Grand County
Colorado

INFORMATION SECURITY MANUAL

Approved and adopted by Grand County Board of County Commissioners through Resolution Number 2021-3-23

Table of Contents

(THE REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK)

1 INTRODUCTION

1.1 Statement of Purpose

The purpose of this manual is to establish and maintain a uniform system for managing information security; to comply with applicable laws; and to provide for an information security standard for Grand County in a clear and comprehensive manner to maximize the efficiency and effectiveness of operations. It is further intended by adoption and periodic amendments of these policies that they serve as a guide for County employees in their routine work activities, relationships, and interactions.

THE POLICIES OUTLINED IN THIS MANUAL ARE SUBJECT TO CHANGE OR REVISION AT ANY TIME, WITH OR WITHOUT NOTICE, AS MAY BE DEEMED NECESSARY BY THE BOARD OF COUNTY COMMISSIONERS. THEREFORE, THIS MANUAL IS NOT INTENDED TO BE, NOR DOES IT CONSTITUTE, A CONTRACT BETWEEN THE COUNTY AND ANY OF ITS EMPLOYEES.

1.2 Statement of Applicability

The policies and procedures outlined in this manual apply to all County employees unless otherwise indicated. The ultimate authority for interpretation, application, and enforcement of these policies rests with the Board of County Commissioners, County Manager, and Chief Information Security Officer (CISO), and appropriate elected or appointed officials. The Chief Information Security Officer may be contacted regarding questions or concerns regarding interpretation of these policies.

1.3 Prior Policies and Procedures

The policies and procedures contained in this manual supersede all prior County information security policies and procedures and apply to all County departments and employees, unless otherwise indicated.

1.4 Employee Acknowledgement

Employees must acknowledge annually that they are aware a copy of the policy is available and have reviewed the policies.

1.5 Disclaimer

Each section of this Information Security Manual is to be considered separately, and a change in one section does not invalidate any remaining sections of the manual.

1.6 Conflict with State or Federal Laws

In the event there is a conflict with a State or Federal law, the applicable law prevails and notification of such conflict will be submitted to the Chief Information Security Officer for resolution.

1.7 Additional Departmental Policies

County employees function under a wide variety of conditions and circumstances. It is anticipated that some departments may need to supplement this manual with Appointed Official/Elected Official instituted policies (Supplemental Policies) to meet the specific needs of that department. Where possible this manual should be updated instead of the use of a supplemental policy. Any proposed supplemental information security policies may be reviewed and must be placed on file with the County Manager and Chief Information Security Officer. Supplemental policies instituted by the department may not contradict policies contained in this manual. If differences occur, this manual supersedes supplemental policies.

1.8 Amendment Procedures

The County reserves the right to modify, revoke, suspend, terminate, or otherwise change any of these policies and procedures, in whole or in part, at any time, at the County's sole discretion.

Amendments to the information security manual may be proposed by any employee, Elected Official or Appointed Official. Any proposed amendment must be submitted in written form to the County Manager, County Attorney and Chief Information Security Officer for review regarding appropriateness, cost, legality, consistency in relation to current provisions, and other relevant practices and regulations.

Following review and comment, the Board of County Commissioners will:

a) Reject the proposed amendment; or
b) Adopt the amendment as presented or with amendments.

The decision of the Board of County Commissioners is final.

2 ADMINISTRATION

2.1 Information Security Policy Interpretation

The Chief Information Security Officer may be contacted regarding questions or concerns regarding interpretation of these policies. All County personnel in the capacity of a supervisory position (Elected, Appointed, or otherwise) are responsible for the day-to-day administration of the provisions in this information security manual and are obligated to report promptly any discrepancies or violations to the County Manager and Chief Information Security Officer.

2.2 Chief Information Security Officer

If any County personnel disagree with the interpretation by the Chief Information Security Officer, they and the Chief Information Security Officer shall, on an informal basis, attempt to reconcile their differences of opinion. In the event the differences cannot be reconciled, the matter will be presented to the County Manager.

2.3 County Manager

If any Appointed Official disagrees with the interpretation by the County Manager, they and the County Manager shall, on an informal basis, attempt to reconcile their differences of opinion.

The County Manager may report any continuing or willful disregard of these policies and procedures to the Board of County Commissioners.

2.4 Board of County Commissioners

Under its administrative and legislative powers, information security policies and procedures of the County are adopted or revised by the Board of County Commissioners. Departments with Elected Officials requires that the chief Elected Official endorse these Information Security Policies. The Board of County Commissioners may take whatever action it deems appropriate and legal to gain compliance with this information security manual. The decision of the Board of County Commissioners as to the meaning of any of the provisions of these policies and procedures shall be final.

2.5 Elected Officials and Administrative Boards

This manual is not intended to supersede authority of the Board of County Commissioners, other Elected Officials, or administrative boards as is provided by the constitution and statutes of the State of Colorado or federal law.

2.6 Managers and Appointed Officials

In the administration of the provisions of this manual, it is understood that Managers and Appointed Officials will delegate functions and duties to employees under their supervision.

2.7 Information Systems Department

The Information Systems Department, under the direction of the Chief Information Security Officer, will maintain a repository of all information security policies.

3 GOVERNANCE AND OVERSIGHT POLICY

3.1 Statement of Purpose

The purpose of this policy is to provide guidelines for governance and oversight of privacy and security matters.

3.2 Statement of Applicability

This policy covers Grand County information security and privacy practices across all departments and business units. All Grand County workforce members are required to comply with this policy.

3.3 Regulatory Compliance

1. Grand County is committed to conducting business in compliance with all applicable laws and Grand County policies.
2. Grand County is committed to compliance with the regulatory requirements established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and all subsequent updates.
3. Grand County is committed to compliance with the Criminal Justice Information Services (CJIS) Security Policy which integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) and nationally recognized guidance from the National Institute of Standards and Technology (NIST).
4. Grand County is committed to compliance with all state-level regulatory compliance requirements that apply to its area of operations.

3.4 Commitment to Information Security and Privacy

1. Senior leadership actively supports information security and privacy within Grand County through clear direction, demonstrated commitment, incorporation into strategic planning, and acknowledgment of information security and privacy responsibilities.
2. Capital planning and investment requests will show consideration for information security and privacy.

3.5 Privacy and Security Council Charter

1. A Privacy and Security Council (Council) is established as the governing and decision-making body.
2. The members of the Council consist of:
    a. Board of County Commissioners
    b. County Manager
    c. Chief Information Security Officer
    d. Clerk & Recorder
    e. County Attorney
    f. EMS Chief
    g. Human Resources Director
    h. Human Services Director
    i. Office of Emergency Management
    j. Public Health Director
    k. Sheriff

l. Treasurer

3. To fulfill its obligations under Grand County policies, the Council meets on a regular basis and a simple majority of the Council exists at each meeting.
4. A member of the Council may appoint a designee on an extended or temporary basis.
5. The Council may add additional individuals as it deems necessary and appropriate.

3.6 Privacy and Security Council Responsibilities

1. The Council is responsible for the management and oversight of Grand County policies, including, but not necessarily limited to development, approval, implementation, review and periodic updating of policies.
2. Policies under the Council's responsibilities will subject to the following controls:
    a. The policy documents state the purpose and scope of the policy, describe roles and responsibilities as applicable, and establish Grand County's approach to managing information security and privacy.
    b. The policies are published, communicated, and disseminated to all workforce members.
    c. The policies are subject to the Record Retention Policy.
3. The Council reviews Grand County policies at least annually and makes updates as needed.
    d. The policy review includes assessing opportunities for improvement of the policy and Grand County's approach to managing changes related to the organization's environment, business circumstances, legal conditions or technical environment.
4. The Council will define and implement a process that allows for individuals to make complaints concerning policies and procedure or Grand County's compliance with the policies and procedures. Complaints and requests for changes will be document, including the disposition.
5. The Council reviews privacy and information security practices at least annually.
6. The Council will be informed of privacy and information security projects.
7. The Council will be informed of audit results, statistics and trends.

3.7 Information Security and Privacy Coordination

1. Protecting Grand County confidential data and reducing information security risks is the responsibility of all Grand County workforce members. These risk reduction activities are coordinated and communicated by representatives from different parts of Grand County respective to their roles and job functions.
2. An internal privacy information sharing mechanism exists to communicate non-conformities and lessons learned to senior leadership.

3.8 Information Security and Privacy Responsibilities

1. All information security and privacy responsibilities are formally defined in writing in the Information Security and Privacy Roles and Responsibilities Standard.
2. The CISO and County Manager are senior-level employees.

3.9 Review of Information Security

1. Grand County's approach to managing information security and its implementation control objectives, controls, policies, processes, and procedures is reviewed annually, or when significant changes occur.
2. The review is carried out by individuals with the necessary expertise.
3. When an independent external review is conducted, the organization conducting the review will generate a corrective action plan that is reported to senior leadership and the CISO.

3.10 Policy References

3.10.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(a)(2), CFR TITLE 45 § 164.308(a)(1)(i), CFR TITLE 45 § 164.308(a)(1)(ii)(A), CFR TITLE 45 § 164.308(a)(1)(ii)(B), CFR TITLE 45 § 164.308(a)(1)(ii)(D), CFR TITLE 45 § 164.308(a)(2), CFR TITLE 45 § 164.308(a)(5)(ii)(A), CFR TITLE 45 § 164.308(a)(8), CFR TITLE 45 § 164.310(a)(2)(ii), CFR TITLE 45 § 164.312(c)(1), CFR TITLE 45 § 164.316, CFR TITLE 45 § 164.316(a), CFR TITLE 45 § 164.316(b)(1), CFR TITLE 45 § 164.316(b)(1)(i), CFR TITLE 45 § 164.316(b)(2)(iii), CFR TITLE 45 § 164.316(b)(2)(iii), CFR TITLE 45 § 164.414(a), CFR TITLE 45 § 164.530(a), CFR TITLE 45 § 164.530(i), CFR TITLE 45 § 164.530(h)

3.10.2 NIST References

NIST SP 800-53 R4 AR-1, NIST SP 800-53 R4 AR-2, NIST SP 800-53 R4 PM-11, NIST SP 800-53 R4 PM-4, NIST SP 800-53 R4 PM-9, NIST SP 800-53 R4 RA-1, NIST SP 800-53 R4 RA-3, NIST SP 800-53 R4 CA-2, NIST SP 800-53 R4 CA-2(1), NIST SP 800-53 R4 CA-5, NIST SP 800-53 R4 CA-5(1), NIST SP 800-53 R4 PM-4, NIST SP 800-53 R4 CM-3

4 DATA CLASSIFICATION AND HANDLING POLICY

4.1 Statement of Purpose

The purpose of this policy is to establish a framework for classifying data in the possession of Grand County and to define the baseline security controls for handling and safeguarding such data in accordance with this classification category.

The purpose of this policy is to establish the minimum-security controls for handling, labeling and storing Grand County data to protect the data from unauthorized disclosure or misuse.

4.2 Statement of Applicability

All workforce members who may have access or exposure to Grand County data are required to comply with this policy. Such data may be in electronic and/or hardcopy formats and are generated or used as part of Grand County's business operations whether on Grand County owned or managed systems or on third party hosted systems on behalf of Grand County.

4.3 Classification of Data

Grand County Elected Officials and Department heads are designated as Data Owner's and accountable for their departments data that is transmitted, used, and stored on a system. All Grand County data is classified into one of three sensitivity levels (tiers):

- Tier 1: Confidential Data
- Tier 2: Internal Only Data
- Tier 3: Public Data

4.4 Tier 1: Confidential Data

1. Based on state, federal, and contractual requirements, personally identifiable information (PII), criminal justice information (CJI), and protected health information (PHI) covered under HIPAA is defined as confidential data and must be protected.
2. Data is classified as confidential data when the unauthorized disclosure, alteration or destruction of that data causes a significant level of risk for unauthorized disclosure or misuse.
3. The highest level of security controls is applied to confidential data. Access to confidential data must be controlled from creation to destruction. Access will only be granted to those persons who require such access in order to perform their job ("need-to-know") in accordance with the

principle of least privilege. Access to confidential data may be authorized to groups of persons based on job classification or responsibilities ("role-based" access).
4. Access to confidential data must be authorized by the data owner who is responsible for the data.
5. Publicly accessible computers shall not be used to access, process, store, or transmit CJI.
6. The storage of CJI, regardless of encryption status, shall only be permitted in environments which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada).

4.4.1 Tier 1: Confidential Data Examples

1. Data protected by state or federal regulations including:
   a. Protected Health Information (PHI)
   b. Personally Identifiable Information (PII)
   c. Criminal Justice Information (CJI)
   d. Social Security Numbers (SSN)
   e. Payment Card Information (PCI or Credit/Debit Card Data)
   f. Financial Account Data
2. Data protected by confidentiality agreements, including:
   a. Employee personnel records
   b. Non-Disclosure Agreements (NDA).
3. Internal Grand County information that must be protected from unauthorized internal or external disclosure, including:
   a. Credentialing information (e.g., credentials, password data) that grants access to systems storing confidential data
   b. Legal products, including legal correspondence and data that is subject to attorney-client privilege
4. Legal hold data that are the subject of (or are anticipated to be the subject of) any type of investigation and/or legal proceeding.

4.5 Tier 2: Internal Use Only Data

1. Data is classified as internal use only data when the unauthorized disclosure, alteration or destruction causes a low-to-moderate level of risk for unauthorized disclosure or misuse. Internal use only data is not for release to the general public. Internal use only data is always sensitive.
2. A reasonable level of security controls is applied to internal use only data.
3. By default, all data that are not explicitly classified as confidential data or public data is treated as internal use only data.
4. Access to internal use only data must be authorized by the data owner who is responsible for the data. Access to internal use only data may be authorized to groups of persons based on job classification or responsibilities ("role-based" access).

4.5.1 Tier 2: Internal Use Only Data Examples

1. Internal newsletters
2. Training program materials
3. Project plans / documentation
4. Operations meeting notes
5. Operations policies and procedures

4.6 Tier 3: Public Data

1. Data is classified as public when the unauthorized disclosure, alteration or destruction of that data would result in minimal risk for unauthorized disclosure or misuse.
2. As public data is not considered sensitive, access may be granted to any requester or published with no restrictions.

4.6.1 Tier 3: Public Data Examples

1. Provider directory information
2. Public event information
3. Research publications

4.7 Data Collections

1. Data owners may assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements is used to classify the entire body of data as a whole.

4.8 Data Handling, Labeling, and Storage Requirements

1. All Grand County data is handled, labeled, and stored in accordance with this policy. Data handling is conducted based upon its data classification.
2. Procedures for handling, processing, communication and storage of information (including information media awaiting disposal) is established to protect data from unauthorized disclosure or misuse including:
   a. Physical and technical access restrictions commensurate with the data classification level
   b. Handling and labeling of all media according to its indicated classification (sensitivity) level
   c. Periodic review (at a minimum annually) of distribution and authorized recipient lists
   d. Monitoring the status and location of media containing unencrypted confidential information
3. Any data covered by federal or state laws or regulations or contractual agreements must also meet the security requirements defined by those laws, regulations, or contracts in addition to the requirements of this policy.

4.9 Minimum Security Controls

The minimum-security controls for Grand County confidential data, internal-use-only data, and public data is included in the table below.

Security Control Category	Tier 1: Confidential Data	Tier 2: Internal-Use-Only Data	Tier 3: Public Data
Access Controls	Viewing and modification restricted to authorized individuals as needed for business-related roles. Data owner or designee grants permission for access. Authentication and authorization required for access. Confidentiality Agreement required.	Viewing and modification restricted to authorized individuals as needed for business-related roles. Data owner or designee grants permission for access. Authentication and authorization required for access.	No restrictions.
Auditing	Logins, access and changes.	Logins	No restrictions.
Backup/Disaster Recovery	Daily backups required. Off-site storage of backup media in a secure location.	Daily backups required. Off-site storage of backup media.	No restrictions.

Security Control Category	Tier 1: Confidential Data	Tier 2: Internal-Use-Only Data	Tier 3: Public Data
Copying/ Printing **(applies to both paper and electronic forms)**	Data should only be printed when there is a legitimate need. Copies must be limited to individuals authorized to access the data and who have signed a confidentiality agreement. Data must not be left unattended, such as on a printer/fax, desktop, or any public location. Copies must be conspicuously labeled “Confidential”. If sent via internal mail, must be must be marked “Confidential”.	Data should only be printed when there is a legitimate need. Copies must be limited to individuals with a need to know. Data must not be left unattended on a printer/fax, desktop, or any public location. May be sent via Internal Mail.	No restrictions.
Data Storage	Should not permanently store on an individual workstation or Mobile Computing Device (e.g., a laptop computer). If stored on a workstation or Mobile Computing Device, that device must use whole-disk encryption. Encryption on Backup Media required. Paper/hard copy: do not leave unattended where others may see it; store in a secure location.	Should not store on an individual's workstation or a mobile device.	No restrictions.
Media Sanitization and Disposal **(hard drives, CDs, DVDs, tapes, paper, etc.)**	Shred paper. Re-use or destroy electronic media at end of life according to the *Secure Disposal Policy*.	Recycle paper. Wipe/erase electronic media.	No restrictions.
Mobile Computing Devices	Password protected, locked when not in use, encryption required. Remote delete capability of Confidential Data.	Password protected, locked when not in use.	No restrictions.
Network Security	Protection with a Network Firewall using "default deny" (Deny All, Permit by Exception [DAPE]) rule set required. IDS or IPS protection required. Protection with router ACLs optional. Servers hosting the data must not be visible to the entire Internet, nor to unprotected subnets like the guest wireless networks. Logical and/or physical Network partitioning of Confidential Data from other types. The Firewall rule set must be reviewed periodically.	Protection with a Network Firewall required. IDS or IPS protection required. Protection with router ACLs optional. Servers hosting the Data must not be visible to the entire Internet. May be in a shared Network server subnet with a common Firewall rule set for the set of servers.	No restrictions.
Physical Security	Computing Devices must be locked or logged out when unattended. Servers hosted in a secure Data Center required. Physical access to primary Data Center must be monitored, logged, and limited to authorized individuals 24x7.	Computing Devices must be locked or logged out when unattended. Hosted in a secure location required.	No restrictions.

Security Control Category	Tier 1: Confidential Data	Tier 2: Internal-Use-Only Data	Tier 3: Public Data
Remote Access to systems hosting the data	Access restricted to local network or secure VPN group. Remote Access by Third Party for technical support limited to authenticated, temporary access vis secure protocols over the Internet. Two-factor authentication required.	Access restricted to local Network or VPN. Remote Access by Third Party for technical support limited to authenticated, temporary access via secure protocols over the Internet.	No restrictions.
System Security	Must follow Grand County-specific and Operating System (OS)-specific best practices for system management and security. Host-based Advanced Threat Protection and Firewall required.	Must follow Grand County-specific and OS-specific best practices for system management and security. Host-based Advanced Threat Protection and Firewall required.	No restrictions.
Training	General security awareness training required. Data security training required. Applicable policy and regulation training required.	General security awareness training required. Data security training required.	No restrictions.
Transmission	Encryption required in accordance with the *Encryption Policy*. Cannot transmit via email unless encrypted.	No requirements.	No restrictions.
Virtual Environments	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines.	May be hosted in a virtual server environment. All other security controls apply to both the host and the guest virtual machines. Should not share the same virtual host environment with guest virtual servers of other security classifications.	No restrictions.

4.10 Policy References

4.10.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(a)(1)(ii)(A), CFR TITLE 45 § 164.308(a)(1)(ii)(B), CFR TITLE 45 § 164.308(a)(3)(ii)(A), CFR TITLE 45 § 164.310(b), CFR TITLE 45 § 164.310(c), CFR TITLE 45 § 164.310(d)(1), CFR TITLE 45 § 164.310(d)(2)(iv), CFR TITLE 45 § 164.312(c)(1)

4.10.2 NIST References

NIST SP 800-53 R4 CM-8, NIST SP 800-53 R4 CM-8(7), NIST SP 800-53 R4 RA-2

4.10.3 CJIS References

CJIS V5.9 Sections 5.5.2.1, 5.5.6.2, 5.10

5 RECORD RETENTION POLICY

5.1 Statement of Purpose

The purpose of this policy is to ensure proper and lawful retention of documentation and organizational records.

5.2 Statement of Applicability

All workforce members who have access or exposure to Grand County confidential data and/or Grand County information assets are required to comply with this policy.

5.3 Protection of Organizational Records

1. Grand County protects organizational records from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
2. Grand County retains individual Information Security training records for at least two (2) years from the date of its creation.
3. Grand County retains emails for six (6) months.
4. Grand County retains records under current litigation and/or if there is a high potential for litigation, for the duration of the litigation and/or litigation potential.
5. Grand County retains all election testing records and documentation for (25) months following an election.
6. Grand County ensures that Protected Health Information (PHI) is safeguarded for a period of (50) years following the death of the individual.
7. Grand County retains the following documentation for at least six (6) years from the date of its creation or the date when it was last in effect, whichever is later:
    a. Information security and privacy policies and procedures implemented to comply with regulatory requirements.
    b. All documentation that supports HIPAA compliance.
    c. All signed authorizations.
    d. Accountings of disclosures of PHI.
    e. Documentation of the titles of the persons or offices responsible for HIPAA compliance, including not only those with over-all responsibility for compliance, but also those responsible for receiving and processing requests from individuals.
8. Grand County permits access by the HHS Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including PHI, that are pertinent to ascertaining compliance.

