6.1.1 Administrative Computing Systems

Last updated on:
06/15/2009
Formerly Known As Policy Number:
61
This Guide Memo describes the policy that governs the Administrative Computing Systems at Stanford University and identifies Administrative Computing System ownership, development and management responsibilities. This policy applies to all computerized systems involved with the creation, updating, processing, outputting, distribution, and other uses of administrative information at Stanford.

Authority:
Approved by the Vice President for Business Affairs and Chief Financial Officer.

Policy Statement:
Every Administrative Computing System at Stanford University must have a designated Business Owner who ensures that the system meets the business needs of the University and is appropriately available, secure and sustainable.

Purpose:
The purpose of this policy is to establish system ownership responsibility and to ensure that each system meets its functional requirements, is appropriately documented, is secure and controlled, has been adequately tested, and is maintainable.

1. Scope and Availability

The specifications in this policy are independent of system architecture and delivery platforms—i.e., it makes no difference whether an application resides in mainframe, web, client/server, peer-to-peer, or other present or future environments. This policy applies to applications developed at Stanford, acquired from external vendors, built from open-source components, as well as those extended from existing or purchased applications, whether the systems are developed in central offices, in schools or in departments. This policy applies to all administrative applications that deal with financial, administrative, or other information that is an integral part of running the business of the University.

The standards in this policy specifically apply to the Business Owner of any Administrative Computing System at Stanford University and to all persons who develop, implement, maintain or use any University Administrative Computing System.

2. Definitions

Administrative Computing System
Any computing system that directly or indirectly deals with or supports financial, administrative, or other information that is an integral part of running the business of the University.

Business Owner
The Business Owner of an Administrative Computing System is usually the owner of the primary business functions served by the system, the system's largest stakeholder. When the system serves several different functional business areas of the University, the Vice President of Business Affairs and Chief Financial Officer will designate the Business Owner.

Data Owner
The Dean, Director or Department Head of the administrative department having primary responsibility for creation and maintenance of the data content in an Administrative Computing System. In some cases, a single Administrative Computing System may have multiple Data Owners.

System Administrator
Manages the day-to-day operation of the computer system(s) within an organization that supports the Administrative Computing System. These support functions may include any or all of the following functions: database management, software distribution and upgrading, user profile management, version control, backup & recovery, system security and performance and capacity planning.

System Developer
A person who designs and writes software. The term generally refers to designers and programmers in the commercial software field. However, it may also refer to professionals developing internal business applications within an enterprise. With increasing complexity of technology, and organizations' desire for complete solutions to information problems, requiring hardware, software and networking expertise in a multi-vendor environment, System Developers are integral to the implementation of Administrative Computing Systems.

System Integrator
A person who takes responsibility for delivering a system solution which will solve a business problem. Systems Integrators are individuals or organizations that build systems froma variety of diverse components. With increasing complexity of technology, and organizations' desire for complete solutions to information problems, requiring hardware, software and networking expertise in a multi-vendor environment, Systems Integrators are often key in the implementation of Administrative Computing Systems.

System User

Any individual who interacts with the computer at an application level. Programmers, System Administrators and other technical personnel are not considered System Users when working in a professional capacity on the Administrative Computer System.

3. Guidelines and Responsibilities

a. Business Owner

(1) General

- Define the scope and strategic objectives of the Administrative Computing System
- Oversee the development of a project plan, selection of the project development team, assignment of responsibilities, and management of the project.
- Plan for the ongoing support and maintenance of the Administrative Computing System, including appropriate technical and functional staffing resources.

A Business Owner who does not use the services of Administrative Systems for design, development, integration or maintenance of an Administrative Computing System must assume Business Owner, System Developer, System Integrator and System Administrator responsibilities.

