President’s Directive Number 13
Information Security

I.  Directive

Securing information protected by federal and state law as well as California State University (CSU) policies and procedures, is essential. As such, the University will:

- Comply with all federal and state laws and regulations, as well as CSU policies and procedures, concerning the collection, use, maintenance, and release of protected information.
- Develop, implement, and monitor administrative, technical, and physical safeguards to mitigate unauthorized intrusion, malicious misuse, or inadvertent compromise of protected information.

II.  Authority

Several federal and state laws, as well as CSU policies, govern access to information collected, used, maintained, and released by the University, including but not limited to the:

- Family Education Rights and Privacy Act
- California’s Information Practices Act
- Title V
- California’s Public Records Act
- Gramm-Leach-Bliley Act
- Health Information Portability and Accountability Act
- CSU Information Security Policy

III.  Scope

This Directive applies to the collection, use, maintenance, and release of protected information by the University or, when applicable, by any of its auxiliary or affiliate organizations and the development of a campus wide information security strategy.

IV.  Definitions, Implementation & Accountability

A. The University Chief Information Security Officer; CISO; is the campus Chief Information Technology Officer who has been designated by the President to oversee Information Security policy and the coordination of information security efforts across the university. Working with CSUF senior management the CISO coordinates the process to build a university-wide information security strategy and vision. The CISO is charged with the responsibility for building an information security-conscious culture and infrastructure for CSUF.

B. The University Information Security Officer; ISO; is an appropriate administrator designated by the President and delegated responsibility by the CISO for the security of all protected information collected, used, maintained, or released by the University as well as leads the development of a campus wide information security strategy.
The Information Security Officer directly reports to the University’s Chief Information/Technology Officer and is a member of the Information Technology Leadership Team. The ISO works in collaboration with other managers in Information Technology and administrators from other divisions to establish an effective information security program and support the University mission.

The Information Security Officer recommends and develops information security solutions to provide detection, prevention, containment, and deterrence mechanisms to protect and maintain the integrity of the campus data infrastructure, systems, applications and physical assets.

C. **Custodians of Records** are defined as appropriate administrators in charge of offices or departments with functional ownership of protected information (e.g., the Director of Admissions & Records, the Director of Financial Aid, the Director of the Student Health Center, and the Executive Director of Human Resources). Custodians of Records are responsible for securing protected information under the control of their respective department or area of responsibility, including electronic databases, printed reports, and submitted materials.

D. **Technical Security Officers** are defined as technical administrators responsible for the security of protected information maintained by the University (e.g., Chief Information/Technology Officer, Director of Administrative Computing, Director of Network Computing & Security, and the Senior Director of Information Technology, BFA). Technical Security Officers are responsible for applying appropriate technical safeguards to protect information collected and maintained by the University.

E. **Appropriate Administrators** are supervisors or managers included in the Management Personnel Plan. Appropriate administrators are responsible for applying federal and state laws and CSU and policies and procedures regarding protected information, and for granting, monitoring, and managing access to protected information by employees or contractors reporting to them.

F. **All individuals** working with protected information are responsible for collecting, using, maintaining, and releasing it in accordance with federal and state laws or regulations, as well as CSU policies and procedures.

G. **Protected Information** includes information identifying or describing an individual. Different language is used in various federal and state regulations and CSU policies to describe protected information. Protected information may include:

- Social security number
- Ethnicity
- Financial matters
- Home address
- Gender
- Medical information
- Home telephone number
- Employment history
- Education (e.g., grades)
- Performance evaluations
- Physical description
- Statements made by, or attributed to, the individual
Failure to comply with applicable federal and state laws and regulations may result in fines, penalties, exclusion from government funded programs, litigation, adverse publicity, and an array of other impacts that could impede the mission of the University.

**Contact Person:** Chief Information Technology Officer/Chief Security Officer:CISO@fullerton.edu

Interim Information Security Officer:ISO@fullerton.edu

Reviewed and Approved By President Gordon Approved: March 12, 2004
Revised and Reissued: August, 2008

---

1 Complete list included in information security procedures document.
2 Complete list included in information security procedures document.