

## University Information and Confidentiality Annual Agreement

This agreement appraises custodians of their obligations and responsibilities in the use of Cornell University information. A custodian is an individual who possesses or has access to university information. Inappropriate management or disclosure of university information may violate applicable federal, state, and local laws as well as place the university in a position of significant legal liability or reputational risk. Numerous university policies pertain to the appropriate management of institutional information. University policies relevant to institutional information are listed below.

Cornell University Policy 4.4, Access to Cornell Alumni Affairs Information

<https://www.dfa.cornell.edu/tools-library/policies/access-cornell-alumni-affairs-and-development-information>

Cornell University Policy 4.5, Access to Student Information

<https://www.dfa.cornell.edu/tools-library/policies/access-student-information>

Cornell University Policy 4.6, Standards of Ethical Conduct

<https://www.dfa.cornell.edu/tools-library/policies/standards-ethical-conduct>

Cornell University Policy 4.7, Record Retention Policy

<https://www.dfa.cornell.edu/tools-library/policies/retention-university-records>

Cornell University Policy 4.12, Data Stewardship and Custodianship

<https://www.dfa.cornell.edu/tools-library/policies/data-stewardship-and-custodianship>

Cornell University Policy 5.10, Information Security

<https://www.dfa.cornell.edu/tools-library/policies/information-security>

In addition to compliance with these policies, all custodians must comply with the following rules taken from University Policy 4.12, Data Stewardship and Custodianship:

- Do not make unauthorized changes to institutional information.
- Do not disclose inappropriately institutional information.
- Do not look up, review, or analyze restricted or confidential institutional information outside the scope of your employment, even if you have access to that information, unless authorized to do so.
- Do not circumvent the nature or level of information access given to others by providing access or information sets that are broader than those available to them via their own approved levels of access (e.g., providing a university-wide information 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 information by sharing your passwords or other access information or devices.
- Do not violate university policies or applicable federal, state, or local laws in accessing, manipulating, or disclosing institutional information. If you are unsure of the meaning or implication on your job duties of a specific policy or law, ask your supervisor about it.
- Do not access, manipulate, or change information involving you or a family member.

If you believe Cornell information or your computer may be at risk of compromise, contact your supervisor and/or the IT Security Office.

If you ever feel pressured by anyone to use the information to which you have access in a way that may violate this agreement, report your concern immediately to your supervisor or to the Cornell University Hotline: [hotline.cornell.edu](http://hotline.cornell.edu)

**Signature**

I acknowledge that I am bound by university policies as well as applicable federal, state, and local laws. I understand that a violation of these policies or laws could result in disciplinary action up to and including termination.

Signed: \_\_\_\_\_

Employee

Date

Please print name: \_\_\_\_\_