Information Security Policy

Effective Date

This Information Security Policy is effective [Month] [Day], 2024.

For questions about this Information Security Policy, please email Cybersecurity@arapahoegov.com or contact the County Attorney's Office at (303) 795-4639.

1. Table of Contents

1. Introduction

A. Purpose

The purpose of this Information Security Policy ("policy") is to promote a risk-aware and secure enterprise culture and protect the County's technology devices and data from unauthorized access, breaches, and cyber threats.

B. Scope

This policy defines the mandatory minimum information security requirements for all departments/offices within Arapahoe County Government. Any department/office may, based on its individual business needs and specific legal and federal requirements, exceed the security requirements put forth in this policy, but must, at minimum, achieve the security levels required by this policy.

This policy defines the responsibilities of all County Department/Offices to:

- Protect and maintain the integrity and availability of data and related infrastructure assets.
- Protect information that is legally required to be kept confidential from unauthorized disclosure.
- Promptly report Technology Related Security Incidents, including the loss or theft of a County asset to the IT Service Desk.
- Manage the risk of security exposure or compromise.
- Ensure a secure and stable information technology (IT) environment and business continuity.
- Promote and increase the awareness of information security.

This policy applies to all County department and office employees, staff, and other workforce members including temporary and grant funded employees, volunteers and contractors while using the internet or technology to engage in County business and/or while using County Technology or County Data for any purpose.

C. Related Policies

The following is a non-exclusive list of related County policies:

- Acceptable Use Policy for Computing and Related Technology
- Securing and Disposing of Personal Identifying Information
- Social Media Policy
- Mobile Device Policy
- Cell Phone Policy

For copies of the above policies see:

http://inside.arapahoegov.com/319/County-Policies-and-Procedures

2. Employee Responsibilities

A. Password Management

1. System level and user level passwords must comply with the password requirements established by the IT Department.
2. The use of the same password for multiple accounts and services is strongly discouraged. The damage of a lost or stolen password must be limited to a single account.
3. County employees must not reveal the password for their county account under any circumstances, even to their supervisor. IT staff are prohibited from asking anyone for their password.
4. Any password loss or exposure must be promptly reported to the IT Service Desk so that accounts with lost or exposed passwords can be locked or have their passwords changed immediately.
5. County employees are encouraged to use an electronic password management application (password safe) to generate and store their passwords. Contact the IT Service Desk for a list of approved password management applications.
6. County employees are encouraged to enable Multi-Factor Authentication when creating website and software as a service (SaaS) accounts.

B. Email and Electronic Communication

1. County issued email addresses must be used for all County business. This includes creating accounts on websites for services that will be used by the County. Accounts created with non-County email addresses are difficult to recover.
2. County employees are not permitted to transmit restricted, non-public, personal, private, sensitive, or confidential County information to or from personal email accounts (e.g., Gmail, Hotmail, Yahoo) or use a personal email account to conduct County business.
3. County employees are required to exercise caution in the use of email, attachments, shared documents, text messages, chat sessions, and other electronic communication. These communications can be used by bad actors for malicious reasons and must be screened by the recipient for fraud. Examples: fake login prompts designed to harvest passwords; infected files or links to untrusted websites that could result in malware infection; and requests for information or actions that are not in the best interest of the County.
4. County employees are required to protect personal, private, sensitive, or confidential information (such as Personal Identifying Information (PII)) from unauthorized use or disclosure when transmitting an email outside of the organization through the process of encryption.
5. County employees may under no circumstances distribute, transmit, store, or delete any electronic communications, material or correspondence that is threatening, obscene, harassing, pornographic, offensive, defamatory, discriminatory, inflammatory, illegal, or intentionally false or inaccurate. Any concerns or issues should be reported to the respective supervisor, IT Service Desk, and Legal Department.

