RESOLUTION NO. 24-41

THE BOARD OF COUNTY COMMISSIONERS
OF HUERFANO COUNTY, COLORADO

A RESOLUTION TO ADOPT AN INFORMATION SECURITY POLICY

WHEREAS, the Board of County Commissioners recognizes the importance of managing risks to the County including those risks to information systems and the data contained therein; and,

WHEREAS, C.R.S. § 30-11-103, as amended, provides that the Board of County Commissioners shall exercise the powers of a County as a body politic and corporate; and,

WHEREAS, C.R.S. § 30-11-107(1)(a), as amended, provides that the Board of County Commissioners has the power at any meeting to make such orders concerning the property belonging to the County as it deems expedient; and,

WHEREAS, C.R.S. § 30-11-107(1)(e), as amended, provides that the Board of County Commissioners has the power at any meeting to represent the county and have the care of the county property and the management of the business and concerns of the county in all cases where no other provisions are made by law; and,

WHEREAS, the Board of County Commissioners deems it necessary and appropriate to adopt a policy for the protection of information, as required by state and federal law.

NOW, THEREFORE, BE IT RESOLVED by the Board of County Commissioners of Huerfano County, Colorado that the following are hereby adopted:

Section 1. Purpose.

1. The purpose of these policies are to provide direction for effectively and efficiently managing the risks to Huerfano County Government's information assets against accidental or malicious disclosure, modification or destruction whether internal or external, deliberate, or accidental.
2. Security is critical to the organization's survival. This policy also defines the access controls that must be put into place to protect information by controlling who has the right to access the information assets, whether it is actual data, the hardware on which the data resides, or the application software used to manipulate data on systems installed throughout the County.
3. This policy acts as an umbrella document to all other security policies and associated standards.

Section 2. Scope.

This policy applies to:

1. All systems, automated and manual, for which the County has administrative responsibility, including systems managed or hosted by third parties on behalf of

the County. It addresses all information, regardless of the form or format, which is created or used in support of business activities.
2. All facilities and property owned by the County as well as all elected officials, employees, volunteers, or contractors of the County.

Section 3. Authority and Responsibility

1. The Board of County Commissioners bears the ultimate authority and responsibility for Huerfano County Government's information security. As such, the Board has established this Policy and directs Huerfano County Government personnel to implement these policies as follows:
    a. The County Administrator shall approve and enforce all security policies and associated standards under the umbrella of this policy.
    b. The County Administrator shall designate the Information Security Officer to provide the direction and technical expertise to ensure that Huerfano County Government's information is properly protected.
    c. There is hereby created an Information Security Committee consisting of the County Administrator, Emergency Manager, and the Information Security Officer.
    d. There is hereby created an Information Security Policy Group consisting of all County Elected Officials, the County Attorney, Emergency Manager, and the County Administrator.
2. All Huerfano County Department Heads and County Elected Officials are directly responsible for implementing these policies and any security policies and associated standards under the umbrella of this policy developed by the Information Security Officer, and approved by the County Administrator, within their areas of responsibility and for adherence by their staff.
3. Any appeals of decisions based on this policy shall be made to the Board.

Section 4. Information Security Program

1. The Information Security Program is a set of policies, procedures, and guidelines that help an organization protect its data and information. The Information Security Committee is responsible for the overall governance of the County's Information Security Program and will consult with the Information Security Policy Group on decisions, policies, and standards.
2. The Information Security Officer shall develop and maintain a County Cybersecurity Policy that provides minimum requirements, standards, and protective measures for all information and systems that transmit, receive, or store confidential, sensitive, internal use, or public use information regardless of electronic or digital media format, processing method, or platform, for or interactive with Huerfano County unless otherwise determined.
3. Any such County Cybersecurity Policy should be developed in consultation with the Information Security Policy Group and use the National Institute of Standards and Technology (NIST) Cybersecurity Framework as a guide as far as practicable.
4. Any system or process that supports business functions must be appropriately managed for information risk and undergo information risk assessments, at a minimum annually, as part of a secure system development life cycle.
5. County information and systems are the property of the Huerfano County Government and are intended for official government use only. Huerfano County shall retain property rights to all information created, generated, replicated,

processed, stored, transmitted, and received by users in the course of using County systems and software.

6. Huerfano County information systems transmit, receive, process, and store information that shall be protected according to federal, state, and local laws and regulations. The development of specific policy for County agencies shall take into consideration those laws and regulatory issues applicable to the operating environments.

