DATE: October 31, 2014

TO: HONORABLE HANK COE
HONORABLE MATT TEETERS

FROM: Wyoming Department of Education

SUBJECT: Data Security Plan Required by W.S. 21-2-202(a)(xxxiv)A-J

CC: Cindy Hill, Superintendent of Public Instruction
Flint Waters, State Chief Information Officer

EXECUTIVE SUMMARY:

As required by the W.S. 21-2-202(a)(xxxiv)A-J, the Wyoming Department of Education (WDE) with the Wyoming Department of Enterprise Technology Services (ETS) is providing an update on activities related to the Data Security Plan and data collection inventory, and recommendations.

- A Collaborative Workgroup was created on March 13, 2014, meeting weekly and including the following WDE and ETS members:
  - Finance and Data Division Director, WDE
  - IT Service Manager, WDE
  - Data Collection and Reporting Supervisor, WDE
  - Data Governance Coordinator, WDE
  - Enterprise Security Architect, ETS
  - Enterprise Education Architect, ETS
  - Enterprise System Architect, ETS
  - IT Governance Program Coordinator, ETS

- The working group has created a Data Security Report focusing on the core legislative requirements:
  - Creating a WDE Data Security Plan
  - Apprising the committee of the security plan implementation status
  - Making appropriate recommendations based on findings
  - Providing data collection inventory information
  - Making data collection recommendations

- Highlights of the data security requirements already being implemented include:
  - Developing data security policies;
  - Breach notification procedures;
  - System and data access procedures;
  - Distribution and use of full disk encryption for laptop based systems. Additionally, the WDE has purchased and started the distribution of encrypted “thumb drives” for use by WDE employees; and
  - Additional contract language requiring data security and privacy measures provided by WDE.

- WDE has developed preliminary recommendations focused on carrying out the responsibilities detailed in the Data Security Plan:
  - WDE will perform, in coordination with ETS, a third party risk assessment to include a physical and environmental assessment.
  - In order to accomplish the task outlined in the Data Security Plan, the WDE has identified staffing deficiencies; five (5) Data Security roles and three (3) Data Security positions
  - WDE has also identified the need for recurring, specialized training for critical Data Security roles

Wyoming Department of Education in Collaboration With
Wyoming Department of Enterprise Technology Services

Data Security Report

(SF0079/SEA0066 of 2014 Budget Session Response)

31 October, 2014

Contents

DATA SECURITY PLAN

Introduction

Purpose

The goal of this Data Security Plan is to protect information assets while aligning with privacy and confidentiality regulations and educational requirements. The use of data is vital to ensure the best education for our children. However, the benefits of using student data must always be balanced with the need to protect students' privacy rights. Students and their parents should expect that their personal information is properly and safely collected, maintained, used only for appropriate purposes, and not improperly disclosed. It is imperative to protect students' privacy to avoid discrimination, identity theft, or other malicious and damaging criminal acts. All education data holders must act responsibly and be held accountable for safeguarding students' personally identifiable information (PII).

High quality data and robust data systems will help measure progress towards the Wyoming Department of Education's (WDE) goal to better meet the needs of parents, teachers, and students. Whether we are referring to student-level or aggregated data collected by the State or student-level data stored by a school – we all share responsibility for data, and how it is accessed and used in a secure manner that protects students privacy and confidentiality. The current and proposed Family Educational Rights and Privacy Act (FERPA) regulations are a critical piece of this effort; however, it is equally important to consider that FERPA does not address the full scope of policies and procedures that should be in place to adequately protect student privacy in today's world of evolving technology and information use.

Keeping this in mind, establishing the WDE Data Security Plan is a start to a multi-layered data security approach in which resources will be required to complement a fully developed WDE data security architecture. Resources for such an endeavor will include: funding for training, technology, internal and external risk assessments, and staffing for implementation, continued maintenance, and monitoring.

Scope

The State Superintendent of Public Instruction, with the Director of Enterprise Technology Services (ETS), establishes criteria for the collection, storage, management, and reporting of the WDE data related to teacher certification, Statewide education accountability and assessment, and the administration of the school finance system. In carrying out this effort the WDE, in collaboration with ETS, will develop a Data Security Plan that includes:

- Guidelines for authorizing access to student data, including authentication of authorized access
- Privacy compliance standards; where they may exceed the requirements established by ETS
- Privacy and security audits, when applicable, coordinated with ETS
- Breach planning, notification and procedures pertaining thereto
- Data retention and disposition policies
- Data security policies including electronic, physical, and administrative safeguards such as data encryption and employee training
- Routine and ongoing compliance with FERPA and other privacy laws and policies as defined by WDE
- Prohibition of the sale, commercial, non-educational, or for-profit use, of student data to private entities or organizations
- All personally identifiable student information being reported to the WDE by a student's Wyoming Integrated Statewide Education (WISE) Student Record ID (WISER ID) as issued by the WDE. NOTE: No personally identifiable student data is reported to ETS. ETS provides enterprise infrastructure that is only a subset of WDE technical infrastructure and systems that transmit, handle and maintain personally identifiable student data.

This Data Security Plan is a living document. It contains, in this baseline version, the WDE in collaboration with ETS's understanding of the regulatory requirements for protecting the privacy of student data and the initial determination of technical, physical, and administrative controls we will implement to safeguard State infrastructure and student data. The Data Security Plan will mature over time with more specific security controls and methods and will be the foundation for to the final security plan. The security plan will encompass effective security management processes that will target specific

areas of risk, implement focused security controls for those areas, and automate the monitoring and measurement of the controls.

Roles and Responsibilities

Wyoming Department of Education

Information Security Officer (ISO)

The WDE employee performing information security duties performs such a role as their primary role in the organization. The ISO will head an office with the mission and resources to assist in ensuring agency compliance with information security requirements. He or she periodically assesses risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the WDE. The ISO develops and maintains risk-based, cost-effective information security policies, procedures, and control techniques to address all applicable requirements throughout the life cycle of the WDE information systems in order to ensure compliance with applicable Federal and State requirements. Additionally he or she facilitates development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems. The ISO periodically tests and evaluates the effectiveness of information security policies, procedures, and practices in addition to establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the WDE. The ISO develops and implementing procedures for detecting, reporting, and responding to security incidents and ensures preparation and maintenance of plans and procedures to provide continuity of operations for information systems that support the operations and assets of the WDE. The ISO has the overall responsibility of supervising the associated duties of those reporting to him or her. Lastly the information security representative serves as the primary liaison between the WDE and ETS; as it applies to data security requirements.

Training and Education Coordinator

The Training and Education Coordinator will be responsible for designing a successful data privacy and security educational program consisting of: 1) assisting in the development of data security policies that reflects business needs tempered by known risks; 2) informing users of their data security responsibilities, as documented in agency data security policy and procedures; and 3) establishing processes for monitoring and reviewing the program. The Training and Education Coordinator ensures that agency personnel, including full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers, and anyone else granted access to sensitive student information, receive appropriate information security awareness training and trains and oversees personnel with significant responsibilities for information security with respect to such responsibilities. He or she will organize and develop training manuals, reference library, testing and evaluation procedures, multimedia visual aids, and other educational materials. The Training and Education Coordinator designs training procedures, utilizing knowledge of effectiveness of such methods as individual training, group instruction, lectures, on-the-job training, demonstrations, conferences, meetings, and workshops. He or she will coordinate established courses with technical and professional courses offered by community educational entities. He or she will write applications and proposals to submit for fund-granting authorities, as it applies to awareness, education, and training; such as government and foundations. The Training and Education Coordinator will report directly to the ISO.

Data Security Application Manager

The Data Security Application Coordinator is responsible for creating the overall functional applications data security matrix for applications the WDE is responsible for. In doing so, the Data Security Application Coordinator will be responsible for ensuring no conflict of interest, separation of duties, and valid need to know is established and verified, before application access is granted. It will be the responsibility of the coordinator to ensure system access request are coordinated correctly in addition to maintaining the completed access request forms for audit processes. He or she will create a quarterly report and presentation, detailing current application access to student information while identifying any potential issues and the best method to mitigate any problems. The data security application coordinator will review all application access controls to include Oracle databases, SQL databases, and the WDE functional applications. Additionally he or she will be responsible for daily monitoring of access to ensure proper data usage and identify any abuse. The coordinator will report directly to the ISO.

Data Security Auditor

The Information Security Auditor will be responsible for the scheduling, coordinating, and auditing the WDE technology resources in addition to providing an in-depth annual audit reports of the WDE data security as it applies to applications the WDE own. As part of these duties he or she will establish internal audit procedures and standards that comply with Federal and State requirements. He or she will develop a crosswalk matrix identifying Federal and State requirements and how they correlate with internal audit checklist and categories. The Data Security Auditor will provide advice and assistance with the WDE, State or third party assessments, targeted the WDE data security needs, establish a data security baseline, and define gap analysis priorities. He or she will provide ongoing assessments of the overall efficiency and effectiveness of the WDE data governance initiatives. The Data Security Auditor will provide feedback on and consider the effectiveness of audit contributions to the WDE data security and internal data related initiatives. He or she will use lessons learned to adapt and improve audit approaches to future data audit activities. The Data Security Auditor will provide ongoing audits based on an integrated governance approach, using criteria shared with the WDE leadership based around common, accepted frameworks i.e. National Institute of Standards and Technology (NIST) Guidelines. He or she will assist with the development of policies and procedures based on audit findings, in addition to assisting with risk assessments, and the tracking and investigating of data security incidents. The Data Security Auditor will audit the use of educational data by other organizations to ensure it is consistent with the use agreed between the parties and to confirm the appropriate and thorough destruction of data upon completion of the task. Likewise, he or she will further confirm that anonymity of individual students is preserved during such use. The Data Security Auditor will report directly to the ISO.

Asset Inventory Specialist

The Asset Inventory Specialist will be responsible for ensuring that the state collect all data required by law pertaining to students but no additional data and that the districts are not collecting student data beyond that which is permitted by law. For example, that districts are not conducting their own research by collecting data that is not otherwise permitted to be collected, such as asking for student data on the political affiliation of parents, or religious beliefs of parents. He or she will be the one to monitor district collections and to receive and investigate parental/student complaints about district collections. The Asset Inventory Specialist will ensure the accurate and ongoing inventory, tracking, receiving, handling, and issuing of technology related equipment for the WDE. He or she will be responsible for the continuous updating of the hardware asset inventory database detailing system identification information, device location, and to whom it is assigned to. Additionally he or she will be required to inventory software applications, on each WDE system, ensuring software license compliance and authorized application use. The Asset Inventory Specialist will be responsible for identifying and reporting unauthorized applications usage in addition to the removal of said applications. He or she will be responsible for assisting in identifying ongoing hardware and software requirements while meeting operational security standards developed for the WDE. He or she will coordinate with the WDE divisions, to ensure proper and timely reclamation of assets while maintaining established requirements of retention and disposition of data; includes but not limited to, sanitation of media for reuse, portable media device data wipes, and the physical destruction of media. He or she will assist with identifying needed hardware and software resources in preparation for contingency operations effecting the WDE. The Asset Inventory Specialist will generate quarterly reports to verify inventory levels and to in assist in identifying trends and forecasting. He or she will prepare and ensure the accuracy of documentation relating to assets and inventory. He or she will develop a process around continuous improvement to maximize or exploit underutilized technology assets to achieve efficiency and Return On Investment (ROI) for the WDE. The Asset Inventory Specialist will report directly to the ISO.

