Uintah School District Data Governance Plan

PURPOSE

Data governance is an organizational approach to data and information management that is formalized as a set of policies and procedures that encompass the full life cycle of data; from acquisition, to use, to disposal. Uintah School District takes seriously its moral and legal responsibility to protect student privacy and ensure data security. Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401 requires that Uintah School District adopt a Data Governance Plan.

SCOPE AND APPLICABILITY

This Governance Plan is applicable to all employees, temporary employees, and contractors of the Agency. The plan must be used to assess agreements made to disclose data to third-parties. This plan must also be used to assess the risk of conducting business. In accordance with Agency policy and procedures, this plan will be reviewed and adjusted on an annual basis or more frequently, as needed. This plan is designed to ensure only authorized disclosure of confidential information. The following 7 subsections provide data governance policies for Uintah School District:

1. Data Advisory Groups
2. Non-Disclosure Assurances for Employees
3. Data Disclosure
4. Data Breach
5. Record Retention and Expungement
6. Quality Assurances and Transparency Requirements
7. Data Transparency
8. Cybersecurity Framework

Furthermore, this Data Governance Plan works in conjunction with our cybersecurity framework which outlines:

- Systems administration
- Network security
- Application security
- Endpoint, server, and device Security
- Identity, authentication, and access management
- Data protection and cryptography
- Monitoring, vulnerability, and patch management
- High availability, disaster recovery, and physical protection
- Incident responses
- Acquisition and asset management, and
- Policy, audit, e-discovery, and training

1 DATA ADVISORY GROUPS

Uintah School District hereby designates the Student Services Director as the Student Data Manager.

Uintah School District hereby designates the Coordinator of Educational Technology as the Information Security Officer.

1.1 STRUCTURE

Uintah School District has a Student Services policy committee approved by the board to ensure that data is protected at all levels of Uintah School District educational system.

1.2 GROUP MEMBERSHIP

Membership in the groups require board approval. Group membership is at least two years. If individual members exit the group prior to fulfilling their two-year appointment, the board may authorize a replacement member. The group will be made up of LEA student Data Manager, IT Systems Security Manager and the Student Policy committee which fulfills the requirement of this plan.

1.3 INDIVIDUAL AND GROUP RESPONSIBILITIES

The following table outlines individual Uintah School District staff and advisory group responsibilities.

Role	Responsibilities
LEA Student Data Manager	1. authorize and manage the sharing, outside of the education entity, of personally identifiable student data from a cumulative record for the education entity 2. act as the primary local point of contact for the state student data officer. 3. A student data manager may share personally identifiable student data that are: a. of a student with the student and the student's parent b. required by state or federal law c. in an aggregate form with appropriate data redaction techniques applied d. for a school official e. for an authorized caseworker or other representative of the Department of Human Services or the Juvenile Court f. in response to a subpoena issued by a court. g. directory information h. submitted data requests from external researchers or evaluators, 4. A student data manager may not share personally identifiable student data for the purpose of external research or evaluation. 5. Create and maintain a list of all LEA staff that have access to personally identifiable student data. 6. Ensure annual LEA level training on data privacy to all staff members, including volunteers. Document all staff names, roles, and training dates, times, locations, and agendas.

Information Security Officer	1. Acts as the primary point of contact for state student data security administration in assisting the board to administer this part; 2. ensures compliance with security systems laws throughout the public education system, including: a. providing training and support to applicable Uintah School District employees; and b. producing resource materials, model plans, and model forms for LEA systems security; 3. investigates complaints of alleged violations of systems breaches; 4. provides an annual report to the board on Uintah School District's systems security needs
Educators	1. Participates in policy committee meetings to oversee the writing and revision of the Data governance plan

2 NON-DISCLOSURE ASSURANCES FOR EMPLOYEES

Employee non-disclosure assurances are intended to minimize the risk of human error and misuse of information.

2.1 SCOPE

All Uintah School District board members, employees, contractors and volunteers must complete the Uintah School District mandatory training annually which describes the permissible uses of state technology and information.

