



Fresno County Board of Supervisors

ADMINISTRATIVE POLICY

NUMBER 49

Information Technology ~~and~~ ~~Telecommunications~~ Security Policy

Effective Date: November 26, 2002

Revised: June 22, 2021

POLICY STATEMENT

The County's Information Technology (IT) ~~telecommunications~~ environment includes ~~IT communications infrastructure, technologies intended to manage and protect~~ information processing, ~~voice telecommunication, video, imaging and data systems employed by the County's, network, and digital resources to securely facilitate~~ departmental business functions. It is the County's policy that an IT Security Program provide ~~for a business-~~ appropriate level of security and protection ~~in order to prevent~~ disruption, loss, destruction, corruption, misappropriation, ~~or misuse of information, data and/or computing resources.~~

~~As departments increasingly move business processes from paper to technology, routine responsibilities for assuring security of data, privacy and confidentiality are no longer satisfied with paper controls. Responsibility for technology-based security, privacy, and confidentiality controls expands in this new business environment to include~~ every individual employed ~~in Fresno or contracted by the County government who uses a computer or telecommunications device.~~ The security of Fresnothe County's IT ~~telecommunications~~ environment is dependent upon effective tools and trained, informed individuals.

POLICY PROVISIONS

A. ~~Information Technology~~IT security measures ~~having the highest priority~~ encompass enterprise-~~wide~~ systems and ~~mission-critical~~ business functions, ~~business applications/systems and operations. Mission-critical systems are those that support public safety, health and welfare, and financial data. Within that overall framework, the~~ The level of IT security investment is ~~deemed to be~~ a business ~~or~~ risk-based decision-making process. The issues to be considered are:

- ~~The~~ 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 ~~potential~~ risk exposure.
 - ~~The cost of a risk occurrence that would most likely be created by an IT security failure.~~
 - ~~The potential cost of such risk occurrence.~~
- B. Guarding against the ~~potential risk that of~~ County government operations ~~might being~~ severely disrupted during a ~~n~~ unplanned technical outage, cyber security breach or ~~man-made or natural~~ disaster is a critical element of the County's IT Security Policy. Appropriate risk management plans addressing ~~the areas of~~ operational recovery, disaster recovery, and business continuity, must be in place ~~to maintain prescribed operations and service levels.~~
- ~~C. Constituents and business partners must be assured that their privacy and confidentiality, including personal, health and financial information, will not be abused when doing business with the County through any medium.~~
- ~~D.C.~~ D.C. Security measures ~~that must~~ appropriately protect information ~~and data that is~~ deemed non-public under the California Public Records Act ~~must be in place as a component or~~ Federal Freedom of the County's IT Security Program Information Act. Requests for public records will be managed according to the County's Public Records Policy.
- ~~E. Security measures must be in place to assure the integrity of financial transactions and protect County and personal financial information.~~
- ~~F.D.~~ F.D. Business ~~appropriate~~ security measures will be ~~taken~~ implemented to protect the County's information, ~~data, and computing resources~~, as well as the privacy and confidentiality of personal, health, and financial information of those with whom the County does business ~~in all Internet based e-Government or e-Commerce business applications.~~
- ~~G. The Internet~~ County's IT environment may not be used for any unauthorized outside business ~~activity~~, unethical, or unlawful activity. Misuse ~~of the Internet~~ will result in disciplinary action.
- ~~H. E-mail is available to employees to enhance their personal productivity when carrying out County assigned job responsibilities. Misuse of the e-mail facility will result in disciplinary action.~~
- ~~I. The County's Web Site offers the County an opportunity to interface efficiently and effectively with the County's business, civic and constituent communities. Government service web-based offerings must be designed and implemented in such a way that they do not compromise the County's IT security methodologies.~~
- ~~J. In the case of Internet-based business applications, departments must post privacy policies on principal web sites, as well as at any other known, major entry points to sites and at any web page where substantial amounts of personal information are collected.~~
- ~~K.E.~~ K.E. Appropriate security measures must be in place to assure that telephone networks are not a point of entry through which the County's data and computing resources can be compromised.
- ~~L.F.~~ L.F. All new County employees must receive training on the County's IT Communications Security Policies prior to being granted access to any County information system. 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 of time.](#)

MANAGEMENT RESPONSIBILITIES

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