Policy 5.8
Information Access Policy

This policy version was not current at the time of printing. Please see http://policies.emory.edu/5.8 for the current version.

Responsible Official: Enterprise CIO and Sr. Vice Provost for Library Services and Digital Scholarship
Administering Division/Department: LITS: Library & IT Services
Effective Date: March 31, 2007
Last Revision: March 29, 2007

Policy Sections:

I. Overview
II. Applicability
III. Policy Details
IV. Definitions
V. Related Links
VI. Contact Information
VII. Revision History

Overview

The policy establishes the basic use, protection, and preservation of all information, in any form, which is generated by, owned by, or otherwise in the possession of the University, including all administrative and academic data (Patient health care information and all research data are excluded from this policy).

Applicability

This policy applies to anyone who needs to access administrative or academic data owned by Emory University.

Policy Details

Preamble

It is a long-standing educational value that information be shared subject to privacy and confidentiality requirements; this reflects the fact that information is a unique resource that increases rather than dissipates when it is used. Consistent with this principle, Emory University seeks to provide appropriate access to University information among its students, staff, and faculty. Access to University information, however, carries with it the responsibility to protect privacy, confidentiality and integrity. So, to enhance access to University information, this policy sets forth rules for its handling and use.

Purpose

To establish the basic policy of Emory University for the use, protection, and preservation of all information, in any form, which is generated by, owned by, or otherwise in the possession of the University, including all administrative and academic data (Patient health care information and all research data are excluded from this policy).

Information Access Policy Statement

Emory University Information is one of the most valuable assets of the University and must, therefore, be safeguarded...
by all agents representing Emory University. Unless otherwise stated in writing, all University Information is considered confidential.

Employees, contract employees, students, or other agents who as either data providers or data users intentionally and without proper authorization (1) access or disclose confidential University Information or (2) modify or destroy University Information, are in direct violation of the Emory University Information Access Policy. Such violations may lead to disciplinary action by the University up to and including dismissal from the University. Under certain circumstances, such violations may give rise to civil and/or criminal liability.

The Emory University Information Access Review Board maintains oversight responsibility for this policy. Comprising key data custodians or their designees, this board is charged with custody of University Information. The Academic and Administrative Information Technology (AAIT) Division provides access to data and implements security, as authorized by the Information Access Review Board. The Information Technology Policy Committee has authority to resolve conflicts, and arbitrate disputes.

Scope

This policy applies to:

- all data supporting the business and operational needs of Emory University.
- information and data in all forms, including information-processing activities, computerized data—whether kept on mainframes, servers or personal workstation—and manually maintained files.
- all application, network, and operating system software used for computerized management of this data.
- computerized data-processing activities related to research and instruction only where the Information Access Review Board determines that such activities should specifically be covered by this policy.

[DEFINITIONS MOVED TO DEFINITIONS SECTION]

Statement of Responsibilities

Academic and Administrative Information Technology (AAIT) Division

- access data, as authorized by custodians, when performing the tasks necessary to assure its availability and accessibility.
- implements data access security as specified by the custodian and the data access standards and guidelines.
- implements adequate controls to protect data from unauthorized access.
- assures that custody has been established for all data.
- assures that proper physical safeguards are in place to protect data.
- provides and supports the systems and application code required to meet custodian specifications for maintenance and dissemination of data.
- monitors the effectiveness of physical, procedural, and data access controls against unauthorized attempts at intrusion.
- protects data from unauthorized destruction, modification, or access during the electronic or physical transfer of the data from one location to another.
- periodically assesses the global and functional area information access policies to ensure that they are current.

Custodian

- assumes responsibility for custody of the data.
- determines the security classification of data.
- specifies access security requirements.
- establishes procedures for obtaining authorization for access to data.
- determines how authorization for access to data is to be granted.
- Authorizes access to the data.
- creates and maintains a published access policy for his/her area.
- reviews access activities against the data and reports access breaches.

Data Provider

- accesses data, as authorized by custodians, when performing information-processing tasks in support of Data Users.
- obtains appropriate authorization before disclosing University data.
- assures that proper physical safeguards are in place to protect data.
- monitors the effectiveness of physical, procedural, and data access controls against unauthorized attempts at intrusion.

Data User

- access data as authorized by custodians.
- obtains appropriate authorization before disclosing University data.
- assures that proper physical safeguards are in place to protect data.
• complies with all applicable data access practices, standards and guidelines as defined by data custodians.
• informs the custodian when he/she no longer needs access to information or an element of data.

**Information Access Review Board**

• reviews, recommends, and approves policies and procedures relating to the use and access of Emory University Information.
• determines whether such policies and procedures comply with the Emory University Information Access Policy.

**Information Technology Policy Committee**

• has authority to resolve all conflicts and disputes that arise due to the implementation or administration of this policy.
• has authority regarding general policies for access to data.

**Definitions**

**Academic and Administrative Information Technology (AAIT) Division**

the organization within Emory University specifically charged with performing information-processing services in support of Emory University's business, academic, and/or research activities.

**Access**

permission, privilege or ability to read, enter, update, manage, or administer access to Emory University's information assets. Authorized by the custodian of the data, access is dependent upon the sensitivity of the data. "Sensitivity" is determined by legal responsibility of the University and the specific job responsibilities of the individual(s) for whom access is requested.

**Agent**

Anyone empowered to act for Emory University. This includes, but is not limited to, faculty, staff, contract employees, and vendors.

**Custodian**

University officials or their designated representatives responsible for data in their areas.

**Data**

factual information including measurements, statements, and statistics.

**Data Provider**

any person or other agent who provides information processing services in support of Emory University's Data Users.

**Data User**

any person authorized to read, enter, and/or update data.

**Emory University**
Information

data that are organized in a meaningful manner.

Information Access Review Board

comprising of the key data custodians, or their designees, specifically charged by the University with
custody of University Information. This includes, but is not limited to, the Vice President of Human
Resources, the Vice President for Business, the Vice President for Finance, the Vice President for
Communications, the University Registrar, and the Director of Institutional Planning and Research.

Information Technology Policy Committee

Executive Vice President, Vice President for Health Affairs, Provost and Vice President for Academic
Affairs, Vice President for Information Technology.

Related Links

- Current Version of This Policy: http://policies.emory.edu/5.8

Contact Information

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clarification of Policy</td>
<td>AAIT Security Team</td>
<td>404-727-4962</td>
<td><a href="mailto:securityteam-l@listserv.emory.edu">securityteam-l@listserv.emory.edu</a></td>
</tr>
</tbody>
</table>

Revision History

Emory University policies are subject to change at any time. If you are reading this policy in paper or PDF format, you are strongly encouraged to visit policies.emory.edu to ensure that you are relying on the current version.