2.2 NON-COMPLIANCE

Non-compliance with the agreements shall result in consequences up to and including removal of access to Uintah School District network; if this access is required for employment, employees and contractors may be subject to dismissal.

2.3 NON-DISCLOSURE ASSURANCES

All student data utilized by Uintah School District is protected as defined by the Family Educational Rights and Privacy Act (FERPA) and Utah statute. This governance plan outlines the way Uintah School District staff is to utilize data and protect personally identifiable and confidential information. Annual mandatory training is to be completed by all employees to verify agreement to adhere to/abide by these practices and will be maintained in Uintah School District Human Resources. All Uintah School District employees (including contract or temporary) will:

1. Complete a Security and Privacy Fundamentals Training.

2. Consult with Uintah School District internal data owners when creating or disseminating reports containing data.
3. Use password-protected accounts when accessing any student-level or staff-level records.
4. NOT share individual passwords for personal computers or data systems with anyone.
5. Log out of any data system/portal and close the browser after each use.
6. Store sensitive data on appropriate-secured location. Unsecured access to flash drives, DVD, CD-ROM or other removable media, or personally owned computers or devices are not deemed appropriate for storage of sensitive, confidential or student data.
7. Keep printed reports with personally identifiable information in a locked location while unattended, and use the secure document destruction service provided at Uintah School District when disposing of such records.
8. NOT share personally identifying data during public presentations, webinars, etc. If users need to demonstrate child/staff level data, demo records should be used for such presentations.
9. Redact any personally identifiable information when sharing sample reports with general audiences, in accordance with guidance provided by the student data manager, found in Appendix A (Protecting PII in Public Reporting).
10. Take steps to avoid disclosure of personally identifiable information in reports, such as aggregating, data suppression, rounding, recoding, blurring, perturbation, etc.
11. Delete files containing sensitive data after using them on computers, or move them to secured servers or personal folders accessible only by authorized parties.
12. NOT use email to send screenshots, text, or attachments that contain personally identifiable or other sensitive information. If users receive an email containing such information, they will delete the screenshots/text when forwarding or replying to these messages. If there is any doubt about the sensitivity of the data, the Student Data Privacy Manager should be consulted.
13. Use secure methods when sharing or transmitting sensitive data. Sharing within secured server folders is appropriate for Uintah School District internal file transfer.
14. NOT transmit child/staff-level data externally unless expressly authorized in writing by the data owner and then only transmit data via approved methods such as described in item ten.
15. Limit use of individual data to the purposes which have been authorized within the scope of job responsibilities.

2.4 DATA SECURITY AND PRIVACY TRAINING

2.4.1 Purpose

Uintah School District will provide a range of training opportunities for all Uintah School District staff, including volunteers, contractors and temporary employees with access to student educational data or confidential educator records in order to minimize the risk of human error and misuse of information.

2.4.2 Scope

All Uintah School District board members, employees, and contracted partners.

2.4.3 Compliance

New employees that do not comply may not be able to use Uintah School District networks or technology.

2.4.4 Policy

1. Within the first week of employment, all Uintah School District board members, employees, and contracted partners must sign and follow the Uintah School District Employee Acceptable Use Policy, which describes the permissible uses of state technology and information.
2. New employees that do not comply may not be able to use Uintah School District networks or technology. All current Uintah School District board members, employees, and contracted partners are required to participate in an annual Security and Privacy Fundamentals Training Curriculum.
3. Uintah School District requires a targeted Security and Privacy Training for Data Stewards and IT staff for other specific groups within the agency that collect, store, or disclose data.
4. Participation in the training will be annually monitored by supervisors who will report all non-attending employees and contracted partners to the Student Data Manager.

3 DATA DISCLOSURE

3.1 PURPOSE

Providing data to persons and entities outside of the Uintah School District increases transparency, promotes education in Utah, and increases knowledge about Utah public education. This governance plan establishes the protocols and procedures for sharing data maintained by Uintah School District. It is intended to be consistent with the disclosure provisions of the federal Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, 34 CFR Part 99 and Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401.