6. The IT Department employs advanced email filtering mechanisms as a proactive approach to identify, quarantine, and prevent delivery of emails that pose security risks to the County (e.g., phishing, malware distribution, spoofed emails, business email compromise, spam and unsolicited emails, Denial-of-Service (DoS) attacks, or attachment-based threats). Filtering criteria will focus on technical aspects of emails, such as attachments, links, and known malicious patterns.
7. The Information Technology Department manages the County's Microsoft 365 Exchange Online Mailbox limits including address book limits, mailbox capacity alerts, distribution group limits, inbox rule limits, mailbox folder limits, storage limits and message limits.

C. Personal Devices

1. Unapproved and non-County-owned devices (such as computers, mobile devices, hotspots, routers, iPads, tablets, etc.), are not allowed to connect to the County Network or County IT resource without proper IT Authorization. This does not include the Arapahoe County Public Guest Wireless Network.

D. Secure Device Settings

1. The default settings on computers and mobile devices are often not secure. The following settings will make County technology more resistant to unauthorized access, malware infection, and theft (the IT Department will centrally manage these settings wherever possible):
    a. Computers and mobile devices must be set up to screen lock automatically after a short period of inactivity.
    b. Computers and mobile devices must be set up to require a password, PIN, or biometric reading to unlock the device.
    c. Mobile devices must have encrypted storage enabled if possible.
    d. Security updates must be promptly applied to all County technology devices and mobile devices, and applications. Examples: County computers, laptops, mobile phones, and tablets.
    e. Computers must have security software (antivirus and local firewall) installed.
    f. Portable electronic storage devices such as thumb drives and hard disk enclosures must have encryption and password protection enabled.

E. Security Behavior

1. County employees are required to lock the screens of computers and mobile devices when leaving their workstations unattended to prevent unauthorized access and protect sensitive information.
2. Untrusted or unknown portable electronic storage devices such as thumb drives and hard disk enclosures must not be connected to County Technology. Those devices pose a significant threat of infecting the County with malware.

3. County employees must use caution when connecting County mobile devices to untrusted or public wireless networks. Communication on such networks is potentially subject to being monitored by unauthorized third parties.
4. The loss or theft of a personal device which is set up to access County Technology resources or a County issued computer or mobile device must be promptly reported to the IT Service Desk.
5. Any employee who will be traveling internationally, and will be traveling with a County owned laptop, mobile phone, or any other technology equipment must inform the IT Service Desk to ensure the security and integrity of our data and devices.
6. Any communication with the potential to harm the County must be promptly reported to the appropriate manager and the IT Service Desk to help safeguard our systems from harmful content.

F. Information Security Awareness Training

1. County employees, including those who are full-time, part-time, grant-funded, and temporary, who access County technology or the network, should be adequately informed and educated about security best practices to protect the confidentiality, integrity, and availability of County information and assets.
2. All County employees must complete the initial Security Awareness Training within 30 days of employment, or by the quarterly security awareness training due date.
3. Training may be delivered through online courses using Arapahoe Learns, in-person sessions, or a combination of both, as deemed appropriate by County leaders.
4. Training materials and content will be reviewed and updated regularly to stay current with emerging security threats and best practices.
5. The Information Security and Compliance Manager and designated personnel will maintain records of employee training completion.
6. Supervisors will monitor their employees' compliance with this policy and ensure that all eligible employees complete the required training.
7. Failure to complete required Security Awareness Training will be reported to the Department Director to take appropriate disciplinary action.

Refer to the Arapahoe County Acceptable Use Policy for Computers and Related Technology for further examples of permissible uses and prohibited uses of Arapahoe County Computing Equipment.

3. Administrator Responsibilities

Administrators are County employees that have elevated privileges to monitor and manage county systems, manage security setting, County Technology, and protect County Data. Because of this role, they have additional responsibilities.