5.4 Access Privilege Changes

1. Logs of access privilege changes shall be maintained for a minimum of one year.

5.5 Policy References

5.5.1 HIPAA Regulatory References

CFR TITLE 45 § 164.414(a), CFR TITLE 45 § 164.502(f), CFR TITLE 45 § 164.520(e), CFR TITLE 45 § 164.522(a)(3), CFR TITLE 45 § 164.524(e), CFR TITLE 45 § 164.528(d), CFR TITLE 45 § 164.530(j)

5.5.2 NIST References

NIST SP 800-53 R4 AU-9, NIST SP 800-53 R4 DM-2, NIST SP 800-53 R4 DM-2(1), NIST SP 800-53 R4 SI-12, NIST SP 800-53 R4 RA-2, NIST SP 800-53 R4 AT-4

5.5.3 CJIS References

CJIS V5.9 Sections 5.5.2.1

5.5.4 Code of Colorado Regulations References

8 CCR 1505-1 Rule 11.5

6 RISK MANAGEMENT POLICY

6.1 Statement of Purpose

The purpose of this policy is to develop and implement a Risk Management Plan that addresses risk assessments, risk mitigation, and risk evaluation.

6.2 Statement of Applicability

All workforce members, including third parties, who may have access or exposure to Grand County enterprise data are required to comply with this policy.

6.3 Risk Management Plan Development

1. Grand County develops and implements a formal, comprehensive Risk Management Plan to manage risk associated with the operation and use of information systems, including physical and environmental hazards, to an acceptable level.

6.4 Risk Assessments

1. Grand County performs risk assessments in a consistent way and identifies information security risks to the organization.
2. Grand County accounts for risks from prior incidents, changes in the environment, and third parties.
3. Formal risk assessments are performed at planned intervals (e.g. at least annually), or when major changes occur in the environment, and the results reviewed.
4. Risk assessments are used to determine whether a breach of unsecured protected health information (PHI) is reportable to the HHS Secretary. Risk assessments must demonstrate there is a low probability of compromise rather than a significant risk of harm.

6.5 Risk Mitigation

1. Grand County reduces risk to the lowest acceptable level.
2. Grand County defines and documents the criteria to determine whether or not a risk is avoided, accepted, transferred or treated in the Risk Management Plan.
3. Grand County implements a process for ensuring that security corrective action plans are prioritized and maintained; and the remedial information security actions necessary to mitigate risk to operations and assets, individuals, and other organizations are documented.

6.6 Privacy Risk Assessments

1. The need for privacy monitoring or auditing is based on the identification of compliance concerns or risk areas. The type of action that may be taken by the County Manager or designee in response to identification of concerns or risk areas such as ongoing monitoring and frequency of audits is determined by the scope of the concern, potential for non-compliance and previous outcomes, if any.
2. The Office of Regulatory Compliance (ORC), local Compliance Officer (CO) and Compliance Committees coordinate the process for identification of risk through analysis of areas such as clinical outcomes, benchmarks, quality indicators, satisfaction surveys, complaints, CMS or state survey reports, reports of possible non-compliance, other ongoing monitoring, federal and state governments, including, but not limited to federal and state laws pertaining to provider Compliance Programs, CMS publications; OIG and state specific work plans, and other relevant guidance materials and self-auditing.
3. The ORC, with the assistance of Compliance Committee members, is responsible for tracking internal concerns, risk areas and potential risks from external sources.

6.7 Policy References

6.7.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308 (a)(1)(i), CFR TITLE 45 § 164.308 (a)(1)(ii)(A), CFR TITLE 45 § 164.308 (a)(1)(ii)(B), CFR TITLE 45 § 164.308 (a)(2), CFR TITLE 45 § 164.308 (a)(7)(ii)(E), CFR TITLE 45 § 164.316(a), CFR TITLE 45 § 164.402

6.7.2 NIST References

NIST SP 800-53 R4 AR-1, NIST SP 800-53 R4 AR-2, NIST SP 800-53 R4 PM-11, NIST SP 800-53 R4 PM-4, NIST SP 800-53 R4 PM-9, NIST SP 800-53 R4 RA-1, NIST SP 800-53 R4 RA-3, NIST SP 800-53 R4 CA-2, NIST SP 800-53 R4 CA-2(1), NIST SP 800-53 R4 CA-5, NIST SP 800-53 R4 CA-5(1), NIST SP 800-53 R4 PM-4, NIST SP 800-53 R4 CM-3

7 THIRD PARTY RISK MANAGEMENT POLICY

7.1 Statement of Purpose

The purpose of this policy is to establish how Grand County ensures the integrity of the security of Grand County and its information assets when risks may be introduced by third parties.

7.2 Statement of Applicability

This policy applies to all third-party arrangements, including those with business associates.

7.3 Third Party Risk Management Policy

1. Grand County establishes a third-party risk management function with the purpose of governing security risks of third-party organizations that have access to Grand County data, or provide products or services for Grand County.
2. Responsibilities for the third-party risk management function include:
    a. Identifying all Grand County Business Associates, according to the HIPAA Security and Privacy rules.
    b. Vetting the security controls of third parties before establishing a third-party contract relationship, where feasible.
    c. Ensuring an approved and current Grand County Business Associate Agreement (BAA) is in place and has been signed by appropriate third party.
    d. Maintaining a current and accurate listing of all Grand County business associates.
    e. Performing routine reviews of security measures implemented by third parties, as feasible.

7.4 Third Party Risk Identification

1. The potential risks to Grand County information assets involving third parties are identified, and appropriate controls are implemented to mitigate these risks when granting access.

7.5 Third Party Agreements

1. The specific limitations of access, arrangements for compliance auditing, penalties, and the requirement for incident notification are identified in the third-party agreements, in accordance with applicable provisions of the Use and Disclosure of Protected Health Information Policy.
2. A standard BAA is defined and made available to appropriate workforce members.
3. The BAA includes provisions for breach notification and termination upon breach.
4. The BAA defines the disposition of PHI upon termination of the agreement.

7.6 Third Party Service Delivery

1. SLAs, or contracts with an agreed service arrangement, address liability and other aspects of services management as appropriate.
2. Grand County develops and updates at least annually a list of current active service providers.

7.7 Third Party Monitoring and Review

1. The services, reports and records provided by the third party are regularly monitored and reviewed, and audits are carried out regularly to govern and maintain compliance with the third-party agreements.
2. Network connections with third parties are periodically audited to ensure that third parties have implemented any required security features and that third parties meet all requirements agreed to with Grand County. (See Network Protection Policy).

7.8 Third Party Change Management

1. Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, are managed, considering the criticality of business systems and processes involved and re-assessment of risks.
2. Third parties are required to coordinate, manage and communicate changes that will have an impact to Grand County information, systems or processes.

7.9 Policy References

7.9.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(a)(3)(ii)(A), CFR TITLE 45 § 164.308(a)(4)(ii)(B), CFR TITLE 45 § 164.308(b)(1), CFR TITLE 45 § 164.308(b)(3), CFR TITLE 45 § 164.314(a)(1), CFR TITLE 45 § 164.314(a)(2)(i), CFR TITLE 45 § 164.314(a)(2)(ii), CFR TITLE 45 § 164.314(b)(1), CFR TITLE 45 § 164.314(b)(2)(i), CFR TITLE 45 § 164.314(b)(2)(ii), CFR TITLE 45 § 164.314(b)(2)(iii), CFR TITLE 45 § 164.314(b)(2)(iv), CFR TITLE 45 § 164.404(b), CFR TITLE 45 § 164.410(a)(1), CFR TITLE 45 § 164.410(a)(2), CFR TITLE 45 § 164.410(b), CFR TITLE 45 § 164.410(c)(1), CFR TITLE 45 § 164.410(c)(2), CFR TITLE 45 § 164.414(b)

7.9.2 NIST References

NIST SP 800-53 R4 AC-17(2), NIST SP 800-53 R4 AC-3(8), NIST SP 800-53 R4 AC-6, NIST SP 800-53 R4 CA-3, NIST SP 800-53 R4 MA-4, NIST SP 800-53 R4 SC-8(1), NIST SP 800-53 R4 AC-8, NIST SP 800-53 R4 CA-3, NIST SP 800-53 R4 PL-4, NIST SP 800-53 R4 TR-3, NIST SP 800-53 R4 CA-7(1), NIST SP 800-53 R4 PS-7, NIST SP 800-53 R4 SA-9

8 BUSINESS ASSOCIATES POLICY

8.1 Statement of Purpose

The purpose of this policy is to protect an individual's privacy and security through appropriate contracts with Business Associates to assure compliance, and to mitigate non-compliance and breaches.

8.2 Statement of Applicability

All Grand County business associates are required to comply with this policy.

8.3 Disclosures of PHI to Business Associates

1. Grand County does not allow a Business Associate to create or receive PHI on its behalf in the absence of an approved and signed BAA.

2. Grand County does not legally execute any BAA, addendum or other amendment other than the standard BAA, unless approved as an exception. The approved BAA may not be negotiated or modified in any way without the approval of the Grand County Attorney and Chief Information Security Officer.

8.4 Violations of the Business Associate Agreement

1. If Grand County becomes aware of a pattern of activity or practice violating the satisfactory assurances the Business Associate has provided to Grand County, the Business Associate is deemed non-compliant with the agreement, and immediate action is taken as noted within the provisions of the BAA.
2. Violations of the terms of the BAA must be immediately reported to the County Manager, County Attorney, and CISO.

8.5 Policy References

8.5.1 HIPAA Regulatory References

CFR TITLE 45 § 164.502(e), CFR TITLE 45 § 164.504(e), CFR TITLE 45 § 164.504(f), CFR TITLE 45 § 164.504(g)

9 PHI BREACH NOTIFICATION POLICY

9.1 Statement of Purpose

Compliance with HIPAA's notification requirements for breaches of "unsecured" (unencrypted or not destroyed) Protected Health Information (PHI) is mandatory and failure to comply can bring severe sanctions and penalties.

9.2 Statement of Applicability

All workforce members and Business Associates of Grand County must comply with this policy.

9.3 PHI Breach Definition

1. Breach means the acquisition, access, use, or disclosure of PHI in a manner which compromises the security or privacy of the PHI.
2. Breach excludes:
    a. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure.
    b. Any inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted.
    c. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
3. An acquisition, access, use, or disclosure of PHI in a manner not permitted is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on an assessment including the following factors:
    a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

   b. The unauthorized person who used the PHI or to whom the disclosure was made;
   c. Whether the PHI was acquired or viewed; and
   d. The extent to which the risk to the PHI has been mitigated.
4. Unsecured PHI means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons using a technology or methodology specified by the Secretary of HHS.

9.4 Determining a PHI Breach

1. When a security or privacy incident occurs that may be a breach under HIPAA regulations, the County Manager or designee determines whether a breach has occurred.
2. An acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rules is presumed to be a breach unless Grand County can demonstrate that there is a low probability that the PHI has been compromised based on an assessment.

9.5 PHI Breach Notification Standard

1. Grand County develops and implements breach notification procedures.
2. Grand County provides timely notifications about breaches of individually identifiable health information as follows:
   a. Notice to clients according to the terms stated in the contract.
   b. Notice to residents alerting them to breaches without unreasonable delay, but no later than 60 calendar days after discovery of the breach.
   c. Notice to next of kin about breaches involving decedents.
   d. Notice to the Secretary of Health and Human Services (HHS) and media outlets regarding breaches involving more than 500 participant records.
   e. Annual notice to the Secretary of HHS 60 days after the end of the calendar year regarding breaches involving fewer than 500 participant records.
3. Notices include the details of the breach, steps taken to help mitigate harm to residents, and the incident response.
4. All Business Associate Agreements (BAAs) include breach notification requirements.
5. Business Associates of Grand County are required to report all breaches, losses, or compromises of individually identifiable health information–whether secured or unsecured–to Grand County within 10 days according to the terms of the contract.
6. Sanctions are applied to all workforce members who caused or created the conditions that allowed the breach to occur, according to the Sanctions Policy.
7. All breach-related activities and investigations are thoroughly documented.

9.6 PHI Breach Reporting

1. Grand County submits an annual summary of breaches to the Secretary of the HHS that includes the following:
   a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   b. The unauthorized person who used the PHI or to whom the disclosure was made;
   c. Whether the PHI was acquired or viewed; and
   d. The extent to which the risk to the PHI has been mitigated.

9.7 Policy References

9.7.1 HIPAA Regulatory References

CFR TITLE 45 § 164.400 to § 164.414, CFR TITLE 45 § 164.530

10 NON-PHI BREACH NOTIFICATION POLICY

10.1 Statement of Purpose

Compliance with regulatory requirements for breaches is mandatory and failure to comply can bring severe sanctions and penalties.

10.2 Statement of Applicability

All workforce members must comply with this policy.

10.3 Non-PHI Breach Definition

A Non-PHI breach is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses Grand County Confidential Information, or (2) an authorized user accesses Grand County Confidential Information for an unauthorized purpose.

10.4 Determining a Non-PHI Breach

1. Notification of an incident that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies will be provided to the County Manager, or designee, and CISO to determine if a breach has occurred.

10.5 Non-PHI Breach Notification Standard

1. Grand County develops and implements breach notification procedures.
2. Grand County provides timely notifications about breaches as follows:
    a. If a breach is suspected, the following information is collected prior to submission to the County Manager, or designee, and CISO for determination:
        a. The current level of impact to County functions or services is identified; this is referenced as “Functional Impact”.
        b. The type of information lost, compromised, or corrupted is identified; this is referenced as “Information Impact”.
        c. An estimate of the scope of time and resources needed to recover from the event is identified; this is referenced as “Recoverability”.
        d. Identification of when the adverse activity was first detected.
        e. Identification of the number of systems, records, and users impacted.
        f. Identification the network location(s) of the observed adverse activity.
    b. Notification is provided to the County Manager, or designee, and CISO for breach determination.
    c. If the event is declared to meet the criteria of a breach, the Grand County Cybersecurity Incident Response Plan will be used to guide further coordination activities.
    d. Notifications will be sent to external entities as appropriate, to include:
        a. Colorado Attorney General (if over 500 Colorado residents impacted)
            i. databreach@coag.gov
        b. Colorado Secretary of State
            i. SCORE.CUSTOMERSUPPORT@SOS.STATE.CO.US
            ii. +1-888-271-2077
        c. Multi-State Information Sharing & Analysis Center (MS-ISAC)
            i. SOC@CISecurity.org
            ii. +1-866-787-4722
        d. FBI Criminal Justice Information Services (CJIS)
            i. ISO@FBI.GOV

ii. +1-304-625-3660

e. Consumer Reporting Agencies (if over 1,000 Colorado residents impacted)

i. https://www.equifax.com/personal/

ii. https://www.transunion.com

iii. https://www.experian.com/

3. Sanctions are applied to all workforce members who caused or created the conditions that allowed the breach to occur, according to the Sanctions Policy.
4. All breach-related activities and investigations are thoroughly documented.

10.6 Policy References

10.6.1 NIST References

NIST SP 800-53 R4 IR-1, NIST SP 800-53 R4 IR-4, NIST SP 800-53 R4 IR-5, NIST SP 800-53 R4 IR-6, NIST SP 800-53 R4 IR-7, NIST SP 800-53 R4 IR-8, NIST SP 800-53 R4 IR-9

10.6.2 CJIS References

CJIS V5.9 Sections 5.3.1

10.6.3 CRS References

C.R.S. § 24-73-103

11 ACCOUNTING OF PHI DISCLOSURES

11.1 Statement of Purpose

The purpose of this policy is to ensure that Grand County complies with the HIPAA requirement to provide an accounting of certain disclosures of Protected Health Information (PHI).

11.2 Statement of Applicability

This policy applies to all work force members, including, but not limited to contractors, sub-contractors and vendors.

11.3 Accounting of Disclosures Policy

1. Grand County keeps a written record of disclosures of PHI for six years from the date of disclosure.
2. The following disclosures are included in the accounting:
    a. required by law (e.g., mandated reporting under state law)
    b. for public health activities and reporting
    c. about victims of abuse, neglect or domestic violence
    d. for health oversight activities (e.g., licensure actions)
    e. in response to a court order
    f. in response to a subpoena or discovery request
    g. for law enforcement purposes
    h. to a medical examiner, funeral director or for cadaveric organ donation
    i. for certain specialized government functions (e.g., regarding armed forces personnel)
    j. as authorized by and to the extent required to comply with worker's compensation laws
    k. to business associates (if not in an excluded category)
    l. made subsequently by business associates (if not in an excluded category)
    m. not permitted by HIPAA
    n. to the Secretary of the federal Department of Health and Human services
    o. any other disclosure of PHI that is not specifically excluded.
3. The following disclosures are excluded from the accounting:

a. to carry out treatment, payment or health care operations
b. to the individual or the individual's personal representative
c. pursuant to an authorization
d. disclosures incidental to a permitted disclosure
e. for a facility directory
f. to persons (e.g. family) involved in the individuals care
g. for national security or intelligence purposes
h. to correctional institutions or law enforcement officials about an inmate or other individual in legal custody
i. as part of a limited data set with a data use agreement
j. as de-identified information
k. prior to April 14, 2003
l. more than 6 years prior to the request for accounting

4. The standard accounting includes:
    a. Date of disclosure;
    b. Name of the recipient and address, if known;
    c. Brief description of the PHI disclosed; and
    d. Brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the request for a disclosure.
5. If multiple disclosures of PHI are made to the Secretary or to the same person or entity for a single purpose, the accounting includes:
    a. the standard accounting information for the first disclosure during the accounting period;
    b. The frequency, periodicity, or number of disclosures; and
    c. The date of the last disclosure.

11.4 Accountings Suspended by Law Enforcement or Health Oversight Officials

1. Upon request by a health oversight agency or law enforcement official, Grand County suspends the accounting of the disclosures made to the agency or official for the period specified in the request.
    a. The request states that the accounting will likely impede the agency's activities and must specify the period of the suspension.
    b. Any such request is documented and the accounting for the disclosures must be renewed at the end of the specified period.
    c. If the initial statement by the agency or official is oral, the temporary suspension cannot exceed 30 days, unless a written statement is submitted by the agency or official within 30 days of the oral request.

11.4.1 Period for Action

1. Grand County acts on an individual's request for an accounting within 60 days from receipt of the request.
2. The time for action on a request may be extended for an additional 30 days if Grand County is unable to act within the original period for action.
3. To extend the period for action, Grand County provides a written statement of the reasons for the delay to the individual within 60 days from receipt of the request.
4. One extension of the period for action is allowed per request.

11.4.2 Fees

1. Grand County provides the first accounting during any 12-month period at no charge.
2. Grand County charges a reasonable, cost-based fee for subsequent requests during any one 12-month period.

3. The individual is informed in advance of the fee and given an opportunity to withdraw or modify the request.

11.5 Policy References

11.5.1 HIPAA Regulatory References

CFR TITLE 45 § 164.520, CFR TITLE 45 § 164.528(a), CFR TITLE 45 § 164.528(b), CFR TITLE 45 § 164.528(c), CFR TITLE 45 § 164.530(j)

12 ACCOUNTING OF PII DISCLOSURES

12.1 Statement of Purpose

The purpose of this policy is to ensure that Grand County complies with requirements to provide an accounting of certain disclosures of Personally Identifiable Information (PII) to parties outside of Grand County.

12.2 Statement of Applicability

This policy applies to all work force members, including, but not limited to contractors, sub-contractors and vendors.

12.3 Accounting of Disclosures Policy

1. Grand County keeps a written record of disclosures of PII for five years from the date of disclosure to parties outside of Grand County.
2. Disclosures of PII to parties outside of Grand County will require acceptance of a Non-Disclosure Agreement (NDA).
    a. NDA's will be reviewed by Grand County legal prior to the NDA being submitted to outside parties for acceptance.
    b. Grand County legal will assign a unique NDA record number.
    c. Grand County Elected Officials and Department heads are considered duly authorized representatives and can sign NDA's upon legal review and approval.
3. The following disclosures are included in the accounting:
    a. required by law (e.g., mandated reporting under state law)
    b. any other disclosure of PII that is not specifically excluded.
4. The following disclosures are excluded from the accounting:
    a. to Grand County workforce members in the performance of their authorized duties
    b. pursuant to the individual's written authorization
    c. as de-identified information
5. The standard accounting includes:
    a. Date of disclosure;
    b. Name of the recipient and address, if known;
    c. Brief description of the PII disclosed; and
    d. Brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the request for a disclosure.

12.4 Accountings Suspended by Law Enforcement

2. Upon request by a law enforcement official, Grand County suspends the accounting of the disclosures made to the agency or official for the period specified in the request.
    a. The request states that the accounting will likely impede the agency's activities and must specify the period of the suspension.
    b. Any such request is documented and the accounting for the disclosures must be renewed at the end of the specified period.

c. If the initial statement by the agency or official is oral, the temporary suspension cannot exceed 30 days, unless a written statement is submitted by the agency or official within 30 days of the oral request.

12.4.1 Period for Action

5. Grand County acts on an individual's request for an accounting within 60 days from receipt of the request.
6. The time for action on a request may be extended for an additional 30 days if Grand County is unable to act within the original period for action.
7. To extend the period for action, Grand County provides a written statement of the reasons for the delay to the individual within 60 days from receipt of the request.
8. One extension of the period for action is allowed per request.

12.4.2 Fees

4. Grand County provides the first accounting during any 12-month period at no charge.
5. Grand County charges a reasonable, cost-based fee for subsequent requests during any one 12-month period.
6. The individual is informed in advance of the fee and given an opportunity to withdraw or modify the request.

12.5 Policy References

12.5.1 Regulatory References

Privacy Act (5 U.S.C. § 552a)

12.5.2 NIST References

NIST SP 800-53 R4 AP-1, AP-2, AR-4, AR-8, IP-2

13 HUMAN RESOURCES SECURITY POLICY

13.1 Statement of Purpose

The purpose of human resources security controls is to ensure that Grand County information assets are protected from the adverse actions of personnel. The term “human resources” does not mean these controls are the exclusive responsibility of the Grand County Human Resource Department, rather they pertain to all individual departments/offices and employees.

13.2 Statement of Applicability

This policy covers Grand County human resources practices across all departments and business units. Elected Officials and Department heads are responsible for ensuring adherence to this policy within their offices and departments. Elected Officials and Department heads may request support from the Grand County CISO and/or Human Resources department as required. All Grand County workforce members are required to comply with this policy.

