Administrative Guide

6.3.1 Information Security

Last updated on:

06/15/2009

Formerly Known As Policy Number:

63

The purpose of this policy is to ensure the protection of Stanford's information resources from accidental or intentional unauthorized access or damage while also preserving and nurturing the open, information-sharing requirements of its academic culture. This Guide Memo states requirements for the protection of Stanford's information assets.

Authority:

Approved by the President.

Applicability:

This policy is applicable to all University students, faculty and staff and to all others granted use of Stanford University information resources. Every user of any of Stanford's information resources has some responsibility toward the protection of those assets; some offices and individuals have very specific responsibilities. This policy refers to all University information resources whether individually-controlled or shared, stand-alone or networked. It applies to all computer and communication facilities owned, leased, operated, or contracted by the University. This includes networking devices, personal digital assistants, telephones, wireless devices, personal computers, workstations, mainframes, minicomputers, and any associated peripherals and software, regardless of whether used for administration, research, teaching or other purposes.

1. Principles of Information Security

The purpose of information security is to protect the information resources of the University from unauthorized access or damage. The underlying principles followed to achieve that objective are:

a. Information Resource Availability

The information resources of the University, including the network, the hardware, the software, the facilities, the infrastructure, and any other such resources, are available to support the teaching, learning, research, or administrative roles for which they are designated.

b. Information Integrity

The information used in the pursuit of teaching, learning, research, or administration can be trusted to correctly reflect the reality it represents.

c. Information Confidentiality
The ability to access or modify information is provided only to authorized users for authorized purposes.

d. Support of Academic Pursuits
The requirement to safeguard information resources must be balanced with the need to support the pursuit of legitimate academic objectives.

e. Access to Information
The value of information as an institutional resource increases through its appropriate use; its value diminishes through misuse, misinterpretation, or unnecessary restrictions to its access.

2. Classification of Information

All University information is classified into one of 4 levels based on sensitivity and risk. These classifications take into account legal protections, contractual agreements, ethical considerations, privacy issues, and strategic or proprietary worth. The classification level determines the security protections and access authorization mechanisms which must be used for the information. Security guidelines can be found in the ISO Secure Computing Guidelines [1]. The information classifications are as follows:

a. Prohibited Information
Information is classified as "Prohibited" if protection of the information is required by law or government regulation, *or* Stanford is required either to provide notice to the individual if information is inappropriately accessed or to report unauthorized access to the government

b. Restricted Information
Information is classified as "Restricted" if (i) it would otherwise qualify as "Prohibited" but it has been determined by the Data Governance Board [2] that prohibiting information storage on Computing Equipment would significantly reduce faculty, staff, or student effectiveness when acting in support of Stanford's mission, or (ii) it is listed as Restricted in the Classification of Common Data Elements [3].

c. Confidential Information
Information is classified as "Confidential" if (i) it is not considered to be Prohibited or Restricted and is not generally available to the public, or (ii) it is listed as Confidential in the Classification of Common Data Elements [3].

d. Public Information
All information which does not fall into one of these categories is considered to be "public." Please see the Information Security Office [4] for a list of frequently used public information.

3. Responsibilities

a. Information Security Officer
The Information Security Officer is responsible for providing interpretation of this and other related policies and disseminating related information.

b. University Privacy Officer
The University Privacy Officer is responsible for developing and implementing policies and procedures governing the privacy of data that the University is required or elects to protect.

c. Data Governance Board
The Data Governance Board is an advisory group charged with oversight of policies and procedures relating to the protection and use of Stanford's non-public information.

d. Business and Data Owners
System Business and Data Owners are responsible for the application of this and related policies to the systems, data, and other information resources under their care or control.

e. System Administrators
System Administrators are responsible for the application of this and related policies to the systems, information, and other information resources in their care at the direction of the Business and Data Owners.

f. System Developers and Integrators
System Developers and Integrators are responsible for the application of this and related policies to the systems, information, and other information resources in their care at the direction of the Business and Data Owners.

g. Users
Every user of Stanford's information resources is responsible for the application of this and related policies to the systems, information, and other information resources which they use, access, transmit or store.

h. Third-party Affiliates
Stanford expects all partners, consultants and vendors to abide by Stanford's information security and privacy policies. If non-public information is to be accessed or shared with these third parties, they should be bound by contract to abide by Stanford's information security and privacy policies.

4. Violations of Policy and Misuse of Information

Violations of this policy include, but are not limited to: accessing information to which the individual has no legitimate right; enabling unauthorized individuals to access information; disclosing information in a way that violates applicable policy, procedure, or other relevant regulations or laws;

inappropriately modifying or destroying information; inadequately protecting information; or ignoring the explicit requirements of Data Owners for the proper management, use, and protection of information resources.

Violations may result in network removal, access revocation, corrective action, and/or civil or criminal prosecution. Violators may be subject to disciplinary action up to and including dismissal or expulsion, pursuant to campus policies, collective bargaining agreements, codes of conduct, or other instruments governing the individual's relationship with the University. Recourse shall be available under the appropriate section of the employee's personnel policy or contract, or by pursuing applicable legal procedure.

a. Any School or Department found to have violated this policy may be held accountable for the financial penalties and remediation costs associated with a resulting information security incident.

b. Third party vendors found to have violated this policy may incur financial liabilities, in addition to termination of contract.

5. Cognizant Office

Information Security Office

6. Sources of More Information

- Guide Memo 6.1.1 [5]: Administrative Computing Systems
- Guide Memo 6.2.1 [6]: Computer and Network Usage
- Information Security Office [7]
- Classification of Information [3]
- Student Discipline—See Student Life/Codes of Conduct/Fundamental Standard/Honor Code
- Staff Discipline—See Guide Memo 2.1.16 [8]: Addressing Conduct & Performance Issues
- Faculty Discipline— See the Statement on Faculty Discipline
- Health Insurance Portability and Accountability [9] Act of 1996 (HIPAA)
- Family Educational Rights and Privacy Act [10] of 1974 (FERPA)
- Graham-Leach-Bliley Act [11] of 1999 (GLBA)
- Specific information security guidelines, procedures, standards, and practices can be found at Stanford's Information Security Office [12] website; a more detailed breakout of criteria used to determine which information classification is appropriate for a particular information or infrastructure system can be found in the Data Classifications [4] chart.
- University Privacy Officer, privacyofficer@stanford.edu [13]

Guidelines on requesting a memo change can be found at https://adminguide.stanford.edu/change-request-guidelines

Source URL (modified on 01/19/2016 - 10:42): https://adminguide.stanford.edu/chapter-6/subchapter-3/policy-6-3-1

Links

[1] http://www.stanford.edu/group/security/securecomputing/iso-guidelines.html

[2] http://dg.stanford.edu

[3] http://securecomputing.stanford.edu/dataclass_chart.html

[4] http://www.stanford.edu/group/security/securecomputing/dataclass_chart.html

[5] https://adminguide.stanford.edu/6-1-1

[6] https://adminguide.stanford.edu/6-2-1

[7] http://security.stanford.edu

[8] https://adminguide.stanford.edu/2-1-16

[9] http://hipaa.stanford.edu/

[10] https://registrar.stanford.edu/students/student-record-privacy

[11] http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

[12] http://securecomputing.stanford.edu

[13] mailto:privacyofficer@stanford.edu