3.2 POLICY FOR DISCLOSURE OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

3.2.1 Student or Student's Parent/Guardian Access

Parents are advised that the records maintained by Uintah School District are provided by the school district in which their student is/was enrolled, and access to their student's record can be obtained from the student's school district. In accordance with FERPA regulations 20 U.S.C. § 1232g (a)(1) (A) (B) (C) and (D), LEAs will provide parents with access to their child's education records, or an eligible student access to his or her own education records (excluding information on other students, the financial records of parents, and confidential letters of recommendation if the student has waived the right to access), within 45 days of receiving an official request. Uintah School District is not required to provide data that it does not maintain, nor is Uintah School District required to create education records in response to an eligible student's request.

3.2.2 Third Party Vendor

Third party vendors may have access to students' personally identifiable information if the vendor is designated as a "school official" as defined in FERPA, 34 CFR §§ 99.31(a)(1) and 99.7(a)(3)(iii). A school official may include parties such as: professors, instructors, administrators, health staff, counselors, attorneys, clerical staff, trustees, members of committees and disciplinary boards, and a contractor, consultant, volunteer or other party to whom the school has outsourced institutional services or functions.

All third-party vendors contracting with Uintah School District must be compliant with Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401. Vendors determined not to be compliant may not be allowed to enter into future contracts with Uintah School District without third-party verification that they are compliant with federal and state law, and board rule.

3.2.3 Internal Partner Requests

Internal partners to Uintah School District include LEA and school officials that are determined to have a legitimate educational interest in the information. All requests shall be documented.

3.2.4 Governmental Agency Requests

Uintah School District may not disclose personally identifiable information of students to external persons or organizations to conduct research or evaluation that is not directly related to a state or federal program reporting requirement, audit, or evaluation. The requesting governmental agency must provide evidence the federal or state requirements to share data in order to satisfy FERPA disclosure exceptions to data without consent in the case of a federal or state

a) reporting requirement
b) audit
c) evaluation

3.3 Policy for External disclosure of Non-Personally Identifiable Information (PII)

3.3.1 Scope

External data requests from individuals or organizations that are not intending on conducting external research or are not fulfilling a state or federal reporting requirement, audit, or evaluation.

3.3.2 Student Data Disclosure Risk Levels

Uintah School District has determined three levels of data requests with corresponding policies and procedures for appropriately protecting data based on risk: Low, Medium, and High.

3.3.2.1 Low-Risk Data Request Process

Definition: High-level aggregate data
Examples:

- Graduation rate by year for the state
- Percent of third-graders scoring proficient on the SAGE ELA assessment

3.3.2.2 Medium-Risk Data Request Process

Definition: Aggregate data, but because of potentially low n-sizes, the data must have disclosure avoidance methods applied.

Examples:

- Graduation rate by year and LEA
- Percent of third-graders scoring proficient on the SAGE ELA assessment by school
- Child Nutrition Program Free or Reduced Lunch percentages by school

3.3.2.3 High-Risk Data Request Process

Definition: Student-level data that are de-identified.

Examples:

- De-identified student-level graduation data
- De-identified student-level SAGE ELA assessment scores for grades 3-6.

Process: Outlined in Uintah School District policy 007.0305 EDUCATION RECORDS ACCESS

3.4 Data Disclosure to a Requesting External Researcher or Evaluator

Responsibility: The Student Data Manager will ensure the proper data is shared with external researcher or evaluator to comply with federal, state, and board rules.

Uintah School District may not disclose personally identifiable information of students to external persons or organizations to conduct research or evaluation that is not directly related to a state or federal program audit or evaluation. Data that do not disclose PII may be shared with external researcher or evaluators for projects unrelated to federal or state requirements if:

1. A Uintah School District Director, Superintendent, or board member sponsors an external researcher or evaluator request.
2. Student data that is not PII and has been de-identified through disclosure avoidance techniques and other pertinent techniques as determined by Student Data Manager.
3. Researchers and evaluators supply the Uintah School District a copy of any publication or presentation that uses Uintah School District data 10 business days prior to any publication or presentation.

