CORNELL UNIVERSITY
POLICY LIBRARY

Stewardship and Custodianship of Electronic Mail

POLICY 5.5

Volume 5, Information Technologies
Chapter 5, Stewardship and Custodianship of Electronic Mail
Responsible Executive: Chief Information Officer and Vice President for Information Technologies
Responsible Office: Office of Information Technologies
Issued: February 10, 2005
Last Updated: June 21, 2019

POLICY STATEMENT

Cornell University owns and operates its electronic mail (e-mail) infrastructure, which must be managed for the entire university community in a manner that preserves a level of privacy and confidentiality in accordance with relevant laws, regulations, and university policy. While the university permits limited personal use of its e-mail infrastructure, those availing themselves of this privilege do not acquire a right of privacy in communications transmitted or stored on university information technology resources.

E-mail custodians must not inappropriately access or disclose the content of mail transmitted or stored on Cornell-owned or Cornell-controlled information technology resources (e.g., desktop computers, routers, servers, personal digital assistants, etc.), except in the following situations: (1) as a response to a court order or other compulsory legal process; (2) in certain other circumstances only with the permission of authorized individuals (see E-mail Steward in the definitions) or the provost; (3) when the correspondent is unavailable and the information is necessary to conduct university business; or (4) in health and safety emergencies.

REASON FOR POLICY

The university strives to protect electronic mail from inappropriate access or disclosure in order to contribute to the trust of university information technology systems and comply with relevant regulations, laws, and policies regarding the protection of certain types of data.

ENTITIES AFFECTED BY THIS POLICY

All units of the university, including the Weill Cornell Medical College, which will develop separate procedures and processes

WHO SHOULD READ THIS POLICY

- All members of the university community

WEB ADDRESS FOR THIS POLICY*

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

**The University Policy Office webpages house the most current versions of all standardized university policies, at www.policy.cornell.edu.*

Cornell Policy Library
Volume 5, Information Technologies
Responsible Executive: Chief Information Officer and Vice President for Information Technologies
Responsible Office: Office of Information Technologies
Issued: February 10, 2005
Last Updated: June 21, 2019

Policy 5.5
Stewardship and Custodianship of Electronic Mail

CONTENTS

Policy 5.5
Stewardship and Custodianship of Electronic Mail

RELATED DOCUMENTS

Table 1
Related Documents

University Documents	Other Documents
University Policy 4.5, Access to Student Information	Electronic Communication Privacy Act of 1986
University Policy 4.6, Standards of Ethical Conduct	Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
University Policy 4.12, Data Stewardship and Custodianship	Financial Services Modernization Act of 1997
University Policy 4.13, Acceptance of Legal Papers	Health Insurance Portability and Accountability Act of 1996 (HIPAA)
University Policy 5.1, Responsible Use of Information Technology Resources	USA Patriot Act of 2001
Cornell University Policy Regarding Abuse of Computers and Network Systems	

Policy 5.5
Stewardship and Custodianship of Electronic Mail

CONTACTS

Direct any general questions about University Policy 5.5, Stewardship and Custodianship of Electronic Mail, to your unit administrative office. If you have questions about specific issues, call the offices listed in Table 2, below.

Table 2
Contacts

Subject	Contact	Telephone	E-mail/Web Address
Policy Clarification and Interpretation	IT Security Office	(607) 255-8421	security@cornell.edu www.it.cornell.edu/security/
Violations	Local human resources representative	Unit-specific	
	Judicial Administrator	(607) 255-4680	judadmin@cornell.edu
	IT Security Director	(607) 255-8421	security@cornell.edu www.it.cornell.edu/security/
	Chief Information Officer and Vice President for Information Technologies	(607) 255-7445	www.cio.cornell.edu

DEFINITIONS

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

Table 3
Definitions

Access	The ability to obtain e-mail content.
Correspondent	Any individual listed in the "To:," "From:," "Cc:," or "Bcc:" fields in the header of an electronic mail message
Custodian	An individual with access to electronic mail data on electronic mail systems.
Disclosure	The act of releasing the content of electronic mail to a third party (e.g., through accessing, intercepting, forwarding, rerouting, etc.)
E-mail	Electronic mail messages and their associated attachments in a mail user agent (MUA). ◆**Note:** When data contained in an e-mail message or attachment has been printed or stored outside of the MUA, it is no longer considered e-mail.
E-mail Steward	The individual, other than a correspondent, with the authority to grant permission for the disclosure of electronic mail content in the cases of human resource matters or potential policy or legal violations.
Health and Safety Emergency	A situation involving an imminent threat of death or serious injury to any person.
Local Support Provider	An individual with principal responsibility for the installation, configuration, security, and ongoing maintenance of an information technology device (e.g., system administrator or network administrator).
Mail User Agent (MUA)	A program, application, or method used to store, transmit, or receive e-mail.