A. Account Management

1. The IT Department is responsible for maintaining an account management system that provides employee accounts and enforces password requirements. Administrators must integrate the County Technology for which they are responsible with the account management system. This integration ensures that accounts are centrally managed and that employees do not have to maintain multiple usernames when technically feasible.
2. Accounts must be setup to require Multi-Factor Authentication wherever possible. Exceptions will be made where Multi-Factor Authentication is not compatible with the business purpose of the account.
3. PCs are setup to automatically log out after a period of inactivity.
4. Accounts must be assigned to an individual or service. Generic or multi-user accounts are prohibited unless approved by the IT Department. If a group of people need access to a system, an account must be created for each person in the group.
5. Administrators who manage accounts within an application must control the privileges associated with each account. Accounts with administrator privileges and other types of elevated permissions are to be provided only to meet a business need, to be revoked when no longer needed, and must be provided with an expiration date whenever possible.
6. Accounts with administrator privileges and other types of elevated permissions may only be used for the exact purpose for which those privileges were provided. Administrators must log out of accounts with administrator privileges before returning to non-administrator duties such as web browsing or reading email.

B. Inventories and Secure Settings

1. Administrators are required to maintain all inventory of all hardware and software for which they are responsible. County Technology that is unknown cannot be protected.
2. It is required that County Technology and specific data types classified by either protective or sensitive be set up to use encrypted storage and encrypted protocols.
3. Security logs must be enabled on County Technology wherever possible.
4. Administrators are required to manage the application of security updates to the County Technology for which they are responsible. The IT Department will centrally manage the application of security updates for County-issued computers and mobile devices.
5. When decommissioning County Technology, storage media must be irreversibly erased prior to physical disposal.
6. County Technology which is externally accessible or subject to regulatory requirements is required to undergo security assessment before being put into production. Security Assessments are facilitated by the IT Security Team and StateRAMP.
7. Systems which are unauthorized, unsupported, or outdated are a significant risk to the County. The IT Department may seek to remove or apply restrictive safeguards to such systems to protect the environment.
8. All software and hardware belonging to the County including software services, such as web presence; customer relations; accounting; tax assessments; benefits enrollment; records

management; geographic information (GIS); point of sale; or asset management and network connected hardware such as building energy systems; door card and gate access; credit card readers; environmental sensors; traffic signals; cameras, must adhere to updates issued by the County and/or vendor recommendations.

4. Confidential Information

A. General

Each County department and office is responsible for knowing and understanding the laws and regulations that govern the confidentiality of the information stored or used by such department or office. Information which is required to be kept confidential by law or regulation must be kept secure and safe from unauthorized access in strict compliance with the law or regulation. Questions as to the applicability of legal confidentiality requirements to specific information should be addressed to the County Attorney's Office.

B. Applicable Laws

Below are examples of some of the more widely applicable laws that require confidentiality with respect to certain information:

- Protection of Personal Identifying Information, C.R.S. Section 24-73-102
- Colorado Open Records Act (CORA), C.R.S. Section 24-72-201 et seq.
- Colorado Criminal Justice Records Act (CCJRA), C.R.S. Section 24-72-301 et seq.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations, 45 C.F.R. Parts 160, 162 and 164
- Address Confidentiality Program (domestic violence victims), C.R.S. § 24-30-2102 et seq.

C. Personal Identifying Information

All offices and departments are required by state law to maintain the confidentiality of Personal Identifying Information ("PII") and to destroy such information when no longer needed. See the definition of Personal Identifying Information in the definitions section below for a description of the types of information that are considered PII. For the County's policy regarding PII please also refer to the document titled "Securing and Disposing of Personal Identifying Information" at http://inside.arapahoegov.com/319/County-Policies-and-Procedures

D. Access Controls

Effective internal (i.e., between County staff) and external (i.e., with non-County staff) data sharing is crucial for accountability, accessibility, inclusivity, and integrity. Sharing methods should be regularly reviewed to ensure they are secure and reliable. The Information Technology (IT) Department can assist with recommending and setting up secure methods for sharing confidential data with internal and external parties.