Process: Outlined in Uintah School District policy 007.0305 EDUCATION RECORDS ACCESS

4 Data breach

4.1 Purpose

Establishing a plan for responding to a data breach, complete with clearly defined roles and responsibilities, will promote better response coordination and help educational organizations shorten their incident response time. Prompt response is essential for minimizing the risk of any further data loss and, therefore, plays an important role in mitigating any negative consequences of the breach, including potential harm to affected individuals.

4.2 POLICY

Uintah School District shall follow industry best practices to protect information and data. In the event of a data breach or inadvertent disclosure of personally identifiable information, Uintah School District staff shall follow industry best practices outlined in the Agency IT Security Policy for responding to the breach. Further, Uintah School District shall follow best practices for notifying affected parties, including students, in the case of an adult student, or parents or legal guardians, if the student is not an adult student.

Concerns about security breaches must be reported immediately to the IT security manager who will collaborate with appropriate members of the Uintah School District executive team to determine whether a security breach has occurred. If the Uintah School District data breach response team determines that one or more employees or contracted partners have substantially failed to comply with Uintah School District's Agency IT Security Policy and relevant privacy policies, they will identify appropriate consequences, which may include termination of employment or a contract and further legal action. Concerns about security breaches that involve the IT Security Manager must be reported immediately to the Superintendent.

Uintah School District will provide and periodically update, in keeping with industry best practices, resources for Utah LEAs in preparing for and responding to a security breach.

4.3 PROCEDURES

The following table outlines the procedures and responsible parties in the event of a data breach:

Assess, Contain and Recover Data:

Step	Action	Notes
A	Containment and Recovery:	Contain the breach, limit further organizational damage, seek to recover/restore data.
1	Breach Determination	Determine if the Incident needs to be classified as a Breach.
2	Ascertain the severity of the Incident or Breach and determine the level of data involved.	See Incident Classification
3	Investigate the Breach or Incident and forward a copy of the Incident report to the Data Manager	Ensure investigator has appropriate resources including sufficient time and authority. If PII or confidential data has been breached, also contact the Data Manager. In the event that the Incident or Breach is severe, district executive management, general counsel shall be contacted.
4	Identify the cause of the Incident or breach and whether the situation has been contained. Ensure that any possibility of further data loss is removed or mitigated as far as possible. If this loss cannot be mitigated, any Incident will be characterized as a Breach.	Compartmentalize and eliminate exposure. Establish what steps can or need to be taken to contain the threat from further data loss. Contact all relevant departments who may be able to assist in this process. This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff members until more is known about the Incident.

5	Determine depth and breadth of losses and limit exposure/damages	Can data be physically recovered if damaged through use of backups, restoration or other means?
6	Notify authorities as appropriate	For criminal activities where property was stolen or fraudulent activity occurred, contact the appropriate authorities and general counsel.
7	Ensure all actions and decisions are logged and recorded as part of incident documentation and reporting.	Complete Incident Report and file with the Data Manager.

Assess Risk and Incident Scope:

B	Risk Assessment	Identify and assess ongoing risks that may be associated with the Incident or Breach.
1	Determine the type and breadth of the Incident or Breach	Classify Incident or Breach type, data compromised, and extent of breach
2	Review data sensitivity	Determine the confidentiality, scope and extent of the Incident or Breach.
3	Understand the current status of the compromised data	If data has been stolen, could it be used for purposes that harm the individuals whose identity has been compromised; If identity theft is involved, this poses a different type and level of risk.
4	Document risk limiting processes or technology components that contain and manage the Incident	Does encryption of data/device help to limit risk of exposure?
5	Determine what technologies or processes will mitigate the loss and restore service	Are there backups of the compromised data? Can they be restored to a ready state?
6	Identify and document the scope, number of users affected, and depth of Incident or Breach	How many individuals' personally identifiable information were affected?
7	Define individuals and roles whose data was compromised	Identify all students, staff, districts, customers or vendors involved in the Incident or Breach
8	If exploited, what will the compromised data tell a third party about the individual? Could it be misused?	Confidential Information or PII could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a criminal build up a detailed picture associated with identity theft or fraud.