13.3 Requirements for Workforce Members Performing in Information Security Roles

1. Grand County defines and documents roles and responsibilities for workforce members performing information security work and/or duties.
2. Grand County CISO assigns a risk designation to all security roles and job functions regardless of job title.
3. Grand County CISO reviews and revises risk designations annually.
4. Grand County defines screening criteria for information security roles per individual department and job function.

5. Grand County hiring managers ensure security roles and responsibilities are clearly communicated to potential job candidates.

13.4 Information Security Roles and Responsibilities

1. Grand County defines and documents security roles and responsibilities for workforce members in the Information Security and Privacy Roles and Responsibilities Standard.
2. Security roles and responsibilities are defined and documented in job descriptions by the Grand County CISO.
3. Grand County ensures that workforce members are suitable for their roles to reduce the risk of fraud.

13.5 Screening

13.5.1 Common Screening

1. Grand County attempts to hire workforce members with the appropriate credentials, certifications, licenses, experience, and training to meet the needs of our residents are hired.
2. Grand County Elected Officials and Department heads are responsible for oversight of Grand County personnel screening for their offices and departments.

13.5.2 Workforce with PHI Access

1. Grand County carries out background verification checks on all candidates for employment.
    a. The screening is done in accordance with relevant laws, regulations and ethics.
    b. The screening is proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
2. Prior to hire and regularly thereafter, workforce members are screened to determine if they are excluded or disqualified from participating in Federal or State funded healthcare programs.

13.5.3 Workforce with CJI Access

1. The Grand County Sheriff's Office will verify identification, state of residency and national fingerprint-based record checks prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing).

13.5.4 Workforce with Access to Elections/Voting Equipment

1. The Grand County Clerk & Recorder's Office will ensure all permanent and temporary county staff and all vendor staff who have access to the voting system or any voting or counting equipment must pass a criminal background check. A person convicted of an election offense or an offense containing an element of fraud may not have access to a code, combination, password, or encryption key for the voting equipment, ballot storage area, counting room, or tabulation workstation.

13.5.5 Information Systems Department Workforce

1. Screening will include all requirements stated for workforce with PHI, CJI, and Elections/Voting Equipment access.

13.6 Terms and Conditions of Employment

1. Grand County maintains a personnel manual that defines the terms and conditions of employment in terms of the organization's policies and procedures. Additionally, individual departments/offices may have additional policies and procedures that are not included within the personnel manual maintained by the Grand County Human Resources Department.

13.7 Senior Leadership Responsibilities

1. Senior leadership (i.e. Elected, Appointed, or Management positions) requires workforce members to apply security in accordance with established policies and procedures of Grand County.
2. Senior leadership ensures that workforce members are aware of the following:
    a. Information security threats and concerns
    b. Security and privacy responsibilities and liabilities
    c. Supporting policies during their normal work
    d. Reducing the risk of human error
3. Acceptable use of information assets by workforce members is defined and explicitly authorized in the Acceptable Use Policy section of this manual.
4. Managers ensure that users under their control and/or within their area of responsibility receive appropriate and enough training and materials to learn and remain up-to-date on issues, requirements, expectations and procedures for protecting computing devices.

13.8 Confidentiality Agreements for PHI Access

1. Confidentiality Agreements are applicable to all workforce members accessing PHI data.
2. Confidentiality Agreements address the requirement to protect confidential information using legally enforceable terms.
3. Confidentiality Agreements comply with all applicable laws and regulations for the jurisdiction to which they apply.
4. Confidentiality Agreements are reviewed at least annually and when changes occur that influence these requirements.

13.9 Policy References

13.9.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(a)(3)(ii)(A), CFR TITLE 45 § 164.308(a)(3)(ii)(B), CFR TITLE 45 § 164.308(a)(3)(ii)(C), CFR TITLE 45 § 164.308(a)(4)(ii)(B), CFR TITLE 45 § 164.308(b)(1), CFR TITLE 45 § 164.310(b), CFR TITLE 45 § 164.310(d)(2)(iii), CFR TITLE 45 § 164.314(a)(1), CFR TITLE 45 § 164.314(a)(2)(i), CFR TITLE 45 § 164.314(a)(2)(ii)

13.9.2 NIST References

NIST SP 800-53 R4 PL-4, NIST SP 800-53 R4 PS-1, NIST SP 800-53 R4 PS-2, NIST SP 800-53 R4 PS-3, NIST SP 800-53 R4 PS-6, NIST SP 800-53 R4 AT-3, NIST SP 800-53 R4 PM-13, NIST SP 800-53 R4 PM-14, NIST SP 800-53 R4 PM-15, NIST SP 800-53 R4 PM-2, NIST SP 800-53 R4 PS-7

13.9.3 CJIS References

CJIS V5.9 Sections 5.12

13.9.4 Code of Colorado Regulations References

8 CCR 1505-1 Rule 11.1.3

13.9.5 Colorado Revised Statutes References

CRS 24-72-305.6

14 INFORMATION SECURITY TRAINING AND AWARENESS POLICY

14.1 Statement of Purpose

The purpose of information security awareness and training is to ensure that Grand County workforce members are continually educated to help protected Grand County information assets.

14.2 Statement of Applicability

This policy applies to all workforce members who use Grand County information assets and related resources.

14.3 Information Security Training Policy

1. All Grand County workforce members who access information assets are required annually to take the Grand County Cybersecurity Awareness training course which at a minimum will contain the following topics:
    a. Protection from malicious software; and
    b. Password management; and
    c. Log-in monitoring; and
    d. Identifying and responding to suspect or known security incidents.
2. All Grand County workforce members who have an email address will be subject to simulated phishing exercises on at least a quarterly basis.
3. The CISO will be responsible for ensuring:
    a. Basic security awareness training is provided to all workforce members; and
    b. Practical exercises are conducted regularly that simulate actual cyber-attacks; and
    c. Training includes recognizing and reporting potential indicators of insider threat; and
    d. Additional role-based training is provided to workforce members in information security roles and/or who frequently interact with confidential information and data.

14.4 Information Security Awareness Policy

1. Grand County establishes contact with select groups and associations within the security community to:
    a. facilitate ongoing security education and training; and
    b. maintain currency with recommended security practices; and
    c. share current security-related information include threats, vulnerabilities, and incidents.
2. All workforce members within the Information Systems team are required to join the Multi-State Information Sharing and Analysis Center (MS-ISAC).
3. The CISO will be responsible for ensuring:
    a. The county receives information system security alerts/advisories on a regular basis; and
    b. Issues alerts/advisories to the appropriate county personnel; and
    c. Documents the types of actions to be taken in response to security alerts/advisories; and
    d. Ensures the appropriate actions are taken in response.
4. Where possible, Grand County will employ automated mechanisms to make security alert and advisory information available throughout the county as appropriate.

14.5 Workforce Members with Access to CJI

1. All workforce members who have access to CJI will at a minimum be required to:
    a. Conduct security awareness training, at the appropriate level (levels 1-4), within six months of initial assignment, and biennially thereafter.
2. The Grand County Sheriff's office is responsible for providing, auditing, are reporting on this training.

14.6 Workforce Members with Access to PHI

1. All workforce members who have access to PHI will at a minimum be required to:
    a. Conduct PHI-specific security awareness training annually.

14.7 Workforce Members with Access to PCI

1. All workforce members with access to PCI will at a minimum be required to:
    a. Conduct PCI-specific security awareness training annually.

14.8 Workforce Members with Access to Voting/Elections

2. All workforce members with access to voting/election systems will at a minimum be required to:
    a. Conduct training and certification in accordance with 8 CCR 1505-1, which is developed and administered by the Colorado Secretary of State Office.

14.9 Policy References

14.9.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(a)(5)

14.9.2 NIST References

NIST SP 800-53 R4 AT-1, AT-2, AT-3, AT-4, PM-15

14.9.3 CJIS References

CJIS V5.9 Sections 5.10.4.4

14.9.4 Code of Colorado Regulations References

8 CCR 1505-1 Rule 19

14.9.5 Colorado Revised Statutes References

CRS 1-1-302

15 ACCEPTABLE USE POLICY

15.1 Statement of Purpose

The purpose of this policy is to set standards and expectations for Grand County workforce members regarding access to Grand County information assets.

15.2 Statement of Applicability

This policy applies to all workforce members and all personnel affiliated with third parties who use Grand County information assets.

This policy applies to information technology administered centrally; personally-owned computing devices connected by wire or wireless to the Grand County network; and to off-site computing devices that connect remotely to the Grand County network.

15.3 Workforce Members Responsibilities and Acceptable Use

1. Grand County provides information assets as resources to Grand County workforce members. It is the workforce member's responsibility to properly use and protect information assets.
2. Workforce members comply with all Grand County policies, state and federal laws, regulations, and contractual obligations when accessing Grand County information assets.
3. Workforce member’s actions may be monitored.

4. Workforce members access to Grand County information assets is restricted based on need-to-know and in accordance with the minimum necessary principle.
5. Workforce members can use Grand County information assets:
    a. To which they have been granted authorized access.
    b. For Grand County business purposes.
6. Workforce members are made aware of their responsibilities for maintaining effective access controls and are required to follow Grand County policies.
7. Workforce members are required to handle, label, and store confidential data in accordance with the Data Classification and Handling Policy.
8. Each workforce member bears the responsibility for knowing and complying with applicable laws, Grand County privacy and security policies, and rules; for appropriately securing their computers and other electronic devices from misuse or theft by others; and for avoiding any use that interferes with others' legitimate access to and use of Grand County information assets.

15.4 Internet Access from Grand County Locations

1. Connection to the Internet, or use of a website, is a privilege and not a right. Any abuse of that privilege can result in legal and/or administrative action.
2. Internet access is granted with the expectation that workforce members and visitors act responsibly and use good judgment.
3. Internet access may be monitored at any time by Grand County. Any website or online activity may be blocked if it is determined to be harmful or disruptive to the organization or other workforce members.
4. A separate network is established to provide Internet access to visitors (where applicable).
5. Individually assigned passwords and accounts must not be shared.

15.5 Responsibilities for Unattended Information Assets

1. Workforce members log-off computing devices when the session is finished (i.e., not just switch off the PC screen or terminal) in accordance with the Clear Desk and Clear Screen Policy.
2. Workforce members safeguard unattended information system output devices (e.g., printers) to prevent unauthorized individuals from obtaining the output.

15.6 Code of Conduct

1. Workforce members agree to NOT:
    a. Post, use or transmit content that you do not have the right to post or use, for example, under intellectual property, confidentiality, privacy or other applicable laws.
    b. Post, use or transmit unsolicited or unauthorized content, including:
        i. Advertising or promotional materials
        ii. "Junk mail"
        iii. "Spam"
        iv. "Chain letters"
        v. "Pyramid schemes"
        vi. Political campaign promotional material
        vii. Any other form of unsolicited or unwelcome solicitation or advertising
2. Infringe upon copyrighted material of any kind, including the unauthorized downloading, copying, displaying, and/or distributing of copyrighted material. All such works should be considered protected by copyright law unless specifically stated otherwise. Any use of Grand County information assets (e.g., network, email system, website, etc.) to access, display, send,

transfer, modify, store or distribute copyrighted material (e.g., video/movies, music/audio, images, documents, software, text, etc.) is strictly prohibited.

3. Post, use or transmit content that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment or otherwise interfere with or disrupt Grand County information assets.
4. Post or transmit content that is harmful, offensive, obscene, abusive, invasive of privacy, defamatory, hateful or otherwise discriminatory, false or misleading, incites an illegal act, or is otherwise in breach of your obligations to any person or contrary to any applicable laws and regulations.
5. Intimidate or harass one another using Grand County information assets.
6. Allow unauthorized use or attempt to use another workforce member's individual account or credentials, service, or personal information.
7. Modify workstations without IT approval or remove, circumvent, disable, damage or otherwise interfere with any security-related features.
8. Install or use unauthorized or malicious software, or obtain unauthorized data and software from external networks.
9. Transmit (e.g., messaging, email, texting, etc.) confidential data over open, unprotected wireless networks unless approved security controls such as strong encryption are in place.
10. Forward confidential data to any unauthorized recipient.
11. Use Grand County demographic data such as business email address for personal use (e.g., register for software, complete a web form).
12. Attempt to gain unauthorized access to Grand County information assets, other workforce member's accounts, computing devices or networks connected to Grand County information technology resources, through hacking, password mining or any other means, or interfere or attempt to interfere with the proper working of Grand County information assets or any activities conducted through those information assets.
13. Impersonate another person or entity, or falsely state or otherwise misrepresent your affiliation with a person or entity without authorization.
14. Open emails, attachments, or click links from unknown sources.

15.7 Policy References

15.7.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308 (a)(5)(ii)(D), CFR TITLE 45 § 164.310(a)(1), CFR TITLE 45 § 164.310(b), CFR TITLE 45 § 164.310(c), CFR TITLE 45 § 164.312(a)(2)(iii)

15.7.2 NIST References

NIST SP 800-53 R4 IA-5, NIST SP 800-53 R4 AC-11, NIST SP 800-53 R4 PE-18, NIST SP 800-53 R4 PE-5, NIST SP 800-53 R4 SC-10, NIST SP 800-53 R4 AC-17, NIST SP 800-53 R4 AC-17(1), NIST SP 800-53 R4 AC-17(2), NIST SP 800-53 R4 AC-17(4), NIST SP 800-53 R4 AC-18, NIST SP 800-53 R4 AC-2, NIST SP 800-53 R4 AC-6(3), NIST SP 800-53 R4 CM-2, NIST SP 800-53 R4 CM-2(2), NIST SP 800-53 R4 IA-2, NIST SP 800-53 R4 IA-3, NIST SP 800-53 R4 IA-8, NIST SP 800-53 R4 IA-8(1), NIST SP 800-53 R4 IA-8(2), NIST SP 800-53 R4 IA-8(3), NIST SP 800-53 R4 IA-8(4), NIST SP 800-53 R4 MA-4

15.7.3 CJIS References

CJIS V5.9 Sections 5.6.2.1.1.2

16 CLEAR DESK AND CLEAR SCREEN POLICY

16.1 Statement of Purpose

The purpose of this policy is to ensure confidential data is kept private and protected from unauthorized access and viewing. The goal is to reduce the risks of unauthorized access to, or loss of, or damage to, Grand County enterprise data.

16.2 Statement of Applicability

This policy applies to all Grand County confidential data, computing devices, and users.

16.3 Clear Desk and Clear Screen Policy

1. Confidential data on paper media or in removable media is not be left unattended and unsecured.
2. Confidential data on paper media is protected from access by unauthorized individuals when not in use by storing in a locked drawer or room.
3. Confidential data on removable media is protected from access by unauthorized individuals when not in use according to the Encryption Policy.
4. Confidential data on paper media is immediately removed from printers, copiers, or fax machines to prevent access by unauthorized individuals.
5. Reproduction technology (e.g., printers, copiers, scanners, cameras, facsimile machines, etc.) is protected physically from use by unauthorized individuals to prevent unauthorized reproduction of confidential data.
6. Passwords are not posted on, under, or near a computer or other computing device according to the Acceptable Use Policy.
7. Incoming and outgoing distribution points for inter-office mail are protected from physical access by unauthorized individuals so that mail cannot be stolen or lost.
8. Confidential data that has been copied or printed is protected during transport using internal or external (e.g., USPS) mail services. This includes ensuring non-address information is not visible through envelope windows and marking the envelopes confidential when necessary.

16.4 Workstation Security

1. All users close all applications, logout, or lock their computer when they are away from their desk to protect confidential data from unauthorized access and viewing.
2. Workstations that process or store Confidential data are configured to automatically lock the screen in accordance with the Access Control Policy.
3. Workstations that process or store Confidential data require a password to deactivate the screen saver.

16.5 Policy References

16.5.1 HIPAA Regulatory References

CFR TITLE 45 § 164.310(b), CFR TITLE 45 § 164.312(a)(2)(i)

16.5.2 NIST References

NIST SP 800-53 R4 IA-5, NIST SP 800-53 R4 AC-11, NIST SP 800-53 R4 PE-18, NIST SP 800-53 R4 PE-5, NIST SP 800-53 R4 SC-10, NIST SP 800-53 R4 AC-17, NIST SP 800-53 R4 AC-17(1), NIST SP 800-53 R4 AC-17(2), NIST SP 800-53 R4 AC-17(4), NIST SP 800-53 R4 AC-18, NIST SP 800-53 R4 AC-2, NIST SP 800-53 R4 AC-6(3), NIST SP 800-53 R4 CM-2, NIST SP 800-53 R4 CM-2(2), NIST SP 800-53 R4 IA-2, NIST SP 800-53 R4 IA-3, NIST SP 800-53 R4 IA-8, NIST SP 800-53 R4 IA-8(1), NIST SP 800-53 R4 IA-8(2), NIST SP 800-53 R4 IA-8(3), NIST SP 800-53 R4 IA-8(4), NIST SP 800-53 R4 MA-4

17 SANCTIONS POLICY

17.1 Statement of Purpose

The purpose of this policy is to ensure that violations of policies, procedures, regulations, and standards are addressed through a Grand County disciplinary process that includes sanctions.

17.2 Statement of Applicability

This policy applies to all workforce members regardless of physical location.

17.3 Sanctions Policy

1. Grand County workforce members must comply with Grand County policies and procedures, federal regulations (e.g., HIPAA, HITECH), state regulations (e.g., data breach notification laws, health codes), and accreditation standards (e.g., Joint Commission).
2. Grand County ensures that policies, procedures, regulations, and standards are followed and that appropriate sanctions are taken against workforce members who violate them.

17.4 Disciplinary Process

1. Grand County develops and employs a formal disciplinary process for workforce members who fail to comply with Grand County policies, federal regulations (e.g., HIPAA, HITECH), and state regulations (e.g., data breach notification laws, health codes).
2. The formal disciplinary process is commenced after verification that an incident has occurred.
3. The formal disciplinary process ensures correct and fair treatment for workforce members who are suspected of committing incidents.
4. Potential sanctions resulting from the disciplinary process may include but are not limited to:
    a. Remedial training
    b. Performance evaluation impacts and documentation
    c. Suspension or removal of access rights to Grand County information assets
    d. License, registration, or certification denial or revocation
    e. Termination of employment and/or relationship with Grand County.
5. Grand County appoints a contact in Human Resources to handle incidents involving workforce members.
6. Grand County maintains a list of workforce members involved in incidents including the outcome of the investigation.
7. In cases where civil or criminal charges are involved, the CISO works together with Human Resources and Legal Counsel to determine and take appropriate legal action.

17.5 Policy References

17.5.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(a)(1)(ii)(C), CFR TITLE 45 § 164.414(a), CFR TITLE 45 § 164.530(e)

17.5.2 CJIS References

CJIS V5.9 Sections 5.12

18 TERMINATION POLICY

18.1 Statement of Purpose

The purpose of this policy is to ensure Grand County-owned information assets are retrieved, and logical and physical access is revoked or updated, when a workforce member's or third-party individual's employment, contract, or agreement is terminated, or in certain cases when their roles and/or responsibilities are significantly altered upon a change of employment status (e.g., job transfers, job re-grading, restructuring, etc.).

18.2 Statement of Applicability

This policy applies to all workforce members and all personnel affiliated with third parties regardless of physical location.

18.3 Termination Policy

1. Grand County develops and implements termination procedures.
2. Terminations and changes of job position resulting in changes of roles and responsibilities (e.g., job transfers, job re-grading, restructuring, etc.) are communicated in a timely manner by Human Resources.
3. Whenever there is a change in employment status or responsibilities, logical and physical access is reviewed and updated or revoked as necessary according to this policy and the Access Control Policy.
4. Responsibilities for removing or updating workforce member's or third parties' logical and physical access are clearly defined and assigned.
5. All workforce members and third parties return any Grand County information assets and property in their possession upon termination of their employment, contract, or agreement.

18.4 Voluntary Termination

1. The departing workforce member or third party deletes all files and email messages that are of a personal nature.
2. The CISO decides to transfer all Grand County files and email messages to the Grand County network prior to the workforce member's or third-party individual's departure.
3. Grand County explicitly maintains ownership of confidential data.
4. All other accounts are disabled within 24 hours according to the Access Control Policy.
5. The workforce member or third-party individual surrenders all Grand County property (e.g., information assets, documents, credit cards, access cards, media, removable media, business mobile computing devices, etc.) prior to departure.

18.5 Involuntary Termination

1. Grand County immediately terminates physical and logical access rights whenever there is increased risk (e.g., in the case of serious misconduct).
2. The CISO retrieves all Grand County property (e.g., information assets, documents, credit cards, access cards, media, removable media, business mobile computing devices, etc.) during the termination process.
3. Termination procedures allow for immediate escorting off site, if necessary.

18.6 Revocation of Access Rights

1. The access rights of all workforce members and third parties are removed upon termination of their employment, contract or agreement, or adjusted upon a change of employment (e.g., job transfers, job re-grading, restructuring, etc.) in accordance with this policy and the Access Control Policy.

2. Upon termination or changes in employment for workforce members or third-party users, physical and logical access rights and associated materials (e.g., passwords, access cards, keys, etc.) are removed or modified to restrict access within 24 hours.
3. Changes of employment or other workforce arrangement (e.g., transfers) are reflected in removal of all access rights that were not approved for the new employment or workforce arrangement.
4. Access changes due to personnel transfer are managed effectively.
5. The access rights that are removed or adapted include physical and logical access, keys, identification cards, IT systems and applications, subscriptions, and removal from any documentation that identifies them as a current member of the organization.
6. If a departing workforce member or third party has passwords for accounts that will remain active, these account passwords are changed upon termination or change of employment, contract, agreement, or another workforce arrangement.
7. Access rights to information assets and facilities is reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors including:
    a. Whether the termination or change is initiated by the workforce member or third-party user, or instead by management.
    b. The underlying reason for the termination.
    c. The current responsibilities of the workforce member or third party involved.
    d. The value of Grand County information assets currently accessible to the workforce member or third party.