(2) Development Phase

- Define the functions, procedures and audit requirements of the Administrative Computing System
- Ensure the design meets the Administrative Computing System requirements
- Ensure adequate controls, audit trails, security, backup, recovery and restart procedures are included in the design
- Ensure the design and development of the Administrative Computing System meet all appropriate business standards
- Ensure the design and development of the Administrative Computing System meets the Principles of Information Security as stated in Administrative Guide Memo 6.3.1 [1]: Information Security.
- Ensure an adequate test plan is prepared and monitor the testing and review of the Administrative Computing System during development
- Ensure that the appropriate hardware and software environment is selected for the development and operation of the Administrative Computing System
- Define and manage data sharing procedures to ensure the integrity of interfacing Administrative Computing Systems
- Define and ensure compliance with the Administrative Computing System installation procedures
- Define and ensure compliance with Administrative Computing System acceptance criteria
- Define and monitor procedures for modifying the Administrative Computing System
- Define and monitor approval process for all program changes
- Provide for the completeness and accuracy of all required user and system documentation for the Administrative Computing System

- Ensure the implementation of an adequate campus readiness plan, which includes system roll-out plans, adequate user communications, the quality of user training and the related training documents and preparedness of help desk support
- Formally accept the Administrative Computing System as complete and ready for production

(3) Production Phase

- Ensure and monitor the availability, reliability and security and auditability of the Administrative Computing System
- Develop the system's upgrade and enhancements plans to integrate the functionality mandated by business requirements and vendor upgrades into the production Administrative Computing System
- Ensure adequate backup and recovery procedures are implemented, and existence of a tested business continuity plan
- Ensure a System Administrator is responsible for day-to-day decisions regarding the operation of the Administrative Computing System
- Ensure the availability and quality of user training and related materials, reliability and the preparedness of help desk and other technical support processes and personnel

b. Data Owner

- Ensure the availability, reliability and security of the administrative data
- Oversee the management and control of administrative data, ensuring compliance with existing policies
- Report all unauthorized use to the Information Security Office, as described in Guide Memo 6.6.1 [2]: Information Security Incident Response

c. System Developer

- Develop the Administrative Computing System to the satisfaction of the Business Owner, translating the design requirements into a viable service
- Design, code and test the service in compliance with all appropriate standards
- Design the service with the most effective methods of satisfying the control and auditability requirements established by the Business Owner
- Design the service with the most appropriate methods of meeting the system security standards, following the Principles of Information Security outlined in Administrative Guide Memo 6.3.1 [1]: Information Security.

d. System Integrator

- Integrate the service to the satisfaction of the Business Owner, translating the system requirements into design requirements
- Create a design that provides for functionality and ease of use, or select a product that meets System Owner requirements
- Design, code, install, test and deploy the service in compliance with all appropriate standards
- Implement the most effective methods of satisfying the control and auditability requirements established by the Business Owner, or resulting from design decision
- Implement the most appropriate methods of meeting system security standards, following the

Principles of Information Security outlined in Guide Memo 6.3.1 [1]: Information Security.

e. System Administrator

- Create and maintain a stable operating platform that supports the service and any related databases and systems
- Create a secure operating environment that promotes efficient use, including appropriate procedures to protect and recover data and a secure physical environment
- Protect against, monitor for, and detect unauthorized access to the system or data files and report to the appropriate security officer

System Administrators of distributed computing systems, remote network servers, or small stand alone systems may in fact perform the roles, and have the responsibilities of, Business Owner, Data Owner, System Developer, System User and System Administrators in succession, and on an ongoing basis.

f. System User

- Use the application in the manner and for the purpose it was designed
- Comply with all control requirements specified by the Business and Data Owners
- Comply with security requirements defined in the Administrative Guide and further documented in Computer Security Risks and Mitigations [3].

4. Cognizant Office

Information Security Office [4], (650) 723-2911.

5. Sources of More Information

a. Computer and Network Usage
Guide Memo 6.2.1 [5]: Computer and Network Usage

b. Information Security
Guide Memo 6.3.1 [1]: Information Security

c. Information Security Incident Response
Guide Memo 6.6.1 [2]: Information Security Incident Response

d. Specific security guidelines, procedures, standards, and practices
Information Security Office website, Secure Computing section [6].

e. Online Accessibility Policy
http://ucomm.stanford.edu/policies/accessibility-policy.html [7]

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

6/subchapter-1/policy-6-1-1

Links

[1] https://adminguide.stanford.edu/6-3-1

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

[3] http://www.stanford.edu/group/security/securecomputing/

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

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

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

[7] http://ucomm.stanford.edu/policies/accessibility-policy.html

---