Wyoming Department of Enterprise Technology Services

Director, Department of Enterprise Technology Services (otherwise known as the State Chief Information Officer)

Per Statute 9-2-2906 & W.S. 40-21-118 the state CIO's role in data security is to

Establish and enforce data security policies and standards for the state data infrastructure. These provisions shall be the minimum security requirements adhered to by all agencies. Agencies may choose to set additional security requirements to exceed but not in lieu of or that in any way interfere with the standards set… Upon request of an agency, provide enterprise data analytics services; Data analytics security services and validation services…

Information Security Representative

The Information Security Representative, for this Data Security Plan, representing ETS is the IT Security Enterprise Architect. The position's primary and general objectives are to help maintain the confidentiality, integrity, and availability of State systems and ensure the protection of the State's information assets. Related to this Data security Plan, the responsibility of the Information Security Representative is to the enterprise and the underlying infrastructure(s) that the WDE system will utilize but he or she will also provide information and collaboration as requested by the WDE.

Today's information technology landscape is changing rapidly. New technologies, new threat models, and continuously changing user patterns create a dynamic threat environment that must be carefully monitored and analyzed as it relates to the ETS infrastructure but also other agencies, such as the WDE. It is this position that actively oversees the vulnerability discovery and mitigation process for the infrastructure. Such information is shared with agencies, such as the WDE, in order to prevent the exploitation of vulnerability in their system that could lead to loss of confidentiality, integrity, and availability of student data.

The Information Security Representative with ETS' Office of Enterprise Architecture can provide technical assistance and information related to the selection, implementation, and maintenance of security controls necessary for the WDE to maintain compliance requirements. He or she will assist WDE in disseminating awareness of developing threats that are identified, and share the information with WDE's Information Security Officer (ISO) (Reference the Data Security Needs Assessment for WDE identified roles). It is anticipated that ETS will provide assistance to the WDE, at their request, with the selection and implementation of security controls and practices that the WDE selects to appropriately meet the security, compliance, and functional needs of the WDE. Selection of the controls by the WDE should address underlying security requirements to ensure regulatory compliance, as well as the potential impact of their decisions on the agency's mission, operations, strategic functions, and resources. The systematic selection and management of IT security services is critical to the confidentiality, integrity, and availability of State systems.

A comprehensive approach to the WDE's IT security service selection with assistance in the security control options from ETS, is imperative and is specific to the needs defined in SEA0066 of 2014 Budget Session. ETS will assist the WDE in reviewing appropriate elements. Note, that depending on the element and the assistance necessary it will be determined at that time if these are core ETS services or enhanced services.

If they are enhanced services then there may be an additional cost associated with those items. These elements include:

- Assess the risk to operations and assets related to student data
- Determine the level of security appropriate to protect the student data and system
- Develop and maintain a current security plan for each system housing student data
- Develop the WDE security incident handling procedures and work with ETS to ensure interoperability and efficiency in the identification, containment, mitigation and response to incidents
- Develop processes for communicating effective information potential vulnerabilities and security issues with all applicable parties
- Develop a set of effective security controls related to student data and for the system
- Develop a set of IT security metrics that enable both the WDE and ETS to effectively assess the adequacy of in-place security controls, policies, and procedures specific to WDE data.

Core Addressable Items

Guidelines for authorizing access to student data

FERPA requires that educational agencies and institutions use reasonable methods to identify and authenticate the identity of parents, students, school officials, and other parties before disclosing or permitting access to PII (34 CFR § 99.31[c]). This includes disclosures of PII made with the written consent of a parent or eligible student, as required under FERPA (34 CFR §99.30), as well as disclosures made without consent under one of the FERPA exceptions listed in 34 CFR §99.31(a). The WDE identifies and authenticates the identity of a parent or student before allowing them to inspect and review the student's own records, as permitted under FERPA (34 CFR §99.10). No individual or entity is allowed unauthenticated access to confidential educational records or data at any time.

The WDE's goal and objective is to continue its practices conforming to the core privacy and security measures of confidentiality, integrity, and availability of student data. The WDE utilizes the principle of least privilege (PoLP) when assigning user access to student level information. PoLP in conjunction with role-based access, defined by a user's

assigned duties within the organization, assist in reducing potential data security compromises due to unauthorized access. As part of the WDE's process, the WDE Data Security Application Manager (Reference the Data Security Needs Assessment for WDE identified role) will examine and determine if existing processes are adequate, establishing a documented, organizational baseline. The WDE Data Security Application Manger's objective is to continue with and modify, as needed, a formalized process for access request to all the WDE Systems; as outlined in the "Authentication of Authorized Access" section below. In doing so, he or she will continually identify automated resources, to include functional systems, where student level information is housed. The WDE Data Security Application Manager will continue to identify and document access control mechanisms for each system. All of these initiatives will continue to be conducted in accordance to Federal, State, NIST, and industry best practices[1] .

Authentication of authorized access

The WDE assigns access to internal data systems when the WDE System Access Request Form is complete and submitted to the system owner. The system owner reviews the form and grants access to the user. Employee exit procedures remove access on the final day of employment. The WDE System Access Request forms are reviewed on an annual basis, for all employees, to ensure job duties still align with granted access. Third party access must be defined in a Memorandum of Understanding (MOU) or contract. MOUs and contracts are required to define data access and destruction protocols.

The WDE creates all confidential data reports with role based access controls. Reports are displayed through the Wyoming Education Fusion portal; Fusion access is role based. District administrators are responsible for assigning staff roles, therefore controlling who has access to confidential student-level data. Districts are responsible for deactivating accounts for separated staff. Inactivating an account automatically strips the user's ability to access confidential student-level data.

As FERPA does not provide a detailed Access Control Methodology and in order to establish a scope for continued privacy and security initiatives, the WDE Data Security Application Manager will utilize the NIST guidelines where no Federal or State requirements have been established. In doing so, he or she, in collaboration with, ETS will use NIST Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations[2] subject areas to advance privacy and security initiatives:

Applicable NIST Access Controls:

{AC-1} Access Control Policy and Procedures
{AC-2} Account Management
{AC-3} Access Enforcement
{AC-4} Information Flow Enforcement
{AC-5} Separation of Duties
{AC-6} Least Privilege
{AC-7} Unsuccessful Logon Attempts
{AC-8} System Use Notification
{AC-11} Session Lock
{AC-12} Session Termination
{AC-14} Permitted Actions without Identification or Authentication
{AC-17} Remote Access
{AC-18} Wireless Access
{AC-19} Access Control for Mobile Devices
{AC-20} Use of External information systems
{AC-21} Information Sharing
{AC-22} Publicly Accessible content

> *FERPA requires that educational agencies and institutions use reasonable methods to identify and authenticate the identity of parents, students, school officials, and other parties before disclosing or permitting access to PII (34 CFR § 99.31[c]). So the question becomes, "How can an educational agency or institution determine the appropriate level of identity authentication assurance?"*

[1]The U.S. Department of Education, Privacy Technical Assistance Center has outlined the following "Identity authentication Best Practices" Document; http://ptac.ed.gov/sites/default/files/authentication.pdf
[2] NIST Special Publication 800-53r4, Security and Privacy Controls for Federal Information Systems and Organizations, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

To address this question, the WDE should be allowed and funded to contract with a third-party to conduct a risk assessment once per biennium, or whenever there is a significant change in the environment, to determine the threats to its data and evaluate the likelihood of inappropriate data disclosure based on its specific situation. This assessment should include a review of a potential impact of unauthorized disclosure or, conversely, of inappropriate denial of access to education data (e.g., when an authorized staff member is unable to perform his or her duties due to limited access to data). The analysis of the risks of a potential authentication failure and associated impact should then be used to determine the necessary levels of identity authentication assurance the organization needs to establish. Each organization must individually determine the appropriate level of assurance that will provide, in its specific environment, reasonable means for protecting the privacy of education data it maintains.[3]

Privacy Compliance Standards

Today's global environment requires agencies to comply with a growing set of regulations. The ethical and legal issues facing information and data use are leading governments to establish new laws and standards. There is no one prescribed way of implementing data security to meet privacy and confidentiality requirements.

While complying with Federal and State mandates, the WDE has implemented the following data aggregation process of student data.

The aggregation of student-level data into school-level (or higher) reports removes much of the risk of disclosure, since no direct identifiers (such as a name, Social Security Number, or student ID) are present in the aggregated data. Some risk of disclosure does remain, however, in circumstances where one or more students possess a unique or uncommon characteristic (or a combination of characteristics) that will allow them to be identified in the data table (this commonly occurs with small populations), or where some easily observable characteristic corresponds to an unrelated category in the data table (e.g., if a school reports that 100% of males in grade 11 scored at "Below Proficient" on an assessment). In these cases, some level of disclosure avoidance is necessary to prevent disclosure in the aggregate data table. (Reference Appendix A, Statistical Methods Employed by the WDE for Disclosure Avoidance)

Privacy and Security Audits

The WDE Data Security Auditor (Reference the Data Security Needs Assessment for WDE identified roles) will establish internal privacy and security audit procedures in coordination with ETS when enterprise infrastructure or services are involved. Additionally, there will be a requirement for the WDE Data Security Auditor that perform the audits to attend training to ensure compliance knowledge. Also to ensure compliance the WDE, in collaboration with ETS, will contract with a third party compliance auditor to conduct a privacy/security audit, every two years or when there has been a significant change in the environment warrantying an assessment of newly established policies, procedures, and application.

As FERPA does not provide a detailed privacy and security audit methodology, the WDE has opted to utilize the NIST guidelines. In doing so, the WDE Data Security Auditor, in collaboration with ETS, will use NIST SP 800-53 Revision 4[4] to advance our audit procedures:

Applicable NIST Audit Procedures:

{AU-1} Audit and Accountability Policy and Procedures
{AU-2} Audit Events
{AU-3} Content of Audit Records
{AU-4} Audit Storage Capacity
{AU-5} Response to Audit Processing Failures
{AU-6} Audit Review, analysis, and Reporting

[3] The U.S. Department of Education, Privacy Technical Assistance Center has outlined the following "Identity Authentication Best Practices" Document; http://ptac.ed.gov/sites/default/files/authentication.pdf

[4] NIST Special Publication 800-53r4, Security and Privacy Controls for Federal Information Systems and Organizations, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

{AU-7} Audit Reduction and Report Generation
{AU-8} Time Stamps
{AU-9} Protection of Audit Information
{AU-11} Audit Record Retention
{AU-12} Audit Generation

Breach Planning, Notification and Procedures

FERPA is not a breach-notification law and imposes no affirmative notification requirement. FERPA does, however, require that the institution maintain a record of each unauthorized disclosure, and this record must be available to students and parents exercising their right, granted by FERPA, to examine their files. Regardless of whether an unauthorized release of information requires notification, the WDE ISO, in collaboration with ETS, will conduct a review to determine why the incident occurred and to address any technical or procedural deficiencies that emerge.

As FERPA does not address the full scope of breach planning, notification and procedures, the WDE ISO will utilize U.S. Department of Education resources[5] along with setting standard organizational guidelines based on NIST SP 800-53 Revision 4[6] and NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)[7]. In doing so, we have identified the following as core addressable items:

Applicable NIST Incident Response procedures:

{IR-1} Incident Response Policy and Procedures
{IR-2} Incident Response Training
{IR-3} Incident Response Testing
{IR-4} Incident Handling
{IR-5} Incident Monitoring
{IR-6} Incident Reporting
{IR-7} Incident Response Assistance
{IR-8} Incident Response Plan

With the WDE's implementation of the core items the WDE ISO, in collaboration with ETS, will clearly define what constitutes a breach of student data. Additionally, the WDE ISO will establish and lead a WDE Incident Response Team (IRT) comprised of organizational leadership, subject matter experts, stakeholders, and external agency contacts with a defined methodology of leveraging the appropriate ETS resources, if necessary. Due to the unique knowledge and skill set required for members of the IRT, training will need to be funded. The WDE ISO, in collaboration with ETS, will need to establish incident reporting methods to include a centralized contact (email and phone number), suspicious activity form, and a management reporting structure in which employees know whom to contact. In addition to incident/breach handling, monitoring, and reporting there is a need to establish specific incident detection, analysis, containment, eradication, and recovery procedures based on the type of incident/breach. The WDE ISO, in collaboration with ETS, will establish formalized procedures for incident response assistance, i.e. whom to contact and contact information (DCI, FBI, etc.). The WDE employee training and education will be critical in our incident/breach procedures; the WDE Training and Education Coordinator (Reference the Data Security Needs Assessment for WDE identified roles) will implement a formalized educational training instructing employees on proper incident/breach identification and notification process and procedures. As indicated in the core plan requirements the WDE ISO, in collaboration with ETS, will lead annual training exercises to simulate an incident and test whether the response plan is effective and whether the staff members understand and are able to perform their roles effectively.

