MEMORANDUM

Date: December 19, 2017

To: The Honorable Chair and Members
Pima County Board of Supervisors
Presiding Judge, Superior Court
Elected Officials
Appointing Authorities

From: C.H. Huckelberry
County Administrator

Re: **Revised Board of Supervisors Policy 27.1, Information Technology Program**

In my memo dated December 7, 2017 to the Board of Supervisors I alluded to the release of a completely rewritten policy D27.1. The rewritten draft policy is attached. I am requesting that your departments review and comment on the proposed policy. This document was redrafted to accommodate some of the concerns expressed during the earlier comment period. It also incorporates new language regarding cybersecurity.

Your comments and questions should be referred to Jesse Rodriguez, Chief Information Officer.

CHH/mp

Attachment

PIMA COUNTY, ARIZONA
BOARD OF SUPERVISORS POLICY

Subject: Pima County Information Technology Program	Policy Number	Page
	D 27.1	1 of 5

PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment, systems, and applications at Pima County. These rules are in place to protect the employee and Pima County. Inappropriate use exposes Pima County to risks including virus attacks, compromise of network systems and services, and legal issues.

This policy covers Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Pima County. These systems are to be used for business purposes in serving the interests of the organization, and of our constituents, clients and customers in the course of normal operations.

This policy acknowledges that cyber-security is a key component of the Information Technology program and that effective security is a team effort involving the participation and support of every Pima County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know the Pima County IT procedures and guidelines, and to conduct their activities accordingly.

SCOPE

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Pima County business or interact with internal networks and business systems, whether owned or leased by Pima County, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Pima County are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Pima County policies and standards, and local laws and regulation. Exceptions to this policy are documented in the Policy Compliance Section.

This policy applies to employees (temporary or permanent), contractors, consultants, and other workers at Pima County, including all Elected Officials, Special Districts, and personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Pima County.
This policy is closely tied to Board of Supervisors Policy D 27.2 – Pima County Information Technology Program Lifecycle Management Plan.

1. General Use and Ownership
   a. Pima County proprietary information stored on electronic and computing devices whether owned or leased by Pima County, the employee or a third party, remains the sole property of Pima County. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*
   b. Employees have a responsibility to promptly report the theft, loss or unauthorized disclosure of Pima County proprietary information.
   c. Employees may access, use or share Pima County proprietary information only to the extent it is authorized and necessary to fulfill their assigned job duties.

d. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
e. For security and network maintenance purposes, authorized individuals within Pima County may monitor equipment, systems and network traffic at any time, per Pima County's *Administrative Information Technology Audit Procedure*.
f. Pima County reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2. Security and Proprietary Information
   a. All mobile and computing devices that connect to the internal network must comply with the *Administrative Remote Access Procedure*.
   b. System level and user level passwords must comply with the *Administrative Password Protection Procedure*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
   c. All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. Users must lock the screen or log off when the device is unattended.
   d. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. Employees should submit suspicious emails through the Report Possible Spam button within Microsoft Outlook.

3. Unacceptable Use

   The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

   The lists below are not exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

   a. System and Network Activities

      The following activities are strictly prohibited, with no exceptions:

      i. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Pima County.
      ii. Attempts to influence the outcome of an election, referendum, initiative, or recall (Arizona Revised Statute § 11-410).
      iii. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music. The installation of any copyrighted software for which Pima County or the end user does not have an active license is strictly prohibited.
      iv. Accessing data, a server, or an account for any purpose other than conducting Pima County business (even if you have authorized access) is prohibited.
      v. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. Information Technology Department staff should be consulted prior to export of any material that is in question.

vi. The use of personal computing devices which can lead to the introduction of malicious programs into the network such as viruses, worms, Trojan horses, e-mail bombs, etc. when connecting into the County network.
vii. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
viii. Using a Pima County computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace policies.
ix. Making fraudulent offers of products, items, or services originating from any Pima County account.
x. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
xi. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data for which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
xii. Port scanning or security scanning is expressly prohibited unless prior notification to the Information Technology Department is made.
xiii. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
xiv. Circumventing user authentication or security of any host, network or account.
xv. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
xvi. Providing information about, or lists of, Pima County employees to parties outside Pima County without prior consent of County Administrator, or designee, or as a part of normal job duties.

b. Email and Communication Activities
i. The expression of personal opinions using Pima County resources is prohibited, unless it is an authorized function of the employee's regular duties (e.g., Elected Officials).Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
ii. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
iii. Unauthorized use, or forging, of email header information.
iv. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
v. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
vi. Use of unsolicited email originating from within Pima County's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Pima County or connected via Pima County's network.
vii. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

c. Blogging and Social Media
i. Blogging by employees, whether using Pima County's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional internal use of Pima County's SharePoint application to engage in blogging is acceptable, provided that it is done in a professional and responsible manner,

does not otherwise violate Pima County's policy, is not detrimental to Pima County's best interests, and does not interfere with an employee's regular work duties. Blogging outside of the County's SharePoint system must comply with the guidelines set forth by the Communications Department. Blogging from Pima County's systems is also subject to monitoring.

ii. Pima County's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any Pima County confidential or proprietary information, trade secrets or any other material covered by Pima County's *Confidential Information Procedure* when engaged in blogging.

iii. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Pima County and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Pima County's *Non-Discrimination and Anti-Harassment Procedure*.

iv. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Pima County's trademarks, logos and any other Pima County intellectual property may also not be used in connection with any blogging activity.

POLICY COMPLIANCE

1. Compliance Measurement
   The Information Technology Department will verify compliance to this procedure through various methods, including but not limited to, business tool reports, and internal and external audits, and feedback to the Appointing Authority.

2. Exceptions
   Any exception to the procedure must be approved by the County Administrator or designee in advance.

3. Non-Compliance
   An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

RELATED POLICIES AND PROCEDURES, STANDARDS AND GUIDELINES

The following links contain the appropriate IT related Policies, Administrative Procedures, Standards, and Guidelines.

1. Board of Supervisor Policies
2. General IT Administrative Procedures
3. Application Security Administrative Procedures
4. General Cyber Security Administrative Procedures
5. Network Security Administrative Procedures
6. Server Security Administrative Procedures
7. IT Standards
8. IT Guidelines

DEFINITIONS

1. "County Administrator" means the County Administrator or designee
2. "Information Technology Program" is comprised of all of the components of the IT Environment, IT Resources, Enterprise Applications, and Business Applications and the content therein.
3. "Blogging" a website containing a writer's or group of writers' own experiences, observations, opinions, etc., and often having images and links to other websites.
4. "Proprietary Information" is that information unique to a company and its ability to compete, such as customer lists, technical data, product costs, and trade secrets.
5. "Spam" is electronic junk mail or junk newsgroup postings.