

## Policy 1601 Information Access and Security

<b>Responsible Office</b>	Office of the Provost Office of the Vice President for Finance and Administration	<b>Effective Date</b>	11/1/00
<b>Responsible Official</b>	University Director of Information Technology Services	<b>Last Revision</b>	4/20/05

Policy Sections.....	2
1601.1 Authorization to Grant or Revoke Access to University Information .....	2

### Scope

This policy establishes requirements for staff, faculty and students regarding access to University information as well as the responsibilities for stewardship of University information. University information is all information generated or acquired, in printed or machine-readable form, by Yale faculty, staff, students, contractors or others engaged on the University's behalf, in the course of carrying out the University's mission or conducting its business.

### Policy Statement

University information shall be used only for appropriate University purposes. Information is a resource analogous to University financial and physical resources. All members of the University community should be aware of their obligations to protect University information. In particular:

- University information may not be accessed by or disclosed to anyone who does not need the information to perform the activities and fulfill the responsibilities associated with his or her University position.
- Those authorized to access University information are responsible for properly storing and securing it from unauthorized access, as well as for securing and protecting passwords, keys, and other forms of access control.
- Those authorized to grant or revoke access to University information (as specified in Section 1601.1) are responsible for following procedures to ensure that access is appropriately assigned, modified as needed, and canceled promptly when individuals transfer to other positions or leave the University.
- Those accepting confidential information on behalf of the University, e.g., for clinical trials, must ensure that the requirements related to the acceptance of that information are followed.
- Misuse of University information will be regarded with utmost seriousness. Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff and students, and when indicated, sanctions up to and including dismissal or expulsion will be imposed.

Additionally, there are certain categories of information, such as student records and personal health information that are accorded confidentiality under the law as well as under University policy. Examples include *student information*, which is covered by the Family Educational Rights and Privacy Act, also called 'the Buckley Amendment' and the *personal health information* which is covered by the Health Insurance Portability & Accountability Act (HIPAA) when used by a covered entity. Anyone who violates state or federal law is personally liable for such actions under the law as well as under University policy.

Violations of this policy should be reported to individuals authorized to grant access to University systems and information, or to the University Auditing Department.

## Policy Sections

### 1601.1 Authorization to Grant or Revoke Access to University Information

The following University officials are authorized to grant or revoke access to University information:

Type of Information	Official Authorized to Grant or Revoke Access
Academic and educational information	Office of the Provost
Financial information	Controller
Purchasing information	Executive Director of Procurement
Budget information	Budget Director
Human Resources information	Associate Vice President for Administration
Facilities information	Associate Vice President for Facilities
Student information	Associate Vice President for Student Financial and Administrative Services
Protected Health Information (Clinical or Research )	University Chief Privacy Officer

## Related Information

[Policy 1605](#) Faculty Access to University Services and Facilities Prior to Appointment Date

[Policy 1607](#) Information Technology Appropriate Use Policy

## Procedures

[Procedure 1601 PR.1](#) User Access to Oracle Financial and Human Resources Applications

[Procedure 1601 PR.2](#) Multiple NetIDs and Sharing NetIDs for Network or Application Access

[Procedure 1601 PR.3](#) Access Control for Protect Health Information (PHI)

## Contacts

Subject	Contact	Phone
Interpretation of policy	Office of the Provost	432-4453
	Manager of ITS Administrative Systems Integration and Planning	436-3902
Protected Health Information (PHI)	University Chief Privacy Officer	436-3650

The official version of this information will only be maintained in an on-line web format. Any and all printed copies of this material are dated as of the print date. Please make certain to review the material on-line prior to placing reliance on a dated printed version.