[5] The U.S. Department of Education, Privacy Technical Assistance Center has outlined the following checklist for "Data Breach Response"; http://ptac.ed.gov/document/checklist-data-breach-response-sept-2012
[6] NIST Special Publication 800-53r4, Security and Privacy Controls for Federal Information Systems and Organizations; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
[7] NIST, Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII); http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

Data Retention and Disposition

FERPA does not provide specific requirements for educational agencies and institutions regarding disposition or destruction of the data they collect or maintain themselves, other than requiring them to safeguard FERPA-protected data from unauthorized disclosure, and not to destroy any education records if there is an outstanding request to inspect or review them. The WDE complies with the following:

> CFR-2012 Title 7 Volume 4 Section 210.23; (c) Retention of records. State agencies and school food authorities may retain necessary records in their original form or on microfilm. State agency records shall be retained for a period of 3 years after the date of submission of the final Financial Status Report for the fiscal year. School food authority records shall be retained for a period of 3 years after submission of the final Claim for Reimbursement for the fiscal year. In either case, if audit findings have not been resolved, the records shall be retained beyond the 3-year period as long as required for the resolution of the issues raised by the audit.
>
> Wyoming Statute § 9-2-410 states: "All public records are the property of the State. They shall be delivered by outgoing officials and employees to their successors and shall be preserved, stored, transferred, destroyed or disposed of, and otherwise managed, only in accordance with W.S. § 9-2-405 through 9-2-413."
>
> Wyoming Department of Education, Retention Schedule (Reference Appendix B)

Additional to the Federal and State Retention and Disposition requirements, the WDE's Asset Inventory Specialist (Reference the Data Security Needs Assessment for WDE identified roles) objective is to review processes and procedures to ensure compliance and make appropriate modifications as necessary. To assist in this process the he or she will survey educational program managers, data stewards, and leadership in order to identify any new or modified requirements. The WDE Asset Inventory Specialist will also utilize the US Department of Education Data Destruction Best Practices document as a guide.[8]

Data Security Policies

The WDE strives to meet and exceed Federal and State student data security requirements. In continuing the process development of a multi layered security approach the WDE ISO will formalize internal policies and procedures complimenting Wyoming State policies[9] while complying with Federal mandates. In creating these policies the WDE ISO will devise a detailed plan for annual review to ensure compliance and address technology changes as needs occur.

Administrative Safeguards

The WDE ISO, in collaboration with ETS, will ensure administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect student data and to manage the conduct of the educational entity's workforce in relation to the protection of that information.

Additionally, the WDE ISO, in collaboration with ETS, will review, establish, and implement (as needed):

- Security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to ensure compliance with FERPA and all other Federal requirements as they apply
- Security awareness and training program for all members of its workforce (including management).
- Policies and procedures to/for WDE, in collaboration with ETS:
    - Regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports
    - Ensure that all members of its workforce have appropriate levels of access to student data and to prevent those workforce members who do not have authorized access from obtaining access to student data
    - Determine that the access of a workforce member to student data is appropriate

[8] The U.S. Department of Education, Privacy Technical Assistance Center, "Best Practices for Data Destruction" document; http://ptac.ed.gov/sites/default/files/Best%20Practices%20for%20Data%20Destruction%20%282014-05-06%29%20%5BFinal%5D.pdf

[9] Wyoming State Policies, http://ets.wyo.gov/resources/policies-and-standards

- Terminating access to student data when the employment of a workforce member ends or as the employee's role changes in the organization
- Authorizing access student data that are consistent with the applicable requirements defined by their roles and responsibilities within the WDE
- Granting access to student data, for example, through access to a workstation, transaction, program, process, or other mechanism
- That, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process
- Address security incidents
- Periodic testing and revision of contingency plans
- Enable continuation of critical business processes for protection of the security of student data while operating in emergency mode
- Guarding against, detecting, and reporting malicious software
- Monitoring log-in attempts and reporting discrepancies
- Responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain student data
- Create and maintain retrievable exact copies of student data
- Restore any loss of student data

- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of student data held by the WDE
- Apply appropriate disciplinary actions against workforce members who fail to comply with the security policies and procedures
- Identify the security official who is responsible for the development and implementation of the policies and procedures required by the WDE
- Ensure third party vendors/contractor, researchers, and educational entities implement policies and procedures that protect the WDE owned student data from unauthorized access
- Perform periodic security reviews and updates
- Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the agency; and document security incidents and their outcomes
- Assess the relative criticality of specific applications and data in support of other contingency plan components
- Periodic technical and nontechnical evaluation, based initially upon the standards implemented under FERPA and applicable State and industry best practices subsequently, in response to environmental or operational changes affecting the security of student data that establishes the extent to which the agencies security policies and procedures meet the requirements

In order to comply with the Health Insurance Portability Accountability Act (HIPAA), 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards, Final Rule; the following required and addressable implementation specifications will need to be reviewed, modified and/or implemented with regards to the WDE data covered under HIPAA:

Standards	**Sections**	**Implementation Specifications**	
Security Management Process	164.308(a)(1)	Risk Analysis	Required
		Risk Management	Required
		Sanction Policy	Required
		Information System Activity Review	Required
Assigned Security Responsibility	164.308(a)(2)		Required
Workforce Security	164.308(a)(3)	Authorization and/or Supervision	Addressable
		Workforce Clearance Procedure	Addressable
		Termination Procedures	Addressable
Information Access Management	164.308(a)(4)	Isolating Health Care Clearinghouse Functions	Required
		Access Authorization	Addressable
		Access Establishment and Modification	Addressable

Security Awareness and Training	164.308(a)(5)	Security Reminders	Addressable
		Protection from Malicious Software	Addressable
		Log-in Monitoring	Addressable
		Password Management	Addressable
Security Incident Procedures	164.308(a)(6)	Response and Reporting	Required
Contingency Plan	164.308(a)(7)	Data Backup Plan	Required
		Disaster Recovery Plan	Required
		Emergency Mode Operations Plan	Required
		Testing and Revision Procedures	Addressable
		Applications and Data Criticality Analysis	Addressable
Evaluation	164.308(a)(8)		Required
Business Associate and Contracts and Other Arrangements	164.308(b)(1)	Written Contract or Other Arrangement	Required

HIPAA compliance is related to a small subset of data associated with the Court Ordered Placement Systems (COPS) that houses some Protected Health Information (PHI.)

Physical Safeguards

Physical controls are an essential part of IT Security controls. Both physical and environmental security controls will be implemented to protect the facilities housing the WDE systems and resources. Basic facility services for systems are provided by the WDE but the infrastructure is housed and managed by ETS. There also will be a third party that hosts the system. These services will need to have the appropriate controls implemented. The services include:

- Floor space for system equipment, including computer racks and auxiliary desks and/or tables
- Floor space for personal workstations, including but not limited to desks, tables, safes, and filing cabinets
- Adequate power to the room for system equipment, to include individual computers, equipment racks, and workstation equipment
- Fire protection
- General room lighting
- Temperature control and monitoring
- Humidity control and monitoring
- Heating, ventilation, and air conditioning (HVAC)
- Emergency lighting
- Door lock releases for emergency egress from the building
- Gate, fence, parking lot barriers or other outdoor perimeter controls
- Emergency power shut off controls
- Emergency water shut off controls
- Grounds maintenance
- Trash disposal for individual rooms and the overall facility
- Secure, lockable storage containers (e.g., lockable desks or safes for securing materials overnight) with a limited number of keys issued to authorized personnel
- All building, room, and container key assignments are authorized and maintained; key inventory logs are reviewed annually
- Uninterruptable power supplies (UPS) are also provided within the equipment racks

Specific to the third party hosting in addition to the above services is secure transmission lines. Transmission will be housed with a secure conduit within the hosting facility and within its unique bundle within ETS terminating with a secure demarcation point and secure server room protected behind two levels of security.

Because the WDE systems are considered, in security terms, moderate systems the WDE Asset Inventory Specialist, in collaboration with ETS, will utilize NIST SP 800-53 Revision 4[10] to include the following controls under the Physical and Environmental Family.

Applicable NIST Physical Procedures:

{PE-1} Physical and Environmental Protection Policy and Procedures
{PE-2} Physical Access Authorizations
{PE-3} Physical Access Control
{PE-4} Access Control for Transmission Medium
{PE-5} Access Control for Output Devices
{PE-6} Monitoring Physical Access
{PE-8} Visitor Access Records
{PE-9} Power Equipment and Cabling
{PE-10} Emergency Shutoff
{PE-11} Emergency Power
{PE-12} Emergency Lighting
{PE-13} Fire Protection
{PE-14} Temperature and Humidity Controls
{PE-15} Water Damage Protection
{PE-16} Delivery and Removal
{PE-18} Location of Information System Components
{PE-19} Information Leakage
{PE-20} Asset Monitoring and Tracking

Because the WDE will rely on hosting services provided by a third party, outside of the traditional security authorization boundaries established for information systems it is important to verify the physical and environmental security controls of the third party provider. In the instance that data is housed within a cloud environment, data must be maintained securely and compliant with WDE requirements.

In order to comply with HIPAA, 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards, Final Rule; the following required and addressable implementation specifications will need to be reviewed, modified and/or implemented with regards to the WDE data covered under HIPAA:

Standards	Sections	Implementation Specifications	
Facility Access Controls	164.310(a)(1)	Contingency Operations	Addressable
		Facility Security Plan	Addressable
		Access Control and Validation Procedures	Addressable
		Maintenance Records	Addressable
Workstation Use	164.310(b)		Required
Workstation Security	164.310(c)		Required
Device and Media Controls	164.310(d)(1)	Disposal	Required
		Media Re-Use	Required
		Accountability	Addressable
		Data Backup and Storage	Addressable

[10] NIST Special Publication 800-53r4, Security and Privacy Controls for Federal Information Systems and Organizations; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Electronic (Technical Safeguards)

A combination of mutually-reinforcing security controls implemented by technical means, physical means, and procedural means creates layers of defense called defense in depth to maintain confidentiality, integrity and availability. This important principle will be used for the WDE and ETS systems and related student data to achieve information assurance focusing on three primary elements: people, technology, and operations. This section will discuss, in general, the technical controls also known as logical controls. ETS will leverage a wide range of technologies for providing information assurance services and for detecting intrusions. To insure that the right technologies are procured and deployed, the WDE ISO will work collaboratively with ETS to define WDE requirements and share with the WDE its security policy information assurance principles, system level information assurance architectures and standards, configuration guidance, and processes for assessing the risk of the interfaced systems.

The defense in depth strategy will include several information assurance principles. These are based on: defend the network and infrastructure by protecting the data transmitted through the use of encryption; defend the enclave boundaries by the use of firewalls and intrusion detection; defend the computing environment by enforcing access control; and defend the supporting infrastructures by using defense in depth.

ETS will work proactively with the WDE ISO to assist in defining the appropriate technical controls necessary to maintain the security of the WDE systems and data.

