CORNELL UNIVERSITY
POLICY LIBRARY

Data Stewardship and Custodianship

POLICY 4.12

Volume: 4, Governance/Legal
Chapter: 12, Data Stewardship and Custodianship
Responsible Executive: Provost
Responsible Office: Cornell Information Technologies
Originally Issued: May 29, 2003
Last Full Review: August 15, 2018
Last Updated: August 15, 2018

POLICY STATEMENT

The university expects all stewards and custodians of university data to manage, access, and utilize this data in a manner that is legal and consistent with the university's need for security and confidentiality. Cornell University unit custodians (operating unit heads) must develop and maintain clear and consistent operating unit procedures for access to university data, as appropriate.

REASON FOR POLICY

The university facilitates access to data supporting the educational or administrative responsibilities within the institution; ensures that data access restrictions are based on legal, ethical, competitive, and practical considerations; and informs stewards and custodians of university data of their responsibilities.

ENTITIES AFFECTED BY THIS POLICY

☑ Ithaca-based locations

☑ Cornell Tech campus

☐ Weill Cornell Medicine campuses

WHO SHOULD READ THIS POLICY

– All members of the Cornell University community
– Anyone granted access to university data

MOST CURRENT VERSION OF THIS POLICY

– www.dfa.cornell.edu/policy/policies/data-stewardship-and-custodianship

CONTENTS

RELATED RESOURCES

University Policies and Information

University Policy 4.1, Formulation and Issuance of University Policies

University Policy 4.4, Access to Cornell Alumni Affairs Information

University Policy 4.5, Access to Student Information

University Policy 4.6, Standards of Ethical Conduct

University Policy 4.7, Retention of University Records

University Policy 5.1, Responsible Use of Information Technology Resources

University Policy 5.11, Administrative Data Store Registry

Abuse of Computers and Network Systems

Campus Code of Conduct

Office of Human Resources Policy 6.13.4, Personnel Files

IT Governance Process

External Documentation

Americans with Disabilities Act of 1990

The Electronic Communications Privacy Act of 1986 (ECPA)

Federal Educational Rights and Privacy Act of 1974 (FERPA)

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

University Forms and Systems

Annual Confidentiality Attestation (Available in Workday)

CONTACTS

Direct any general questions about this policy to your college or unit administrative office. If you have questions about specific issues, contact the following offices.

Contacts, Ithaca-Based Locations and Cornell Tech

Subject	Contact	Telephone	Email/Web Address
Policy Clarification	Vice President and Chief Information Officer, Information Technologies	(607) 254-8621	it.cornell.edu/office-cio

DEFINITIONS

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

Data Steward	The identified vice president, vice provost, or committee responsible for data types as defined in this policy.
Individual Custodian	An individual who possesses or has access to university data, regardless of form.
ITGC	Information Technology Governance Committee. A provost-charged group of senior administrators with final decision-making authority for information technology across the Ithaca campus, including Cornell Tech. ITGC will coordinate with counterparts at Weill Cornell Medicine.
Legitimate Interest	A need for university data that arises within the scope of university employment and/or in the performance of authorized duties.
Operating Unit	An operating unit of the university, as defined in University Policy 4.2, Transaction Authority and Payment Approval.
Operating Unit Head	The dean or vice president with responsibility for an operating unit, who acts as the unit custodian of university data.
Supervisor	An operating unit supervisor or manager who has been given the authority by the operating unit head to provide access to university data to individual custodians.
Unit Custodian	The *Operating Unit Head* dean or vice president with responsibility for an operating unit.
University Data	Data steward-regulated data, in any form, stored on or off campus, locally generated or acquired from an external service.

RESPONSIBILITIES

The major responsibilities each party has in connection with this policy are as follows:

Data Steward	Defines appropriate use of assigned data types. Understands all legislation that regulate data class use. Work in concert with the vice president for information technologies to define baseline security rules and/or policies for those data sets.
Individual Custodian	Access and/or release university data only as allowed by university policy and as authorized by the operating unit. Access, use, and disclose university data responsibly. Recognize the consequences of improper custodianship of university data.
ITGC	Receive and rule on any appeals to a data steward's decision regarding appropriate use of university data. Assign data stewards and committees.
Supervisor	Authorize access to university data only when appropriate and required to fulfill assigned university duties.
Unit Custodian (Operating Unit Head)	Gain approval from the vice president for information technologies for the management process for any repository of university data within the unit. Participate in the IT governance process as defined by ITGC. Understand the rules for data access as defined by data stewards and applicable university policy. Address consequences of improper unit custodianship of university data. Present to ITGC any appeals of the data steward appropriate use guidelines.
Vice President for Information Technologies	Review and approve resources and management process used to support IT Support data stewards in the development of policies and/or access rules for their data.

