ADMINISTRATIVE REGULATION	AR: 16.04-1	DATE APPROVED
		January 12, 2016
SUBJECT:		**ORIGINATING DEPARTMENT:**
Security Policy for Computers		**Systems Management**

POLICY:

It is the intent of the Board of County Commissioners to establish standards of practice to protect data, information, networks, and other County Information Technology resources.

PROCEDURE:

1. Systems Management will establish and maintain standards for information technology and network security. As technology changes new methods to compromise security are being developed. The defenses against them must continually adapt. This section offers broad guidelines to protect the County. In the interest of security, specific tactics and techniques may be employed without specifically addressing them in this section.

2. This policy applies to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any County facility, has access to the County's network, uses County information technology, uses County computers, or to remotely hosted systems that host County data.

3. All users will be issued a unique User ID and password. New network accounts must be requested by the employee's supervisor using the Computer Change Form found on the Intranet Forms section. Standard access grants rights to the employee's home folder on the default file server and access to a divisional shared folder. Memberships of security groups will automatically grant access to folders or applications commonly used by employees in that work center. Supervisors must request access not already granted through standard protocols.

4. It is the responsibility of supervisors to notify Systems Management of employee status changes, including termination, administrative leave, leave of absence, suspensions, or any other employment condition that would necessitate the temporary or permanent disabling of network accounts. In the event of termination or suspension the Division Director is required to notify Systems Management either by phone or in person prior to the action. Email is not an acceptable form of notification.

5. Employees shall prohibit non authorized third parties such as citizens, vendors and consultants from attaching their equipment to the County's network. If network access is required, a determination will be made by Systems Management. Violation of this policy can result in disciplinary action up to and including termination of employment.

6. No one may set up remote access to a County resource without coordination of the installation or implementation through Systems Management. The only time this activity will be permitted is to facilitate employees working from home or to allow vendors to offer remote support.

7. No one may alter their network settings without Systems Management's involvement.

8. Attempting to login to networking equipment, servers, routers, switches, printers, or any other network-connected device other than that authorized for access is prohibited.

9. All Administrator or root passwords will be changed when a Systems Management staff member is terminated or transferred who may have known or had access to administrator passwords or whose account had administrator equivalencies.

10. Discussion about passwords, firewalls, network types, server types, what kinds of access methods or any such topic that a requestor could use to breach network security, is prohibited. All inquiries of that nature shall be forwarded to Systems Management.

11. No one is permitted to connect a router, a switch, a wireless access point, or any other networking device that expands or extends the County network unless approval by Systems Management is obtained prior to connection occurring.

12. Users of network resources must report the discovery of excessive network rights to Systems Management. If someone discovers access to files, folders, servers, or other network resources to which they do not believe they should have access, they must contact Systems Management immediately and report what they have discovered for review and possible remediation.

13. Firewalls will be installed between the County network and Internet connections and configured to block as much traffic as possible while allowing only the required traffic for the County to conduct business.

14. When new software upgrades are installed, where possible and practical the upgrades shall be tested in a non-production environment. When the software is Enterprise in nature (used by more than one Division or Branch) Systems Management will notify all affected Divisions to begin testing. Divisions shall begin testing in a timely manner and report problems to Systems Management or the designated agent. Systems Management will get post testing approval from all Divisions affected prior to installing the upgrade into the Production System.

15. If an employee believes they (or their equipment) have experienced a security incident the employee shall immediately notify Systems and then follow these guidelines:
    a. Stop working on the computer immediately
    b. Do not close programs so as not to erase any useful information
    c. Do not resume using a workstation until Systems inspects and declares it safe
    d. Note the date and time of the incident

FOOTNOTES & REFERENCES TO RELATED AR's: Supersedes AR 16.10 adopted January 27, 2009; AR 16.04 dated June 22, 2010.