18.7 Email Access Revocation

1. Grand County email accounts are deactivated upon termination of employment, contract, agreement, or other workforce arrangement, or if the email account is no longer sponsored, unless otherwise allowed under this policy.
2. On the date of termination, Grand County email accounts expire unless a temporary extension has been requested by the CISO following an assessment of information security and institutional risks (e.g., legal exposure, reputational, access to Grand County enterprise data, etc.) that could potentially result should the account be extended.

18.8 Policy References

18.8.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308 (a)(3)(ii)(A), CFR TITLE 45 § 164.308 (a)(3)(ii)(B), CFR TITLE 45 § 164.308 (a)(3)(ii)(C), CFR TITLE 45 § 164.308 (a)(4)(i), CFR TITLE 45 § 164.308 (a)(4)(ii)(B), CFR TITLE 45 § 164.308 (a)(4)(ii)(C), CFR TITLE 45 § 164.308 (a)(5)(ii)(C), CFR TITLE 45 § 164.308(a)(3)(ii)(C), CFR TITLE 45 § 164.308(a)(3)(ii)(C), CFR TITLE 45 § 164.312(a)(2)(i), CFR TITLE 45 § 164.312(a)(2)(ii)

18.8.2 NIST References

NIST SP 800-53 R4 PS-4, NIST SP 800-53 R4 PS-5, NIST SP 800-53 R4 AC-2, NIST SP 800-53 R4 PS-4(2)

19 BUSINESS CONTINUITY MANAGEMENT POLICY

19.1 Statement of Purpose

The purpose of this policy is to ensure that strategies and plans are in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

The purpose of this policy is to ensure the maintenance, integrity, and availability of essential enterprise data including data backup and storage requirements.

19.2 Statement of Applicability

This policy applies to all workforce members, users, and all personnel affiliated with third parties who access or use Grand County information assets, regardless of physical location.

19.3 Business Continuity Management Policy

1. Grand County develops, implements, tests, and maintains a Business Continuity Plan (BCP) that covers all assets that deliver or support core critical business functions.
2. The BCP ensures that Grand County maintains compliance with statutory requirements (e.g., HIPAA, HITRUST, PCI, applicable state regulations, etc.) during and after a business disruption.
3. Grand County develops, implements, tests, and maintains a contingency plan in accordance with 8 CCR 1505-2 Rule 20.12.
4. On a weekly basis, Grand County makes full backup of essential enterprise data, system documentation, and software using an automated backup system.
5. Daily, Grand County makes an incremental backup of essential enterprise data, system documentation, and software using an automated backup system.
6. Grand County stores backups in a physically secure remote location, at enough distance to make them reasonably immune from damage to data at the primary site. Physical and environmental controls are in place for the backups.
7. Grand County maintains records of the backups, including content and current location.
8. Backups are encrypted according to the Encryption Policy.
9. Grand County Information Systems conducts regular tests of the backup media and restoration process.
10. Backup media at Grand County premises is physically protected according to the Physical and Environmental Security Policy.
11. When backup service is delivered by a third party, the Service Level Agreement (SLA) includes details on controlling confidentiality, integrity, and availability of the backup information according to the Third-Party Risk Management Policy.

19.4 Business Impact Analysis

1. Grand County conducts a risk assessment of events that can cause interruptions to its operational processes and identify, estimate, and prioritize risks to these processes.
2. Grand County conducts a business impact analysis to identify critical operational processes and to determine recovery criticality.
3. Grand County identifies outage impacts and estimated down time.
4. Grand County identifies resource requirements.
5. Grand County identifies recovery priorities for critical systems.
6. Grand County identifies mitigation options, steps, and costs.

19.5 Data Criticality Analysis

1. Grand County assesses the relative criticality of all data, so that such data may be properly protected during emergencies and during normal business operations.

2. Data subject to criticality analysis includes individually identifiable health information, including PHI.
3. Criticality analysis is the responsibility of the Privacy Officer (County Manager), who works in cooperation with legal counsel and other internal parties as necessary to execute and document such analyses.
4. The most critical data and applications are given the given the highest priority in terms of investment and emergency protection preparations; with less critical categories or types of data and applications receiving proportionately less funding and attention, as appropriate.
5. In conducting data and applications analyses, the CISO employs the technical guidance and recommendations of the National Institute of Standards and Technology (NIST), or other information technology industry leading practices, as appropriate.
6. Grand County fully documents all analyses of the relative criticality of both data and applications.

19.6 Design and Develop the Business Continuity Plan

1. Grand County develops and implements the BCP to ensure Grand County can restore operations and establish availability of information in the required time frame following interruption to, or failure of, critical operational business processes.
2. Grand County identifies roles and responsibilities and designates the BCP owner.
3. Grand County ensures the secure protection of confidential data, and ensure that confidentiality, accessibility and integrity are preserved.
4. Grand County develops BCP activation criteria including notification and escalation plans.
5. Grand County develops BCP deactivation criteria including notification of the return to normal operations and clean up procedures.

19.7 Design and Develop the Back Up Plan

1. Grand County identifies and implements an alternate, geographically-separated site for back-up and recovery continuity support, including equipment and budget for the site.
2. Grand County implements a Backup Plan containing the following for each system:
   a. Scope of data to backup
   b. Frequency of backup including time of day
   c. Type of backup (e.g., full, differential, incremental)
   d. Location of backup
   e. Retention of backup
   f. Restoration procedures including restoration time
3. The Backup Plan defines the storage location for backup logs automatically generated by the backup system.
4. The Backup Plan defined the email notifications automatically generated by the backup system.

19.8 Implement the Business Continuity Plan

1. Grand County prepares emergency response and detailed recovery procedures and checklists.
2. Grand County stores the BCP in a geographically separate remote location.
3. Grand County develops a BCP distribution list and distribute copies of the BCP to key contingency personnel.
4. Grand County provides business continuity and crisis management awareness to all workforce members on an annual basis.

19.9 Testing the Business Continuity Plan

1. Grand County tests the BCP annually at a minimum to ensure that it is up-to-date and effective.
2. Grand County defines testing exercises and testing scenarios.
3. Grand County ensures that all workforce members can perform their roles and carry out their responsibilities when the BCP is activated.

4. Grand County evaluates the results of BCP tests and provide a report to senior leadership, including improvement recommendations and resource requirements.

19.10 Maintaining the Business Continuity Plan

1. Grand County reviews and updates the BCP annually, at a minimum.
2. Grand County updates the BCP with lessons learned during the testing exercises.
3. Grand County updates the BCP upon acquisition of new equipment, upgrading of systems, or other business events including but not limited to the following:
    a. Changes in personnel, location, facilities, or resources
    b. Revisions in legislation
    c. Updated processes and procedures
    d. Changes to operational and financial risk
4. Grand County distributes the updated BCP to key contingency personnel on the BCP distribution list.

19.11 Policy References

19.11.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(a)(1)(ii)(A), CFR TITLE 45 § 164.308(a)(7)(i), CFR TITLE 45 § 164.308(a)(7)(ii)(A), CFR TITLE 45 § 164.308(a)(7)(ii)(B), CFR TITLE 45 § 164.308(a)(7)(ii)(C), CFR TITLE 45 § 164.308(a)(7)(ii)(D), CFR TITLE 45 § 164.308(a)(7)(ii)(E), CFR TITLE 45 § 164.310(a)(2)(i), CFR TITLE 45 § 164.310(d)(2)(iv), CFR TITLE 45 § 164.312(a)(2)(ii), CFR TITLE 45 § 164.312(c)(1)

19.11.2 NIST References

NIST SP 800-53 R4 CP-1, NIST SP 800-53 R4 CP-2, NIST SP 800-53 R4 CP-2(8), NIST SP 800-53 R4 PM-9, NIST SP 800-53 R4 PM-8, NIST SP 800-53 R4 RA-3, "NIST SP 800-53 R4 CP-1, NIST SP 800-53 R4 CP-10, NIST SP 800-53 R4 CP-10(2), NIST SP 800-53 R4 CP-10(4), NIST SP 800-53 R4 CP-11, NIST SP 800-53 R4 CP-2(1), NIST SP 800-53 R4 CP-2(2), NIST SP 800-53 R4 CP-2(3), NIST SP 800-53 R4 CP-2(5), NIST SP 800-53 R4 CP-6, NIST SP 800-53 R4 CP-6(1), NIST SP 800-53 R4 CP-6(3), NIST SP 800-53 R4 CP-7, NIST SP 800-53 R4 CP-7(1), NIST SP 800-53 R4 CP-7(2), NIST SP 800-53 R4 CP-7(3), NIST SP 800-53 R4 CP-7(4), NIST SP 800-53 R4 CP-8, NIST SP 800-53 R4 CP-8(1), NIST SP 800-53 R4 CP-8(2), NIST SP 800-53 R4 CP-9, NIST SP 800-53 R4 CP-9(2), NIST SP 800-53 R4 CP-4, NIST SP 800-53 R4 CP-4(1), NIST SP 800-53 R4 CP-4(2), NIST SP 800-53 R4 CP-4(4)

19.11.3 Code of Colorado Regulations References

8 CCR 1505-1 Rule 20

20 INCIDENT MANAGEMENT POLICY

20.1 Statement of Purpose

The purpose of this policy is to ensure that information security events, and weaknesses associated with information systems, are handled in a timely manner and allow corrective action to be taken.

This policy governs the actions required for reporting and responding to security incidents involving Grand County information assets. The policy is provided to ensure effective and consistent handling of such events to limit any potential impact to the confidentiality, availability and integrity of Grand County information assets.

20.2 Statement of Applicability

This policy applies to all workforce members, users, and all personnel affiliated with third parties who access or use Grand County information assets, regardless of physical location.

20.3 Information Security Incident Response Capability

1. The Information Security Incident Response Capability (ISIRC) is documented in the Incident Response Plan which includes the following at a minimum:
    a. Incident Response Team (IRT) roles and responsibilities
    b. Incident Response Procedures
    c. Incident Response Communications Plan
2. Grand County implements an insider threat program that includes a cross-discipline insider threat IRT.
3. All workforce members receive mandatory incident response training.
4. Grand County adheres to regulatory requirements for responding to a data breach of protected health information (PHI) and reporting the breach to affected individuals, media, and federal agencies in accordance with federal and state laws and regulations.

20.4 Reporting Security Incidents

1. Security Incidents must be reported immediately to the CISO. All workforce members and third-party users are aware of their responsibility to report any security incidents as quickly as possible.
2. Workforce members who report security incidents in good faith are protected against retaliation.
3. Grand County provides a means for anonymously reporting security incidents.
4. All workforce members and third-party users of information assets and services report any observed or suspected security weaknesses in information assets or services to the CISO.
5. Security Incidents involving civil or criminal charges are promptly reported to law enforcement (e.g., FBI, district attorney, state and local law enforcement, etc.) and incident reporting organizations (e.g., US-CERT) by the CISO and by Legal Counsel.
6. The CISO develops and maintains a contact list for reporting security incidents to law enforcement if it is suspected that laws may have been broken.
7. The CISO develop and maintain a contact list of third parties for reporting security incidents in case of a reportable security incident.
8. Reports and communications to the OCR are made without unreasonable delay and no later than 60 days after the discovery of a security incident, unless otherwise stated by law enforcement orally or in writing, according to the incident response communication plan.
9. A log is maintained of unauthorized disclosures of PHI and submitted to the appropriate parties annually (e.g., HHS).

20.5 Reporting Voter System Malfunctions

1. Voter system malfunctions must be reported immediately to the Clerk & Recorder and CISO as these incident reports are required no later than 24 hours to the Colorado Secretary of State
    a. The notice must include a description, date, and the names of those who witnessed the malfunction, as well as the procedures followed before the malfunction, and any error messages displayed. The notice may be verbal, but a written notice must follow.

20.6 Responding to Security Incidents

1. Management responsibilities and incident response procedures are established to ensure a quick, effective, and orderly response to security incidents.
2. The CISO (or designee appointed by ISIRC) is the point of contact for coordinating security incident responses.

3. Grand County implements a formal Incident Response Plan to handle different types of information security incidents including, but not limited to:
    a. information system failures and loss of service
    b. malicious code
    c. denial of service
    d. errors resulting from incomplete or inaccurate business data
    e. breaches of confidentiality and integrity
    f. disclosures of unprotected health information
    g. misuse of information systems
    h. identity theft
    i. unauthorized wireless access points
4. In addition to normal contingency plans, the Incident Response Plan also covers:
    a. analysis and identification of the cause of the incident;
    b. containment;
    c. increased monitoring of system use;
    d. planning and implementation of corrective actions to prevent recurrence;
    e. assigning a single point of contact responsible for sharing information and coordinating responses.
5. The Incident Response Plan is communicated to the appropriate individuals in Grand County.
6. Following a security incident, audit trails and evidence are secured, system and data access controlled, emergency actions documented, actions reported to senior leadership, and system and control integrity confirmed.
7. Change management requests are opened for events that require permanent fixes.
8. Where action against a person or organization after a security incident involves legal action (either civil or criminal), evidence is collected, retained, and presented in support of potential legal action in accordance with the rules for evidence in the relevant jurisdictions.

20.7 Reviewing Security Incidents

1. Grand County quantifies and monitors the types, volumes, and costs of security incidents.
2. The information gained from the evaluation of security incidents is used to identify recurring or high impact security incidents.
3. Security incidents (or a sample of security incidents) are reviewed on an annual basis to identify necessary improvements to security controls.
4. Incident response testing exercises are conducted at least annually. The results of the exercises must be documented and must be used to update the Incident Response Plan and incident response procedures.

20.8 Policy References

20.8.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(a)(1)(ii)(D), CFR TITLE 45 § 164.308(a)(6)(i), CFR TITLE 45 § 164.308(a)(6)(ii), CFR TITLE 45 § 164.314(a)(2)(i), CFR TITLE 45 § 164.404(a)(1), CFR TITLE 45 § 164.404(a)(2), CFR TITLE 45 § 164.404(b), CFR TITLE 45 § 164.404(c)(1), CFR TITLE 45 § 164.404(c)(2), CFR TITLE 45 § 164.404(d)(1), CFR TITLE 45 § 164.404(d)(2), CFR TITLE 45 § 164.404(d)(3), CFR TITLE 45 § 164.406(a), CFR TITLE 45 § 164.406(b), CFR TITLE 45 § 164.406(c), CFR TITLE 45 § 164.408(a), CFR TITLE 45 § 164.408(b), CFR TITLE 45 § 164.408(c), CFR TITLE 45 § 164.410(a)(1), CFR TITLE 45 § 164.410(a)(2), CFR TITLE 45 § 164.410(b), CFR TITLE 45 §

164.410(c)(1), CFR TITLE 45 § 164.410(c)(2), CFR TITLE 45 § 164.412, CFR TITLE 45 § 164.414(b), CFR TITLE 45 § 164.530(f)

20.8.2 NIST References

NIST SP 800-53 R4 CP-2, NIST SP 800-53 R4 CP-4, NIST SP 800-53 R4 IR-4, NIST SP 800-53 R4 IR-6, NIST SP 800-53 R4 IR-7(2), NIST SP 800-53 R4 PM-15, NIST SP 800-53 R4 SI-5, NIST SP 800-53 R4 SI-5 (1), NIST SP 800-53 R4 IR-1, NIST SP 800-53 R4 IR-2, NIST SP 800-53 R4 IR-4(1), NIST SP 800-53 R4 IR-4(7), NIST SP 800-53 R4 IR-6(1), NIST SP 800-53 R4 PM-12, NIST SP 800-53 R4 SI-4, NIST SP 800-53 R4 CA-7, NIST SP 800-53 R4 PL-4, NIST SP 800-53 R4 SI-2, NIST SP 800-53 R4 IR-3, NIST SP 800-53 R4 IR-3(2), NIST SP 800-53 R4 IR-5, NIST SP 800-53 R4 IR-7, NIST SP 800-53 R4 IR-7(1), NIST SP 800-53 R4 IR-8, NIST SP 800-53 R4 SE-2, NIST SP 800-53 R4 IR-4(4), NIST SP 800-53 R4 IR-5, NIST SP 800-53 R4 IR-5(1), "NIST SP 800-53 R4 AU-11, NIST SP 800-53 R4 AU-9

20.8.3 CJIS References

CJIS V5.9 Sections 5.3, 5.13.5

20.8.4 Code of Colorado Regulations References

8 CCR 1505-1 Rule 11.7

21 INFORMATION ASSET MANAGEMENT POLICY

21.1 Statement of Purpose

The purpose of this policy is to establish requirements for management of Grand County information assets. The recording, documenting, classifying, and maintenance of information assets is critical for protecting the confidentiality, integrity, and availability of confidential data.

21.2 Statement of Applicability

This policy addresses all information assets that are utilized at Grand County.

21.3 Information Asset Management Policy

1. Grand County information assets belong to Grand County, which possesses the exclusive right to manage and direct actions regarding those information assets in accordance with organizational policies and procedures so long as asserting and exercising this right does not conflict with federal or state law or regulations.
2. No expectation of privacy exists regarding Grand County information assets in accordance with organization policies and procedures, excepting privacy rights explicitly protected according to federal or state law or regulation, or in Grand County policies and procedures (e.g., privacy of PHI protected under HIPAA, etc.).
3. Data contained on Grand County systems are the sole property of the organization. Users do not own or have rights to Grand County data outside of its use in the performance of their Grand County duties.
4. Rules for the acceptable use of information assets are identified, documented, and implemented according to the Acceptable Use Policy.
5. Grand County uses the Data Classification and Handling Policy to classify information assets into one of three sensitivity levels (tiers).
6. Procedures for information asset labeling, handling, and storage are developed and implemented in accordance with the Data Classification and Handling Policy.

21.4 Inventory of Information Assets

1. All information assets are clearly identified and an inventory of all information assets drawn up and maintained.
2. All information assets, hardware and software, which are capable of communicating externally (IP network, phone line, cellular, etc.) from themselves are required to be reported to the Grand County Information Systems department to be recorded within the Configuration Management Database (CMDB).
3. The information asset inventory must include enough details to recover from a disaster.
4. Grand County is responsible for establishing procedures to issue information assets to employees and contractors.
5. An inventory for each component of the voting system will be maintained by the Clerk & Recorder.
    a. The records will include manufacturer, make, model, serial number, and date of acquisition.
    b. The inventory must be in an electronic format and exportable to a comma separated file.
6. The information asset inventory is reviewed annually.

21.5 Ownership of Information Assets

1. All information assets are owned by a designated information asset owner.
2. The information asset owner is assigned, at a minimum, the responsibility for creating, updating, and removing information assets from the information asset inventory by contacting the Grand County Information Systems department.

21.6 Secure Disposal or Re-Use of Information Assets

1. All information assets that are being reused or released outside of organizational control are checked to ensure that all confidential data and licensed software has been removed.
2. All information assets that are being taken out of service permanently are processed to render all confidential data on the information asset non-retrievable by any means.
3. All information assets being permanently taken out of service are removed from the information asset inventory.

21.7 Policy References

21.7.1 HIPAA Regulatory References

CFR TITLE 45 § 164.310(b), CFR TITLE 45 § 164.310(c), CFR TITLE 45 § 164.310(d)(1), CFR TITLE 45 § 164.310(d)(2)(iii)

21.7.2 NIST References

NIST SP 800-53 R4 CM-8, NIST SP 800-53 R4 CM-8(1), NIST SP 800-53 R4 CM-8(3), NIST SP 800-53 R4 CM-8(5), NIST SP 800-53 R4 MP-1, NIST SP 800-53 R4 PM-5, NIST SP 800-53 R4 SE-1, NIST SP 800-53 R4 CM-10, NIST SP 800-53 R4 AC-20, NIST SP 800-53 R4 PL-4, NIST SP 800-53 R4 PL-4(1), NIST SP 800-53 R4 CM-8(7), NIST SP 800-53 R4 RA-2, NIST SP 800-53 R4 AC-16, NIST SP 800-53 R4 AC-8, NIST SP 800-53 R4 MP-3

21.7.3 Code of Colorado Regulations References

8 CCR 1505-1 Rule 11.2

22 CONFIGURATION MANAGEMENT POLICY

22.1 Statement of Purpose

The purpose of this policy is to minimize risk to Grand County and to ensure the operational effectiveness and continuity of Grand County's Information Technology (IT) environment by managing the configuration of Grand County's information assets.

22.2 Statement of Applicability

This policy applies to all Grand County information assets, services, and associated documentation.

22.3 Configuration Management Plan

1. The Configuration Management Plan includes, at a minimum:
   a. Roles and responsibilities.
   b. Configuration management processes and procedures.
   c. A definition of the items in the IT Infrastructure that must be placed under configuration management.
   d. Processes for putting IT acquisition and development (pre-production) items under configuration management.
   e. Processes for managing, testing, documenting, deciding upon, and communicating status of the configuration of the items that are subject to configuration management.

22.4 Security of System Configuration Documentation

1. System configuration documentation is treated as confidential data with minimum necessary and need-to-know access, and is protected against unauthorized access in accordance with the Access Control Policy.

22.5 Baseline Configurations

1. Grand County develops, documents, controls, and maintains current baseline configurations for all managed information systems.
2. Grand County reviews and updates the baseline configurations of the managed information systems at least annually.
3. Grand County retains older versions of baseline configurations as deemed necessary to support continuity of operations (e.g., rollback of a system update).
4. Grand County ensures voting system configuration complies with 8 CCR 1505-1 Rule 20.

22.6 Configuration Settings

1. Grand County establishes and documents mandatory configuration settings for IT infrastructure items using a security configuration checklist that reflects the least privilege mode consistent with operational requirements.
2. Grand County identifies and documents exceptions from the mandatory configuration settings for individual components within information systems based on explicit operational requirements. Exceptions are managed through the exception waiver process.
3. Grand County incorporates detection of unauthorized, security-relevant configuration changes into the Incident Response Plan to ensure that such detected events are tracked, monitored, corrected, and available in accordance with the Incident Management Policy.