PRINCIPLES

Purpose of this Policy

The proper stewardship and custodianship of university data will facilitate appropriate and secure access to data that supports the work of those with official educational or administrative responsibilities within the institution, consistent with legal, ethical, competitive, and practical considerations and inform users and custodians of data of their responsibilities.

◆ **Note:** Nothing in this policy precludes or addresses the release of institutional data to external organizations or governmental agencies as required by legislation, regulation, or other legal vehicle.

This policy serves two primary purposes:

1. Assigns stewardship for classes of university data (see Table 1).
2. Sets forth a standard for unit and individual custodianship of university data, and requires unit custodians to promote operating unit compliance with this policy .

   For examples of appropriate use of university data, see University Policy 4.4, Access to Cornell Alumni Affairs Information and University Policy 4.5, Access to Student Information.

◆ **Note:** The vice president for information technologies and the IT security officer will release guidelines for appropriate IT systems operation and security practices. For more information, see University Policy 5.10, Information Security; University Policy 5.4.1, Security of Information Technology Resources; and University Policy 5.4.2, Reporting Electronic Security Incidents.

Data Stewards

Data stewards are responsible for approving the release of university data for which they are responsible, and may issue detailed guidelines for appropriate use.

Table 1
University Data Types and Associated Data Stewards (as assigned by the ITGC):

Alumni Affairs and Development Data	Vice President, Alumni Affairs and Development
Facilities Data	Vice President, Facilities Services
Financial Data	Vice President, Financial Affairs
Human Resources Data	Vice President, Human Resources
Information Technology Data	Vice President, Information Technologies
Planning and Budget Data	Vice President, Planning and Budget
Sponsored Research Data	Vice Provost for Research
Student Data	Student Data Committee
Video Surveillance Data	Executive Vice President and CFO

PRINCIPLES, continued

Unit Custodians

The unit custodian (the head of the operating unit) is responsible to promote compliance with this policy at the operating unit level. Additionally, the unit custodian is the only individual who may appeal, to the ITGC, a data steward’s decision regarding appropriate use guidelines for university data. In such cases, the ITGC is the final ruling authority.

Individual Custodians

Any individual requesting, using, possessing, or having access to university data is considered an “individual custodian.” Individual custodians must agree to and comply with certain guidelines. Below are examples of some of these guidelines in the form of general prohibitions. These prohibitions apply to all areas.

General Prohibitions

As an individual custodian, you are prohibited from accessing, manipulating, or changing data in the following ways without prior authorization. In addition, you may access, manipulate, or change data only as authorized.

◆ **Note:** These examples are illustrative, not exhaustive.

- Do not change data about yourself or others for other than usual business purposes. Do not use information (even if authorized to access it) to support actions by which individuals might profit (e.g., a change in salary, title, or band level; a better grade in a course). Do not disclose information about individuals without prior supervisor authorization.
- Do not engage in what might be termed “administrative voyeurism” (e.g., tracking the pattern of salary raises; determining the source and/or destination of telephone calls or Internet protocol addresses; exploring race and ethnicity indicators; looking up grades), unless authorized to conduct such analyses.
- Do not circumvent the nature or level of data access given to others by providing access or data sets that are broader than those available to them via their own approved levels of access (e.g., providing a university-wide data set of human resource information to a coworker who only has approved access to a single human resource department), unless authorized.
- Do not facilitate another's illegal access to Cornell’s administrative systems or compromise the integrity of the systems data by sharing your passwords or other information.
- Do not violate university policies or federal, state, or local laws in accessing, manipulating, or disclosing university data.

◆ **Note:** These prohibitions do not apply to self-service applications designed to permit you to change your own data.

PRINCIPLES, continued

◆**Note:** Individual custodians may be asked to sign an attestation of compliance with university policy (see Related Resources).

◆**Note:** Access to university data should be, whenever possible, to the data necessary to perform the task. In addition, the individual with the legitimate interest must remain mindful of any applicable law or policy specifically related to the handling and/or disclosure of that data (e.g., educational records under the Family Educational Records Privacy Act, codified in University Policy 4.5, Access to Student Information).

Improper Custodianship

In assuming responsibility for the interpretation and use of university data, individual custodians are expected to recognize the following potential consequences of their improper custodianship.

Entity	Possible Consequence
University	• loss of funding • lawsuits • loss of employee and student faith and trust
Individual or Group	• violation of privacy • grievous bodily harm and/or mental duress • loss of opportunity or exclusion • discrimination
Violator	• disciplinary action, including fines, suspension, or dismissal • loss of credibility • lawsuits from the university or individuals

Suspected violations will be investigated by the appropriate office, and disciplinary measures may be taken in accordance with applicable regulations or university policy, up to and including termination.