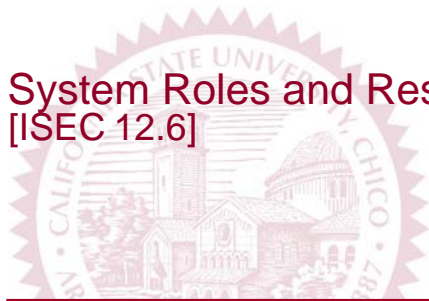


# System Roles and Responsibilities

[ISEC 12.6]



OWNER Brooke Banks  
APPROVED BY CISC  
ISSUED 3/25/2007

REVIEW 3/26/2008  
Page 1 of 5

CALIFORNIA STATE UNIVERSITY, CHICO

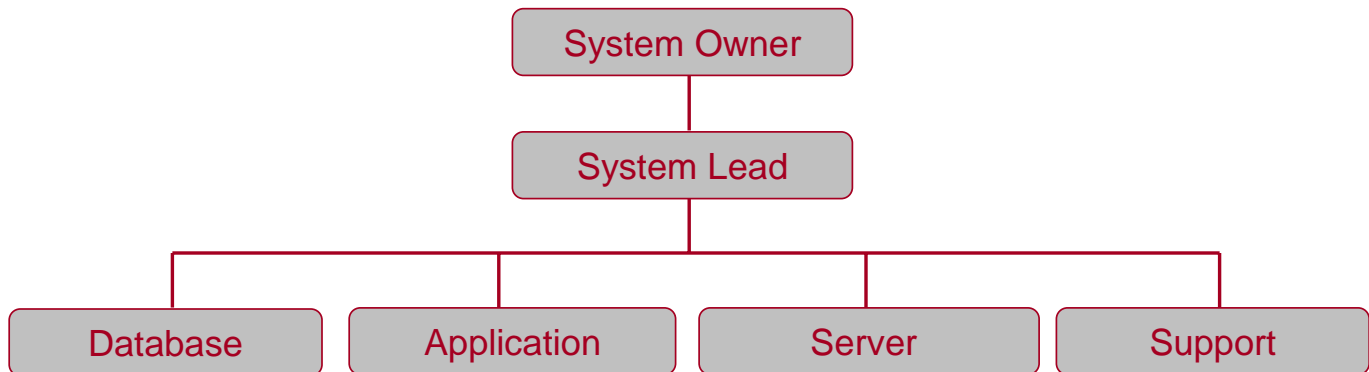
## Purpose

To effectively implement standard security procedures, the Information Security Office has defined roles and responsibilities related to system security. A System is defined as the application, database, network and servers that offer a campus service (e.g., Student e-mail, LDAP, Portal, WebCT, etc.). The diagram below illustrates, at a high level, how these roles interact. Note that an employee may fill multiple roles in the diagram.

## Benefits

- Sets a standard for professional management of systems
- Provides a baseline of understanding across the organization
- Avoids re-inventing procedures
- Reduces risk and error
- Improves ability to monitor and manage processes
- Increased standards lead to cost reduction
- Provides ability to benchmark services and standards against other CSU campuses and industry

## System Security Roles



The System Owner plays a critical role for the system in that they are ultimately responsible for providing the system's service/functionality to the campus. Often the system owner is a manager/director, department chair, or dean. The System Lead has the day to day responsibility to provide the system's service/functionality to the campus. The System Owner and System Lead may be the same person, or the System Lead responsibility may be delegated depending on the size and structure of the organization.

The Server function manages the health and security of servers and other hardware. The Application function manages the day-to-day support and use of applications, where the database function manages the day-to-day

**For Campus use only. Shred on disposal**



support and use of databases. The Support function manages end user support activity for the system. Like the System Owner and System Lead, these roles may be performed by different people or a single person.

Each of these roles works closely with the Information Authority and Information Security Office to ensure confidentiality, integrity and security of campus information and systems. The Information Authority is responsible for data in a system or process and is usually charged by policy or law with responsibility for granting access to and ensuring the appropriate use of the data. The Information Security Office works with the campus community to secure system and network resources, and protect the confidentiality of student, faculty, and staff information.

Additional details regarding each of these roles are provided in the next section.



## Role and Responsibility Definitions

The definitions in this section are not intended to be job descriptions or job titles but define common responsibilities of faculty, managers, supervisors and staff for systems they support. These definitions are not meant to be an inclusive list of responsibilities associated with each role. As additional security procedures are developed it is expected that new responsibilities will be defined.