22.7 Configuration Change Control

1. The implementation of changes, including patches, service packs, and other updates and modifications, is controlled by the Change Management Policy.
2. Where feasible, Grand County audits activities associated with configuration-controlled changes to information systems.

22.8 Information System Boundary Protection Mechanisms

1. Operational failure of the boundary protection mechanism will not result in any unauthorized release of information outside of the information system boundary (i.e. the device "fails closed" vs. "fails open").

22.9 Least Functionality

1. Grand County configures information systems to provide only essential capabilities and specifically prohibit or restrict the use of non-essential functions, ports, protocols, and/or services to reduce risk.

22.10 IT Infrastructure Inventory

1. Grand County develops, documents, and maintains an inventory of IT Infrastructure items. Inventory detail must be maintained at enough level for purposes of tracking and reporting.
2. Grand County continuously updates the IT Infrastructure inventory as an integral part of installations, removals, and information system updates.

22.11 Information Systems Diagrams

1. Grand County Information Systems will ensure that complete diagrams depicting the interconnectivity of the network are maintained in a current state.
2. The library of available information systems diagrams will include:
    a. All communication paths, circuits, and other components used for the interconnection, beginning with the county-owned system(s) and traversing through all interconnected systems to the county endpoint.
    b. Identification if the information system contains PHI, PII, PCI or CJI information.

22.12 Policy References

22.12.1 HITRUST References

09.r Security of System Documentation, 10.h Control of Operational Software

22.12.2 NIST References

NIST SP 800-53 R4 SA-5, NIST SP 800-53 R4 CM-2(3), NIST SP 800-53 R4 CM-3, NIST SP 800-53 R4 CM-3(2), NIST SP 800-53 R4 CM-4, NIST SP 800-53 R4 CM-6, NIST SP 800-53 R4 CM-6(1), NIST SP 800-53 R4 CM-6(2), NIST SP 800-53 R4 SA-22, NIST SP 800-53 R4 CM-7(4)

22.12.3 CJIS References

CJIS V5.9 Sections 5.7, 5.10

22.12.4 Code of Colorado Regulations References

8 CCR 1505-1 Rule 20

23 CHANGE MANAGEMENT POLICY

23.1 Statement of Purpose

The purpose of this policy is to ensure that changes are effective and efficient with minimal disruption to Grand County's operations.

23.2 Statement of Applicability

This policy must be followed by all workforce members and third parties who work on Grand County IT systems and infrastructure.

Changes to systems that are exclusively used for development, testing, or staging are excluded from this policy. Shared systems, such as routers that serve multiple environments, are included in this policy because a change to a shared system might have an unexpected impact on the production environment.

23.3 Change Management Policy

1. Grand County manages changes through a change control process. This change control process ensures that changes are effective and efficient with minimal disruption to Grand County.
2. Any IT infrastructure change that has the potential to negatively impact the ability of Grand County to conduct business must be managed in accordance with this policy.
3. Prior to implementing changes, the following must occur, at a minimum:
    a. A written change request must be submitted
    b. Change requests are reviewed by the requisite business executive(s), IT, management, and where appropriate the CISO from a security perspective
    c. Where feasible, changes must be tested on a non-production system
    d. A roll back plan must be in place
4. Any decision to upgrade an information system to a new release considers:
    a. Business requirements for the Change
    b. Security and privacy impacts
    c. Risks
5. Changes are scheduled in a manner designed to minimize disruption of and impact upon Grand County's ability to conduct business.
6. All changes affecting computing facilities (e.g., air-conditioning, water, heat, plumbing, electricity, alarm systems, etc.) must be reported to IT management prior to implementation.
7. The Clerk & Recorder must perform tests in accordance with 8 CCR 1505-1 section 11.3 no later than ten (10) days prior to an election for a voting system being placed into production for usage during said election.
8. Any unauthorized changes that are detected are reported to the CISO.

23.4 Segregation of Duties

1. Where feasible, separation of duties for execution and auditing is enforced to reduce opportunities for unauthorized or unintentional modification or misuse of Grand County's information assets.
2. Where feasible, no single person shall access, modify, or use information systems without authorization or detection.

23.5 Separation of Development, Test, and Production Environments

1. Where feasible, development, test, and operational environments are separated and controlled to reduce the risks of unauthorized access or changes to production.
2. Testing is completed in a testing environment, where feasible.
3. Confidential data in the production environment is not copied into a development or testing environment.

23.6 Policy References

23.6.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(a)(3)(i), CFR TITLE 45 § 164.308(a)(4)(i), CFR TITLE 45 § 164.308(a)(4)(ii)(A), CFR TITLE 45 § 164.310(a)(2)(iv), CFR TITLE 45 § 164.312(a)(1)

23.6.2 NIST References

NIST SP 800-53 R4 AC-1, NIST SP 800-53 R4 AT-1, NIST SP 800-53 R4 AU-1, NIST SP 800-53 R4 CA-1, NIST SP 800-53 R4 CM-1, NIST SP 800-53 R4 CP-1, NIST SP 800-53 R4 IA-1, NIST SP 800-53 R4 IR-1, NIST SP 800-53 R4 MA-1, NIST SP 800-53 R4 MP-1, NIST SP 800-53 R4 PE-1, NIST SP 800-53 R4 PL-1, NIST SP 800-53 R4 PM-1, NIST SP 800-53 R4 PS-1, NIST SP 800-53 R4 RA-1, NIST SP 800-53 R4 SA-1, NIST SP 800-53 R4 SC-1, NIST SP 800-53 R4 SI-1, NIST SP 800-53 R4 CM-3, NIST SP 800-53 R4 CM-4, NIST SP 800-53 R4 CM-5, NIST SP 800-53 R4 CM-9, NIST SP 800-53 R4 AC-5, NIST SP 800-53 R4 CM-2, NIST SP 800-53 R4 SA-10, NIST SP 800-53 R4 CM-2(3), NIST SP 800-53 R4 CM-3, NIST SP 800-53 R4 CM-3(2), NIST SP 800-53 R4 CM-4, NIST SP 800-53 R4 CM-6, NIST SP 800-53 R4 CM-6(1), NIST SP 800-53 R4 CM-6(2), NIST SP 800-53 R4 SA-22, NIST SP 800-53 R4 CM-7(4), NIST SP 800-53 R4 AC-3, NIST SP 800-53 R4 CM-2(1), NIST SP 800-53 R4 CM-2(2), NIST SP 800-53 R4 CM-2(6), NIST SP 800-53 R4 CM-3, NIST SP 800-53 R4 CM-3(1), NIST SP 800-53 R4 CM-4(1), NIST SP 800-53 R4 CM-4(2), NIST SP 800-53 R4 CM-5(1), NIST SP 800-53 R4 CM-5(2)

23.6.3 CJIS References

CJIS V5.9 Sections 5.7

23.6.4 Code of Colorado Regulations References

8 CCR 1505-1 Rule 11.3

24 PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

24.1 Statement of Purpose

The purpose of this policy is to ensure that Grand County provides adequate physical and environmental safeguards to avoid damage or unauthorized access to confidential data and information assets.

24.2 Statement of Applicability

This policy applies to all Grand County facilities and to all Grand County information assets regardless of physical location.

24.3 Physical and Environmental Security Policy

1. Grand County prevents unauthorized physical access, damage, and interference with the organization's premises and information assets.

24.4 Physical Security Perimeters

1. Grand County designs and implements physical security perimeters (e.g., walls, controlled entrances, staffed reception desks, etc.) to protect areas that contain confidential data and information assets.
2. All external doors are protected against unauthorized entry with control mechanisms (e.g., bars, alarms, locks etc.).
3. Windows that can be opened are kept locked and additional protection is provided for all accessible windows.

24.5 Physical Entry Controls

1. Grand County reviews and updates the physical access lists and authorization credentials on a regular basis.
2. Where feasible, Grand County enforces physical access controls and maintain an audit trail of access according to the Audit Logging, and Monitoring Policy.

3. Grand County develops and implements visitor access logs to record access to secure areas by visitors and third-party support personnel.
4. Grand County reviews the visitor access logs periodically or on occurrence of a security incident as defined in the Incident Management Policy.
5. The visitor logs are retained for at least 3 months or in accordance with the Record Retention Policy.

24.6 Facility Security Maintenance Records Policy

1. Grand County maintains facility security maintenance records to document repairs and changes to physical elements of a facility related to security.

24.7 Protecting Against External and Environmental Threats

1. Grand County designs and implements physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster.
2. Fire suppression systems (e.g., sprinklers, gas, etc.) and fire detection systems (e.g., smoke or heat activated) are installed, protected and maintained according to applicable laws and regulations.

24.8 Working in Secure Areas

1. Vacant secure areas are physically locked and periodically checked.
2. Workforce members do not use photographic, video, audio, or other recording equipment such as cameras in mobile devices, to record confidential data.
3. Keypad door codes or locks and vault combinations to areas in which election management software is used at least once per calendar year prior to the first election of the year.
4. Access to code, lock, or combination to ballot storage areas, counting room, and election equipment is restricted to employees who have successfully passed a criminal background check.

24.9 Public Access, Delivery, and Loading Areas

1. Where feasible, delivery and loading areas are designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building and to secure areas.

24.10 Equipment Siting and Protection

1. Information assets are physically located to minimize potential damage from physical and environmental threats and hazards, and to minimize the opportunities for unauthorized access.
2. Hazardous or combustible materials are stored at a safe distance from a secure area.
3. Bulk supplies such as printer paper, etc. are not stored within a secure area.
4. Backup information assets and media are stored at a safe distance from the main site to avoid damage from disaster affecting the main site.
5. Where feasible, information assets processing confidential data are positioned, and the viewing angle restricted, to reduce the risk of information being viewed by unauthorized persons.
6. Where deemed appropriate by the CISO, device locks (e.g., slot locks, port controls, peripheral switch controls, cable traps, etc.) are implemented for information assets containing confidential data.
7. Where feasible, Grand County restricts physical access to wireless access points, networking and communications hardware, and telecommunication lines.
8. Grand County protects election equipment using physical locking mechanisms and seals in accordance with 8 CCR 1505-1 rule 20.

24.11 Supporting Utilities

1. Information assets supporting critical business operations is protected from power failures and other disruptions caused by failures in supporting utilities (e.g., electricity, water supply, steam pipes, sewage, heating/ventilation, and air conditioning).
2. Supporting utilities are regularly inspected and tested to ensure their proper functioning and to reduce any risk from malfunction or failure.
3. A suitable electrical supply is provided that conforms to the equipment manufacturer's specifications.
4. An uninterruptable power supply (UPS) is required for Information Assets that support critical business operations to support orderly close down or transition to generators.
5. Power contingency plans cover the action to be taken on failure of the UPS.
6. UPS equipment and generators are regularly tested in accordance with the manufacturer's recommendations to ensure they have adequate capacity.
7. The water supply is stable and adequate to supply air conditioning, humidification equipment, and fire suppression systems.

24.12 Cabling Security

1. Where feasible, power and telecommunications cabling carrying data or supporting information services is protected from interception or damage.
2. Access to patch panels and cable rooms is controlled.
3. Clearly identifiable cable and equipment markings is used to minimize handling errors, such as accidental patching of wrong network cables.

24.13 Information Asset Maintenance

1. Only authorized maintenance personnel carry out repairs and service information assets.
2. Appropriate controls (e.g., authorization levels) is implemented and considers whether the maintenance is performed by workforce members or third parties.
3. Grand County establishes a process for requesting and approving physical access for maintenance personnel.
4. Grand County maintains a list of approved maintenance organizations and authorized maintenance personnel.

24.14 Remote Maintenance

1. Grand County approves and monitors remote maintenance and diagnostic activities.
2. Grand County employs strong identification and authentication techniques when establishing remote maintenance and diagnostic sessions.
3. Grand County does not allow the use of generic accounts by third parties.
4. Grand County maintains records of remote maintenance and diagnostic activities.
5. Grand County terminates all remote sessions and network connections when maintenance is complete.

24.15 Security of Information Assets Off-Premises

1. Security is applied to off-site information assets considering the different risks of working outside of Grand County premises.
2. Regardless of ownership, the use of any information asset outside of Grand County premises must be authorized. This includes information assets used by remote workers, even where such use is permanent (i.e., a core feature of the employee's role).
3. Information assets and media taken off the premises are not left unattended in public places.
4. Portable computing devices (e.g., laptops, tablets, etc.) are carried as hand luggage, disguised where possible, and are protected from damage when traveling.

5. Manufacturers' instructions for protecting information assets are observed at all times (e.g., protection against exposure to strong electromagnetic fields).
6. Adequate insurance coverage is in place to protect information assets off-site.
7. Transportation and transmission of data and information assets will comply with all applicable United States and foreign export laws and regulations.

24.16 Policy References

24.16.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(a)(3)(ii)(A), CFR TITLE 45 § 164.310(a)(1), CFR TITLE 45 § 164.310(a)(2)(i), CFR TITLE 45 § 164.310(a)(2)(ii), CFR TITLE 45 § 164.310(a)(2)(iii), CFR TITLE 45 § 164.310(a)(2)(iv), CFR TITLE 45 § 164.310(b), CFR TITLE 45 § 164.310(c), CFR TITLE 45 § 164.310(d)(1), CFR TITLE 45 § 164.310(d)(2)(iii), CFR TITLE 45 § 164.312(c)(1)

24.16.2 NIST References

NIST SP 800-53 R4 SC-24, NIST SP 800-53 R4 PE-2, NIST SP 800-53 R4 PE-3(1), NIST SP 800-53 R4 PE-6, NIST SP 800-53 R4 PE-6(1), NIST SP 800-53 R4 PE-8, NIST SP 800-53 R4 PE-3, NIST SP 800-53 R4 PE-6(2), NIST SP 800-53 R4 AT-3(1), NIST SP 800-53 R4 PE-1, NIST SP 800-53 R4 PE-13, NIST SP 800-53 R4 PE-13(1), NIST SP 800-53 R4 PE-13(2), NIST SP 800-53 R4 PE-13(3), NIST SP 800-53 R4 PE-15, NIST SP 800-53 R4 PE-15(1), NIST SP 800-53 R4 PE-16, NIST SP 800-53 R4 AC-18, NIST SP 800-53 R4 PE-14, NIST SP 800-53 R4 PE-18, NIST SP 800-53 R4 PE-18(1), NIST SP 800-53 R4 CP-8, NIST SP 800-53 R4 PE-10, NIST SP 800-53 R4 PE-11, NIST SP 800-53 R4 PE-12, NIST SP 800-53 R4 PE-9, NIST SP 800-53 R4 CM-8(3), NIST SP 800-53 R4 PE-4, NIST SP 800-53 R4 MA-1, NIST SP 800-53 R4 MA-2, NIST SP 800-53 R4 MA-3, NIST SP 800-53 R4 MA-3(1), NIST SP 800-53 R4 MA-3(2), NIST SP 800-53 R4 MA-3(3), NIST SP 800-53 R4 MA-4, NIST SP 800-53 R4 MA-4(1), NIST SP 800-53 R4 MA-4(2), NIST SP 800-53 R4 MA-4(3), NIST SP 800-53 R4 MA-5, NIST SP 800-53 R4 MA-6, NIST SP 800-53 R4 AC-20, NIST SP 800-53 R4 MP-5, NIST SP 800-53 R4 PE-17

24.16.3 CJIS References

CJIS V5.9 Sections 5.13

24.16.4 Code of Colorado Regulations References

8 CCR 1505-1 Rule 20

25 AUDIT LOGGING AND MONITORING POLICY

25.1 Statement of Purpose

The purpose of this policy is to address the regulatory requirements for safeguarding the confidentiality, integrity, and availability of Grand County information assets through auditing, logging, and monitoring activities.

25.2 Statement of Applicability

This policy applies to all workforce members, users, and all personnel affiliated with third parties who access or use Grand County information assets, regardless of physical location.

This policy applies to information technology administered centrally; personally-owned computing devices connected by wire or wireless to the Grand County network; and to off-site computing devices that connect remotely to Grand County's network.

25.3 Audit Logging, and Monitoring Policy

1. Grand County implements processes to create audit trails of user activity and monitors access of information systems on a routine basis.
2. Whenever possible, Business Associate Agreements (BAAs) with third parties require the creation of an audit trail of user activity. Grand County retains the right to audit the audit trail.
3. Grand County audits, logs, and monitors access and events to detect, report, and guard against:
    a. Network vulnerabilities and intrusions
    b. Performance problems and flaws in applications
    c. Privacy and security violations
    d. Unauthorized access to confidential data
    e. Breaches in confidentiality and security of confidential data
    f. Degradation or loss of information integrity (e.g., improper alteration or destruction of confidential data)

25.4 Auditable Events

1. Grand County develops and implements an Audit Event Plan to identify which systems, applications, and processes carry out auditing activities.
2. The Audit Event Plan defines what types of events are subject to auditing. At a minimum, the following events must be audited where feasible:
    a. Normal system events (e.g., startup, shutdown, login attempts, errors, security policy changes, software installations, etc.).
    b. User account permission changes.
    c. Account password changes.
    d. Audit log file changes.
    e. Information changes (e.g., create, read, update, delete) including confidential data.
    f. Unauthorized access to confidential data to detect the snooping of records.
3. The CISO periodically reviews and updates the Audit Event Plan. This review includes consideration of events that require auditing on a continuous basis, and events that require auditing in response to specific situations based upon an assessment of risk.

25.5 Content of Audit Records

1. Audit record content provides enough detail to determine whether a given individual took an action.
2. Audit records containing confidential data include the date, time, origination and destination of the message, but not its contents.

25.6 Audit Record Retention

1. Grand County retains source audit records for a minimum of 90 days to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational record retention requirements.
2. Audit Records are archived and retained for a minimum of one (1) year in accordance with the Record Retention Policy.

25.7 Audit Monitoring, Review, Analysis and Reporting

1. Grand County reviews and analyzes audit records at a minimum of once per week for evidence of suspicious, unusual, and inappropriate activity.
2. Grand County reports anomalous auditable events and related security incidents to the CISO, who is responsible for reporting security and compliance issues to senior leadership as appropriate.

3. Grand County adjusts the level of audit review, analysis, and reporting within systems when there is a change in risk to operations, assets, individuals, and other organizations based on law enforcement information, intelligence information, or other credible sources of information.
4. Grand County establishes procedures for monitoring the use of systems and facilities to test the effectiveness of access control and security mechanisms. The results of the monitoring activities are reviewed on a regular basis.
5. Monitoring activities include execution of privileged operations, authorized access, unauthorized access attempts, and system alerts or failures.

25.8 Policy References

25.8.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(a)(1)(ii)(B), CFR TITLE 45 § 164.308(a)(1)(ii)(C), CFR TITLE 45 § 164.308(a)(1)(ii)(D), CFR TITLE 45 § 164.308(a)(3)(ii)(A), CFR TITLE 45 § 164.308(a)(4)(i), CFR TITLE 45 § 164.308(a)(4)(ii)(B), CFR TITLE 45 § 164.308(a)(5)(ii)(C), CFR TITLE 45 § 164.310(a)(2)(ii), CFR TITLE 45 § 164.312(b), CFR TITLE 45 § 164.316(a), CFR TITLE 45 § 164.316(b)(1), CFR TITLE 45 § 164.316(b)(2)(iii)

25.8.2 NIST References

NIST SP 800-53 R4 AU-1, NIST SP 800-53 R4 AU-2, NIST SP 800-53 R4 CA-2, NIST SP 800-53 R4 PL-2, NIST SP 800-53 R4 AC-6(1), NIST SP 800-53 R4 AU-9, NIST SP 800-53 R4 AC-2(4), NIST SP 800-53 R4 AC-6(9), NIST SP 800-53 R4 AR-4, NIST SP 800-53 R4 AU-11, NIST SP 800-53 R4 AU-2(3), NIST SP 800-53 R4 AU-3, NIST SP 800-53 R4 AU-3(1), NIST SP 800-53 R4 AU-5, NIST SP 800-53 R4 AU-5(4), NIST SP 800-53 R4 AU-8, NIST SP 800-53 R4 AU-9(4), NIST SP 800-53 R4 AU-9(5), NIST SP 800-53 R4 AC-2(12), NIST SP 800-53 R4 AU-6, NIST SP 800-53 R4 AU-6(1), NIST SP 800-53 R4 AU-6(3), NIST SP 800-53 R4 AU-6(9), NIST SP 800-53 R4 AU-7, NIST SP 800-53 R4 AU-7(1), NIST SP 800-53 R4 PE-6, NIST SP 800-53 R4 SI-3, NIST SP 800-53 R4 SI-4, NIST SP 800-53 R4 SI-4(1), NIST SP 800-53 R4 SI-4(2), NIST SP 800-53 R4 SI-4(3), NIST SP 800-53 R4 SI-4(4), NIST SP 800-53 R4 SI-4(5), NIST SP 800-53 R4 SI-7(2) "NIST SP 800-53 R4 AU-5, NIST SP 800-53 R4 AU-5(1), NIST SP 800-53 R4 AU-5(2), NIST SP 800-53 R4 AU-9(1), NIST SP 800-53 R4 AU-9(2), NIST SP 800-53 R4 AU-9(3), NIST SP 800-53 R4 AU-12, NIST SP 800-53 R4 SI-11, NIST SP 800-53 R4 AU-8, NIST SP 800-53 R4 AU-8(1)

25.8.3 CJIS References

CJIS V5.9 Sections 5.4, 5.10

26 AUTHENTICATION MANAGEMENT POLICY

26.1 Statement of Purpose

The purpose of this policy is to protect Grand County information assets by managing and enforcing password requirements.

26.2 Statement of Applicability

This policy applies to all workforce members who use Grand County information assets and related resources.

This policy applies to all Grand County information assets, personal computing devices connecting to the Grand County network, and to off-site computing devices connecting remotely to the Grand County network.

This policy applies to system administrators who manage or design systems that require passwords for authentication.