1. Sharing Confidential Data

   Internal Sharing: Participants in the sharing of confidential data are required to use sharing methods that do not create copies of the data outside of the system record. The best way to accomplish this is to link to the system of record. Sharing confidential data through unprotected methods, such as email, puts that data and the County at significant risk.

   External Sharing: Sharing of confidential data requires a written and signed agreement. These documents should clearly define the expectations and responsibilities of each entity to safeguard County data and the penalties if they fail to do so. In all cases, it is required that each non-County staff person handling the data sign an executed Non-Disclosure Agreement (NDA). Participants in confidential data sharing are required to select secure and encrypted methods such as those described in ***Section E, Data Transmission***.

2. Sharing Sensitive Data

   Internal Sharing: Participants in the sharing of data that is sensitive (but not legally confidential) are encouraged to select sharing methods that do not create copies of the data outside of the system of record. The best way to accomplish this is to the link to the system of record. Sharing sensitive data through unprotected methods, such as email, puts that data and the County at significant risk.

   External Sharing: External sharing of any sensitive data may require a written and signed agreement. These documents should clearly define the expectations and responsibilities of each entity to safeguard County data and the penalties if they fail to do so. In all cases, it is required that each non-County staff person handling the data sign an executed Non-Disclosure Agreement (NDA). Participants in Sensitive Data sharing are required to select secure and encrypted methods such as those described in ***Section E, Data Transmission***.

E. Encryption Standards

County data must be transmitted using methods appropriate to the confidentiality or sensitivity of the data. Departments/offices with questions about which method is most appropriate should work with the IT Business Relations Department, and Information Security Manager, to make that determination.

Sharing County data using informal methods, such as email, puts that data at significant risk. Secure and encrypted data sharing mechanisms include Office 365 external file sharing, secure file transfer protocol (SFTP), or an IT-approved application programming interface (API).

F. Data Ownership/Privacy/Public Records

All information or data contained or stored in or on any County Computing Resources including email and other communication systems is the property of the County. Any information or data contained or stored in or on any County Computing Resources is always available to the County and its authorized elected and appointed officials, employees, agents or other representatives, and employees, officials and other users shall have no expectation of privacy with respect to such information or data. All employees and officials should be aware that information and data contained on networks, data storage devices or services, computers, cell phones, including correspondence in the form of e-mail or messaging systems, may be considered public records subject to public disclosure pursuant to the Colorado Open Records Act, C.R.S. 24-72-201, et

seq. or the Colorado Criminal Justice Records Act, C.R.S. 24-72-301, et seq. The Arapahoe County Information Technology Director is the official custodian of e-mail and other electronic messages. If such information is requested and it is determined that it is a public record available for inspection, it will be released for public review. Please refer to the County's Public Records Policy for more information regarding public records requests and consult with the County Attorney's Office if there are questions.

5. Information Security Management

A. Software as a Service

1. Arapahoe County is committed to protecting the security of its technology and data. For this reason, the County follows all federal and state standards to ensure compliance with all applicable laws and regulatory requirements.
2. Any Software as a Service (SaaS) that supports County business functions must appropriately be managed for information risk and undergo risk assessments before procurement and, contract renewal.
3. Arapahoe County uses StateRAMP as its risk and authorization management program.
4. Any SaaS provider that transmits, stores, and/or processes confidential or sensitive data is required to:
    a. Provide proof of a current StateRAMP Authorized or Provisional status in the form of a StateRAMP letter; or
    b. Provide proof of current StateRAMP Ready or Authorized status in the form of a StateRAMP letter; or
    c. Provide a valid StateRAMP Security Snapshot Score, and proof of enrollment in the StateRAMP Progressing Security Snapshot Program; and has 18 months to become StateRAMP Ready, and 24 months to become StateRAMP Authorized.