9	Determine actual or potential harm that could come to any individuals	Identify risks to individuals: • Physical Safety • Emotional Wellbeing • Personal or Business Reputation • Financial Implications • Identity Concerns
10	Are there wider consequences to consider?	Is there risk to another LEP, the state, or loss of public confidence?
11	Are there others who might provide support or advise on risks/courses of action?	Contact all local education providers, agencies, or companies impacted by the breached data, notify them about the Incident, and ask for assistance in limiting the scope of the Incident.

Notification and Incident Communications:

C	Notification and Communications	Notification enables affected stakeholders to take precautionary steps and allow regulatory bodies to act on the Incident or Breach.
1	Notify impacted individuals of Incident or Breach remedies.	Provide individuals involved in the Incident or Breach with mitigation strategies to re-secure data (e.g. change user id and/or passwords etc.)
2	Determine Internal Communication Plans	Work with senior leadership and provide regular internal updates on status of Incident or Breach, remedies underway, and current exposure and containment strategies. This messaging should be provided to all internal state stakeholders and management.
3	Determine Public Messaging	Prepare and execute a communication and follow-up plan with senior leadership. Communication strategies need to define audience(s), frequency, messaging, and content.

4	Execute Messaging Plan	Working through appropriate leadership, execute the public and internal communication plans. Depending on the nature and scope of the Incident or Breach, multiple messages may need to be delivered as well as press and public communiques. Minimally notifications should include: • A description of the Incident or Breach (how and when it occurred) • What data was involved and whose data was compromised • Details of what has been done to respond to the Incident or Breach and any associated risks posed • Next-steps for stakeholders • District contacts for the Incident or Breach, any follow-, and other pertinent information • When notifying individuals, provide specific and clear advice on the steps they can take to protect themselves and what the district and/or third party vendor will do to help minimize their exposure Provide a way in which they can contact the district for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page)

5 RECORD RETENTION AND EXPUNGEMENT

5.1 PURPOSE

Records retention and expungement policies promote efficient management of records, preservation of records of enduring value, quality access to public information, and data privacy.

5.2 SCOPE

Uintah School District board members and staff.

5.3 RECORD RETENTION POLICY

The Uintah School District, staff, Utah LEAs and schools shall retain and dispose of student records in accordance with Section 63G-2-604, 53A-1-1407, and shall comply with active retention schedules for student records per Utah Division of Archive and Record Services.

5.4 Expungement Request Policy

Uintah School District shall review all requests for records expungement from parents and make a determination based on the following procedure.

The following records may not be expunged: grades, transcripts, a record of the student's enrollment, assessment information.

The procedure for expungement shall match the record amendment procedure found in 34 CFR 99, Subpart C of FERPA.

1. If a parent believes that a record is misleading, inaccurate, or in violation of the student's privacy, they may request that the record be expunged.
2. Uintah School District shall decide whether to expunge the data within a reasonable time after the request.
3. If Uintah School District decides not to expunge the record, they will inform the parent of their decision as well as the right to an appeal hearing.
4. Uintah School District shall hold the hearing within a reasonable time after receiving the request for a hearing.
5. Uintah School District shall provide the parent notice of the date, time, and place in advance of the hearing.
6. The hearing shall be conducted by any individual that does not have a direct interest in the outcome of the hearing.
7. Uintah School District shall give the parent a full and fair opportunity to present relevant evidence. At the parents' expense and choice, they may be represented by an individual of their choice, including an attorney.
8. Uintah School District shall make its decision in writing within a reasonable time following the hearing.
9. The decision must be based exclusively on evidence presented at the hearing and include a summary of the evidence and reasons for the decision.

If the decision is to expunge the record, the LEA will seal it or make it otherwise unavailable to other staff and educators.

