issues regarding University Policy 5.3, Escrow of Encryption Keys, contact the following offices:

Subject	Contact	Telephone	E-mail/URL
Policy Clarification	IT Security Office	(607) 255-8421	security@cornell.edu www.it.cornell.edu/security/
Computers and Network Systems	Chief Information Officer and Vice President for Information Technologies	(607) 255-7445	www.cio.cornell.edu
Legal Issues	Office of University Counsel	(607) 255-5125	counsel.cornell.edu
Security of Network Systems	OIT, Security	(607) 255-2522	www.it.cornell.edu/security/

To call any campus number from 253, 254, or 255, dial only the last five digits.

Policy 5.3
Use of Escrowed Encryption Keys

DEFINITIONS

These definitions apply to these terms as they are used in this policy.

Custodian	An individual who possesses or has access to data. This individual must have a need to access university data to perform assigned duties as an employee or volunteer of the university. Alternatively, the individual must be employed by or under contract to the university to perform special tasks, such as an outside attorney, external auditor or other consultant.
Encryption	An algorithmic process of encoding data to make it unintelligible except to users with the keys to decode the data.
Escrow	The secure storage of keys used to encrypt and decrypt data. The purpose of escrowing keys is to provide access to institutional administrative data and to insure that access does not become dependent on a single individual or an obscure method of storing and/or protecting keys.
Institutional Administrative Data	Any digital information owned by Cornell University that is used for administrative purposes, (including, but not limited to electronic mail, digital images, text , student records, payroll records, financial information, human resource records, etc.) that is stored on a computer owned by the university or used for university business.
Key	A mathematic variable required to encrypt and to decrypt the algorithms of encoded data.

Policy 5.3
Use of Escrowed Encryption Keys

PROCEDURES

General Policy Restrictions

1. Any unit that encrypts data must obtain the permission of the associated data steward (for more information, see University Policy 4.12, Data Stewardship and Custodianship).
2. Custodians or users of institutional administrative data who deploy software or algorithmic programs for encryption must establish procedures ensuring that the university has access to all such records and data.
3. Each major operating unit deploying encryption is required to develop and to disseminate procedures consistent with this policy to enable key recovery in a secure manner (see the appendix for a sample unit policy).
4. Any custodian or user of institutional administrative data who deploys software or algorithmic programs to encrypt data is required to inform his or her supervisor prior to deployment and disclose, in a comprehensible form, the keys, or other means to access the data.

Questions about what constitutes institutional administrative data may be directed to the steward for that data (for more information on stewardship and custodianship, see University Policy 4.12, Data Stewardship and Custodianship).

◆**Note:** This policy does not require any particular technological protection of institutional administrative data.

◆**Note:** This policy does not establish a central repository for the management of keys or data.

◆**Note:** This policy does not mandate a single or specific method for the escrow of encryption keys.

APPENDIX: SAMPLE UNIT POLICY

CIT ENCRYPTION KEY RECOVERY PROCESS POLICY

Context

This policy outlines encryption key recovery procedures as required by University Policy 5.3, Use of Escrowed Encryption Keys. Procedures outlined in this document are required for all employees of Cornell Information Technologies (CIT) and all service providers under CIT contract.

Procedure Detail

- Storing university administrative data[1] in an encrypted state requires the permission of the unit director and/or the chief information officer (CIO) and vice president (VP) for information technologies.
- The CIT encryption committee must approve the encryption service.
- A copy of a key[2] to decrypt this data must be escrowed using the CIT key escrow form.
- General purpose automated encryption systems will be stewarded by the Information Technology Security Program and operated in partnership with CIT Integration and Delivery and CIT technical support staff. Only one production service for each automated solution will be implemented; e.g. Workstations are not allowed to run Microsoft's encrypting file services (EFS) outside of the CIT Microsoft domain controlling EFS key recovery tools.
- A subject area and naming schema approved by the CIT encryption committee must be used on an encryption system that does not automate the paring of escrowed keys to data.

Escrow Form

The escrow process requires the completion of the CIT key escrow form. These forms will be hand delivered to the director of the Information Technology Security Program. Paper copies of this form will be archived in physically separate, secure and fireproof vaults. Access to escrowed keys will require permission from the CIO and VP for information technologies.

CIT Encryption Committee

The CIT Encryption committee will be chaired by the director of the Information Technology Security Program and be comprised of one member from each CIT division.

Grandfathered Collections

Current collections of encrypted data may be exempted from certain aspects of this process if conversion costs are prohibitive and other means to assure access can be demonstrated. Exemption for grandfathered data collections must be approved by the CIT encryption committee.

Questions:

Questions about this policy should be directed to the director of the Information Technology Security Program.

[1] University administrative data, as defined in University Policy 5.3, Use of Escrowed Encryption Keys.
[2] A mathematic variable required to encrypt and to decrypt the algorithms of encoded data.