B. Information Security Incident Management and Reporting

Any County employee who observes or suspects information security incidents or weaknesses including suspected data security or privacy concerns, including the theft, loss, or unauthorized disclosure of Arapahoe County proprietary information, should promptly report the incident to appropriate management, ITServiceDesk@arapahoegov.com and ITCybersecurity@arapahoegov.com as quickly as possible. Incidents will be handled and documented according to the Technology Security Incident Handling Procedure. The procedure includes a mechanism for escalating the incident to local or federal law enforcement when necessary.

For all HIPAA related Privacy and Security questions and concerns, please email HIPAAcompliance@arapahoegov.com , contact the County Attorney's Office at (303) 795-4639 or refer to the *Arapahoe County Administrative Policies: HIPAA Policies and Procedures.*

C. Remote Access

Any requests to provide remote digital access granted to the County's connected partners, volunteers, contractors, subcontractors, and consultants must be documented and approved by the IT Department. Vendors will have a restricted VPN provisioned. Remote Access can be

obtained through consulting with the appropriate Infrastructure Team by contacting the IT Service Desk.

6. Definitions

Administrator

A person within a department or office who has the primary responsible for running and managing the day-to-day operations of IT software or hardware. Examples of both are set forth below.

Software Administrator examples: County employees who administer software services, such as web presence; customer relations; accounting; tax assessments; benefits enrollment; records management; geographic information (GIS); point of sale; or asset management.

Hardware Administrator examples: County employees who administer network connected hardware such as personal computers, servers, data storage devices, building energy systems; door card and gate access; credit card readers; environmental sensors; traffic signals; cameras.

Attachment-based Threats

Malicious attachments in emails that can contain exploits, scripts, or executable files that compromise the recipient's system.

Baiting

Baiting is the use of a false promise to lure the end-user into a trap, including enticing ads that lead to malicious sites or encourage users to download a malware-infected application.

Business Email Compromise (BEC)

Business Email Compromise involves attackers gaining access to a business email account and using it to impersonate an executive or employee for fraudulent purposes.

Confidentiality

Ensuring that information is not made available or disclosed to unauthorized persons or entities.

County Data

Information, whether quantitative or qualitative, that is regularly used by, maintained by, created by or on behalf of, and possessed, owned, or licensed by the County. Data are an asset independent of the systems or formats in which they reside.

County Technology

Technology devices, software, website accounts, knowledge, resources, techniques, and access which are used to conduct Arapahoe County Government business. Examples include County accounts; security groups; access badges/cards; email; databases; storage; cloud storage; applications; cloud applications; computers; mobile devices; networks; and network hardware.

For more information, refer to Arapahoe County's Acceptable Use Policy for Computers and Related Technology.

Data

Information that is in a form that can be processed by a computer.

Data Breach

A data breach is the unauthorized acquisition of data by a person, commercial entity, or governmental entity.

Data Processing

A series of operations on data to retrieve, transform, or classify information, oftentimes manipulating it to produce meaningful information.

Deepfake Technology

Deepfake technology refers to the use of artificial intelligence (AI) and machine learning techniques, to create or manipulate digital content, typically videos or audio recordings, to depict individuals saying or doing things they never said or did. These manipulated media files are often incredibly realistic, making it challenging to distinguish between altered content and authentic recordings.

Denial-of-Service (DoS) Attacks

Denial-of-Service attacks on email servers or network endpoints involve overwhelming the devices with a high volume of traffic, rendering it unavailable for legitimate users.

Email Spoofing

Email Spoofing involves forging the sender's email address to make it appear as if the message is from a trusted source. Email spoofing is often used in phishing attacks, where attackers attempt to trick recipients into believing that the email is from a legitimate source to steal sensitive information or deliver malware.

Encryption

The process of converting data into a code. Data converted in this way can be stored and moved more economically and is more resistant to unauthorized access.

Malware

Malicious software (malware), including viruses, worms, and ransomware, which can be distributed through email attachments or links. Opening these attachments or clicking on links can infect the user's and county systems.

Metadata

Information describing the characteristics of data including structural metadata describing data structures (e.g., data format, syntax, and semantics), descriptive metadata describing data contents (e.g., address, date of birth), and specific acceptable uses or constraints on data use (e.g., data classification).