Section 5. Physical Security

1. Physical security and access control are part of the County's Information Security Program in that the County must provide adequate safeguards to avoid damage or unauthorized access to confidential data and information assets. All physical security systems must comply with applicable regulations including, but not limited to, building and fire prevention codes.
2. The Information Security Program includes the design and implementation of physical security perimeters, such as walls and controlled entrances, to protect areas that contain confidential data and information assets.
3. Where feasible the Information Security Program enforces physical access controls and maintains an audit trail of access.
4. Elected Officials and Department Heads work with the Information Security Committee to designate areas as secured.
5. Access to secured areas must be granted only to County support personnel and contractors whose job responsibilities require access to that area. The process for granting access to a secured area must include the approval of the person responsible for the area.
    a. Access cards and/or keys must not be shared or loaned to others.
    b. Access cards and/or keys that are no longer required must be returned to either Human Resources or the Information Security Officer. Cards shall not be reallocated to another individual bypassing the return process.
    c. Lost or stolen access cards and/or keys must be reported to the Information Security Officer.
    d. A service charge may be assessed for access cards and/or keys that are lost, stolen or are not returned.
    e. The Information Security Officer must remove the card and/or key access rights of individuals who change roles within the County or are separated from their relationship with the County.
6. Visitors must be escorted in secured areas.

Section 6. Data Access

1. The Information Security Program includes requirements to manage and control access to information assets and information service in support of compliance with legal regulations (e.g., HIPAA, PII, data retention) and to protect and lower risk to business operations.
    a. Access to any information system that has security risks requires authentication by user-id or password, biometric system, multi-factor authentication or other mechanism which minimizes unauthorized access to or alteration of the County's data. The Information Security Officer shall approve the appropriate authentication method.
    b. Any password or token used to authenticate a person or process must be treated as confidential and protected appropriately. Passwords or tokens

must not be stored on paper, or in an electronic file, hand-held device or browser, unless they can be stored securely and the method of storing has been approved by the Information Security Officer.

c. The Information Security Officer shall document and maintain appropriate standards for the creation, size, style and expiration period of passwords. All data users shall follow the standards.

2. The Information Security Program is based upon the fundamental principles of information and system ownership and the legal obligations and requirements for protecting information and systems.
    a. A System Owner or Data Custodian is the county official designated as being in responsible change of a given data system.
    b. Formal user access control procedures must be documented, implemented and kept up to date by the Data Custodian for each application and information system to ensure authorized user access only. Data Custodians shall allocate access rights and permissions for each user to computer systems and data that are commensurate with the task they are expected to perform. Users will not be granted access to information that is unnecessary for the performance of their tasks. The system's Data Custodian is responsible for determining the appropriate authorization levels for each data user.
    c. The Information Security Officer shall serve as the initial Data Custodian for the computer systems owned by the County, but may assign an appropriate Data Custodian for any given computer system.
    d. The Data Custodians and Information Security Officer are responsible for safeguarding information assets and information service from unauthorized permanent deletion of County information by system users.
    e. Permanent deletion of County information shall require prior, auditable authorization from either the related Data Custodian, the Information Security Officer, or the County Administrator.
3. The Information Security Program includes requirements to ensure the security of remote access to the County's network in order to protect confidential data and information assets.
    a. Advance approval for any remote access connection must be provided by the Information Security Officer. An assessment must be performed and documented to determine the scope and method of access, the technical and business risks involved and the contractual, process and technical controls required for such connection to take place.
    b. All remote connections must be made through managed points-of-entry reviewed by the Information Security Officer.

Section 7. Separation of Duties

1. To reduce the risk of accidental or deliberate system misuse, separation of duties and areas of responsibility must be implemented where appropriate.
2. Whenever separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision.
3. The audit and approval of security controls must always remain independent and segregated from the implementation of security controls.

Section 8. Non-Compliance and Disciplinary Action

1. Individuals and/or firms contracted with the County who engage in the misuse of County data, whether through negligence or deliberate action, may be considered in breach of contract and may be subject to appropriate legal action upon review of violation severity and applicable legal statutes. Other consequences may involve the removal of access rights, special system privileges, and/or complete removal of system access.
2. Non-compliance with this Policy by Huerfano County employees and system users is a serious matter and will be dealt with accordingly on a case-by-case basis. Depending on the severity of violations and applicable legal statutes, consequences could result in removal of access rights and special system privileges, removal of system access, or, for County employees, disciplinary action to include potential termination of employment. In severe cases of misuse or abuse such as, fraud, improper data destruction, or breach of privacy laws, legal action may be taken.

BE IT FURTHER RESOLVED that this resolution shall be in effect upon its adoption. All resolutions and portions of resolutions in conflict with the above are hereby repealed.

INTRODUCED, READ, APPROVED AND ADOPTED ON THIS 22nd day of OCTOBER 2024.

BOARD OF COUNTY COMMISSIONERS
OF HUERFANO COUNTY, COLORADO

BY_____
Arica Andreatta, Chairman

_____
Karl Sporleder, Commissioner

ATTEST:

_____
County Clerk and Recorder and
Ex-Officio Clerk to said Board

_____
Mitchell Wardell, Commissioner