MARICOPA COUNTY INTERNAL POLICY

Policy Title: **USE OF COUNTY TECHNOLOGY RESOURCES**	Policy Number:	A2611
	Current Adoption Date:	08-17-2020
	Current Implementation Date:	08-17-2020
Approved by: **COUNTY MANAGER**	Board Agenda Number:	N/A
	Original Adoption Date:	07-24-2019

I. PURPOSE

Establish privileges, responsibilities, and restrictions in the use of County Technology Resources (CTR) and devices that access CTR; maximize the value of these resources to securely enable business goals and improve efficiency in delivering the mission of Maricopa County.

II. APPLICATION

This Policy applies to all Maricopa County appointed departments as well as the Flood Control District of Maricopa County, the Maricopa County Library District, and the Maricopa County Stadium District (Special Districts). The Board of Supervisors is authorized to jointly adopt policies applying to the Special Districts under the Intergovernmental Agreement, C-06-18-393-6-00, approved on April 11, 2018.

This policy also applies to employees of County elected offices unless the elected official has implemented a similar specific policy.

III. DEFINITIONS

A. Application Store or Market Place: A digital distribution platform or website for downloading applications. The marketplace provides both free and fee-based applications.

B. Appointing Authority: An elected official, the single administrative or executive head of a department/Special District, or the designated representative authorized to act in this capacity.

C. Authorized Application: An application approved for use on CTRs that satisfies the requirements in section IV.D.

D. Authorized User: An individual approved by the Appointing Authority to use CTRs. This includes County employees, temporary employees and non-employees providing products or services to the County and/or who are given access to County data such as suppliers on contract or outside organizations with IGAs.

E. Bring Your Own Device (BYOD): An optional model whereby an Authorized User employs a personally owned Mobile Device to conduct County business and for which they may receive a Stipend for voice and/or data service.

F. County Data: Electronically Stored Information (ESI) owned by, contracted with, or controlled by the County; or used to conduct County business. The County may be a steward of the information; it does not need to originate within the County.

G. County Technology Resource (CTR): Any computing account; device (e.g., mobile device, smartphone, tablet, computer, communications equipment, video conference, facsimile, or telephone); peripheral; software; local, wireless and wide area networks (i.e., LAN, Wi-Fi and WAN); ESI; website; cloud-based or internally-hosted system; or related consumable (e.g., disk space, processor time, network bandwidth) owned by, contracted with, or controlled by the County.

H. County Telecom Coordinator: The primary individual responsible for the day-to-day administration of the County's telecommunications program, including cell phone plans, equipment, and billing through the Telecom Expense Management System.

I. Department Security Officer (DSO): The individual designated by the Appointing Authority to implement and maintain the Department's compliance with all County information security plans, policies, standards, guidelines, procedures and requirements.

J. Department Telecom Coordinator: The individual designated by the Appointing Authority to exercise control of a department's telecom responsibilities, serve as the primary resource and point-of-contact for staff, and as the liaison with the County Telecom Coordinator.

K. Encryption: The process of making information unreadable without the necessary decryption key to prevent unauthorized access.

L. Electronically Stored Information (ESI): Information that is created, manipulated, communicated, and stored in digital form, requiring the use of computer hardware and software. Such information includes, but is not limited to, emails, databases, logs (phone, voice, access, etc.), scanned or digitally created documents, spreadsheets, recordings, photographs, or any other information as identified under the Federal Rules of Civil Procedure Rule 34(a)(1).

M. IT Provider: The organization, either internal or external to the County, that installs, configures or maintains electronic devices on behalf of an Appointing Authority.

N. Malware: A contraction of "malicious software," referring to software designed to damage or perform other unwanted actions on a computer system. Common categories of Malware include, but are not limited to, adware, backdoors, bots, bugs, phishing, ransomware, rootkits, spyware, Trojan horses, viruses, and worms.

O. Mobile Device: A cellular and/or smart phone, tablet, external air card, Wi-Fi hot spot, or similar device. This includes devices enrolled in the BYOD program.

P. Network: A System of interconnected CTRs designed to facilitate the sharing of devices and information among local and remote electronic systems used by Authorized Users.

Q. Network Scan: Use of a computer to gather information regarding CTRs, typically for conducting security assessments, system maintenance or to detect technical vulnerabilities.