Additionally in order to comply with HIPAA, 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards, Final Rule; the following required and addressable implementation specifications will need to be reviewed, modified and/or implemented with regards to the WDE data covered under HIPAA:

Standards	**Sections**	**Implementation Specifications**	
Access Control	164.312(a)(1)	Unique User Identification	Required
		Emergency Access Procedure	Required
		Automatic Logoff	Addressable
		Encryption and Decryption	Addressable
Audit Controls	164.312(b)		Required
Integrity	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	Addressable
Person or Entity Authentication	164.312(d)		Required
Transmission Security	164.312(e)(1)	Integrity Controls	Addressable
		Encryption	Addressable

Data Encryption

It is anticipated that any databases will use encryption. Based on the vendor's solution we will use either column based or table space encryption using at a minimum AES 128 or 3DES but ideally AES 256 encryption of those data items that require encryption for compliance. The design of the database schema creates very few tables that contain critical PII data related to student data such as social security numbers. The database is also designed based on obfuscation of the tables so in the situation of a breach the data will not be easy to identify per WISER ID hence not tied back to a person. All data at rest and retained will be encrypted using AES 256. Also all data will be encrypted either by an encrypted file system or application based encryption for the all documents.

Both an encrypted file system, and individually encrypted interface files that must be decrypted by the partner system when flat-files must be used. These solutions are highly dependent upon the other data store's system's ability to use SCP to transfer files, vs AES or suitable alternative on individually encrypted files.

ETS's enterprise email system, Gmail, supports the use of encrypted email protocols. The establishment of the necessary security certificates and any necessary exchange of security keys is expected as part of the system configuration including IMAP, POP3, and SMTP.

Data in transit will be encrypted in compliance with best practices. Verification of the hosting providers practices and controls will be conducted by ETS

Employee Training

With Federal and State statutes, the WDE Training and Education Coordinator (Reference the Data Security Needs Assessment for WDE identified roles) will utilize the U.S. Department of Education Data Security and Management Training Best Practices[11]. As indicated in the best practices document he or she will first ensure an awareness of data security. Each person in an organization will understand why security is important both to them and the WDE. Second, the WDE Training and Education Coordinator will create a thorough training program targets all new and current employees, as well as contract workers, temporary workers, and volunteers, if applicable. At a minimum, any member of the staff, regardless of role, who has access to student data and PII, will be trained to protect data confidentiality and preserve system security. Third, the WDE Training and Education Coordinator will integrate data security training within the context of broader employee education efforts. Incorporating data security training into an organization's overarching employee education program ensures that courses get evaluated and refreshed periodically, and that program effectiveness is regularly monitored. Fourth, the WDE Training and Education Coordinator will develop role-based training courses. Everyone needs training, but not everyone needs the same training. Training will be tailored to reflect a user's job responsibilities, the volume of data handled, and the sensitivity of the data that an employee can access. Fifth, the WDE Training and Education Coordinator will incorporate breach detection and escalation in training. In spite of even the best security training, data breaches may still occur—making it critical to train employees to recognize a potential security breach and how to escalate this information to key personnel who are designated first responders. Sixth, the WDE Training and Education Coordinator will include data security messages in employee communications channels. To keep privacy and security at the forefront of activities, engage in ongoing communication with employees about data security via newsletters, emails, login reminders, and other internal channels. Seventh, the WDE Training and Education Coordinator will create a culture of security in the organization. To be truly effective, training and education should be part of the culture rather than just the required act of "taking training" and signing an acknowledgement that time was spent in a seat during the training session. Senior leaders in the organizational hierarchy must demonstrate their commitment to protecting data, securing data systems, and training their staff to do the same.

Security Training Content

Encouraging awareness about data and IT security issues and developing a properly trained staff requires that many content areas be addressed through a comprehensive training program. When developing a security program it will be helpful to include the following essential categories:

- Risk assessment including the identification of system threats and vulnerabilities
- Physical security (e.g., locked doors and windows), desktop security (e.g., password protected computers, mobile device security (e.g., no sensitive data on easily misplaced storage media), and network security (e.g., secure data exchange)
- Access controls including how to password protect files, encrypt transmissions and files, and authenticate users
- Good practices related to the use of email, software/applications, and the internet
- Phishing, hoaxes, malware, viruses, worms, spyware
- Remote access to data and systems
- Data backup and disaster recovery
- Data security breach notification protocols
- Directions for viewing written data security procedures and principles, and providing a forum to answer questions about such guidance as needed to ensure compliance

[11] http://ptac.ed.gov/sites/default/files/issue-brief-security-training.pdf

Training Delivery Methods

Differing training goals, learning styles, participant skills, user roles, employee locations, and budgets might call for different training delivery options. Regardless of the delivery method, it's important to confirm that everyone participates. Even one employee who is unaware of the importance of data management and security and how his or her actions affect security weakens overall system security—after all, a chain is still only as strong as its weakest link.

There are three commonly used methods for delivering the security awareness message and more comprehensive data security training: on demand, virtual, and onsite.

- On Demand Training offers a self-paced learning environment in which participants experience a course delivered by an industry-expert or in-house trainer via a video or other previously developed mechanism (e.g., a flash tutorial). Employees can complete exercises at their own pace and location as long as they have access to a computer and the internet. On demand delivery is a good way for most distributed organizations to reach all employees
- Virtual Classroom Training is delivered at specific times via web conferencing by an instructor and provides employees with remote access to classroom systems in which they can complete virtual activities and tutorials. Because a virtual classroom offers instruction with a live (albeit virtual) instructor, this delivery method enables participants to have their questions answered and comments addressed in real-time
- Onsite Training allows organizations to have an audience-appropriate training delivered at their own facility. Employees can be trained in a manner that is customized to the unique settings and circumstances of the organization, their job responsibilities, and the actual network and operational requirements of their technology environment. Some organizations reserve onsite training for more in-depth role-based training of key staff groups

Applicable NIST Training Procedures:

{AT-1} Security Awareness and Training Policy and Procedures
{AT-2} Security Awareness Training
{AT-3} Role-Based Security Training
{AT-4} Security Training Records

Additional resources that will be utilized in the development of the WDE Security Awareness, Training and Education program, NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role and Performance Based Model"[12] and NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program."[13]

Routine and Ongoing Compliance with FERPA

The WDE has and continues to accept the responsibilities to both protect student information and support effective data use to improve student achievement. When the WDE collects the most relevant data and are able to match individual student records over time, we can answer questions that are at the core of educational effectiveness.

Over the last decade, the State role in education has evolved to keep pace with the increased demand for timely and appropriate education data that are indispensable to policy, management, and instructional decisions. Empowering stakeholders—from parents and teachers to leaders and policymakers—with the high-quality data the need requires limited and appropriate sharing of data on students as they move through the education system.

Use of data for these purposes needs to be harmonized with appropriate protections for the privacy and security of student records. This responsibility for the WDE and State officials includes meeting the moral and legal obligations to respect and protect the privacy and confidentiality of students' personally identifiable information. It also includes mitigating risks related

[12]NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role and Performance Based Model http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf

[13] NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

to the intentional and unintentional misuse of data, which are amplified by the digital nature of today's society in which more information—in education—is housed and shared in electronic and Web-based forms. It further requires clarity around roles and responsibilities, including the States' authority to share data and the form in which the data can be shared as well as with whom the data can be shared and what protections need to be in place.

FERPA imposes limits on the disclosure of student records by educational agencies and institutions that receive funds from the U.S. Department of Education. With State and agency legislation and policies the WDE, complements Federal laws on the privacy of student records and data security that apply to education.

State policymakers, education officials, parents, and other stakeholders will need ongoing clarity about how Federal and State privacy laws apply to emerging roles and responsibilities; guidance on best practices for implementation, including those drawn from other economic sectors and industries; and tools for communicating this information effectively to stakeholders. The WDE will continue to enhance student data security to address Federal and State mandates in addition to evaluating the WDE processes as technology changes.

The WDE ISO will evaluate existing process adequacy to include:

- Justify that the student data being collected and stored is necessary, useful accurate and valid by;
    - Establishing a discrete set of policy, programmatic, and operations needs that require the collection of student data
    - Document how data collections align with these needs and the source of the requirement
    - Regularly review and update data collections to ensure only necessary data is collected to fulfill Federal and State statutes or legislative mandates.
    - Establish policies and procedures for regularly and securely archiving or destroying student records
    - Regularly audit data quality and accuracy processes

- Limit access to personally identifiable information to necessary and appropriate individuals by;
    - Define multiple levels of access based on individual's roles that limit the type of data individuals can access and for which students
    - Take the necessary steps to restrict access to personally identifiable information and to de-identify such information
    - Establish internal procedural controls, including training and confidentiality agreements for staff who have access to data and mechanisms to track data access

- Protect data that are shared from inappropriate use by;
    - Establish policies to guide decisions about whether to share data among State agencies, postsecondary institutions, researchers, or with third-party contractors
    - Ensure when data is shared (including among State agencies, among postsecondary institutions, with researchers, and with third-party contractors), there are data sharing agreements put in place to ensure confidentiality
    - When data are reported publicly in aggregate form, such as through State education agency websites or report cards, are the most robust methods used to protect personally identifiable information

- Implement a security framework that protects student information by;
    - Developed a comprehensive security framework, including administrative, physical, and technical procedures for addressing information technology, project management, data, and security issues
    - Implement training, monitor compliance, and regularly assess security operations
    - Established policies and procedures for incident management, including data losses and security breaches

- Provide public and parental notice about data collection, policies, access, and use by;
    - Communicate with students, parents, and the public about what information is being collected and shared and why
    - Provide guidance to public schools to assist them with notifying students and parents about their rights under Federal and State law, how they can access their student's information, and the processes to request changes to those data

Planned ETS Tool to Assist in Compliance

The Keylight platform will help ETS work most efficiently with agencies related to their compliance requirements. Many agencies have unique compliance requirements that they need to maintain current with. This tool will help agencies maintain the most up to date requirements and share them easily with ETS and other relevant entities.

The platform and the related components are easy to use and are design in an intuitive way using drag-and-drop and point-and-click configurations. It will help the agencies and ETS track regulation changes, manage policies and share them effectively across agencies and departments.

The application will also allow the creation of a compliance documents that can be used by the parties and in the case of an external audit, by the 3rd party auditor.

The tool will also allow us to more effectively manage their controls and identify any controls gaps and even potentially eliminate redundancy in controls. Inherent in the platform are regulatory scenarios mapped to appropriate security controls.

The management of compliance is also made easier by the ability to create and manage workflows. These workflows can be controlled at multiple levels including the identification of regulations, standards and best practice guidelines from the KeyLight's content library that includes over 700 rules, regulations and best practices.

The tool also creates a policy framework that can be leveraged by ETS and then used by agencies to harmonize their policies if they desire.

Prohibition of the Sale of Student Data

FERPA (see 20 U.S.C. § 1232g and 34 CFR Part 99) protects PII from students' education records from unauthorized disclosure. FERPA defines education records as "records that are: (1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution" (see 34 CFR § 99.3 definition of "education record"). FERPA also defines the term PII, which includes direct identifiers (such as a student's or other family member's name) and indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name) (see 34 CFR § 99.3 definition of "personally identifiable information").

Any PII from students' education records that the 3rd party receives under FERPA's school official exception may only be used for the specific purpose for which it was disclosed (i.e., to perform the outsourced institutional service or function, and the school or district must have direct control over the use and maintenance of the PII by the 3rd party receiving the PII). Further, under FERPA's school official exception, the provider may not share (or sell) FERPA-protected information, or re-use it for any other purposes, except as directed by the school or district and as permitted by FERPA.

FERPA is not the only statute that limits what 3rd parties can do with student information. The Protection of Pupil Rights Amendment (PPRA) provides parents with certain rights with regard to some marketing activities in schools. Specifically, PPRA requires that a school district must, with exceptions, directly notify parents of students who are scheduled to participate in activities involving the collection, disclosure, or use of personal information collected from students for marketing purposes, or to sell or otherwise provide that information to others for marketing purposes, and to give parents the opportunity to opt-out of these activities. 20 U.S.C. § 1232h(c)(2)(C)(i). Subject to the same exceptions, PPRA also requires districts to develop and adopt policies, in consultation with parents, about these activities. 20 U.S.C. § 1232h(c)(1)(E) and (c)(4)(A). PPRA has an important exception, however, as neither parental notice and the opportunity to opt-out nor the development and adoption of policies are required for school districts to use students' personal information that they collect from students for the exclusive purpose of developing, evaluating, or providing educational products or services for students or schools. 20 U.S.C. § 1232h(c)(4)(A).