26.3 Password Management

1. Controls are implemented to maintain the security of passwords including:
    a. Strong passwords are required.
        a. At least fourteen (14) characters in length
        b. Containing at least one number and special character
        c. Not the same as the username or email address
        d. Not the same as any of the last 24 passwords used
    b. Passwords do not display as they are entered.
    c. Passwords are changed whenever there is any indication of possible system or password compromise.
    d. User identity is verified before performing password resets.
    e. Passwords are not included in any automated log-on process (e.g., stored in a macro or function key).
    f. Failed log in attempts result in user lock out after 5 attempts in 15 minutes.
    g. Lockout duration is required and implemented at 15 minutes.
    h. Documented approval by the CISO is required for information assets not utilizing an automatic lock out process.
2. Controls are implemented to maintain the security of initial or temporary passwords:
    a. Users are provided with an initial or temporary strong password that is unique and random.
    b. Passwords are provided to users in a secure manner.
    c. Transmitting passwords through the use of unencrypted (clear text) messages is prohibited.
    d. Users acknowledge receipt of passwords.
    e. Initial or temporary passwords are changed at the first log in.
    f. Where possible, initial or temporary passwords expire after 72 hours.
3. Passwords are changed every 90 days for regular accounts and every 60 days for privileged accounts.

26.4 Vendor Password Management

1. Vendor-supplied default accounts are deleted, disabled or otherwise altered.
2. Vendor-supplied passwords are changed.

26.5 Password Management Systems

1. A password management system is implemented to:
    a. Enforce the use of unique individual User IDs and passwords to maintain accountability.
    b. Prevent the use of the same password for multiple System Administrator accounts.
    c. Allow users to select their own passwords and include a confirmation procedure to allow for input errors.
    d. Force users to change temporary passwords at the first log-on.
    e. Prevent the display of passwords on the screen as they are being entered.

26.6 Policy References

26.6.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(a)(5)(ii)(D)

26.6.2 NIST References

NIST SP 800-53 R4 IA-2, NIST SP 800-53 R4 IA-5, NIST SP 800-53 R4 IA-5(1), NIST SP 800-53 R4 IA-5(7), NIST SP 800-53 R4 IA-6

26.6.3 CJIS References

CJIS V5.9 Sections 5.6.2, 5.10.1.4

27 ENCRYPTION POLICY

27.1 Statement of Purpose

The purpose of this policy is to establish the methods for protecting the confidentiality, authenticity and integrity of confidential data at rest, in transit, and in storage with encryption, and to ensure that encryption standards meet regulatory requirements.

27.2 Statement of Applicability

All workforce members who have access or exposure to Grand County confidential data are required to comply with this policy.

27.3 Regulation of Encryption

1. Compliance with all relevant regulations is reviewed no less than annually.

27.4 Policy on the Use of Encryption

1. Confidential information is encrypted prior to being transmitted across the public network.
2. When CJI is transmitted or at rest outside the boundary of the physically secure location, the data shall be immediately protected by FIPS 140-2 certified encryption with a symmetric cipher key strength of at least 128 bits; unless explicitly allowed by exception in CJIS sections 5.10.1.2.1, 5.13.1.2.2 and 5.10.2.
3. Mobile computing devices, and removable media that contain or transmit confidential data must be encrypted to protect against unauthorized access, loss, or alteration.
4. All encryption mechanisms implemented to comply with this policy must support a minimum of 256-bit AES (Advanced Encryption Standard) encryption, or equivalent.
5. When transmitting confidential data using removable media the sending party must:
    a. Use an encryption mechanism to protect against unauthorized access or modification.
    b. Authenticate the requesting person or entity.
6. If un-encrypted confidential data is discovered on removable media, the confidential data is transferred to either to a Grand County managed computing device or to an approved, encrypted removable media format.
7. If un-encrypted media has been used for confidential data storage, the unencrypted media must be turned in to the CISO, or designated representative, for proper disposal as soon as the data has been transferred to an approved, encrypted media and format.

27.5 Encryption Key Management

1. Encryption keys and/or passwords are not printed nor allowed to directly accompany removable media. They must be physically and electronically separate.

2. All communications of encryption keys and/or passwords must take place via a secure method (e.g., telephone, secure email, etc.).
3. Encryption key management is implemented based on specific roles and responsibilities and in consideration of national and international regulations, restrictions and issues.
4. Encryption keys and the equipment to generate, store, and archive keys are logically and physically protected against modification, loss, destruction and disclosure.
5. Access to encryption keys is limited to authorized Grand County employees and not revealed to consultants, contractors, vendors, or other third parties.
6. Where feasible, encryption keys are encrypted in storage by use of a key vault use.

27.6 Policy References

27.6.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(a)(1)(ii)(D), CFR TITLE 45 § 164.312(a)(2)(iv), CFR TITLE 45 § 164.312(e)(2)(ii)

27.6.2 NIST References

NIST SP 800-53 R4 AR-1, NIST SP 800-53 R4 AR-2, NIST SP 800-53 R4 SC-28, NIST SP 800-53 R4 SC-28(1), NIST SP 800-53 R4 SI-12, NIST SP 800-53 R4 IA-7, NIST SP 800-53 R4 CA-2, NIST SP 800-53 R4 CA-2(2), NIST SP 800-53 R4 CA-7, NIST SP 800-53 R4 RA-5, NIST SP 800-53 R4 MP-1, NIST SP 800-53 R4 SC-1, NIST SP 800-53 R4 SC-13, NIST SP 800-53 R4 SC-12, NIST SP 800-53 R4 SC-12(1), NIST SP 800-53 R4 SC-17

27.6.3 CJIS References

CJIS V5.9 Sections 5.10.1

28 NETWORK PROTECTION POLICY

28.1 Statement of Purpose

The purpose of this policy is to ensure the protection of Grand County enterprise data.

28.2 Statement of Applicability

This policy applies to all users and computing devices connecting to any Grand County information systems network.

Remote work and security requirements for wireless connections outside of Grand County premises (e.g., home networks, hot spots, hotel networks, etc.) are outside the scope of this policy.

28.3 Use of Network Services

1. Grand County determines provisioning of access to specific networks and network services, and specifies the means of access allowed, including specific ports, protocols and services.

28.4 Network Controls

1. Grand County manages and control its networks in order to protect Grand County enterprise data and other information assets that access, traverse, or reside within the Grand County network.
2. Information systems diagrams exist and are updated when network changes occur.
3. All databases, servers and other system components storing or processing confidential data are placed behind a firewall to limit external network traffic to the internal network.
4. Changes to the DMZ which affect the security posture are approved by the CISO and documented in the network diagram.
5. Credit card data (subject to PCI-DSS) and transactions are segregated from other network traffic.

6. Where feasible, network devices are identified and authenticated prior to establishing a connection.
7. Firewalls are configured to deny inbound traffic by default (deny all, permit by exception [DAPE]).
8. The firewall rule set(s) is reviewed periodically.
9. Firewalls restrict inbound traffic to the minimum necessary ports and protocols.
10. Grand County utilizes firewalls that employ stateful packet inspection where available.
11. Firewall and router baseline configuration standards are defined and implemented and reviewed at least annually.
12. Firewall, router, and network connection changes are approved prior to implementing the changes. Changes are documented in accordance with the Configuration Management Policy. If testing cannot be accomplished prior to implementation, the proposed changes and a rollback plan must be approved by the CISO prior to implementation.
13. Grand County uses at least two different DNS servers which are geographically separated for public (external) name resolution.
14. Where feasible, Grand County uses at least two different DNS servers for internal name resolution.

28.5 Security of Outsourced Network Services

1. Security features, service levels, and management requirements for all network services are identified and included in any network services agreements.
2. Formal agreements with third party network service providers include specific obligations for security and privacy.
3. Services provided by a third-party network service provider are formally managed and regularly monitored to ensure they are in accordance with the terms of the formal agreements.

28.6 Security of Voting Systems

1. Grand County will not allow any component of the voting system to connect to another device by modem, router, or gateway.
2. Grand County will not connect or allow a connection of any voting system component to the Internet.
3. Voting system providers may not have administrative or user access to the county's election management system.
4. Voting system components which have Wi-Fi capability or a wireless device will have such capability or device disabled before use in an election.

28.7 Wireless Network Controls

1. Grand County maintains an inventory of authorized WAPs (WAP) to support identification of unauthorized WAP's.
2. Grand County identifies rogue Access Points and removes them from the network.
3. Wireless networks are included in network diagrams and other network documentation.
4. Vendor defaults for WAPs are changed prior to implementation of the access point. At a minimum, this includes changing the manufacturer's default settings for encryption keys, SSIDs, known and trusted wireless devices, and passwords.
5. WAPs are configured with strong encryption (WPA2 at a minimum, with a fourteen character minimum key length).
6. Scans are performed routinely to identify unauthorized WAPs. Unauthorized WAPs attached to the Grand County network are disabled and other appropriate incident response measures are taken in accordance with the Incident Management Policy.
7. All wireless network devices are identified and authenticated prior to establishing a connection to an internal (non-guest) network.

8. Only WAPs expressly authorized by the CISO are connected to the Grand County onsite network.

28.8 Wireless Network User Policies

1. Wireless network use is subject to applicable Grand County policies.
2. Guest wireless networks are configured to deny all access to Grand County internal networks.
3. Grand County reserves the right to prohibit or deny connections to its wireless networks at any time for any reason.

28.9 Policy References

28.9.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(b)(1), CFR TITLE 45 § 164.308(b)(3), CFR TITLE 45 § 164.312(a)(2)(i), CFR TITLE 45 § 164.312(c)(1), CFR TITLE 45 § 164.312(c)(2), CFR TITLE 45 § 164.312(d), CFR TITLE 45 § 164.312(e)(1), CFR TITLE 45 § 164.312(e)(2)(i), CFR TITLE 45 § 164.312(e)(2)(ii), CFR TITLE 45 § 164.314(a)(1), CFR TITLE 45 § 164.314(a)(2)(ii)

28.9.2 NIST References

NIST SP 800-53 R4 AC-1, NIST SP 800-53 R4 AC-17, NIST SP 800-53 R4 AC-18, NIST SP 800-53 R4 AC-20, NIST SP 800-53 R4 AC-6, NIST SP 800-53 R4 CM-7, NIST SP 800-53 R4 AC-17(1), NIST SP 800-53 R4 AC-17(2), NIST SP 800-53 R4 AC-17(4), NIST SP 800-53 R4 AC-2, NIST SP 800-53 R4 AC-6(3), NIST SP 800-53 R4 CM-2, NIST SP 800-53 R4 CM-2(2), NIST SP 800-53 R4 IA-2, NIST SP 800-53 R4 IA-3, NIST SP 800-53 R4 IA-8, NIST SP 800-53 R4 IA-8(1), NIST SP 800-53 R4 IA-8(2), NIST SP 800-53 R4 IA-8(3), NIST SP 800-53 R4 IA-8(4), NIST SP 800-53 R4 MA-4, NIST SP 800-53 R4 IA-5, NIST SP 800-53 R4 CM-7, NIST SP 800-53 R4 CM-7(1), NIST SP 800-53 R4 CM-7(2), NIST SP 800-53 R4 CM-7(4), NIST SP 800-53 R4 CM-7(5), NIST SP 800-53 R4 MA-4(2), NIST SP 800-53 R4 MA-4(3), NIST SP 800-53 R4 PE-3(1), NIST SP 800-53 R4 PE-3(4), NIST SP 800-53 R4 AC-4, NIST SP 800-53 R4 AC-4(2), NIST SP 800-53 R4 SC-21, NIST SP 800-53 R4 SC-32, NIST SP 800-53 R4 SC-7, NIST SP 800-53 R4 AC-17, NIST SP 800-53 R4 AC-17(3), NIST SP 800-53 R4 AC-2(11), NIST SP 800-53 R4 SC-7(3), NIST SP 800-53 R4 SC-7(4), NIST SP 800-53 R4 SC-7(5), NIST SP 800-53 R4 SC-7(7), NIST SP 800-53 R4 SC-7(8), NIST SP 800-53 R4 SC-8, NIST SP 800-53 R4 RA-2, NIST SP 800-53 R4 SC-4, NIST SP 800-53 R4 SC-39, NIST SP 800-53 R4 AC-18, NIST SP 800-53 R4 AC-18(1), NIST SP 800-53 R4 AC-18(4), NIST SP 800-53 R4 AC-18(5), NIST SP 800-53 R4 CA-3, NIST SP 800-53 R4 CM-3, NIST SP 800-53 R4 CP-2, NIST SP 800-53 R4 IA-3, NIST SP 800-53 R4 SC-19, NIST SP 800-53 R4 SC-20, NIST SP 800-53 R4 SC-22, NIST SP 800-53 R4 SC-7(18), NIST SP 800-53 R4 SC-7(5), NIST SP 800-53 R4 SC-8(1), NIST SP 800-53 R4 SC-8(2), NIST SP 800-53 R4 SI-4, NIST SP 800-53 R4 CA-3(5), NIST SP 800-53 R4 SA-9, NIST SP 800-53 R4 SA-9(2)

28.9.3 CJIS References

CJIS V5.9 Sections 5.13

28.9.4 Code of Colorado Regulations References

8 CCR 1505-1 Rule 20

29 ACCESS CONTROL POLICY

29.1 Statement of Purpose

The purpose of this policy is to establish Grand County requirements to manage and control access to information assets and information service in support of compliance with legal regulations (e.g., HIPAA) and to protect and lower risk to business operations.

29.2 Statement of Applicability

All workforce members who may have access or exposure to Grand County information assets are required to comply with this policy.

This policy covers access to all enterprise data regardless of whether that data is stored on or provided via Grand County information assets or on a third-party-hosted service or equipment.

29.3 Access Control Policy

1. The access control program is reviewed and updated at least annually.
2. Access control rules and rights for each user or group of users is based on minimum necessary, role-based access rights.
3. Access controls for both logical and physical access are considered together.
4. Where possible, systems and applications will be configured to allow only one active session per user.

29.4 System Use Notification

1. Where possible, information systems will display an approved system use notification message prior to granting access to inform the users of usage and monitoring rules.
2. The system use notification message shall, at a minimum, provide the following information:
    a. Inform the user that they are accessing a restricted information system;
    b. Inform the user that the usage may be monitored, recorded, and subject to audit;
    c. Inform the user that unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties
    d. Inform the user that use of the system indicates consent to monitoring and recording.

29.5 User Registration

1. Grand County has a formal, documented process for establishing, activating, modifying, reviewing, disabling, and removing accounts. This user registration and de-registration process includes workforce member transfers, third party accounts, maintenance accounts, and external access.
2. Grand County defines account types (e.g., individual, shared/group, system, application, guest/anonymous, emergency, temporary, etc.). Guest/anonymous, shared/group, emergency and temporary accounts are specifically authorized and monitored.
3. Default and unnecessary accounts (e.g., system, guest, vendor or other third-party accounts) are removed, disabled, or otherwise secured (e.g., change the default passwords, reduce privileges to the lowest levels of access).

29.6 Privilege Management

1. The allocation and use of privileged access to information systems and services is restricted and controlled.
2. An authorization record of all privileged accounts is maintained. Privileges are not granted until the authorization process is complete.

29.7 Review of Access Rights

1. A full review of user access rights is conducted at least an annual basis following a formal documented process.
2. A user's access rights are reviewed by their supervisor after any changes, such as promotion, transfer, demotion, or termination of employment.
3. Evidence of these reviews, including documented approval, is submitted for review and retention according to the Record Retention Policy. Follow-up actions resulting from the review are documented and included as part of the evidence submitted to the CISO.

29.8 Remote Access

1. Where feasible, multi-factor authentication is implemented for all remote access according to the Remote Access Policy.
2. Where feasible, users are only provided with remote access to network services for which they have been specifically authorized.
3. Where feasible, accounts for remote maintenance and remote administration are authorized and disabled or deactivated when not in use.
4. Encrypted communications (e.g., VPN) solutions are implemented for remote access to the Grand County network.
5. Scans to identify and review any unauthorized remote access connections are performed on a routine basis.

29.9 Remote Diagnostic and Configuration Port Protection

1. Where feasible, access to network equipment is physically protected (e.g., a router must be stored in a room that is only accessible by authorized workforce members or third parties) such that remote diagnostic and configuration ports are protected.

29.10 Network Segregation

1. Where feasible, groups of information services, users, and information systems are segregated on networks.
2. Firewalls maintain segregation between internal, external, and virtual networks, including Demilitarized Zones (DMZ) and enforce access control policies for each of the domains.
3. The Grand County network is logically segmented by a defined security perimeter and traffic is controlled based on functionality required and classification of the associated data, applications, or systems.
4. Network segregation architecture and security design logic are documented and reviewed annually.

29.11 Network Connection Controls

1. At external network interfaces, inbound network traffic is denied by default and allowed by exception (i.e., deny all, permit by exception).
2. Network traffic is controlled through firewall and other network-related restrictions.
3. Transmitted information is secured in accordance with the Data Classification and Handling Policy.

29.12 User Identification and Authentication

1. Grand County requires unique user IDs for all types of users (e.g., employees, contractors, third parties, etc.), and duplicate user IDs are not issued to other users.
2. Passwords are not stored by applications or databases after authorization (even if encrypted).

29.13 Use of System Utilities

1. The use of system utility programs that might be capable of overriding system and application controls is restricted and tightly controlled.

29.14 Session Time-out

1. A password-protected screen saver locks the screen after ten minutes of inactivity. Exceptions to this policy provision may be granted and documented by the CISO.
2. Where feasible, network sessions close after fifteen minutes of inactivity.
3. The system requires the user to re-establish access using appropriate identification and authentication procedures.

4. A limited form of time-out system can be provided for legacy systems that cannot be modified to accommodate this requirement, which clears the screen and prevents unauthorized access through re-authentication requirements.

29.15 Sensitive Systems Isolation

1. Where feasible, information assets containing confidential data have a dedicated and logically and/or physically isolated computing environment.
2. The sensitivity level of applications and systems is explicitly identified and documented according to the *Data Classification and Handling Policy*.
3. The dedicated and isolated computing environment will only be accessible by authorized personnel. The list of authorized personnel is reviewed on an annual basis by the CISO.

29.16 Policy References

29.16.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308 (a)(3)(i), CFR TITLE 45 § 164.308 (a)(3)(ii)(a), CFR TITLE 45 § 164.308 (a)(4)(i), CFR TITLE 45 § 164.308 (a)(4)(ii)(B), CFR TITLE 45 § 164.308(a)(3)(i), CFR TITLE 45 § 164.308(a)(3)(ii)(A), CFR TITLE 45 § 164.308(a)(3)(ii)(B), CFR TITLE 45 § 164.308(a)(3)(ii)(C), CFR TITLE 45 § 164.308(a)(4)(i), CFR TITLE 45 § 164.308(a)(4)(ii)(A), CFR TITLE 45 § 164.308(a)(4)(ii)(B), CFR TITLE 45 § 164.308(a)(4)(ii)(C), CFR TITLE 45 § 164.308(a)(5)(ii)(D), CFR TITLE 45 § 164.310(a)(2)(iii), CFR TITLE 45 § 164.310(b), CFR TITLE 45 § 164.312(a)(1), CFR TITLE 45 § 164.312(a)(2)(i), CFR TITLE 45 § 164.312(a)(2)(ii), CFR TITLE 45 § 164.312(a)(2)(ii)(i), CFR TITLE 45 § 164.312(a)(2)(ii)(iv), CFR TITLE 45 § 164.312(a)(2)(iii), CFR TITLE 45 § 164.312(a)(2)(iv), CFR TITLE 45 § 164.312(d)

29.16.2 NIST References

NIST SP 800-53 R4 AC-1, NIST SP 800-53 R4 AC-2, NIST SP 800-53 R4 AC-5, NIST SP 800-53 R4 MP-1, NIST SP 800-53 R4 AC-2, NIST SP 800-53 R4 AC-2(1), NIST SP 800-53 R4 AC-2(2), NIST SP 800-53 R4 AC-21, NIST SP 800-53 R4 AC-5, NIST SP 800-53 R4 IA-1, NIST SP 800-53 R4 IA-4, NIST SP 800-53 R4 IA-5, NIST SP 800-53 R4 IA-5(3), NIST SP 800-53 R4 AC-10, NIST SP 800-53 R4 AC-2, NIST SP 800-53 R4 AC-21, NIST SP 800-53 R4 AC-3, NIST SP 800-53 R4 AC-3(7), NIST SP 800-53 R4 AC-6, NIST SP 800-53 R4 AC-6(1), NIST SP 800-53 R4 AC-6(10), NIST SP 800-53 R4 AC-6(5), NIST SP 800-53 R4 AC-6(9), NIST SP 800-53 R4 CM-7, NIST SP 800-53 R4 PS-4, NIST SP 800-53 R4 PS-5, NIST SP 800-53 R4 AC-10, NIST SP 800-53 R4 AC-7, NIST SP 800-53 R4 AC-8, NIST SP 800-53 R4 AC-9, NIST SP 800-53 R4 AT-2, NIST SP 800-53 R4 AU-12, NIST SP 800-53 R4 AU-2, NIST SP 800-53 R4 IA-6, NIST SP 800-53 R4 AC-6(2), NIST SP 800-53 R4 IA-2, NIST SP 800-53 R4 IA-2(1), NIST SP 800-53 R4 IA-2(11), NIST SP 800-53 R4 IA-2(12), NIST SP 800-53 R4 IA-2(2), NIST SP 800-53 R4 IA-2(3), NIST SP 800-53 R4 IA-2(8), NIST SP 800-53 R4 IA-4, NIST SP 800-53 R4 IA-5, NIST SP 800-53 R4 IA-5(11), NIST SP 800-53 R4 IA-5(2), NIST SP 800-53 R4 IA-5(3), NIST SP 800-53 R4 IA-5(7), NIST SP 800-53 R4 IA-8, NIST SP 800-53 R4 AC-3, NIST SP 800-53 R4 AC-6, NIST SP 800-53 R4 AU-2, NIST SP 800-53 R4 SC-2, NIST SP 800-53 R4 AC-11, NIST SP 800-53 R4 AC-11(1), NIST SP 800-53 R4 AC-12, NIST SP 800-53 R4 SC-10, NIST SP 800-53 R4 IA-11, NIST SP 800-53 R4 SC-43, NIST SP 800-53 R4 AC-1, NIST SP 800-53 R4 AC-14, NIST SP 800-53 R4 AC-3, NIST SP 800-53 R4 AC-6, NIST SP 800-53 R4 DM-1, NIST SP 800-53 R4 SC-13, NIST SP 800-53 R4 SC-15

29.16.3 CJIS References

CJIS V5.9 Sections 5.5, 5.6

30 REMOTE ACCESS POLICY

30.1 Statement of Purpose

This policy establishes how Grand County ensures the security of remote access to the organization's network in order to protect confidential data and information assets.