R. Sensitive Information: Any information that if compromised through alteration, loss, loss of use, misuse, or unauthorized disclosure, may cause harm to the County, employees, or citizens. This includes, but is not limited to, information that uniquely identifies an individual such as an individual's photograph, social security number, driver license/passport number, email/web addresses, usernames, passwords, employment record, and other information not lawfully accessible from publicly available sources. This also includes any information that is protected by federal and/or state law. The County may be either an originator or steward of the information.

S. Software (Computer Software): Includes, but is not limited to, operating systems, utilities, database management systems, development environments, operational/management tools, business applications, communications programs, packaged personal productivity suites, etc. These can be distributed on electronic media or through electronic transmission. These can include the full products, updates, upgrades, modifications, bug fixes, maintenance releases, as well as the underlying source code.

T. Software Related Materials: Includes printed materials or documentation provided with or supplied subsequently for use with Software, including all updates.

U. Stipend: An amount paid to an Authorized BYOD User for the County's use of time and services on their personal cellular or digital plan.

IV. POLICY

A. Acceptable Use

1. All CTRs are to be used to carry out the responsibilities of County employment, County awarded contracts, or approved IGAs. Incidental, infrequent personal use is permissible so long as it does not interfere with the responsibilities and duties of employment.

2. Employees are responsible for exercising due diligence in protecting the CTRs they use, including County Data, from unauthorized or improper use, at all times. This includes locking the CTR when not within direct line of sight.

3. All activities involving CTR must be uniquely traceable to a specific individual.

4. All use of CTRs must present Maricopa County in a manner that preserves the County's good reputation and high standards of professionalism. Such use must be conducted in accordance with Maricopa County Policy HR2416 *Code of Conduct*.

5. Any electronic communication that constitutes a significant representation of Maricopa County to the public must be approved by the appropriate Appointing Authority and Office of Communications.

6. All County Data used or created to conduct County business is the property of Maricopa County. The processing or storage of County Data must follow County policy, security and privacy requirements, Public Record Laws, and all state and federal regulatory requirements including but not limited to:

   a. A1606 *Public Records Requests*

   b. A2101 *Records Management*

   c. A1512 *Solicitation and Distribution of Literature*

7. All acquisition, development, modification, operation and disposal of CTRs must be conducted in accordance with all County information security plans, policies, standards, guidelines, procedures and requirements.

8. The County must implement systems to monitor, record, control and adjudicate all CTR usage at any time, without prior notice or warning to Authorized Users. Anyone using CTRs has no expectation of privacy in the use of these resources or any content therein.

9. Any unusual electronic activity, including potential Malware, must be reported immediately upon discovery to a supervisor, IT Provider, and cybersecurity@maricopa.gov or 602-506-HELP.

10. Network Scans require coordination between affected Appointing Authorities and IT Providers and approval from the Maricopa County Chief Information Security Officer (CISO) or Maricopa County Chief Information Officer (CIO).

11. Appointing Authorities may further restrict the use of their CTRs through supplemental department policies, standards, guidelines, and procedures as developed in coordination with the CISO.

B. Improper Use

1. CTRs must not be used for illegal, insecure, inappropriate, obscene, political or personal gain purposes, or activities otherwise prohibited by County policy (collectively, Improper Use).

    a. Illegal activity is defined as a violation of local, state, and/or federal laws.

    b. Insecure use is defined as a violation of any County information security plans, policies, standards, guidelines, procedures or requirements.

    c. Inappropriate use is defined as a violation of the intended use of the CTR.

    d. Obscene activity is defined as a violation of generally accepted social standards for use of a publicly owned and operated communications vehicle.

    e. Excessive personal use that interferes with employment duties.

2. Improper Use of CTRs, or any violation of this policy, may result in discipline up to and including termination of employment or contract status. Improper Use or any violation of this policy may also result in reduction, suspension, or revocation of CTR privileges.

3. Any Improper Use of a CTR may result in the removal or disconnection of the resource until compliance with this policy is achieved, with any incurred charges billed to the owning department.