The WDE provides a great deal of data on our website[14]; please see for links to a number of resources already available. When more detailed data is needed, a data request must be entered. The link to the Data Request process is located on the WDE website[15].

[14] http://edu.wyoming.gov/data

[15] http://edu.wyoming.gov/downloads/data/2014/governance/data-request-process-v3.pdf

Pursuant to the Wyoming Public Records Act, WS 16-4-201, the WDE will not charge a fee for the time and effort required to fulfill a data request unless the department first promulgates an agency rule allowing for fees to be collected.

Additionally, third party vendors/partners who have access to student level data are prohibited from selling student data through restrictions in their contract and/or MOU. All contracts and MOUs call for the destruction of student level data upon completion of the project.

In future planning the WDE reserves the right to charge (agencies, researchers, etc.) for the time and materials required to fulfill a data request or research request.

All PII, student data, being reported to the WDE

Statutory Requirement for Student Level Elements by Collection

A list of all WDE data collections can be found on the Data Collection Suite – Forms Inventory page of the Wyoming Department of Education Fusion portal. The forms inventory page lists collection numbers, collection names, the respondent who must submit (district, institution or other) as well as the collection due date. In addition each collection has a link that provides a collection description, steward contact information and links to supporting documentation.

The WDE has identified the following collections to contain student level data elements.

Collection Number	Collection Name	Statute	Description
WDE450	COPS Out-of-State Annual Report	W.S. 21-13-315 WDE Rules and Regulations Chapter 14	Annual Report for Out-of-State Public and Private Institutions receiving state funds for court ordered placements.
WDE451	COPS In-State Annual Report	W.S. 21-13-315 WDE Rules and Regulations Chapter 14	Annual Report for Out-of-State Public and Private Institutions receiving state funds for court ordered placements.
WDE453	Instructional Foundations for Kindergarten (Collected by Data Driven Enterprises)	W.S. 21-4-302(e)	The data is utilized for analysis of kindergarten readiness for districts with preschool programs.
WDE537	Bridges - Summary of Summer Programs	W.S. 21-13-334 WDE Rules and Regulations Chapter 33	Collects operation, enrollment, expenditures, and individual student data records on students completing summer school to enable evaluation of program effectiveness.
WDE567	Institutional Schools Title I Part D Annual Program Evaluation (Will be collected student level in 2015, reported to Feds in aggregates).	Elementary and Secondary Education Act as amended by the No Child Left Behind Act, Title I, Part D	This data for the Consolidated State Performance Report is collected by the WDE for aggregate reporting to the US Department of

			Education for evaluation purposes.
WDE568	District Title 1, Part D Annual Program Review (To be collected student level in 2015, reported out in aggregates)	Elementary and Secondary Education Act as amended by the No Child Left Behind Act, Title I, Part D	This data for the Consolidated State Performance Report is collected by the WDE for aggregate reporting to the US Department of Education for evaluation purposes.
Collection Number	**Collection Name**	**Statute**	**Description**
WDE600	WISE Attendance and Membership	W.S. 21-2-203 W.S. 21-3-110(a)(v) W.S. 21-13-101 through W.S. 21-13-331 WDE Rules and Regulations Chapter 8	District reports aggregate attendance, aggregate membership and truancy by student for the school year just ended for each school in the district or by student for each school in the district. That data is used in the WDE100, School Funding Worksheet, for School Foundation Program funding purposes.
WDE626	Early Literacy - Longitudinal Data	WY S.L. 21-3-401	Reading screener data for K-3 students, IEP student reading assessment outcome and intervention as well as intervention expenditures.
WDE636	WISE Report of Student Disciplinary Actions and Crime and Violence Incidents	W.S. 21-4-305 W.S. 21-4-306 W.S. 21-4-311 through 21-4-315 Federal Safe and Drug-Free Schools and Communities Act (SDFSC) Individuals with Disabilities Act Elementary and Secondary Education Act, Title IV, Part A, Subpart 3	Report of severe disciplinary actions, and incidents of Crime and Violence that occur on school grounds or at school sponsored events occurring during the prior school year.
WDE682	School Choice and Supplemental Services Offered	Elementary and Secondary Education Act as amended by the No Child Left Behind Act, Part A, Subpart 1, Section 1116	Used to report the number of eligible students who applied for transfer and may or may not have transferred from one school to another under choice provisions of NCLB section 1116.

Collection Number	**Collection Name**	**Statute**	**Description**
WDE684A	WISE Teacher/Course/Student - Fall Data	W.S. 21-2-203 W.S. 21-2-204 W.S. 21-2-304(a)(v) Elementary and Secondary Education Act as amended by the No Child Left Behind Act, Title I, Part A	The authoritative collection of student-level demographics and course information. Data is used for school funding, assessment administration as well as AYP and WAEA. It is also utilized for graduation rate, 16 to 1 class ratio calculations and for reporting aggregated figures to the federal government.
WDE684B	WISE Teacher/Course/Student - Spring Data	Same as WDE684 A, collected in the Spring	Used to determine where students are enrolled in the Spring, necessary for Federal and State Accountability
WDE684C	WISE Teacher/Course/Student - End of Year Data	Same as the WDE684A, collected at the end of year	Collects end of year status, data used to determine graduation rates.
WDE686A	Student Demographics for Accredited Institutions	Elementary and Secondary Education Act as amended by the No Child Left Behind Act, Title I, Part A	Used to report aggregated student subgroup counts to the federal government.
WDE687	Student Demographics for Non-accredited Institutions or Private Schools	None – Optional report for private schools.	Student file private schools have the option to submit if they want pre-labeled PAWS assessment booklets.
WDE949	9th Grade Transcripts - Wyoming Transcript Center	W.S. 21-2-204(c)(vi)	Collects ninth grade transcripts used in WAEA school performance calculations.
WDE950	Graduating Student Transcripts - Wyoming Transcript Center	W.S. 21-2-204(c)(vi) W.S. 21-16-1308(c)(vi-viii)	Collects grade twelve transcripts used in administration of the Hathaway Scholarship and WAEA school performance calculations.

Student Level Data Elements

Although the department has publicly posted collection and element information since 2005, persons seeking information about data elements have had to thumb through guidebooks and collection forms. While performing the requirements of Senate Enrolled Act 0066 and in order to support further transparency, the WDE data team started entering all student level elements into a data dictionary. Once data entry is completed for all data collections, links to data element reports will be posted on the WDE public website. Planned reports will include the following:

- An element profile report that displays all WDE elements. Selecting an element will display the data collection/s that collect it, the element description, data type and length, and option set information if applicable.
- A collection description report will be searchable by collection number and name and will display all elements associated with it.
- An element list by category report will allow users the ability to search by element domain (Student, School, Staff etc) and then select a Section (Assessment, Discipline, Enrollment, Food Services etc).

A preliminary Element list by Category report can be accessed at the following link, https://portals.edu.wyoming.gov/Reports/Public/wde-reports-2012/public-reports/wdedatadictionary/elementsbycategory.

This report is still under construction, data entry for domains other than student have not been completed and therefore are not searchable at this time.

Summary

Ensuring data privacy and security has never been as important as it is today. From 2005, to current, there have been over 872,719,000[16] records compromised through unintended disclosures, hacking/malware, physical loss, portable device loss, etc.; keep in mind these are only the breaches that have been reported. The WDE recognizes the need for continued vigilance in protecting our student data and in doing so, WDE has identified five critical roles that will are critical with ensuring the ongoing task of data protection. These roles are defined in the Data Security Needs Assessment portion of the Data Security Report.

[16] https://www.privacyrights.org

DATA SECURITY IMPLEMENTATION STATUS

The Wyoming Department of Education (WDE) has taken the initiative to begin implementing components of the WDE Data Security Plan. These include drafting data and system security policies, breach and incident response procedures, use of disk encryption and developing additional security and privacy language for vendor contracts.

Data and System Security Policies

WDE Policy ID	WDE Policy Name	Effective Date	Expiration Date	Review Period
4000-001	Access Authorization Policy			Annual
4000-002	Applications and Data Criticality Analysis			Annual
4000-003	Assigned Security Responsibility Policy			Annual
4000-004	Audit Controls Policy			Annual
4000-005	Contingency Operations Policy			Annual
4000-006	Data Backup and Storage Policy			Annual
4000-007	Data Breach Discovery			Annual
4000-008	Data Integrity Policy			Annual
4000-009	Data Retention and Disposition Policy			Annual
4000-010	Disposal Policy			Annual
4000-011	E-mail Security Policy			Annual
4000-012	Encryption Policy			Annual
4000-013	Evaluation Policy			Annual
4000-014	Information Access Management Policy			Annual
4000-015	Information Classification Policy			Annual
4000-016	Information Security Strategy Policy			Annual
4000-017	Information System Activity Review Policy			Annual
4000-018	Integrity Controls Policy			Annual
4000-019	Log-In Monitoring Policy			Annual
4000-020	Media Re-Use Draft			Annual
4000-021	Password Management Policy			Annual
4000-022	Portable Devices Policy			Annual
4000-023	Protection from Malicious Software Policy			Annual
4000-024	Remote Access Policy			Annual
4000-025	Risk Management Policy			Annual
4000-026	Security Awareness and Training Policy			Annual
4000-027	Security Incident Policy			Annual
4000-28	Security Management Process Policy			Annual
4000-029	Security Reminders Policy			Annual
4000-030	Termination Policy			Annual
4000-031	Testing and Revision Policy			Annual

4000-032	Unique User Identification Policy			Annual
4000-033	Workstation Security Policy			Annual

Data and System Security Draft Procedures and Documents

The WDE has created draft procedures and documents for the following:

- Breach and incident response procedures (Contact List, Incident Response Team Identification)
- Breach and incident response forms (Communication Log, Contacts List, Containment,, Eradication, Identification Forms, and Lost or Stolen Report/checklist)
- Internal audit forms
- Access request form to be utilized across all functional systems (Access Control)
- Record of property issued to employee form
- Media sanitization procedures and documentation
- Acceptable Use Policy; modifications made to encompass current technologies

Recognizing the need to secure data in a highly mobile environment, the WDE has begun the distribution and use of full disk encryption for laptop based systems. Additionally the WDE has purchased and started the distribution of encrypted "thumb drives" for use by WDE employees.

Data and System Security Contract Updates

The WDE, in coordination with ETS, is developing and expanding contract terminology to include data security requirements. An example of a requirement is:

> *"Contractor will be required to provide a proposed incident response plan as it applies to the any observable occurrence in a system or network that compromises the confidentiality, integrity and availability of WDE data. This includes any suspected violation or threat of violation of computer security policies, acceptable use policies, or standard security practices. Contractor will be required to notify the WDE's authorized representative, within 24-hours, of any suspected breach of data related to the State of Wyoming."*

A checklist of data privacy, security requirements, and best practices related to the Federal Education Rights and Protection Act (FERPA) is now being applied to all contracts sharing confidential and student level data. All contracts must include this information before being approved by the State CIO.

DATA SECURITY PLAN IMPLEMENTATION RECOMMENDATIONS

To implement the requirements detailed in the Data Security Plan the Wyoming Department of Education (WDE) have identified several key, preliminary recommendations. These recommendations are critical to protecting data collected and maintained, in and by, the WDE Systems.

