Fresno County Board of Supervisors

ADMINISTRATIVE POLICY

NUMBER 49
Information Technology Security Policy

Effective Date: November 26, 2002

Revised: July 13, 2021

POLICY STATEMENT

The County's Information Technology (IT) environment includes technologies intended to manage and protect information, network, and digital resources to securely facilitate departmental business functions. It is the County's policy that an IT Security Program provide a business appropriate level of security and protection to prevent disruption, loss, destruction, corruption, misappropriation, or misuse of information.

Responsibility for technology-based security, privacy, and confidentiality controls includes every individual employed or contracted by the County. The security of the County's IT environment is dependent upon effective tools and trained, informed individuals.

POLICY PROVISIONS

A. IT security measures encompass enterprise wide systems and business functions. The level of IT security investment is a business risk-based decision making process. The issues to be considered are:

- Federal and State laws/regulations and/or County ordinances that govern protection of the County's information.
- The sensitive or confidential nature of the information.
- The mission critical nature of the business function/business process.
- The risk exposure.
- The cost of a risk occurrence.

B. Guarding against the risk of county operations being severely disrupted during an unplanned technical outage, cyber security breach or disaster is a critical element of the County's IT Security Policy. Appropriate risk management plans addressing operational recovery, disaster recovery, and business continuity, must be in place.

C. Security measures must appropriately protect information deemed nonpublic under the California Public Records Act or Federal Freedom of Information Act. Requests for public records will be managed according to the County's Public Records Policy.

D. Business appropriate security measures will be implemented to protect the County's information, as well as the privacy and confidentiality of personal, health, and financial information of those with whom the County does business.

E. The County's IT environment may not be used for any unauthorized outside business, unethical, or unlawful activity. Misuse will result in disciplinary action.

F. All new County employees will sign and agree to the IT Acceptable Use Policies prior to being granted access to any County information system and receive training within a reasonable period.

MANAGEMENT RESPONSIBILITIES

The County's Chief Information Officer (CIO) is responsible for implementing and managing the County's IT security program and developing security framework, best practices, and standards and procedures. Compliance with this IT Security Policy, Management Directives, and Standards and Preferred Practices is a countywide responsibility. Managers and employees will be held accountable for such compliance.