6 Quality Assurances and Transparency Requirements

6.1 Purpose

Data quality is achieved when information is valid for the use to which it is applied, is consistent with other reported data and users of the data have confidence in and rely upon it. Good data quality does not solely exist with the data itself, but is also a function of appropriate data interpretation and use and the perceived quality of the data. Thus, true data quality involves not just those auditing, cleaning and reporting the data, but also data consumers. Data quality at is addressed in five areas:

6.1.1 Data Governance Structure

The Uintah School District data governance plan is structured to encourage the effective and appropriate use of educational data. The Uintah School District data governance plan centers on the

idea that data is the responsibility of all Uintah School District sections and that data driven decision making is the goal of all data collection, storage, reporting and analysis. Data driven decision making guides what data is collected, reported and analyzed.

6.1.2 Data Requirements and Definitions

Clear and consistent data requirements and definitions are necessary for good data quality. On the data collection side, the Uintah School District communicates data requirements and definitions to LEAs through the Data Clearinghouse Update Transactions documentation (see http://www.schools.utah.gov/computerservices/Data-Clearinghouse.aspx). The Uintah School District also communicates with LEA IT staff regularly, at monthly Data Warehouse Group meetings and at biannual Data Conferences. Where possible, Uintah School District program specialists are invited to these meetings and the same guidance is given to the appropriate LEA program directors.

On the data reporting side, the production and presentation layers provide standard data definitions and business rules. Data Stewards coordinate data releases through the Data Stewards Group meetings. All data released includes relevant data definitions, business rules, and are date stamped. Further, Data and Statistics produces documentation, trainings and FAQs on key statistics and reports, such as AYP, graduation rate and class size.

6.1.3 Data Collection

Data elements should be collected only once—no duplicate data collections are permitted. Where possible, data is collected at the lowest level available (i.e. at the student/teacher level). Thus, there are no aggregate data collections if the aggregate data can be derived or calculated from the detailed data.

For all new data collections, Uintah School District provides to LEAs clear guidelines for data collection and the purpose of the data request. The Uintah School District also notifies LEAs as soon as possible about future data collections. Time must be given to LEAs in order for them to begin gathering the data needed.

6.1.4 Data Auditing

Data and Statistics Data Analysts perform regular and ad hoc data auditing. They analyze data in the warehouse for anomalies, investigate the source of the anomalies, and work with IT and/or LEAs in explaining and/or correcting the anomalies. Data Analysts also work with School Finance to address findings from the Auditors.

6.1.5 Quality Control Checklist

Checklists have been proven to increase quality (See Appendix B). Therefore, before releasing high-risk data, Data Stewards and Data Analysts must successfully complete the data release checklist in three areas: reliability, validity and presentation.

7 DATA TRANSPARENCY

Annually, Uintah School District will publically post the Metadata Dictionary as described in Utah's Student Data Protection Act (SDPA), U.C.A §53A-1-1401

8 CYBERSECURITY FRAMEWORK

Uintah School District Cybersecurity Framework

Basic Controls:

1. **Hardware Inventory**:
    a. Utilize an active discovery tool to identify devices connected to the organization's network and update the hardware asset inventory. Currently utilizing Asset Manager from Dude Solutions.
2. **Software Inventory:**
    a. Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.
3. **Continuous Vulnerability Management:**
    a. Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.
4. **Controlled Use of Administrative Privileges:**
    a. Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.
5. **Secure Configuration for Hardware Including Laptops, Servers, and Workstations:**
    a. Maintain documented, standard security configuration standards for all authorized operating systems and software.
6. **Maintenance, Monitoring, and Analysis of Audit Logs:**
    a. Ensure that local logging has been enabled on all systems and networking devices.
    b. Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.
7. **Device Patch Management:**
    a. Ensure all systems including Laptops, Desktops, Servers, and Mobile Devices are current in patch level as indicated by Vendor.
    b. Utilize automated systems to discover and deploy vendor patches as soon as they are made public.

Foundational Controls:

1. **Email and Web Browser Protections:**
    a. Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers and email clients provided by the vendor.
2. **Malware Defenses:**
    a. Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.