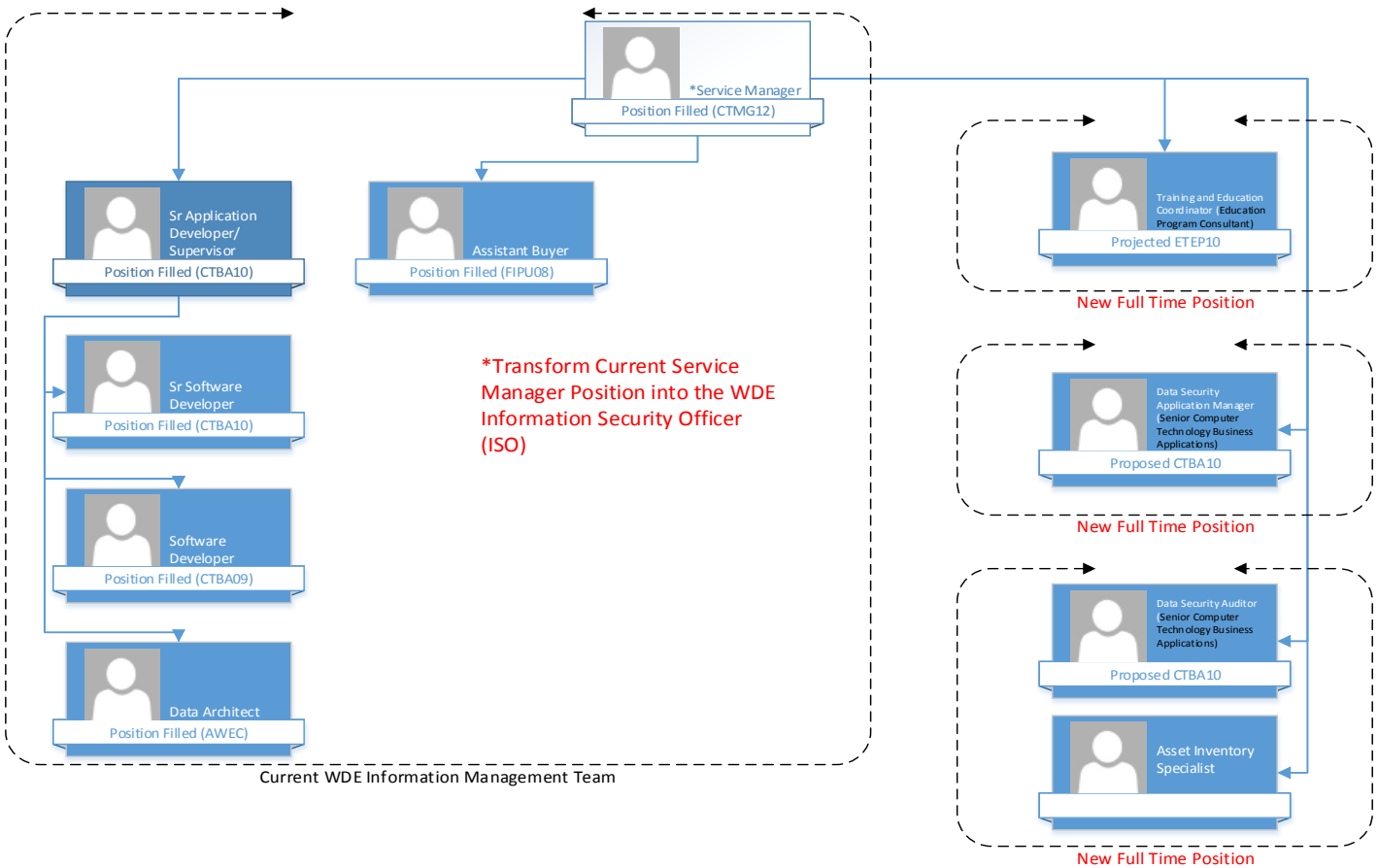
WDE Staffing Needs

The following WDE roles have been identified in order to meet the ongoing, data security, demands of the WDE:

Information Security Officer (ISO)
Training and Education Coordinator
Data Security Application Manager
Data Security Auditor
Asset Inventory Specialist

NOTE: The overall need is to create three (3) new positions within the WDE. These positions will be assigned the security roles, identified throughout the Data Security Plan. ETS has acknowledged the need to fulfill these critical Data Security Roles, within the WDE, but maintains that any increase in FTE count must come through the Governors Office.

In order to incorporate these roles into the WDE the following organizational structure has been proposed:



Third Party Risk Assessment

The WDE has identified the need for an, initial, agency wide, third party risk assessment to include a physical and environmental assessment that will be completed in coordination with ETS. This assessment will better equip WDE to determine the best methodology and mitigation path to a more secure environment in addition to formalizing requirements to establish a needs assessment and gap analysis. This type of risk assessment would be a reoccurring requirement, every two years. Between the two year period the WDE Data Security Team will develop internal audit procedures ensuring federal, state, and organizational requirements are met.

Specialized IT Security Training

In order to meet the increasingly complex data security requirements, the WDE has identified the need for reoccurring, specialized, training for critical data security positions, to include but not limited to the Incident Response Team Members, the Information Security Officer. Training needs should be met through a reputable organization such as SANS (http://www.sans.org/).

Hathaway Building Physical Security

The Hathaway Building is a public space and there are currently no barriers to prevent unauthorized access to the offices on the first floor. Sensitive information held by the agency, including Protected Health Information (PHI) and financial data, are in an area where the general public are not required to sign-in nor monitored by the receptionist. The WDE needs a physical security needs assessment and the associated funding to make the necessary changes to mitigate vulnerabilities identified by the assessment.

DATA COLLECTION INVENTORY & DATA COLLECTION RECOMMENDATIONS

History of Recent Collection Review

The Wyoming Department of Education conducted two other data collection reviews in recent years. In 2011 the department evaluated its student level data collections and determined that we could eliminate four data collections by adding a few fields into the WDE684 student collection. Eliminated Collections included:

- WDE425 – Special Education Snapshot
- WDE427 – Special Education End of Year
- WDE533 – Homeless Night Time Residence
- WDE591 – Distance Education Milestone Report

In 2013 the Wyoming Session Laws, Chapter 73, Section 338 required the WDE to review all data collections and make recommendations for elimination. The Wyoming Department of Education collaborated with the School Finance Data Advisory Committee (SFDAC) to review all data collections. Districts were also provided a list of all data collections and asked to submit their recommendations which were later reviewed at SFDAC meetings. As a result the following recommendations were made.

Collection	SFDAC Recommendation	WDE Recommendation	Legislative Action Needed
WDE100(B) - Voc Ed Student FTE Worksheet WDE100(C) - Voc Ed Teacher FTE Worksheet	Use existing data from staff and student data collections to calculate needed information rather than additional reports.	Further study on the feasibility of automating Voc Ed worksheets will be done in consultation with the SFDAC.	None
WDE104 - Monthly Litigation Expenses	Eliminate collection.	WDE agrees with recommendation.	None
WDE112 – National Board Certified Teacher Paid Report	Promulgate rules and regulations to allow the inclusion of full-time instructional facilitators, certified tutors, librarians and counselors holding national board certification through NBPTS.	WDE agrees with recommendation.	Clarification of “teacher” as used in W.S. 21-7-501(f)(ii) may be needed
WDE140 - Bonded Indebtedness Mill Levy	Eliminate collection and repeal W.S. 21-15-105.	WDE agrees with recommendation.	Yes

Collection	SFDAC Recommendation	WDE Recommendation	Legislative Action Needed
Supplement and/or Capital Lease Grants			
WDE714 - Dual and Concurrent Enrollment Fiscal Collection	Amend W.S. 21-13-310(ix) to exclude dual and concurrent revenues received under W.S. 21-20-201 from local revenue computations.	WDE agrees with recommendation.	Yes
WDE602/652 - WISE School District Staff Member Collection	Eliminate end-of-year staffing collection (WDE652) and eliminate additional teacher quality elements on WDE602/652.	WDE does not agree with recommendation.	None
WDE633 Certified Staff Vacancy and Applicant Information	SFDAC provide recommendations on how to improve the collection to more accurately collect details on staffing vacancies and recruitment processes.	WDE agrees with recommendation and will also continue work with the Research and Planning division of the Department of Workforce services to refine data elements and ensure data quality and validity.	None
WDE684 Consolidation	N/A	The consolidation of six data collections into the WDE684 resulted in the elimination of approximately 50 redundant data elements.	None

Eliminated Collection and Data Elements as Result of SEA066

After careful review of all Wyoming Department of Education data collections, we do not recommend the elimination of any data collections that require statutory changes. However the department did eliminate the WDE686B a collection previously required from Accredited Institutions as well as some WDE626 elements, both of which are described below.

- **Collection WDE686B** (Section Enrollment for Accredited Institutions) – Because accredited institution enrollment information is not utilized to meet any state statutes and the information is not reported in federal reporting this collection was recognized as unnecessary and eliminated prior to the collection opening in the Fall of 2014

- **WDE626 Element – All Students Screened Successfully** – This element was eliminated because all students are required to be reported and this field was unnecessary

- **WDE626 Element – Assist** – Narrative field that is no longer necessary
- **WDE626 – Reasons -** Narrative field that is no longer necessary

Conclusion

The WDE data team strives to find ways to reduce the data burden on all of its stakeholders. In 2013 the WDE created a data governance team that meets weekly. The data governance team ensures information demands are met but not duplicated. This team reviews all data collections six months prior to their opening date to determine if collection changes are required or if elements should be eliminated.

The WDE appreciate the opportunity the legislature has given us to make recommendations and would welcome the chance to make annual recommendations for collection elimination or bring to light shortfalls we find while conducting statutorily required data analysis. Although the department did not recommend the elimination of any data collections which would require statutory change, we would like to encourage the legislature to explore other ways to reduce data burden through technological advances such as SIF Interoperability or a Statewide Student Information System.

Numerical Examples to accompany file "WDE Assessment Public Rpt - v.2011-08-11v2 WDE - Flowchart.pdf"

WDE Assessment Public Rpt - v.2011-08-11v2 WDE - Flowchart.pdf			Examples					
"Actual Input Data" (pgs 1 and 2)	*"Process Input Names" (pgs 1 and 2)*	*Variable*	*#1*	*#2*	*#3*	*#4*	*#5*	*#6*
#_Not_Tested_RAW	#_Not_Tested_RAW	N	3	2	2	2	2	1
#_Tested_RAW	#_Tested_RAW	T	53	18	18	18	17	5
#_Below_Basic_RAW + #_Basic_RAW	#_Perf_A_RAW	PA	12	2	1	17	2	2
#_Proficient_RAW + #_Advanced_RAW	#_Perf_B_RAW	PB	41	16	17	1	15	3
#_Below_Basic_RAW	#_Perf_A1_RAW	PA1	9	1	1	13	1	2
#_Basic_RAW	#_Perf_A2_RAW	PA2	3	1	0	4	1	0
#_Proficient_RAW	#_Perf_B1_RAW	PB1	30	16	13	0	15	1
#_Advanced_RAW	#_Perf_B2_RAW	PB2	11	0	4	1	0	2
#_Tested_RAW for "All Students" subgroup	#_Tested_ALL_RAW	A	72	18	29	29	18	18