4. Examples of Improper Use of CTRs include but are not limited to

    a. Pursues illegal activities such as libel/slander, gambling or other schemes (e.g., pyramid, chain letters, etc.).

    b. Uses the CTRs for fraudulent purposes.

    c. Steals intellectual property, data or CTRs or violates institutional or individual copyrights or other contracts such as license agreements (e.g., downloading or copying of data or software or music that is not authorized or licensed).

    d. Promotes fundraising or advertising of non-County organizations that have not been pre-approved.

    e. Uses CTRs for gaming, shopping, or social networking for non-business purposes unless authorized by the department's Appointing Authority.

    f. Uses CTRs to conduct commercial or private business transactions other than County business (e.g. using facsimile machines or telephones to further an employee's commercial/private business endeavors).

    g. Views, retrieves, saves, or prints text or images of a sexual or violent nature or containing sexual innuendo (e.g. accessing adult-oriented sites or information).

h. Generates or possesses material that is considered harassing, obscene, violent, profane, intimidating or threatening, defamatory to a person or class of persons, or otherwise inappropriate or unlawful including such material that is intended only as a joke or for amusement purposes.

i. Adding, removing or otherwise changing hardware or software, including configurations, without proper authorization.

j. Misrepresents another user's identification (forges or acts as), gains or seeks to gain un-authorized access to another user's account/data or the passwords of other users, or vandalizes another person's data.

k. Shares log-in credentials such as passwords.

l. Invades systems, accounts, and Networks to obtain un-authorized access to and/or to do damage (hacking). This includes un-authorized Network Scans, probes, or system entries.

m. Intentionally intercepts and modifies the content of a message or file originating from or belonging to another person or computer with the intent to deceive or pursue illegal or improper activities.

n. Knowingly, or with willful disregard, initiates activities that disrupt or degrade Network or system performance, or that crashes the Network or other systems or that wastefully uses the finite CTRs.

o. Any use of administrative privilege to perform unauthorized activity or data access.

p. Knowingly or with willful disregard propagates destructive programs into CTRs (e.g., worms, viruses, parasites, Trojan horses, malicious code, email bombs, etc.).

q. Discloses Sensitive Information without proper authority.

r. Fails to comply with instructions from their supervisor, an equivalent individual responsible for assigning or directing work, or the CISO, regarding activities that threaten the operation or integrity of CTRs, are deemed inappropriate, or otherwise violate this policy.

C. Electronically Stored Information (ESI) Availability

1. Text messages must not be used as a communication tool to conduct substantive or official County business unless the Appointing Authority establishes a text message capture and retention procedure in accordance with the appropriate record retention schedule.

2. The Appointing Authority is responsible for the retention of ESI used to conduct their department's business in accordance with A2101 *Records Management*.

D. Software Copyright and License Compliance

1. Maricopa County will only acquire and use properly licensed proprietary, copyrighted, free or open-source Software on CTRs after CISO approval and will comply with the terms of the licenses or other agreements applicable to the Software and Software Related Materials. This includes, but is not limited to, federal, state, and local laws, codes, rules and regulations relating to copyrights, trademarks, trade names, trade secrets, patents and similar rights, and any license agreements that apply to Software and Software Related Materials used by the County. The Software must be procured by and licensed to Maricopa County, except software for personal use on Bring Your Own

Devices (BYOD). Licenses are not standard and therefore must be examined for the rights and obligations of the licensee.

2. The County may develop and use such internally developed Software after CISO approval. In doing so, the County will not infringe on other Software copyrights, patents or similar intellectual property rights in any manner. The County will not market, publish, adapt, publicly display, reproduce, distribute or disclose any internally developed Software or Software Related Materials without making a specific determination that such Software or Software Related Materials do not infringe upon existing copyrights, patents or other rights.

3. The Appointing Authority will ensure that all Software and County Data is completely removed from any CTR prior to disposal. This can include disposal through transfers between County departments, disposal to an outside entity, or final salvage. The Appointing Authority may request assistance from their IT Provider.

4. Encryption algorithms used by CTRs must meet the National Institute of Standards and Technology (NIST) standards.

E. Malware Protection

1. All electronic devices attached to the Maricopa County Network or used to access, process or store County Data must use Malware protection software approved by the CISO, updated and functioning properly, regardless of location, e.g., on-site, remote, home, etc. This includes electronic devices not owned or managed by Maricopa County.

2. IT Providers must ensure Malware protections are implemented and maintained to provide continuous monitoring and remediation. Periodic Malware scans alone do not provide sufficient protection.

3. Malware protection software must not be disabled or removed from any CTR unless specifically approved by the CISO.

4. IT Providers must implement procedures and automated tools to quickly detect, remediate and prevent the spread of Malware that could jeopardize the confidentiality, integrity, or availability of CTRs.

5. All Software must be kept current with patches and updates in accordance with the County information security Vulnerability Management Program.

F. Implementation

1. The Maricopa County Technology Use Statement must appear on all entry points into CTRs, except guest internet access. (see Addendum 1).