**System Owner** - The System Owner is ultimately responsible for providing the system's service/functionality to the campus. Often the system owner is a manager/director, department chair, or dean. The System Owner is responsible to:

- Make strategic decisions
- Approve budget and staffing levels
- Approve security/risk management strategy
- Ultimately responsible for all system problems or security compromises

**System Lead** - The System Lead is responsible to provide the system's service/functionality to the campus. The System Owner and System Lead may be the same person, or the responsibility may be delegated depending on the size and structure of the organization. The System Lead is responsible to:

- Make daily operational decisions related to the system
- Manage budget and staffing levels
- Manage overall system security risk
- Ensure that access to and protection of system data is in compliance with all applicable information security policies and the authorized directives of the Information Authority
- Ensure that the system has all appropriate security features installed. This includes operating systems and systems software, database management systems, applications systems, computer hardware, firewalls where appropriate, and communications hardware and software.
- Approve unmitigated vulnerability exceptions.

**Server** - The Server function manages the health and security of servers and other hardware. The following two roles may be performed by the same person or delegated depending on the size and structure of the organization.

**Server Manager** – The Server Manager oversees the security of servers and other hardware. The Server Manager is responsible to:

- Manage the implementation of appropriate security procedures and tools
- Ensure that server vulnerabilities are remediated
- Communicate unmitigated server risks to the System Lead and System Owner

**Server Administrator** – The Server Administrator maintains the health and security of servers and other hardware. The Server Administrator is responsible to:

- Install, configure and harden the server
- Perform routine server maintenance
- Coordinate vendor hardware support
- Review and remediate system logs
- Review and remediate system scans
- Perform routine vulnerability scans
- Remediate OS related vulnerabilities
- Manage change control to server
- Backup server and restore from backup
- Test backup and restore process



**Application** - The Application function manages the day-to-day support and use of applications. The following two roles may be performed by the same person or delegated depending on the size and structure of the organization.

**Application Manager** – The Application Manager oversees the security of the application. The Application Manager is responsible to:

- Manage the implementation of appropriate security procedures and tools
- Ensure that application vulnerabilities are remediated
- Communicate unmitigated application risks to the System Lead and System Owner
- Audit application user accounts

**Application Administrator** – The Application Administrator runs the day-to-day support and use of applications. The Application Administrator is responsible to:

- Install, configure and harden the application
- Perform application maintenance
- Support application
- Setup application user accounts
- Administrate services required for applications (e.g. web)
- Manage change control to application
- Install application patches
- Remediate application related vulnerabilities

**Database** - The Database function manages the day-to-day support and use of databases. The following two roles may be performed by the same person or delegated depending on the size and structure of the organization.

**Database Manager** – The Database Manager oversees the security of the database. The Database Manager is responsible to:

- Manage the implementation of appropriate security procedures and tools
- Ensure that database vulnerabilities are remediated
- Communicate unmitigated database risks to the System Lead and System Owner

**Database Administrator** – The Database Administrator runs the day-to-day support and use of databases. The Database Administrator is responsible to:

- Install, configure and harden the databases
- Perform database maintenance
- Support databases
- Manage change control to databases
- Remediate database related vulnerabilities

**Developer** – The Developer creates custom systems or configures vendor provided solutions. The Developer is responsible to:

- Develop custom applications
- Test applications
- Perform application maintenance
- Support application
- Remediate programming related vulnerabilities (e.g., caused by bugs or errors)



**Support** - The Support function handles end user support for the system.

**Support Manager** – The Support Manager manages end user support activity for the system. The Support Manager is responsible to:

- Manage the implementation of appropriate security procedures and tools
- Manage communication to end users

**Support Staff** – The Support Staff are supervisors and staff that function as business analysts, help desk staff, trainers, or engage in other end user support activity. The Support Staff are responsible to:

- Provide communication to end users
- Create documents for internal staff , help desk and end-users
- Offer user training
- Understand end users needs and be their voice on the project team

**Information Security Office** – The Information Security Office works with the campus community to secure system and network resources, and protect the confidentiality of student, faculty, and staff information. The Information Security Office is responsible to:

- Develop processes, procedures, and policies required for the protection of confidential information
- Identify risks to the security of information and systems. Mitigate these risks to levels acceptable to the campus
- Define security requirements, establish baselines and measure compliance, based on applicable laws, regulations, and best practices
- Act as third party when investigating or assessing incidents, processes and policy compliance

**Information/Data Authority** –The Information/Data Authority is ultimately responsible for data in a system or process (e.g. database, print outs, copies). This person is usually charged by policy or law, with responsibility for granting access to and ensuring the appropriate use of the data. For example, the Family Educational Rights and Privacy Act requires the campus to appoint a information authority (i.e., the FERPA Compliance Officer) for student academic records. The Information/Data Authority is responsible to:

- Ensure appropriate procedures are established to grant and revoke access privileges
- Ensure that those with access to the data understand their responsibilities for collecting, using and disposing of the data only in appropriate ways
- Monitor the usage of the data

**Information/Data Custodian** –The Information/Data Custodian is responsible for protecting data in a system or process (e.g. database, print outs, copies) for which they are the custodian. The Information/Data Custodian is responsible to:

- Ensure appropriate procedures are used to grant and revoke access privileges.
- Establish communication with the information/data authority to ensure access to data is provided on a need to know basis.
- Monitor the usage of the data.