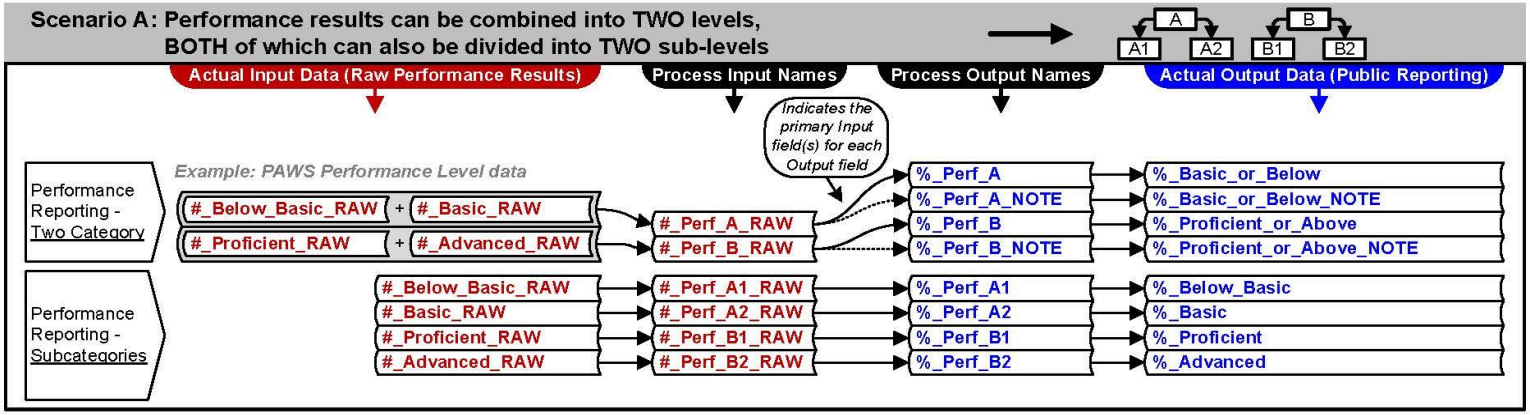
WDE Assessment Public Rpt - v.2011-08-11v2 WDE - Flowchart.pdf			Public Data as displayed					
"Actual Output Data" (pg 1 ; Example: PAWS Performance Level Data)	*Public Data equation when numerical value is to be displayed*							
#_Tested	= 10+(5 * Truncate((T-6)/5))	→	**55**	**20**	**20**	**20**		
#_Tested_NOTE		→					**H**	**L**
%_Tested	=Round(T/(T+N) , 2)	→	**95%**	**90%**	**90%**	**90%**	**89%**	
%_Basic_or_Below	=Round(PA/T , 2)	→	**23%**	**11%**	**6%**			
%_Proficient_or_Above	=Round(PB/T , 2)	→	**77%**	**89%**	**94%**			
%_Basic_or_Below_NOTE		→			**L**	**H**		
%_Proficient_or_Above_NOTE		→			**H**	**L**		
%_Below_Basic	=Round(PA1/T , 2)	→	**17%**	**6%**				
%_Basic	=Round(PA2/T , 2)	→	**6%**	**6%**				
%_Proficient	=Round(PB1/T , 2)	→	**57%**	**89%**				
%_Advanced	=Round(PB2/T , 2)	→	**21%**	**0%**				

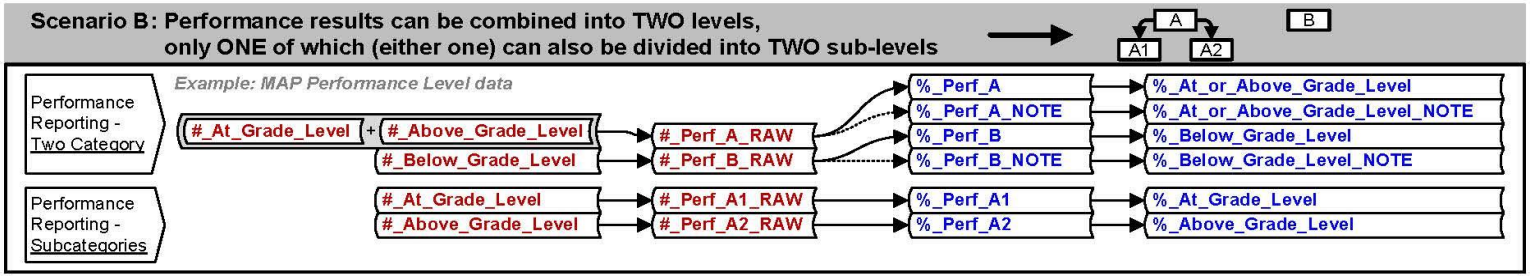
WDE PROCESS	Version 2011-08-11	Page 1 of 5
Public Reporting of Assessment Results		
This page: performance count field mapping for the three possible scenarios		

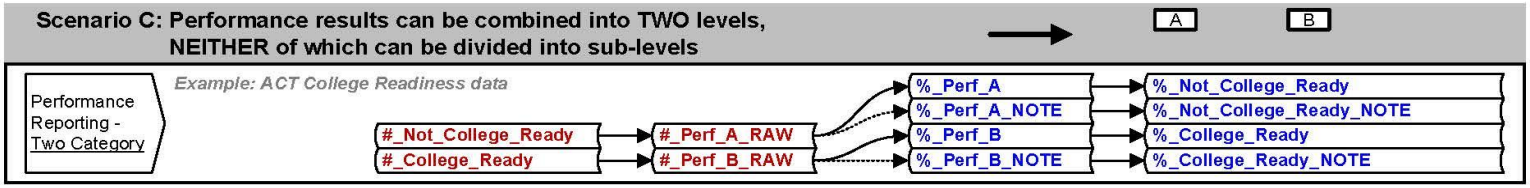
NOTE: See related examples for the three scenarios on page 5 of 5

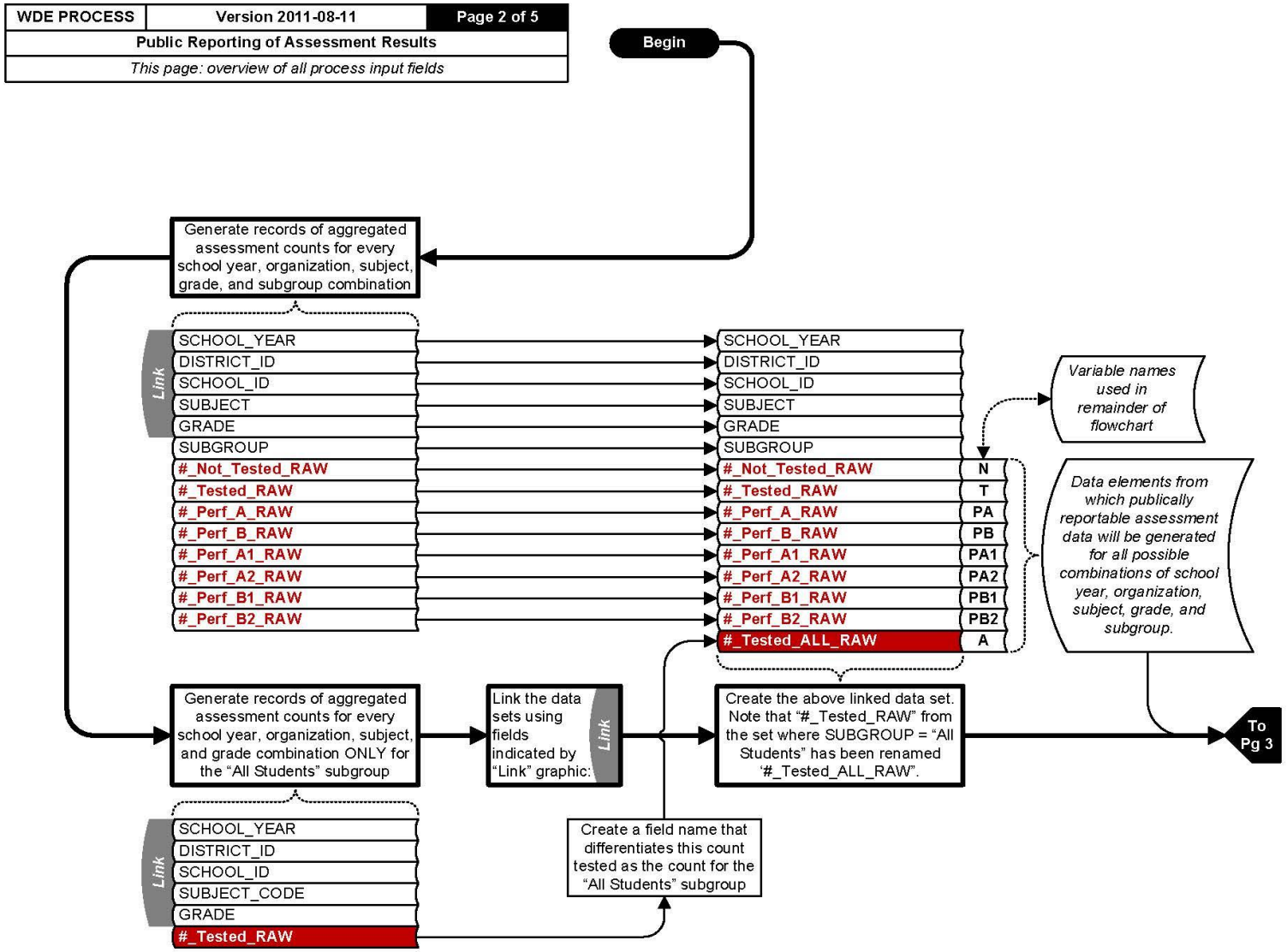
PEFORMANCE DATA field name mapping for the three generic reporting models

"Process Input Names" and "Process Output Names," below, are the generic field names used in the flowchart portion of this process document. The "Actual…" fields represent probable input and output variable names for the examples accompanying each of the three scenarios and how they map to the generic process document field names. Note that the descriptor fields (School Year, School ID, Grade, Subgroup, etc) and the "# tested" fields used in the flowchart are the same for all three scenarios, so do not need to be included in the scenario-example mapping provided below.