2. Maricopa County may offer guest internet access. This access must be physically or logically separate from other County Networks. It would be provided as a courtesy to the guests of Maricopa County's facilities, is not intended for County business purposes and its availability is not guaranteed. It would be offered under the terms of the Maricopa County Guest Internet Access Acceptance Statement. This statement must be presented and accepted before using this resource. (see Addendum 2).

3. The Appointing Authority, CIO or CISO may disable guest internet access, in whole or in part, if it negatively impacts the conduct or security of County business.

4. The establishment of all IT systems must adhere to NIST Special Publication 800-64, Security Considerations in the System Development Life Cycle (SDLC). This must include all 5 phases of the SDLC: initiation, development, implementation, operations/maintenance, and disposal.

G. Mobile Devices

1. Authorized Users that are non-exempt employees are prohibited from using any Mobile Device for County business unless the time spent on the Mobile Device is recorded in the County's payroll system. Non-exempt employees must follow HR2471 *Hours Worked and Overtime* regarding on-call/overtime.

2. Authorized users of Mobile Devices, including BYOD, must:

   a. Not share the Mobile Device with other individuals including family members. This is to protect data and communication records (potential access to County records, email, etc.).

   b. Ensure the Mobile Device's hardware, operating system, and all applications are up-to-date with the latest vendor releases.

   c. Obtain Appointing Authority approval in writing prior to purchasing any item from an Application Store on the Mobile Device for County purposes.

   d. Only download applications from the operating system's official Application Store (i.e., Apple's App Store and Google Play).

   e. Create encrypted backups of information on their mobile device.

   f. Surrender the Mobile Device to the County upon request from their Appointing Authority.

   g. Allow the County to erase any and all data on the Mobile Device if it is compromised, lost, stolen, or the user's association with the County is terminated.

   h. Release Maricopa County from all liability from any loss of personal data stored on a Mobile Device or damage caused by County support personnel or software provided by the County.

   i. Not attempt to bypass security controls on Mobile Devices.

   j. Not move County data from a Mobile Device to an unprotected device or storage unless approved by departmental procedure.

   k. Ensure their Mobile Device service plan is optimized for their use of the device for County business.

   l. Inform the Department Telecom Coordinator immediately upon suspension or termination of cellular service if receiving a BYOD Stipend.

   m. Not request reimbursements from the County for costs incurred on a BYOD due to personal use, fees, device replacement, overages or other additional or unexpected costs that exceed the approved Stipend.

   n. Must record and maintain their cell phone number(s) in ADP or other assigned County HR system to allow for emergency communications.

3. Mobile Device Security and Support

   a. County data must be encrypted when stored on any Mobile Device.

b. The password and Encryption keys used on the Mobile Device must meet the minimum standards set by the CISO.

c. If a Mobile Device is lost or stolen:

i. The Authorized User must report the incident to their Department Telecom Coordinator immediately or as soon as practicable.

ii. The Department Telecom Coordinator must report the incident to the County Telecom Coordinator immediately or as soon as practicable.

V. RESPONSIBILITIES

A. All Authorized Users:

1. Must sign and submit a Maricopa County Use of County Technology Resources Acknowledgment Form, preferably electronically.

2. Acknowledge that accessing any CTRs constitutes their acceptance of all related County IT and security policies and there is no expectation of privacy in the use of these resources or any content therein.

3. Must keep all electronic communications professional and follow established policies regarding workplace professionalism.

4. Must protect and secure their CTRs from un-authorized or improper use. This includes ensuring that any electronic device they use to access, process or store County Data, including personal devices, are secured with properly maintained and updated Malware protection solutions.

5. Must adhere to the “use” restrictions of any external organization with which they interface and declare their identity and affiliation with Maricopa County whenever using CTRs.

6. Who encounter or receive any material that violates this policy must immediately report the incident to the employee’s supervisor and notify the sender that such communication is prohibited under County policy.

7. Must immediately report any suspicious electronic activity to their immediate supervisor, IT Provider, and cybersecurity@maricopa.gov or 602-506-HELP.

B. The Appointing Authority:

1. Ensures compliance with this policy.

2. Identifies and approves Authorized Users of CTRs.

3. Ensures that all Authorized Users sign the Maricopa County Use of County Technology Resources Acknowledgment Form within 10 days of accessing a CTR and within 30 days of any significant change to this policy. This acknowledgement must be tracked electronically via the County Learning Management System (LMS).

4. Determines Employee's eligibility to become an Authorized User of a Mobile Device, select a service plan aligned with the Employee's need to conduct County business, control overall Mobile Device costs, and be responsible for all monthly fees including Stipends associated with Mobile Devices used by the department's Authorized Users.

