County of Yolo
Administrative Policies and Procedures Manual

TITLE: NETWORK SECURITY POLICY	DEPARTMENT: INFORMATION TECHNOLOGY
TYPE: **POLICY**	DATE: NOVEMBER 25, 2003

A. PURPOSE

The purpose of this policy is to protect the integrity of County information technology systems and assets, County employees, and the information we maintain from destruction, misuse, or improper acquisition and/or access. Due to the complexities of new legislation such as the Health Insurance Portability and Accountability Act (HIPAA) and recent electronic system break-ins at other governmental and private entities, Yolo County must increase its information technology security management program.

B. POLICY

Network Security will be managed by the County's Information Technology Division (ITD). ITD will work with, and inform, the Information Technology Planning Committee (ITPC) and the Information Technology Executive Council (ITEC) on standards and protocols. ITD will develop procedures and standards with respect to Network Security Policy.

This policy is a general County policy. It does not preclude any County department from establishing a more restrictive policy based on factual circumstances that exist in that department determined by the Department Head.

C. DEVICES:

No devices shall be connected to any County computer or peripheral device that is, or will be, connected to the County's network without written consent from County ITD. This includes, but is not limited to, PDAs, cell phones, modems, routers, hubs, switches, firewalls, DSL connections, wireless components, VPN devices, workstations, servers, laptops, etc.

Personal devices are not permitted on the County's network.

D. PASSWORDS:

Passwords will be replaced periodically on County operated systems. Passwords will contain a combination of letters, numbers, and special characters. ITD will be responsible for password specification on such systems and will notify departments should specification need to be changed.

Passwords are not to be disclosed to anyone under any circumstance and are not to be written down except as specifically provided below.

A Department Head may direct an employee to disclose his/her password.

E. NETWORK INFORMATION DISCLOSURE:

Information regarding the County's network or infrastructure shall be disclosed solely by ITD. Any requests for such information should be directed to the Information Technology Division Manager. This includes, but is not limited to, IP addressing, network design, topology, operating systems, etc.

F. REMOTE ACCESS

Remote access to County systems for employees and vendors may be granted by Department Head request to the ACAO of Operations.

The department is responsible for purchasing the required security hardware/software as specified by ITD for remote access. ITD is responsible for maintaining all remote access to the County's network.

G. SOFTWARE:

No personal software may be loaded on County equipment. No freeware or shareware software should be installed without clearance from ITD. These packages often carry trojans and viruses that can compromise security, destroy valuable information, and impact the County's ability to provide technical services while these issues are being remedied. Pirated or illegal software shall not be loaded or used on County computer equipment. These restrictions are applicable to personal devices that have been granted access to the County's network, pursuant to the exceptions policy described herein.

No County-installed software should be altered, disabled, removed, or transferred. This includes anti-virus and other county-standard software.

H. PHYSICAL

All network devices shall be physically secure. Telco closets and wiring cabinets shall remain locked. Workstations should be locked or shutdown if the system will be left unattended. Computers should be shutdown overnight if not in use or if not necessary to continue automated functions after hours.

I. ENCRYPTION

No data encryption is to be used without approval of the department head of the affected department and ITD.

J. DESTRUCTION

All County data on fixed computer hard drives and removable media (floppy/Zip disks, CDROMs, hard drives, tapes, etc.) shall be appropriately destroyed by ITD prior to surplus, reallocation or disposal by the department.

K. INTRUSION:

Users of the County's computer resources shall not attempt any hacking or any other form of intrusion into or disruption of County, or any other, systems.

L. INSTANT MESSAGING:

External Instant Messaging (IM) services are not permitted on the County's network.

M. WEB-BASED E-MAIL

The use of web-based email systems for personal email are prohibited.

N. USERS:

Users must use their designated accounts only. Sharing of log on IDs, passwords, and/or accounts is prohibited.

O. AUDITS:

ITD will be responsible for periodic audits to ensure proper security. Any on-site audit will be discussed with the affected Department Head prior to the audit. Any compliance issues will be resolved with the Department Head. This will include, but will not be limited to, physical security assessments and password strength testing.

P. NON-COMPLIANCE WITH POLICY

Failure to properly adhere to this policy is subject to disconnection, account lockout, and/or disciplinary action up to and including termination.

Q. EXCEPTIONS

Specific exceptions for business purposes will be considered and may be granted through written request by the Department Head to the Information Technology Division Manager. Such exemptions will be reviewed and approved or disapproved by the County Administrative Officer or designee.

R. LAW ENFORCEMENT

County Law Enforcement Agencies shall be afforded exemptions to this policy in order to perform required legal investigations. The terms and conditions for such exemptions shall be documented in writing. The exercise of the use of these particular exemptions shall be approved by the Department Head or their designee and will be documented and maintained by that department.