RESPONSIBILITIES

The major responsibilities each party has in connection with University Policy 5.5, Stewardship and Custodianship of Electronic Mail, are as follows:

Table 4
Responsibilities

Cornell Information Technologies Computer Accounts Coordinator	Process requests for rerouting or forwarding electronic mail of staff members.
Director of Cornell Police, Deputy Director of Cornell Police, Head of Investigations, Gannett Health Services, Vice President for Student and Academic Services	In health and safety emergencies, contact the Information Technologies (IT) Security Office with requests to intercept, access, or disclose electronic mail content. In health and safety emergencies, when data has been accessed or disclosed, notify the appropriate e-mail steward of the request and the nature of the information received.
E-mail Steward (Provost, Vice President for Human Resources, or Vice President for Student and Academic Services)	Evaluate, then grant or deny requests to access or disclose electronic mail content in the case of a human resource matter or a potential policy or legal violation. Contact the director of IT policy, IT security director, or the chief information officer (CIO) and vice president for information technologies with requests to reroute, forward, intercept, access, or disclose the content of e-mail.
IT Security Office (ITSO)	In health and safety emergencies, and upon notification by the appropriate university official, access and disclose requested data. In health and safety emergencies, when data has been accessed or disclosed, notify the appropriate e-mail steward of the request, what data was accessed or disclosed, and any other relevant information, such as the approximate time of the request, access, and disclosure, the name and title of the requester, and the nature of the emergency. In health and safety emergencies, when data has been accessed or disclosed, notify the director of IT policy, the director of IT security, and the CIO and vice president for information technologies of the request.
Local Support Provider	Access and disclose specific mail messages in cases when information is necessary to conduct university business and the correspondent is unavailable. Access, observe, or intercept the content of electronic mail messages only when performing network security and maintenance functions (e.g., backups and restores). In the usual course of business, disclose, reroute, or forward the content of electronic mail messages only in the following situations: a. in an emergency involving immediate danger of death or serious physical injury; or b. when evidence has been observed of a potential violation of law or policy (see University Policy 5.1, Responsible Use of Information Technology Resources). In emergencies involving immediate danger of death or serious injury, contact the Cornell Police immediately. As soon as possible, report that contact and the underlying information to the director of IT policy, IT security director, or the CIO and vice president for information technologies.

Policy 5.5
Stewardship and Custodianship of Electronic Mail

RESPONSIBILITIES, CONTINUED

Office of Workforce Policy and Labor Relations	Evaluate, then approve or deny, requests to have mail rerouted or forwarded. Send approved requests for e-mail rerouting or forwarding to the Cornell IT computer accounts coordinator, who will effect the rerouting or forwarding.
OIT (Director of IT Policies, OIT; Security Director, OIT; or Chief Information Officer and Vice President for Information Technologies)	After appropriate permission has been granted, communicate with appropriate staff to initiate interception, access, or disclosure of electronic mail content. When interception, access, or disclosure of electronic mail content has occurred, inform the individual about whom the request was made of the request, access, and disclosure, where possible and appropriate.
Requesting Individual	In cases of human resources matters or potential legal or policy violations, obtain permission from the appropriate e-mail steward(s) for rerouting, forwarding, intercepting, accessing, or disclosing the content of e-mail. In cases when the information is necessary to conduct university business and the correspondent is unavailable, inform the unit human resources representative, unit head, college dean, or vice president at the time of the request; work with the local support provider to obtain the specific mail messages; and inform the correspondent of the request that was made and of the nature of the information received. In a health or safety emergency, please see Health and Safety Emergency in the definitions.
Unit Human Resources Representative	Accept requests to reroute or forward electronic mail when a correspondent is unavailable and the information is necessary to conduct university business.

Policy 5.5
Stewardship and Custodianship of Electronic Mail

PRINCIPLES

Policy Specifics

Custodians of e-mail must not inappropriately access or disclose the content of e-mail in which they are not correspondents, except in the following situations:

A. In response to a court order or other compulsory legal process; or

B. When an e-mail steward (see table 5 in Procedures) has determined that there is a legitimate need to examine e-mail in connection with an investigation involving a human resources matter or a legal or policy violation; or

C. For faculty and staff members only (including student employees), when the information is necessary to conduct university business; or

D. In health and safety emergencies.

◆**Note:** University Policy 4.12, Data Stewardship and Custodianship, covers data that is categorized into the seven functional areas under its purview. In some circumstances, e-mail may be governed by both policies.

◆**Note:** Federal laws protect the privacy of many educational, medical, and banking records.

Policy 5.5
Stewardship and Custodianship of Electronic Mail

PROCEDURES

Requests to Access or Disclose the Content of E-mail

A. Court Order or Other Compulsory Legal Process

For information on these requests, see University Policy 4.13, Acceptance of Legal Papers.

B. Human Resources Matters or Potential Legal or Policy Violations

1. The requesting party must obtain permission from the appropriate e-mail steward(s) of the e-mail or a designee (see Table 5, below).

Table 5
E-mail Stewards

E-mail Correspondent	E-mail Steward(s)
Member of the University Faculty	Provost
Other Academic or Nonacademic Staff Members	Vice President for Human Resources
Student	Vice President for Student and Academic Services
Student Employee	Vice President for Student and Academic Services and Vice President for Human Resources

◆**Note:** In an e-mail file, "e-mail correspondents" includes all individuals listed in the "To:" and "From:" fields. Therefore, an e-mail may have more than one e-mail steward.