5. Appoints a Department Telecom Coordinator.

6. Appoints a Department Security Officer (DSO).

7. Ensures the DSO: (1) has the information, resources, and access to material and personnel necessary to fulfill their responsibilities; (2) is advised of the development of new programs or systems during the early planning stages.

8. Collaborates with the CISO to ensure security is integrated into all IT procurement and development efforts from the initial design phase onward.

9. May define business and Network utilization practices that are more restrictive than standard County practices, as needed.

10. May request exceptions to this policy from the CISO for specific business requirements.

11. Provides training to their employees on the acceptable use of CTR.

12. Ensures the approved Maricopa County Technology Use Statement (see Addendum 1) is displayed for all their entry points to CTRs, or the Maricopa County Guest Internet Access Acceptance Statement on the guest internet access Network (see Addendum 2).

13. Ensures their IT Provider has software and systems in place to monitor, record and report computer usage and to immediately restrict, disable, isolate or disconnect CTRs.

14. May monitor and investigate departmental use of its own CTRs, at any time, without prior notice or warning to any user of its CTRs.

15. May request access to email, Network and/or other CTR usage information for their organization at any time to ensure compliance with this policy.

16. Ensures the tracking of Software licenses to verify their department has paid for all licenses in use.

17. Conducts periodic audits of departmental procedures to ensure that only authorized and properly licensed Software is used on CTRs.

18. Ensure that all authorized radio equipment is used only for County or approved purposes by persons with the authority to use such equipment and in accordance with FCC rules and regulations on County licensed radio frequencies. Willful interference with two-way radio communications is prohibited.

19. Posts current FCC licenses at their operator/dispatcher transmitter and control point and ensure proper operation of the transmitter as defined by FCC rules and regulations.

20. Notifies the CIO and CISO of any suspected violation of this policy immediately upon discovery and initiate appropriate disciplinary action.

21. Is responsible for the business risk of CTRs used to conduct the business of their Department.

22. Collaborates with the CISO to manage and mitigate risk as directed by the CISO.

C. Department Security Officer (DSO):

1. Is the primary security point of contact for the department and work under the direction of the CISO.

2. Understands the business risk of CTRs used to conduct the business of their department.

3. Train, or ensures the training of, department Authorized Users to understand and implement security rules and responsibilities and report training statistics annually to the Appointing Authority and CISO.

4. May define and conduct additional department-specific training or education to support this policy, as needed.

5. Assists in drafting, reviewing, implementing, and enforcing department and County information security plans, policies, standards, guidelines, procedures and requirements for the acceptable and secure acquisition, development, modification, operation and disposal of CTRs.

6. Identifies security issues related to department programs and CTR and monitor the department's compliance with all County security policies.

7. Reports and coordinates remediation of security incidents or violations.

D. Department Telecom Coordinator:

1. Implements written internal procedures and appropriate training to ensure County issued Mobile Devices are authorized, managed, and accounted for in the most cost-effective manner. These procedures will address:

   a. Employee eligibility for receiving a Mobile Device that is based on business needs and cost considerations.

   b. Service plan selection that is most cost-effective for business needs.

   c. Requests for Mobile Devices, upgrades, service changes, dispositions, and a documented approval process.

   d. Document, maintain, and submit to the Appointing Authority quarterly reviews of cellular voice and data usage reports to ensure that underutilized and/or unnecessary services are identified and promptly canceled.

   e. Document, maintain, and submit to the Appointing Authority quarterly reviews of service plan optimization analysis reports, along with current pricing models, to identify plans appropriate for conversion to more cost-effective plans.

   f. Monthly reviews of wireless carrier invoices to ensure that charges comply with contract pricing, service plan selections are correct, and that charges are correct. If correct, acknowledge within the TEMS.

   g. Maintaining accurate and current inventory records of Mobile Devices.

2. Ensures all Mobile Devices used for County business are currently supported by the device vendor (i.e. Apple and Samsung) and the operating system vendor (i.e. Apple and Android).

3. Replaces all County-sponsored Mobile Devices that are no longer supported by the device vendor or operating system vendor with current models as provided by approved County vendors.

E. IT Providers:

1. Install Malware protection software on all CTRs, ensuring that it is active and properly maintained within the departments they service.

2. Install and maintain software and systems to monitor, record and report computer usage; and to immediately restrict, disable, isolate or disconnect CTRs.

