



Northeastern University

Office of Information Security and Identity Services

Institutional Information Asset Administration and Control Policy (Information Security Policy)

Updated Spring 2009

G. Hill, Director, Information Security and Identity Services

Subject Area: **Information Asset Administration and Control**
Policy Title: **Access to Institutional Information Assets**
Policy Number: **DA001**
Responsible Office: **Information Security and Identity Services**

Purpose

To protect the confidentiality, availability, and integrity of University information assets.

Definitions

Access: University-granted permission, privilege or ability to acquire information, gained through official process.

Affiliate: An outside (non-NU) organization contractually engaged by the University to provide one or more services to students, faculty and or staff, whereby the affiliate may legitimately have the need to access institutional information.

Information: Data organized for purposes of conducting the business and/or academic missions of the University.

Information Assets: Data passed on or through University information systems. Also includes equipment through which data is passed, processed, analyzed, modified, stored and/or destroyed.

Institutional Information:

- Information used in planning, managing, directing, controlling, operating or auditing a function of the University.
- Information referenced or required for use by one or more functions, departments and/or units within the University, including students and affiliates.
- Information represented in an official University document, report or submission.
- Information that may be created, developed or enhanced by the University, or by which the University derives value from possession and/or use.

Sensitive Institutional Information:

- Institutional information considered to be administratively or legally privileged due to value, content, regulation, and/or consequences of unauthorized or inappropriate access or use. Restrictions may be imposed by reason of business rule, legal, ethical or other legitimate constraint.
- Information that personally identifies an individual. This classification may not apply when the information is aggregated, or when sufficient identifying information is removed so as to make personal identification impossible.

Scope: All entities with roles at the University.

Policy:

Whereas institutional information is one of the most valued assets of the University, and whereby access carries with it the responsibility to safeguard and protect institutional information from loss of confidentiality, integrity and availability, it is the policy of the University that:

1. All access to institutional data, including but not limited to student-owned data, shall be via legitimate means, such as access granted through official University processes, and/or consent given by the data owner.
2. All access to information and information assets shall be consistent with scope of employment and/or role at the University. The need to access information beyond scope of role or employment requires additional authorization, and may be granted only through consultation with the Office of Information Security and Identity Services, the data owner, and other University officials as may be deemed necessary by the Office of Information Security and Identity Services.
3. All unauthorized access to institutional data and student-owned data is prohibited.
4. Appropriate controls will be implemented as are technically, operationally and financially feasible to ensure data is safeguarded consistent with University policy, law and regulation.
5. Sensitive institutional information and personally-identifiable information will be considered privileged unless otherwise stated in writing, to protect the confidentiality of information pertaining to faculty, staff, student, alumni and external constituents.
6. Data shall be shared and managed as an institutional resource, except only as may be determined by data owners and/or law or regulation.
7. Institutional data is owned by the University; not by any particular individual, unit, department, or system.
8. As with any policy and/or standard, there are situations where business, technology and/or legal imperatives make it impossible or impractical to strictly adhere to policy. In these situations, an "exception" to policy may be warranted. Policy exception requests shall be directed to the relevant Data Managers and the Office of Information Security and Identity Services for review and consideration.
9. All data held on storage media shall be securely destroyed at end of life or end of need. Custodians of storage media are responsible to complete the Asset Disposition Form before disposing of computers and/or storage media of any kind, and to consult and comply with the Asset Disposition Policy.

Consequences of Policy Violation

Entities who without proper authorization access, intercept, steal, disclose, tamper with and/or destroy institutional data are in violation of the policy. Violations may lead to disciplinary action by the University up to and including termination of relationship, as well as legal action.

Implementation Guidelines

1. Each individual requiring data access to a University system shall have unique access. Users will be issued a unique user identification (UID), and a password for their sole use based upon current job requirements and scope of employment. Passwords may not be disclosed or shared with other parties.
2. Accountholders are accountable for any and all activities conducted under their user ID.
3. Managers are responsible to ensure that individuals under their supervision have the appropriate data access based on their current job and/or contractual responsibilities. At least annually, managers will review the access of each of their subordinates for appropriateness, and initiate action to revoke all unnecessary access.
4. Managers are responsible to ensure those under their supervision attend periodic training on Information protection and all trainings required under law and/or regulation.
5. Managers shall consult with the appropriate Data Managers and with the Office of Information Security and Identity Services to discuss alterations or changes to the processes that provide access to institutional data.
6. Data access conflicts shall be brought to the attention of the relevant Data Managers and with the Office of Information Security and Identity Services for appropriate review and resolution.

References (all available at <http://www.infoservices.neu.edu>)

Appropriate Use Policy
Systems Access Request Procedures
SSN Collection, Handling and Use Policy

Reference to Asset Disposition Procedure:

<http://www.northeastern.edu/facilities>