2. The e-mail steward must contact the IT security director or the chief information officer (CIO) and vice president for information technologies, providing the details of the request.
3. The Office of Information Technologies (OIT) will communicate with the appropriate staff member at OIT or the unit level requesting access and disclosure of the data to the requester.
4. This staff member will access and disclose the data to the requester.

◆**Note:** In cases of a potential legal violation, the e-mail steward should contact University Counsel, as appropriate. In cases of potential violation of university policy, the e-mail steward should contact University Audit, as appropriate.

Policy 5.5
Stewardship and Custodianship of Electronic Mail

PROCEDURES, CONTINUED

C. The Information is Necessary to Conduct University Business

◆**Caution:** This procedure must not be used for human resources matters. For requests involving human resources matters, see **B.**, above.

I. Forwarding Your Own Mail

Faculty or staff members who will be away from their workplaces for any period of time during which access or disclosure of their e-mail may be necessary, should consider forwarding their incoming mail to appropriate parties using "Who I Am," at www.whoiam.cornell.edu. For additional information on management methods for business mail (e.g., shared e-mail folders, group accounts, e-mail filtering, etc.) please go to www.it.cornell.edu/policies/university/privacy/emailpolicy.cfm

II. Rerouting or Forwarding Another Person's Mail

1. The requesting party, generally the supervisor, must inform the unit human resources representative of the request to have the mail rerouted to another specific e-mail account.
2. The unit human resources representative will send the request to the Office of Workforce Policy and Labor Relations in the Division of Human Resources.
3. Workforce Policy and Labor Relations in the Division of Human Resources will evaluate the request, notifying the requesting party of the outcome. If approved, Workforce Policy and Labor Relations will send the request to the Cornell IT computer accounts coordinator, and any applicable department systems administrator who will effect the rerouting or forwarding.

III. Accessing a Third Party's Existing Mail

1. The requesting party, generally the party's supervisor or someone approved by that supervisor, must inform one of the following individuals: the unit human resources representative, unit head, department chair, college dean, vice president or college officer at the time of the request.
2. The requesting party may then work with the local support provider to obtain the specific mail messages.
3. The requesting party will inform the e-mail recipient that the request was made and approved, and of the nature of the information received.

PROCEDURES, CONTINUED

◆**Note:** While the university permits limited personal use of Cornell-owned or controlled information technology resources, faculty and staff members (as well as student employees, graduate assistants, graduate research assistants, research assistants, and teaching assistants) do not acquire a right of privacy for communications transmitted or stored on university information technology resources.

IV. When an E-mail Account Holder Wishes to Authorize Access by Another Individual to His or Her Account

An e-mail account holder may authorize access to his or her e-mail account on a case-by-case basis.

◆**Caution:** This provision does not supersede restrictions contained in any other university policies, such as the prohibition of sharing network passwords.

D. Health and Safety Emergencies

In the event of a health and safety emergency, the university will access or disclose the content of e-mail according to the following procedures:

1. Upon request by the director of the Cornell Police; deputy director of the Cornell Police; head of investigations; executive director of Gannett Health Services and director of counseling and psychological services , or a designee; or the vice president for student and academic services or his or her designee, the IT Security Office (ITSO) engineer will access and disclose the data.
2. As soon as is practicable, ITSO engineer will notify the appropriate e-mail steward of the request, what data was accessed and/or disclosed, and any other relevant information, such as the approximate time of the request, access, and disclosure, the name and title of the requester, and the nature of the emergency.
3. As soon as is practicable, the ITSO engineer will notify the director of IT policy, the director of IT security, and the CIO and vice president for information technologies.
4. As soon as is practicable, the requesting individual will contact the appropriate e-mail steward (see table 5, above), informing that individual that the request was made and the nature of the information received.

PROCEDURES, CONTINUED

Local Support Providers: Usual Course of Business

In the course of performing network security and maintenance functions (e.g., backups and restores), local support providers may be required to access, observe, or intercept, but not disclose, reroute, or forward electronic mail messages. There are two circumstances when it is permissible for a local support provider to disclose, reroute, or forward the content of electronic mail messages, as detailed below.

Emergency Exception: Should a local support provider, in the usual course of business, reasonably believe that he or she has accessed information about an emergency involving immediate danger of death or serious injury; the following procedures should be invoked:

1. Contact the Cornell Police immediately.
2. As soon as possible, report that contact and the underlying information to the IT security director or the CIO and vice president for information technologies.

Responsible Use Exception: In situations when a local support provider reasonably believes that he or she may have observed evidence of a violation of law or policy, University Policy 5.1, Responsible Use of Information Technology Resources requires that individual to report this information (see Reporting Alleged Violations, below). For more information, see University Policy 5.1, Responsible Use of Information Technology Resources.

Reporting Alleged Violations

Alleged violations of this policy may be reported to the appropriate individual as detailed in Table 5. Alternatively, you may also contact your supervisor, your local HR representative, the director of IT Security, the university ombudsman, or the judicial administrator.

Policy 5.5
Stewardship and Custodianship of Electronic Mail

INDEX