3. Must promptly remove Malware and isolate a CTR from the rest of the County Network upon detection of any unusual electronic activity.

4. Must immediately notify cybersecurity@maricopa.gov or 602-506-HELP of any unusual electronic activity or action to remediate.

F. The Maricopa County Chief Information Officer (CIO):

1. Appoints the County Telecom Coordinator.

2. Creates and maintains written documentation for the County Telecom Coordinator to implement the Mobile Device and BYOD programs. This documentation must specify the BYOD Stipend amounts.

3. Provides routine training and support to include reviews of cell phone plans, plan updates, billing statements/invoices, and usage for Authorized Users as requested by the Appointing Authority.

4. Coordinates enterprise technology usage requests.

5. Implements into production and maintains information security related technologies and services as directed by the CISO.

6. May authorize monitoring of Authorized User activity upon request from Human Resources or the Appointing Authority.

7. Coordinates the use of external resources, including civil or criminal investigators, to examine suspected violations of this policy, if necessary.

8. Ensures that security is integrated into all IT procurement and development efforts from the initial design phase onward.

9. May approve requests for Network Scans in the absence of the CISO.

10. Is responsible for and is authorized without restriction to obtain Federal Communications Commission (FCC) licenses for all County owned radio transmitters.

11. Review this policy on an annual basis.

G. The Maricopa County Chief Information Security Officer (CISO):

1. Establishes and enforces all County information security plans, policies, standards, guidelines, procedures and requirements for the acceptable and secure acquisition, development, modification, operation and disposal of CTRs.

2. Coordinates with all departments on the development of their own internal policies, standards, guidelines and procedures for acceptable and secure use and approve these as being in accordance with the baselines applied to the County.

3. Adjudicates and tracks exception requests to this policy for specific business requirements.

4. Approves any software, system or configuration for protecting against Malware prior to its use on an electronic device to access, process or store County Data.

5. Remediates, restricts, disables, isolates, or disconnects and adjudicates the use of any CTR and all Network traffic for security purposes, and coordinate with affected departments when taking such action.

6. Establishes a process for coordination and approval of Network Scans.

7. Is responsible for selecting, architecting, purchasing, and piloting all information security related technologies and services for the County.

8. Identifies and directs the mitigation of information security risks to CTRs to protect the confidentiality, integrity, and availability of information and resources of customers, business partners, employees, and the County.

9. Communicates business risk related to information security to County management including Appointing Authorities and the CIO.

H. Maricopa County Human Resources (HR):

1. Ensures this policy is included in the New Employee Orientation (NEO) process via the County LMS.

2. Ensures policy updates are distributed electronically to all employees via the County LMS.

VI. ADDENDUM

A. Maricopa County Technology Use Statement

The following statement must appear on all entry points into CTR, except guest internet access.

Maricopa County Technology Use Statement

By logging into and/or using Maricopa County Technology Resources, I acknowledge that I have read, understand, agree, and will comply with the current County policy, A2611 - Use of County Technology Resources. There is no expectation of privacy. My usage will be monitored for compliance and I accept all consequences associated with any misuse on my part.

B. Maricopa County Guest Internet Access Acceptance Statement

The following statement must appear for entry into County guest internet access.

Maricopa County Guest Internet Access Acceptance Statement

This internet access is provided as a courtesy to the guests of Maricopa County's facilities and its availability is not guaranteed. Use of County network resources for illegal, inappropriate, or obscene purposes, or in support of such activities is strictly prohibited. The County is able and reserves the right to monitor all traffic on the network at any time, without prior notice or warning to the user and may terminate access or discontinue service at any time, for any reason without warning. Acceptance implies understanding these restrictions of use and that there is no expectation of privacy.

Revision History

Version	Revision Date	Description of Revision
1	07-24-2019	Initial Version. Combines nine existing policies for efficiency, clarity, and updated language more consistent with other policies. Rescinds A1201 Telecommunication, A1202 Telephony, A1212 Requesting Telephone Detail Records, A1608 Electronic Mail, A1609 Acceptable Use of County Technology Resources, A1610 Malware, A1612 Mobile Device Usage, A1613 Bring Your Own Mobile Device, A2604 Software Copyright and License Compliance.
2	08-17-2020	In light of recent global events, it is important that the County has access to primary contact numbers of staff members to provide vital information in the event of an emergency. This policy revision requires all staff issued a County issued device or signed up for the BYOD program to include and maintain their cell phone number in ADP so that the County can send timely emergency communications.