30.2 Statement of Applicability

This policy is applicable to all users who work outside of Grand County's environment, who connect to Grand County's network, systems, applications, and data, including but not limited to applications that contain Grand County confidential data, from a remote location. See the Mobile Device Security Policy.

30.3 Remote Access Policy

1. Grand County manages and controls access to its internal and external networks. Users are only provided with access to internal and external networks that they have been specifically authorized to use. Appropriate authentication methods are used to control access by remote users.
2. All users who connect to Grand County's networks from a remote location only use Grand County approved and managed secure remote access technologies, as determined by the CISO
3. Remote access users are responsible for adhering to all of Grand County's policies, not engaging in illegal activities, and not using remote access for interests other than those of Grand County.

30.4 Requesting Remote Access

1. Remote access is strictly controlled and is only granted to workforce members with written approval by both the CISO and appropriate Department Head (or designee).
2. Remote users must sign the Teleworker's Acknowledgment Agreement.
3. All users granted remote access privileges must sign and comply with the Confidentiality Agreement kept on file with Human Resources.
4. Remote access accounts that have shown no activity for 90 days are automatically be disabled. The CISO is responsible for ensuring this occurs.

30.5 Remote Security

1. Connectivity from a user's remote location to Grand County's network is a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees necessary for enabling their connectivity from the remote location. These expenses are not reimbursable.
2. All computing devices that remotely connect to the Grand County network must adhere to the following:
    a. anti-malware software and security patches are kept up-to-date.
    b. configuration of personal routers and wireless networks meet security and configuration standards established by Grand County.
    c. baseline configuration that complies with Grand County policies.
    d. A firewall is in use and may not be disabled without the explicit approval of the CISO.
3. Grand County maintains remote access logs according to the Audit Logging, and Monitoring Policy.
4. System Administrators review remote access logs on a regular basis to detect suspicious activity.
5. Encryption protects the confidentiality and integrity of remote access sessions to the internal network and to external systems.

30.6 Remote Privacy

1. Remote users, including Business Associates and other third parties, log-off and disconnect from Grand County's network when access is no longer required to perform job responsibilities.
2. Remote users comply with the Clear Desk and Clear Screen Policy and lock the workstation and/or system(s) when unattended so that no other individual is able to access any confidential data.
3. Where possible, remote access users are automatically disconnected from the Grand County network when there is no recognized activity for 15 minutes.
4. Remote access users ensure that unauthorized individuals do not access the Grand County network. Remote access users do not provide their username or password to anyone, or configure their remote access device to remember or automatically enter their username and password.
5. Remote access users must take necessary precautions to secure all Grand County information assets and confidential data in their possession.

30.7 Policy References

30.7.1 HIPAA Regulatory References

CFR TITLE 45 § 164.312(e)(1)

30.7.2 NIST References

NIST SP 800-53 R4 AC-17, NIST SP 800-53 R4 AC-17(2), NIST SP 800-53 R4 AC-20, NIST SP 800-53 R4 AC-6, NIST SP 800-53 R4 AT-2, NIST SP 800-53 R4 IA-2, NIST SP 800-53 R4 PE-17, NIST SP 800-53 R4 PL-4

31 MOBILE DEVICE SECURITY POLICY

31.1 Statement of Purpose

The purpose of this policy is to establish security measures that protect against the information security risks associated with using mobile devices.

31.2 Statement of Applicability

This policy applies to all mobile devices that connect to the Grand County network and access confidential data regardless of who owns the device.

All workforce members utilizing mobile devices connecting to the Grand County network and accessing confidential data assume the responsibility for the security and privacy of information contained within.

31.3 Mobile Device Policy

1. Usage of mobile devices must comply with all international, federal and state laws, and Grand County policies. Unauthorized disclosure of confidential data may violate federal and/or state laws, and/or ethical standards, and may cause injury.

31.4 Personal Mobile Device Policy

1. The owner of any personal mobile device connecting to Grand County information assets is fully responsible for the behavior of all users on the mobile computing device, and for all data and network traffic accessed or transmitted to and from the mobile computing device, regardless of whether the owner is aware of the data and network traffic.
2. Personal mobile devices must connect to Mobile Device Management to access the Grand County network.
3. Personal mobile devices may be subject to additional restrictions or security measures as determined by the CISO.

31.5 Business Mobile Device Policy

1. Mobile devices issued by Grand County for business purposes remain the property of Grand County.
2. When the business mobile device is allocated, the user assumes responsibility for physical security of the device and any Grand County data contained within.
3. Prior to leaving the employ of Grand County, the user returns the mobile device in accordance with the Termination Policy.
4. All business mobile devices must be disposed of in accordance with the Media Protection Policy after they reach end of life.

31.6 Acceptable Use Policy

1. The Acceptable Use Policy applies to all mobile devices regardless of ownership.
2. Users are responsible for ensuring mobile device applications and multimedia capabilities are not used to breach privacy and confidentiality according to the Acceptable Use Policy.
3. Users must agree to take responsibility for the security of their mobile device and the Grand County data contained therein.
4. Users have no expectation of privacy associated with any of the Grand County data they store in or send through mobile devices.
5. Users are not permitted to bypass, or attempt to bypass, security protections on mobile devices connected to the Grand County network or communication systems.
6. Users are responsible for ensuring that confidential data is only transmitted using approved and secure communication functions including Grand County email.
7. Users only transmit protected health information (PHI) by secure messaging solutions.

31.7 Physical Protection Policy

1. Any mobile device containing confidential data is not left unattended in public areas (e.g., vehicles, hotel rooms, conference rooms, airports, etc.), even for a short period of time, without being physically protected.
2. All mobile devices containing confidential data are carried as hand luggage when traveling and never checked as baggage nor stored anywhere prohibiting immediate access or visual contact with the device.
3. If a mobile device containing confidential data is lost or stolen, the incident must be reported according to the Incident Management Policy.
4. County provided mobile devices will be equipped with protections (e.g. cases) that protect the device from damage due to unintentional drops.

31.8 Public Places

1. Users of mobile devices containing confidential data take care to avoid the unintentional disclosure of confidential information to unauthorized persons in public places.

31.9 Access Controls

1. All mobile devices require authentication (e.g., password, pin number, biometric, etc.). No mobile device allows unauthenticated (guest) access to the Grand County network.
2. All mobile devices automatically time out within five minutes of inactivity according to the Access Control Policy. If locked, the mobile device requires re-authentication to unlock.

31.10 Encryption

1. All mobile devices are encrypted according to the Encryption Policy.
2. If encryption is not reasonable and appropriate, Grand County documents the acceptance of risk.

31.11 Network Connections

1. Grand County only authorizes connections of mobile devices to the Grand County network if the devices meet the requirements of this policy.
2. Personal mobile devices that access the Grand County network using wireless technology (e.g., Wi Fi, Bluetooth) must be configured to request confirmation before establishing a connection for the first time.
3. Mobile devices that remotely access the Grand County network comply with the Remote Access Policy.
4. Grand County monitors for unauthorized connections of mobile devices to the Grand County network.
5. Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used to access CJI.
6. If Grand County has reason to believe that a mobile device connected to the Grand County network is using information asset resources inappropriately, or is acting in violation of federal and state laws or regulations, network traffic to and from that mobile device may be monitored. If justified, the mobile device is disconnected from the Grand County network, and appropriate actions taken in accordance with the Sanctions Policy and federal and state law and regulations.

31.12 Security Awareness Training

1. Training is arranged for workforce members using mobile devices according to the Privacy and Security Awareness and Training Policy to raise awareness on the additional risks resulting from this way of working and the mobile device controls that are implemented.

31.13 Policy References

31.13.1 HIPAA Regulatory References

CFR TITLE 45 § 164.310 (b)

31.13.2 NIST References

NIST SP 800-53 R4 AC-19, NIST SP 800-53 R4 AC-19(5), NIST SP 800-53 R4 CM-2(7), NIST SP 800-53 R4 SI-4

31.13.3 CJIS References

CJIS V5.9 Sections 5.13

32 ENDPOINT PROTECTION POLICY

32.1 Statement of Purpose

The purpose of this policy is to establish the methods for improving the security of endpoints through effective security configuration, malware detection, and malware prevention.

32.2 Statement of Applicability

All workforce members who may have access or exposure to Grand County enterprise data are required to comply with this policy.

All Grand County workforce members must take responsibility for mitigating the risk of their endpoint user infecting other systems.

32.3 Controls Against Malicious Code

1. All computing devices that connect to the Grand County network will always have anti-malware software installed and running.
2. Where possible, anti-malware software ensures that updates are automatically applied within 24 hours of availability.
3. Where possible, anti-malware software automatically conducts scans of computing devices on boot and at least once every 24 hours.
4. Anti-malware software is configured to scan downloads from external sources as they are downloaded and to prevent infected files from opening or executing.
5. Anti-malware software maintains logs of all scans according to the Audit Logging, and Monitoring Policy.
6. Anti-malware software automatically cleans and removes or quarantines malicious code. Infected computing devices are removed from the Grand County network until they are verified as safe.
7. Anti-malware software is centrally managed and prevents non-privileged users from disabling or modifying the software.
8. All third-party laptops must have up-to-date anti-malware software installed and verified prior to connecting to the Grand County network.
9. All users must take reasonable measures to protect against the installation of unlicensed or unauthorized software in accordance with the Acceptable Use Policy.
10. Any activities with the intention of creating and/or distributing malicious programs using Grand County's network (e.g., viruses, worms, Trojan Horses, etc.) are strictly prohibited, in accordance with the Acceptable Use Policy.

32.4 Operating Systems Controls

1. Operating systems must be maintained by applying any service packs, patches, or security updates that are subsequently released.
2. Where possible, Operating System updates are provided automatically. Users must follow directions from IT Services and Support when Operating System updates are distributed.
3. Unmanaged computing devices which become a security risk to the Grand County environment are disconnected from the Grand County network.
4. Operating Systems which no longer have security updates available to fix vulnerabilities, must be upgraded to a currently supported Operating System. If this is not possible or practical, the risk is documented and measures taken to reduce and mitigate that risk. The CISO determines the risk level and issues a waiver in cases where such a waiver is warranted.

32.5 Policy References

32.5.1 HIPAA Regulatory References

CFR TITLE 45 § 164.308(a)(5)(ii)(B)

32.5.2 NIST References

NIST SP 800-53 R4 CM-11, NIST SP 800-53 R4 SC-2, NIST SP 800-53 R4 SI-16, NIST SP 800-53 R4 SI-3, NIST SP 800-53 R4 SI-3(1), NIST SP 800-53 R4 SI-3(2), NIST SP 800-53 R4 SI-8, NIST SP 800-53 R4 SI-8(1), NIST SP 800-53 R4 SI-8(2)

33 MEDIA PROTECTION POLICY

33.1 Statement of Purpose

The purpose of this policy is to protect all Grand County media containing confidential data in both paper and digital format, to ensure destruction before disposal, and to ensure compliance with federal and state

laws and regulations concerning the security and privacy of confidential data copied onto removable media.

33.2 Statement of Applicability

This policy applies to all media, removable media, and paper media containing Grand County confidential data regardless of physical location.

33.3 Media Protection Policy

1. Grand County physically and logically protects media and paper media containing confidential data while at rest, stored, or actively being accessed.
2. Grand County restricts access of media and paper media containing confidential data according to the Access Control Policy.

33.4 Management of Removable Media

1. Grand County develops and implements processes and procedures for the management of removable media.
2. Grand County restricts the types and use of removable media to maintain security of confidential data.
3. Removable media is encrypted in accordance with the Encryption Policy.
4. Grand County will reformat all removable storage devices immediately before inserting them into any component of the voting system, except as provided in 8 CCR 1505-1 Rule 20.6.2 (b)-(e), or in the conditions of use.

33.5 Media and Paper Media Transport and Storage

1. Grand County must physically control, and securely store, media and paper media within a controlled area such as a locked drawer or room.
2. Grand County protects and controls all media and paper media during transport outside of controlled areas to prevent unauthorized access or use.
3. Grand County maintains accountability for all media and paper media during transport outside of controlled areas.
4. Grand County restricts the transport of media and paper media outside of controlled areas to authorized personnel.
5. Grand County protects the confidentiality and integrity of media during transport outside of controlled areas according to the Encryption Policy.
6. If a third party is responsible for transporting backup media offsite, they are responsible for maintaining security according to the Third-Party Risk Management Policy.

33.6 Secure Disposal of Media

1. Grand County sanitizes all media, paper media, removable media, mobile devices, and information assets prior to disposal, release out of organizational control, or release for reuse to render confidential data permanently non-retrievable by any means.
2. Grand County develops sanitization processes and procedures that include removing and securing confidential data and permanently destroying media, paper media, removable media, mobile devices, and information assets prior to disposal, release out of organizational control, or release for reuse.
3. All media and removable media being taken out of service are destroyed either by an authorized vendor or by industry standard means (e.g., degaussing, using a disk cleaning program, drilling, crushing, or other demolition methods) that render the confidential data non-retrievable by any means.
4. All media and removable media are checked to ensure that all confidential data and licensed software has been securely removed prior to re-use or release outside of organizational control.

5. The data owner determines whether confidential data contained on media, paper media, removable media, mobile devices, and information assets must be retained prior to disposal, release out of organizational control, or release for reuse.
6. Only designated workforce members complete sanitization processes and procedures.
7. Grand County maintains a log and an audit trail of all sanitization activities.
8. Authorized third party vendors are required to provide a certificate of destruction to account for all media, paper media, removable media, mobile devices, and information assets they destroy.
9. Paper media awaiting disposal that contains confidential data is kept in locked bins or a locked room until destruction.
10. Paper media containing confidential data is destroyed either by an authorized vendor or by other methods (e.g., cross-cut shredding, disintegration, incineration, or pulverization).
11. The CISO is responsible for overseeing secure disposal of media. This responsibility may be delegated.

33.7 Policy References

33.7.1 HIPAA Regulatory References

CFR TITLE 45 § 164.310(c), CFR TITLE 45 § 164.310(d)(1), CFR TITLE 45 § 164.310(d)(2)(i), CFR TITLE 45 § 164.310(d)(2)(ii), CFR TITLE 45 § 164.310(d)(2)(iii), CFR TITLE 45 § 164.310(d)(2)(iv), CFR TITLE 45 § 164.312(c)(1)

33.7.2 NIST References

NIST SP 800-53 R4 MP-1, NIST SP 800-53 R4 MP-4, NIST SP 800-53 R4 MP-5, NIST SP 800-53 R4 MP-5(3), NIST SP 800-53 R4 MP-5(4), NIST SP 800-53 R4 MP-7, NIST SP 800-53 R4 MP-7(1), NIST SP 800-53 R4 DM-2, NIST SP 800-53 R4 MP-6, NIST SP 800-53 R4 MP-6(1), NIST SP 800-53 R4 MP-6(2), NIST SP 800-53 R4 AC-1, NIST SP 800-53 R4 AC-17, NIST SP 800-53 R4 AC-17(2), NIST SP 800-53 R4 AC-20, NIST SP 800-53 R4 AC-20(1), NIST SP 800-53 R4 AC-20(2), NIST SP 800-53 R4 AC-3, NIST SP 800-53 R4 AC-4, NIST SP 800-53 R4 PL-4, NIST SP 800-53 R4 PS-6, NIST SP 800-53 R4 SC-1, NIST SP 800-53 R4 SC-15, NIST SP 800-53 R4 SC-15(1), NIST SP 800-53 R4 SC-8

33.7.3 CJIS References

CJIS V5.9 Sections 5.8

33.7.4 Code of Colorado Regulations References

8 CCR 1505-1 Rule 20

34 DEFINITIONS

If any term conflicts with legal definitions under HIPAA, HITECH, and/or other applicable information security/privacy regulations, the definition ascribed to such term under the applicable law prevails.

34.1 A

Access Control is a formal, documented, and auditable method (whether administrative or technical in nature) for controlling access to an information asset. Access Control ensures that resources are only granted to those users who are entitled to them.

Account is the bundle of access rights and privileges granted to a user, computing device, or system governing access to, and use of, an information asset.

Account Administrators are an individual, or group of individuals, who have delegated authority to act on an information asset owner's behalf to administer access rights and privileges associated with an information asset.

Account Owner is an individual, or group of individuals, who have been officially designated as accountable for controlling access to an information asset. Account Owners are associated with the business functions of Grand County rather than the technology functions. Account Owners are appointed by senior leadership, and are typically an administrative officer or department director.

Adverse Events are events with negative consequences (e.g., system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, execution of malware that destroys data, etc.).

Advanced Encryption Standard (**AES**) is a cryptographic cipher that uses a block length of 128 bits and key lengths of 128, 192 or 256 bits.

Annual means calendar year.

Anti-Malware Software provides protective safeguards against malware attacks.

Application is a software program that stores, accesses, and/or manipulates data or which controls a computing device or system.

Application Owner is an individual, or group of individuals, who have been officially designated as having management responsibility for controlling the production, development, maintenance, use and security of an application.

Application Service is any service or function carried out to support, provision, administer, and or provide training for an Application.

Authentication is the process of confirming the correctness of the claimed identity.

Authentication Data is credentials (e.g., username and password) for accessing information.

Authorization is the signed acknowledgment setting forth permissible uses and disclosures of the individual's PHI and/or other confidential information.

Authorized Viewer is a viewer of video surveillance or video surveillance cameras such as the Administrator and/or his/her designee, Legal Counsel on behalf of Grand County, or assigned staff for Grand County.

34.2 B

Backup is the procedure for making copies of information in case the original information is lost or damaged.

Breach has the meaning defined in CFR TITLE 45 § 164.402 Definitions. It is the acquisition, access, use, or disclosure of protected health information or other confidential information in a manner not permitted under law which compromises the security or privacy of the information.

Business Associate is an entity or a person who, on behalf of Grand County, creates, receives, maintains or transmits PHI or who provides Grand County services where the provision of the service involves the disclosure of protected health information.

Business Associate Agreement (BAA) is a legally mandated agreement entered into between Grand County and a Business Associate that establishes permitted and required uses and disclosures of PHI, provides obligations for the Business Associate to safeguard the information and to report any uses or disclosures not provided for in the agreement, and requires the termination of the agreement if there is a material violation.

Business Continuity refers to the activities required to maintain vital Grand County operations at an acceptable level of effectiveness and efficiency during a period of displacement or interruption of normal operations.

Business Continuity Plan (BCP) provides information for continuing business operations under adverse conditions (e.g., storm, crime, emergency, disaster, etc.). From an IT perspective, the BCP should cover at a minimum the following events:

- Equipment failure (such as disk crash)
- Disruption of power supply or telecommunications
- Application failure or corruption of database
- Human error, sabotage or strike
- Malicious software (e.g., viruses, worms, Trojan horses) attacks
- Hacking or other security attacks
- Social unrest or terrorist attacks
- Fire
- Natural disasters (e.g., flood, earthquake, hurricanes)

Business Impact Analysis (BIA) is a process that identifies and evaluates the potential effects (financial, life / safety, regulatory, legal / contractual, reputation and so forth) of natural and man-made events on business operations. A BIA determines what levels of impact to a system are tolerable. A BIA further identifies mitigation options, mitigation steps for each option, and related expenses to support emergency management decisions.

Business Mobile Devices are mobile devices that are the property of Grand County and are provided to support the operations of Grand County. Business Mobile Devices are managed by Grand County Information Systems and all data they access, transmit and store is subject to audit monitoring, and logging by Grand County.

BYOD Mobile Devices (“bring your own device”) refers to personally owned mobile devices. All data BYOD mobile devices access, transmit and store is subject to audit monitoring, and logging by Grand County.

34.3 C

Cache, which is pronounced "cash" (not "catch" or "cashay"), stores recently used information so that it can be quickly accessed later. Computers incorporate several different types of caching to run more efficiently, thereby improving performance. Common types of caches include browser cache, disk cache, memory cache, and processor cache.

Certificate Authorities are entities that issue digital certificates certifying the ownership of a public key by the named subject of the certificate.

Change is defined as any addition, deletion, or alteration of any hardware, software, network, telephony, environment, system, desktop build, or associated documentation in the Grand County IT infrastructure.

Change Management is the identification and implementation of changes to hardware, software, firmware, and documentation. Change Management workflows ensure that changes are made with minimum disruption to the organization.

Change Management Roles ensure clear ownership of the change management process. Change Management Roles are generic and describe change management responsibilities. The roles do not necessarily conform to the job titles in the organizational chart. In addition, one person might fill several roles while another role might require several people. Further, the people fulfilling the roles might be different during an emergency.

Change Request is a formal request for change to any component of the Grand County IT infrastructure or to any aspect of an IT service in the Grand County production environment.

Chief Information Security Officer (CISO) is the most senior person in the organization responsible for establishing and maintaining the enterprise vision, strategy and programs to ensure Information Assets and technologies are adequately protected.

Common Areas may include lobbies, public hallways, nursing station areas, elevators, stairwells, basements, parking lots and building surroundings, dietary services, exits, dining rooms, dayrooms, or any other area where residents and staff do not have a reasonable expectation of privacy.

Complainant is the person who makes or reports a privacy complaint.