Multi-Factor Authentication

A login procedure requiring a username, password, and one or more additional elements. Accounts with Multi-Factor Authentication enabled are more resistant to unauthorized access.

Examples of additional elements: biometric markers such as fingerprint and retinal scans; access codes generated by a mobile application; or the presence of a trusted device.

Personal Identifying Information (PII)

Personal identifying information or data that is defined by state law as protected and confidential. It includes the following:

- social security numbers
- official state or government driver's license numbers or identification card numbers
- passport identification numbers
- employer, student, or military identification numbers
- biometric data (e.g., fingerprints, iris recognition, retinal scans)
- credit cards, banking cards debit cards, electronic fund transfer cards, or guaranteed check cards or numbers from such cards
- account numbers representing financial accounts or affecting financial interests, standing, or obligation of or to an account holder, that can be used to obtain cash, goods, property, or services or to make financial payments; but this does *not* include a "check", a "negotiable order of withdrawal" or a "share draft."

Phishing

Phishing is a digital form of social engineering that uses authentic-looking emails to trick users into sharing personal information. It usually includes a link that takes the user to a fake website. If you cannot verify the source, do not open the link.

Pretexting and Impersonation

Pretexting and Impersonation is where an attacker creates a fictional backstory that is used to manipulate someone into providing private information or to influence behavior. Attackers will often impersonate a person of authority, co-worker, or trusted organization to engage in back-and-forth communication prior to launching a targeted spear phishing attack.

Security Incident

An event during which the confidentiality, integrity, or availability of information (or an information system) has been compromised.

Security Controls

Security Controls are safeguards applied to an information system or organization designed to protect confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Spam

Spam refers to the unwanted, irrelevant, or unsolicited messages, typically sent over the internet, via email. These messages are often sent in bulk to a large number of recipients without their explicit consent.

Technology Devices

Equipment which contains one or more of the following elements: a computer; wired or wireless network interface; or digital storage. This includes an emulation of such equipment provided through virtualization or cloud services.

Examples: servers; personal computers; laptops; tablets; mobile phones; iPads; hard drives; thumb drives; printers; scanners; fax machines; digital cameras; modems; routers; switches; hubs; wireless access points (WAP); industrial control systems (ICS); sensors; and "internet of things" devices.

Emulation examples: virtual servers; application containers; cloud hosted services; software as a service; and infrastructure as a service.

Technology Related Security Incident

Any situation which harms or has the potential to harm residents, property, County employees, or Arapahoe County Government which is specifically related to County Technology or County Data, and which is not appropriate for referral to law enforcement.

Examples: unauthorized access, theft, or loss of County Technology or County Data; password exposure; fraudulent email, voice, or other electronic communication; evidence of malicious software or hardware; denial of service.

Security Controls are safeguards applied to an information system or organization designed to protect confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

7. Compliance and Enforcement

A. Compliance Measurement

The IT Department may monitor compliance with this policy using software and network security tools; incident investigations; internal and external audits; intelligence reports from external agencies; and reports made to the IT Department.

B. Non-Compliance

The Director of the IT Department is responsible for overall compliance with this policy. Any enforcement actions will be imposed in coordination with individual elected offices and departments (disciplinary action requires approval of the employee's office or department). Non-compliance may result in the imposition of additional training requirements, restrictions on access, or disciplinary action up to and including termination of employment or vendor contract.

8. Revision History

Date	Description of Change	Name
10/23/2023	New Document	Nikki Rosecrans
11/15/2023	Peer Reviewed document	Brian Gilpatrick and Nikki Rosecrans
12/26/2023	Director Review	Philip Savino
1/01/2024	Revised Document to update with Directors changes	Nikki Rosecrans
01/31/2024	Added additional information to the document	Nikki Rosecrans
04/03/2024	County Attorney Review	Ron Carl