3. **Limit and Control Network Ports, Protocols, and Services:**
    a. Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.
4. **Data Recovery Capability:**
    a. Ensure that all system data is automatically backed up on regular basis.
    b. Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.
5. **Secure Configurations for Network Devices:**
    a. Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.
    b. Manage all network devices using multi-factor authentication and encrypted sessions.
6. **Boundary Defense:**
    a. Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries.
7. **Data Protection:**
    a. Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.
8. **Controlled Access on the Need to Know:**
    a. Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).
9. **Wireless Access Control:**
    a. Leverage the Advanced Encryption Standard (AES) to encrypt wireless data in transit.
    b. Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.
10. **Account Monitoring and Control:**
    a. Require multi-factor authentication for all administrator accounts, on all systems, whether managed onsite or by a third-party provider.

Organizational Controls:

1. **Implement a Security Awareness and training Program**
    a. Train the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams and impersonation calls.
2. **Incident Response and Management:**
    a. Ensure that there are written incident response plans that defines roles of personnel as well as phases of incident handling/management

9 APPENDIX

Appendix A. Protecting PII in Public Reporting

Data Gateway Statistical Reporting Method for Protecting PII

Public education reports offer the challenge of meeting transparency requirements while also meeting legal requirements to protect each student's personally identifiable information (PII). Recognizing this, the reporting requirements state that subgroup disaggregation of the data may not be published if the results would yield personally identifiable information about an individual student. While the data used by the Uintah School District (Uintah School District) and local education agencies (LEAs) is comprehensive, the data made available to the public is masked to avoid unintended disclosure of personally identifiable information at summary school, LEA, or state-level reports.

This is done by applying the following statistical method for protecting PII.

1. Underlying counts for groups or subgroups totals are not reported.
2. If a reporting group has 1 or more subgroup(s) with 10 or fewer students.
    - The results of the subgroup(s) with 10 or fewer students are recoded as "N<10"
    - For remaining subgroups within the reporting group
        1. For subgroups with 300 or more students, apply the following suppression rules.
            1. Values of 99% to 100% are recoded to ≥99%
            2. Values of 0% to 1% are recoded to ≤1%
        2. For subgroups with 100 or more than but less than 300 students, apply the following suppression rules.
            1. Values of 98% to 100% are recoded to ≥98%
            2. Values of 0% to 2% are recoded to ≤2%
        3. For subgroups with 40 or more but less than 100 students, apply the following suppression rules.
            1. Values of 95% to 100% are recoded to ≥95%
            2. Values of 0% to 5% are recoded to ≤5%
        4. For subgroups with 20 or more but less than 40 students, apply the following suppression rules.
            1. Values of 90% to 100% are recoded to ≥90%
            2. Values of 0% to 10% are recoded to ≤10%
            3. Recode the percentage in all remaining categories in all groups into intervals as follows (11-19,20-29,…,80-89)
        5. For subgroups with 10 or more but less than 20 students, apply the following suppression rules.
            1. Values of 80% to 100% are recoded to ≥80%
            2. Values of 0% to 20% are recoded to ≤20%
            3. Recode the percentage in all remaining categories in all groups into intervals as follows (20-29,30-39,…,70-79)

Appendix B. Example Quality Control Checklist

Reliability (results are consistent)

1. Same definitions were used for same or similar data previously reported **or** it is made very clear in answering the request how and why different definitions were used
2. Results are consistent with other reported results **or** conflicting results are identified and an explanation provided in request as to why is different
3. All data used to answer this particular request was consistently defined (i.e. if teacher data and student data are reported together, are from the same year/time period)
4. Another Uintah School District data steward could reproduce the results using the information provided in the metadata

Validity (results measure what are supposed to measure, data addresses the request)

5. Request was clarified
6. Identified and included all data owners that would have a stake in the data used
7. Data owners approve of data definitions and business rules used in the request
8. All pertinent business rules were applied
9. Data answers the intent of the request (intent ascertained from clarifying request)
10. Data answers the purpose of the request (audience, use, etc.)
11. Limits of the data are clearly stated
12. Definitions of terms and business rules are outlined so that a typical person can understand what the data represents

Presentation

13. Is date-stamped
14. Small n-sizes and other privacy issues are appropriately handled
15. Wording, spelling and grammar are correct
16. Data presentation is well organized and meets the needs of the requester
17. Data is provided in a format appropriate to the request
18. A typical person could not easily misinterpret the presentation of the data