Computing Devices are the computers, business mobile computing devices, printers, networks, online and offline storage media and related equipment, software, and information assets that are owned, managed, or maintained by Grand County.

Confidential Data is the most restricted type of Grand County sensitive data. Confidential Data includes protected health information (PHI and ePHI), Social Security numbers (SSN), and personally identifiable information (PII). The complete list of Confidential Data is defined in the *Data Classification and Handling Policy*.

Configuration Management controls and processes ensure that changes to Grand County information assets are managed, thereby reducing security risks, and ensuring that these changes occur with minimal disruption to Grand County operations.

Conflict of Interest exists any time someone's loyalty to Grand County is, or appears to be, compromised by personal interest, including the ability to provide quality services impartially to residents without favoritism.

Contingency Plans provide the information necessary for the recovery of a system following a disruption, including roles and responsibilities, inventory, assessment procedures, recovery procedures, and testing. Contingency plans can be activated at the current location or at an alternate location.

Covered Entity is defined as health plans, health care clearinghouses, and health care providers who electronically transmit any health information in electronic format. Covered entities can be institutions, organizations, or persons.

Cracker is a person who obtains, or attempts to obtain, unauthorized access to computer resources for specific, premeditated crimes. (See also Hacker)

Cracking Utilities are programs planted in systems by attackers for a variety of purposes such as elevating privileges, obtaining passwords, and disguising the attacker's presence.

Criminal Justice Information (CJI) is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data.

Criminal Justice Information Services (CJIS) is the information, data, and services provided by the FBI to the criminal justice community and its partners.

Criminal History Record Information (CHRI) is a subset of CJI and is considered restricted date. Due to its comparatively sensitive nature, additional controls are required for access, use and dissemination. CFR Title 28, Part 20 defines CHRI and provides regulatory guidance.

Crisis Communications Plan provides information for internal and external communications in the event of a business disruption. The Crisis Communications Plan also designates the specific workforce members who are the only individuals with the authority for providing information to the public and answering questions.

Cyber Incident Response Plan provides information for identifying, mitigating, and recovering from a malicious security incident (e.g., unauthorized access, denial of service, virus, worm, Trojan horse, etc.).

34.4 D

Data is any information that is created or used as part of Grand County's business operations. Data is further classified based on its value, legal requirements, sensitivity, and criticality to the organization.

Data Classification, in the context of information security, is the classification of data based on its value, legal requirements, sensitivity, and criticality. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data.

Data Disclosure is the sharing of data, including PHI, outside of the Grand County work force or affiliated covered entities. There are specific policies regarding data disclosure based on the classification of that data, including the requirement for tracking who has seen, or can see, specific data elements.

Data Owner is an individual, or group of individuals, who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system. Data Owners are associated with the business functions of Grand County rather than the technology functions. Data Owners are appointed by senior leadership, and are typically an administrative officer or department director.

Decedent is a term, generally used in the law governing estates and trusts, to refer to a person who has died.

Demilitarized Zone (DMZ) is a physical or logical sub network that sits between an internal and external network, usually the Internet. DMZs provide sub network segmentation based on security requirements or policy. DMZs provide a transit mechanism from a secure source to an insecure destination or from an insecure source to a more secure destination.

Designated Record Set means:

(1) A group of records maintained by or for a covered entity that is:

- The medical records and billing records about individuals maintained by or for a covered health care provider;
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Used, in whole or in part, by or for the covered entity to make decisions about individuals.

(2) The term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Development Environment is where the programmers develop software. The Development Environment should not contain confidential data unless it is de-identified.

Differential Backup is a cumulative backup of all changes made since the last full backup, i.e., the differences since the last full backup. The advantage is a quicker recovery time, requiring only a full backup and the last differential backup to restore the entire data repository.

Disaster is a sudden event, such as an accident or a natural catastrophe, which causes great damage or loss of life.

Disaster Recovery is the process of rebuilding operations and infrastructure after the disaster is over.

Disaster Recovery Plan (DRP) provides information for handling physical disruptions to service that deny access to the primary infrastructure for an extended period. The DRP includes information for establishing operations at an alternate site during an emergency. The DRP is supported by a Contingency Plan that addresses recovery of individual systems at an alternate site.

Disclosure is the release, transfer, provision of access to, or divulging in any other manner, outside the entity holding the information.

Domain Name System (DNS) is a system for naming computers and network services that is organized into a hierarchy of domains. DNS naming is used in TCP/IP Networks, such as the Internet, to locate and identify computers and services through user-friendly names.

34.5 E

Electronic Commerce Services is the electronic transmission of payment information in exchange for Grand County services and products.

Electronic Protected Health Information (ePHI) is any individually identifiable health information (PHI) protected by HIPAA that is transmitted by, or stored in, electronic media.

Emergency is a serious, unexpected, and often dangerous situation requiring immediate action.

Emergency Plan (EP) provides information for a coordinated first-response that minimizes loss of life and injury in the event of a physical threat (e.g., fire, bomb threat, chemical release, domestic violence, medical emergency, etc.). The EP includes information about sheltering-in-place as well as evacuating.

Encryption is the process of encoding information in such a way that only authorized parties can decrypt it. Encryption does not of itself prevent interception, but denies the message content to unauthorized individuals.

Endpoint is an Internet-capable computer hardware device on a TCP/IP network. The term can refer to desktop computers, laptops, smart phones, tablets, thin clients, printers or other specialized hardware such POS terminals and smart meters.

Enterprise Data is any information that is created or used as part of Grand County's operations. Enterprise data is further classified based on its value, legal requirements, sensitivity, and criticality to the organization.

Event is an observable occurrence in a system or network (e.g., user connects to file share, server receives request for web page, user sends email, firewall blocks connection attempt).

34.6 F

False Claim includes making a false statement in a claim for payment, falsifying a medical record or coding information, and billing for services not provided.

False Positive is an alert that incorrectly indicates that malicious activity is occurring.

Firewall is a logical or physical part of a computer system or network that is designed to block unauthorized access to data.

Full Backup is a complete backup of everything. The advantage is fast restoration since you only need one set of backup data. The disadvantage is that the backup process is slow and requires significant storage capacity.

34.7 G

Governance relates to processes and decisions that seek to define actions, grant power and verify performance.

34.8 H

Hacker is a person who obtains, or attempts to obtain, unauthorized access to a computer for reasons of thrill or challenge. (See also Cracker)

HHS refers to the U.S. Department of Health and Human Services.

HIPAA is the federal Health Insurance Portability and Accountability Act of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information, and help the healthcare industry control administrative costs.

34.9 I

Incident Response is a structured and organized response to any adverse event or security incident that threatens information assets, including systems, networks and telecommunications systems. Incident Response is also the mitigation of violations of security policies and recommended practices. Incident Response provides an action plan for dealing with intrusions, cyber-theft, denial-of-service attacks, fire, floods, and other security-related adverse events.

Incident Response Team (IRT) is a group of individuals trained and chartered to respond to security incidents. The IRT provides both an investigative and problem-solving component. The IRT includes managers with the authority to act, technical resources with the knowledge and expertise to rapidly diagnose and resolve problems, and communication experts that provide external communications.

The IRT typically consists of security analysts who take immediate mitigation actions for containment, eradication, and recovery resulting from security incidents.

Incremental Backup is a copy of all files that have changed since the last backup of any type (full, differential, and incremental). The advantage is fast backup and least storage requirements. The disadvantage is that restoration is slow, and requires several sets of backup data to fully restore all the data.

Indicator is a sign that a security incident may have occurred or may be currently occurring.

Information Assets are elements of software and hardware and associated data that are found in Grand County's operating environment. Information Assets include, but are not limited to:

- Servers
- Workstations (e.g., desktops, laptops, notebooks)
- Network devices (e.g., switches, routers, firmware, firewalls)
- Peripherals (e.g., printers, scanners, monitors)
- Software/ applications (e.g., purchased, licensed or leased)
- Biomedical equipment
- Mobile devices (e.g., smart phones, tablets, USB storage drives)
- Telecommunications equipment (e.g., VOIP phones)

Information Asset Inventory is the identification, recording, and documenting of Information Assets maintained by Grand County.

Information Asset Owner is the individual or organizational unit that has management responsibility for controlling the production, development, maintenance, use and security of information assets. Information asset owners are associated with the business functions of Grand County rather than the technology functions. Information Asset Owners are appointed by senior leadership, and are typically an administrative officer or department director.

Information Exchange Agreements specify the minimum set of controls for an information sharing arrangement, such as: responsibilities, procedures, technical standards, technical solutions, incident management, reporting and notification, access controls, auditing logging and monitoring, and physical safeguards.

Information Security Incident Response Capability (ISIRC) is a capability set up for responding to security incidents.

Information Services are any service or function carried out to support, provision, administer, and / or provide training for with respect to an information asset (e.g., email, database services, etc.).

Information Systems are a subset of information assets that includes information technology hardware and software/applications, but does not include data.

Insider Threat is generally defined as a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally misused that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems. Insider threats, to include sabotage, theft, espionage, fraud, and competitive advantage are often carried out through abusing access rights, theft of materials, and mishandling physical devices. Insiders do not always act alone and may not be aware they are aiding a threat actor (i.e., the unintentional insider threat). It is vital that organizations understand normal employee baseline behaviors and ensure employees understand how they may be used as a conduit for others to obtain information.

Internal Use Only Data represents data classified as Tier 2: Internal Use Only Data according to the data classification scheme defined in the *Data Classification and Handling Policy*.

Internet Service Provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet.

Investigator is the Privacy Officer (County Manager), or the person designated by the Privacy Officer (County Manager), to investigate a privacy complaint.

Involuntary Termination is characterized by an organization taking the decision to terminate the employment relationship. In certain cases, Involuntary Termination can be caused by death or by an accident leaving the workforce member unable to continue employment.

IT Infrastructure includes, but is not limited to, hardware, software, firmware, network, telephony, applications, data, platforms, middleware services, computing facilities, and systems management. IT Infrastructure also applies to the design, configurations, parameters, and documentation of those components.

34.10 K

Kickbacks are any items or services of value including cash, goods, gifts, or services that are received in return for the inducement or acceptance of referrals to the facility or referrals from the facility to another provider. Such remuneration may include, but is not limited to, excessive discounts, the provision of free or discounted supplies and equipment, gifts, waivers, or the granting of professional courtesy discounts. Violation of these laws can result in Jail and large fines to the Facility and individuals.

34.11 L

Least Privilege means giving an account or a process the least amount of permissions necessary to perform their intended function.

Limited Data Set is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) Names; (ii) Postal address information, other than town or city, State, and zip code; (iii) Telephone numbers; (iv) Fax numbers; (v) Electronic mail addresses; (vi) Social security numbers; (vii) Medical record numbers; (viii) Health plan beneficiary numbers; (ix) Account numbers; (x) Certificate/license numbers; (xi) Vehicle identifiers and serial numbers, including license plate numbers; (xii) Device identifiers and serial numbers; (xiii) Web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) Biometric identifiers, including finger and voice prints; and (xvi) Full face photographic images and any comparable images.

Loop Recording is the process of recording audio continuously to an endless tape, computer memory, or recording video surveillance or camera signals on a video server. This process allows for the replacement of previously recorded content material with new content. Thus, at the end of the internal disk drive, the

recording process continues to record at the beginning, erasing the previously recorded material and replacing it with the new content.

34.12 M

Malware, short for malicious software, is any software used to disrupt computer operations, gather sensitive information, or gain unauthorized access to private computer systems. Malware includes viruses, worms, Trojan Horses, ransomware, spyware, adware, scareware, and other malicious programs.

Marketing: Any communication about a product or service that encourages recipients of the communication to purchase or use the product or service, unless the communication is made:

- For treatment of the individual; or
- For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual, or
- Face-to-face, or
- Involving a promotional gift of nominal value (calendar, pen, etc.).

Media includes fixed media that can store confidential information (e.g., internal hard disks, flash drives, and solid-state drives) as well as removable media (e.g., USB flash drives, portable external hard drives, removable hard drives, flash memory cards, CDs, and magnetic tapes).

Media Access Control (MAC) Address is a unique identifier assigned to Network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet.

Message Integrity is the authenticity, validity, and certainty of origin of a transmitted message. Message Integrity deals with methods that ensure that the contents of a message have not been tampered with and altered.

Minimum Necessary the HIPAA Privacy Rule stipulates that covered entities limit the amount of information disclosed to the minimum necessary to achieve the specified goal [45 CFR 164.514(d)(1)]. This requirement does not apply if the disclosure is required by law, authorized by the individual, or for treatment purposes.

Mobile Devices are lightweight, easily transportable devices capable of connecting to Grand County networks and/or accessing Grand County confidential data. Mobile Devices include, but are not limited to, smart phones (e.g., iPhones, Androids), tablets (e.g., iPads, Slates), and Blackberry devices. Mobile Devices may be owned by Grand County (see Business Mobile Devices) or personally-owned by workforce members (see BYOD Mobile Devices).

34.13 N

Need-to-Know means restricting access to confidential data to only those who have a specific need based on their job responsibilities.

Need-To-Share means restricting access to confidential data to only the information that is required for sharing.

Network is any system of IT hardware, software, frequency spectrum, cable and physical surroundings that enables devices to interconnect and share information. Network includes all communications cabling, equipment and infrastructure devices, including but not limited to the following: telecommunications switches, data networking switches and routers, Wireless Access Points (WAPs), cellular distributed antenna systems, cellular repeaters and/or bi-directional amplifiers, cellular macro sites, cable and satellite television reception and distribution equipment.

Network Administrator is an individual, or group of individuals, who have delegated authority to administer a network, including controlling access to the network and configuring the network and the

devices of which it is comprised. It is the responsibility of the Network Administrator to understand the business needs of network users and to facilitate appropriate access to the network.

Network Diagram is a graphical representation of the network. Network Diagrams document and detail the current state of connectivity regarding the network's physical, logical, system-specific, application-specific, and/or other aspects of network hardware, software, frequency spectrum, cabling and connectivity, signaling types, ports, and protocols.

Network Owner is an individual or organizational unit responsible for operating and maintaining the physical and virtual infrastructure which comprises the network, including responsibility for establishing the procedures to be used for maintenance and upgrades.

Network Service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols. Each service is usually provided by a server component running on one or more computers (often a dedicated server computer offering multiple services) and accessed via a network by client components running on other devices. However, the client and server components can both be run on the same machine. Clients and servers will often have a user interface, and sometimes other hardware associated with them.

34.14 O

Operating Procedures provide information for system activities associated with information and communication assets.

Operating System is the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.

34.15 P

Paper Media includes any physical piece of paper that may be photocopied or easily removed from Grand County facilities.

Password is a string of characters that allows access to a computer, interface, or system.

Payment Card Information (PCI) covered under PCI DSS (Data Security Standard) is defined as confidential data and must be protected. Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

- Cardholder name
- Service code
- Expiration date
- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a credit card's magnetic stripe

Personally Identifiable Information (PII) refers to information that can be used to distinguish or trace an individuals identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., Social Security Number (SSN), name, date of birth (DOB), home address, personal email).

Personally-Owned Mobile Computing Devices (with or without phone capability) are Mobile Computing Devices that are purchased with non-Grand County funds.

Personal Representative is a person or persons designated by a resident to receive PHI or an individual who has legal authority to receive a resident's PHI. Grand County may disclose PHI to a designated personal representative upon a resident's request. Should a legitimate need arise, and a Personal

Representative or legal authority is not available, an individual may be designated as the Patient Representative based on the professional judgment of Grand County.

Precursor is a sign that an attacker may be preparing to cause a security incident.

Privacy Officer (County Manager) is the individual responsible for ensuring the compliance with privacy requirements under HIPAA, HITECH and other applicable privacy laws. The Privacy Officer (County Manager) is the primary contact for all notifications regarding potential or actual privacy violations.

Principle of Least Privilege requires that a process, user or program must be able to access only the information and resources necessary for legitimate purposes.

Privacy Complaint is a report (verbal or written) by a person, regardless if such person is a workforce member, claiming that there is a violation of a federal or state privacy law or regulation or Grand County privacy policy.

Privilege refers to the access permissions granted to a specific user within a system.

Protected Health Information (PHI) is defined as individually identifiable health information that is created, maintained or received by Grand County, including demographic information that can or could reasonably identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual.
- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

PHI that is created, received, transmitted or stored in an electronic media is referred to as ePHI.

Production Environment is the setting where executable software is put into operation for their intended uses by end users.

34.16 Q

QA (Quality Assurance) Environment is where an individual or a team can test software without adversely impacting the production environment. The QA Environment should not contain confidential data unless it has been de-identified, where feasible.

Quorum is the minimum number of members that must be present for a meeting to make the proceedings of that meeting valid.

34.17 R

Reasonable Expectation of Privacy Areas include, but are not limited to, restrooms, showers/bath areas, resident rooms, locker rooms, or any place which would be expected to violate a person's dignity.

Remote Access is the ability to access Grand County's network from outside the network perimeter. Common methods of communication from the remote computer to Grand County's network includes, but is not limited to, web-based Secure Socket Layer (SSL) portals, Virtual Private Networks (VPNs), and other methods which employ encrypted communication technologies.

Removable Media are devices external to Grand County computing devices that may be utilized for the storage and/or transfer of enterprise data, and which may be removed from Grand County facilities. This includes, but is not limited to USB flash drives, portable external hard drives, removable hard drives, flash memory cards (e.g., SD cards, XSD), CDs, DVDs, floppy disks, and magnetic tapes.

Risk Management is a continuous process that allows the organization to balance the operational and economic costs of protective measures while achieving gains in protecting the IT Systems and Data that supports organizational goals and objectives. Risk Management encompasses:

- Risk Assessment
- Risk Treatment
- Risk Monitoring and Review

Risk Management Plan is a document prepared to foresee risks, estimate impacts, and define responses to issues. The Risk Management Plan also contains a risk loss exceedance graph.

Roll Back Plan documents the actions to take to restore service if a change fails.

34.18 S

Secretary refers to the Secretary of HHS.

Secure Access is a network technology that hosts applications on central servers and allows users to interact with them remotely or stream and deliver them to user devices for local execution.

Security Incident is an adverse event or group of adverse events in an information system or network or the threat of the occurrence of such an event. A security incident is also a violation, or imminent threat of violation, of information security policies, acceptable use policies, or standard security practices.

Incidents may result from intentional or unintentional actions and the occurrence does or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits. Examples of Security Incidents include:

- Loss of an unencrypted endpoint device (e.g., laptop or portable device)
- Compromise of information integrity
- Inadvertent disclosure of confidential data
- Misuse of service, systems or information
- Hacking, attempts to steal passwords, or other malicious activity
- Damage to systems from malicious code attacks (e.g., viruses, Trojan horses, logic bombs, etc.)

Service Level Agreement (**SLA**) is a contract with a third party that specifies in measurable terms the services to be provided.

Signature is a recognizable, distinct pattern in Network traffic associated with an attack, such as a binary string in a virus or a set of keystrokes used to gain unauthorized access to a system.

Social Engineering is an attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.

Spyware is a type of malware software that enables a hacker to obtain covert information about another's computer activities by transmitting data covertly from their hard drive.

Staging Environment is a mirror image of the production environment.

Stateful Packet Inspection is a firewall architecture that works at the network layer. Stateful Packet Inspection examines both the header information and the contents of the packet up through the application layer to determine more than just information about its source and destination. The firewall is programmed to distinguish legitimate packets from different types of connections.

Static IP Address is a permanent numeric identification assigned by the Network Administrator to a node in a TCP/IP network. Static IP Addresses are used for shared resources such as web servers and webcams.

System is a collection of hardware, software, data, people and procedures that work together to produce quality information.

System Administrator is an individual, or group of individuals, who have delegated authority to administer a system, including controlling access to the system and configuring the system and the

devices of which it is comprised. It is the responsibility of the System Administrator to understand the business needs of system users and facilitate appropriate access to the system.

34.19 T

Third Party is any entity external to Grand County with which Grand County is sharing enterprise data or from which Grand County is obtaining products or services.

Threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or adverse event that could breach security and cause harm.

Trojan Horse is a malware program designed to breach the security of a computer system while ostensibly performing some innocuous function. A Trojan Horse contains an apparent or actual useful function that contains additional (hidden) functions that allow the unauthorized collection, falsification or destruction of data.

34.20 U

Unauthorized Access encompasses a range of incidents from improperly logging into a user's account (e.g., when a hacker logs in to a legitimate user's account) to obtaining unauthorized access to files and directories possibly by obtaining "super-user" privileges. Unauthorized access also includes access to network data gained by planting an unauthorized "sniffer" program (or some such device) to capture all packets traversing the network at a point.

User is any workforce member, independent contractor, consultant, temporary worker, or other person or entity that uses Grand County information assets.

34.21 V

Video Surveillance refers to any installed device with the capacity to record video surveillance images in a designated common area. Such devices include, but are not limited to, a digital recorder, DVD, DVO, VHS tape or other recording device.

Virtual Private Network (VPN) is a networking technology that enables a remote computing device to send and receive data across shared or public networks as if it were a private network with all the functionality, security and management policies of the private network.

Virus is code that can copy itself and typically has a detrimental effect, such as corrupting the system or destroying data. Viruses spread to other machines by the actions of users, such as opening infected email attachments.

Voluntary Termination is characterized by an agreement between the organization and the workforce member regarding the terms and timing of the departure. Voluntary Termination can include retirement.

Vulnerability is a weakness in a system, application, or network that is subject to exploitation or misuse.

Vulnerability Management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities, especially in software and firmware. Vulnerability Management is integral to computer security and network security.

34.22 W

Wireless Access Point (WAP) is a device that allows wireless devices to connect to a wired network using Wi-Fi or related standards. The WAP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself.

Workforce Member is a person who is a Grand County employee, volunteer, board member, community representative, trainee, student, or contractor, and whose conduct, in the performance of work for Grand County, is under the direct control of Grand County, whether by direct employment by or contract with Grand County.

Grand County

Colorado