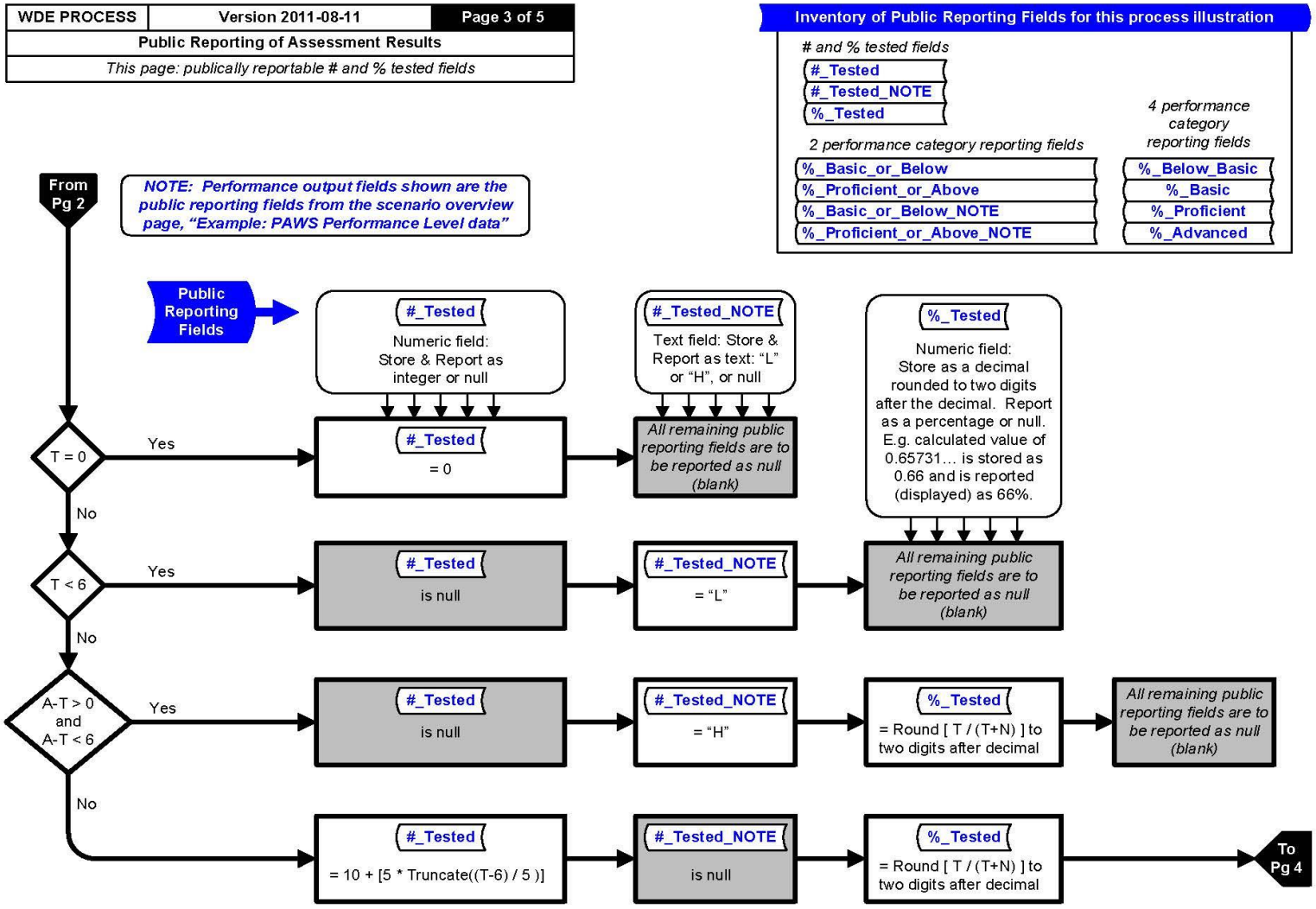






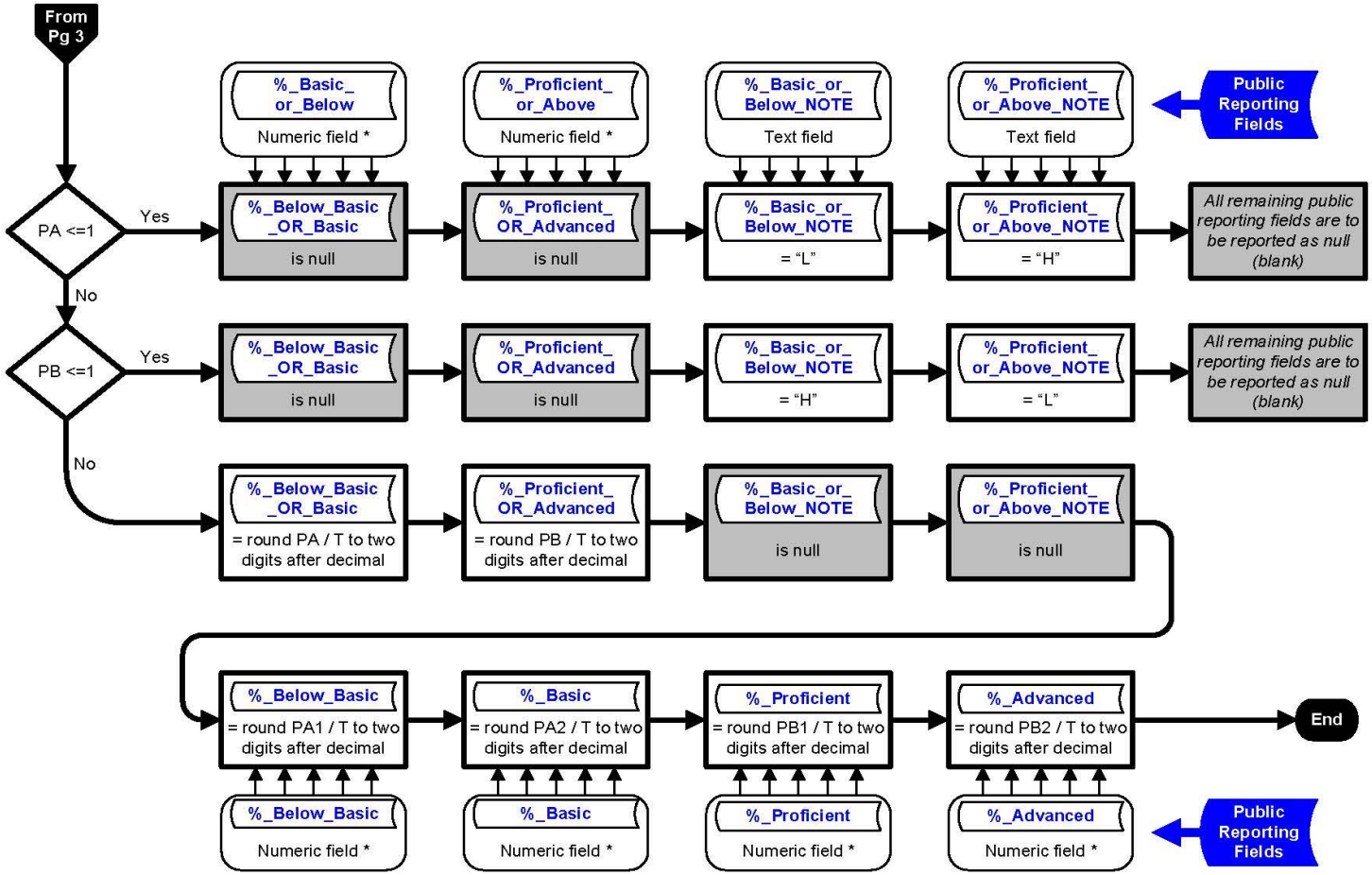

WDE PROCESS
Version 2011-08-11
Page 2 of 5
Public Reporting of Assessment Results
This page: overview of all process input fields
Begin
Generate records of aggregated assessment counts for every school year, organization, subject, grade, and subgroup combination
Link
SCHOOL_YEAR
DISTRICT_ID
SCHOOL_ID
SUBJECT
GRADE
SUBGROUP
#_Not_Tested_RAW
#_Tested_RAW
#_Perf_A_RAW
#_Perf_B_RAW
#_Perf_A1_RAW
#_Perf_A2_RAW
#_Perf_B1_RAW
#_Perf_B2_RAW
#_Tested_ALL_RAW
N
T
PA
PB
PA1
PA2
PB1
PB2
A
Variable names used in remainder of flowchart
Data elements from which publically reportable assessment data will be generated for all possible combinations of school year, organization, subject, grade, and subgroup.
Generate records of aggregated assessment counts for every school year, organization, subject, and grade combination ONLY for the "All Students" subgroup
Link the data sets using fields indicated by "Link" graphic:
Link
Create the above linked data set. Note that "#_Tested_RAW" from the set where SUBGROUP = "All Students" has been renamed '#_Tested_ALL_RAW".
To Pg 3
Link
SCHOOL_YEAR
DISTRICT_ID
SCHOOL_ID
SUBJECT_CODE
GRADE
#_Tested_RAW
Create a field name that differentiates this count tested as the count for the "All Students" subgroup

WDE PROCESS	Version 2011-08-11	Page 3 of 5
Public Reporting of Assessment Results		
This page: publically reportable # and % tested fields		



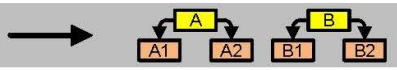
WDE PROCESS	Version 2011-08-11	Page 4 of 5
Public Reporting of Assessment Results		
This page: publically reportable performance % fields		

*Numeric field *:*
Store as a decimal rounded to two digits after the decimal. Report as a percentage or null. E.g. calculated value of 0.65731… is stored as 0.66 and is reported (displayed) as 66%.



NOTE: In ALL cases, "Public Reporting Levels" and "Public Rpt. Sub-Levels" MUST be defined via consultation with a CONTENT expert

Scenario A: Performance results can be combined into TWO levels, BOTH of which can also be divided into TWO sub-levels



Example

Source Data	
1	#_Below_Basic
2	#_Basic
3	#_Proficient
4	#_Advanced

Public Reporting Levels		
A	1+2	%_Basic_or_Below
B	3+4	%_Proficient_or_Above

Public Rpt. Sub-Levels		
A1	1	%_Below_Basic
A2	2	%_Basic
B1	3	%_Proficient
B2	4	%_Advanced

Example

Source Data	
1	#_Novice
2	#_Basic
3	#_Proficient_Minus
4	#_Proficient_Plus
5	#_Advanced

Public Reporting Levels		
A	1+2	%_Basic_or_Below
B	3+4+5	%_Proficient_or_Above

Public Rpt. Sub-Levels		
A1	1	%_Below_Basic
A2	2	%_Basic
B1	3+4	%_Proficient
B2	4	%_Advanced

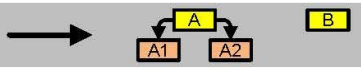
Example

Source Data	
1	#_Performance 1
2	#_Performance 2
3	#_Performance 3
4	#_Performance 4
5	#_Performance 5
6	#_Performance 6
7	#_Performance 7

Public Reporting Levels		
A	1+2+3+4	%_Below_Expectations
B	5+6+7	%_Meets_or_Exceeds_Expectations

Public Rpt. Sub-Levels		
A1	1	%_Severly_Below_Expectations
A2	2+3+4	%_Marginally_Below_Expectations
B1	5	%_Meets_Expectations
B2	6+7	%_Exceeds_Expectations

Scenario B: Performance results can be combined into TWO levels, only ONE of which (either one) can also be divided into TWO sub-levels



Example

Source Data	
3	#_Above_Grade_Level
2	#_At_Grade_Level
1	#_Below_Grade_Level

Public Reporting Levels		
A	3+2	%_At_or_Above_Grade_Level
B	1	%_Below_Grade_Level

Public Rpt. Sub-Levels		
A1	1	%_Above_Grade_Level
A2	2	%_At_Grade_Level

Scenario C: Performance results can be combined into TWO levels, NEITHER of which can be divided into sub-levels

Example

Source Data	
1	#_College_Ready
2	#_Not_College_Ready

Public Reporting Levels		
A	1	%_College_Ready
B	2	%_Not_College_Ready

Example

Source Data	
1	#_Performance 1
2	#_Performance 2
3	#_Performance 3
4	#_Performance 4
5	#_Performance 5

Public Reporting Levels		
A	1+2+3	%_Non_Proficient
B	4+5	%_Proficient

NOTE: This is a case where the content expert has determined that the performance levels are only to be divided into two categories for public reporting, without further breakout into subcategories

Education, Dept of

						Archival Review
Administration and Business Support (ADM)						
Buildings, Facilities and Infrastructure Management (BFI)						
Building Files		**ADM-BFI-02**	**LOA**		**Retain for the Life of the Asset then destroy**	**Yes**
10008	*School Building Plans and Specifications*					
	Permanent or transfer to State Archives.				*0*	
Community and Public Relations (COM)						
Press and News Releases		**ADM-COM-04**	**CR**	**5**	**Destroy 5 years after create date**	**Yes**
91-232	*Press and News Release*					
	Retain 1 year. Evaluate for audit, legal, administrative, and historical value for transfer to State Archives. Destroy remaining records at discretion of director.				*1*	
Education (EDU)						
Assessments		**ADM-EDU-01**	**CP**	**5**	**Retain 5 years after completion then destroy**	**No**
01-120	*Wyoming Comprehensive Assessment System (WYCAS) 1999 Program Records*					
	Permanent or transfer to State Archives				*0*	
04-037	*Wyoming Career Technical Assessment (WCTA) Report*					
	Transfer 1 copy of the report to Wyoming State Archives. Retain remaining copies of the report for 5 years, then destroy.				*5*	
08-059	*PAWS (Proficiency Assessments for Wyoming Students) Records*					
	Retain 5 years, then destroy.				*5*	
08-060	*PAWS - ALT (Proficiency Assessments for Wyoming Students - Alternate) Records*					
	Retain 5 years, then destroy.				*5*	
08-061	*WELLA (Wyoming English Language Learners Assessment) Records*					
	Retain 5 years, then destroy.				*5*	
Course Development and Administration		**ADM-EDU-02**	**CP**	**5**	**Retain 5 years after completion then destroy**	**No**
5485	*Testing Center Files*					
	Retain annual contract until renewed, then destroy. Retain statistical summary for federal government and all correspondence 1 year, then destroy.				*1*	
99-162	*Test Booklet (Completed)*					
	Retain 1 year, then destroy.				*1*	

Administration and Business Support (ADM)

Education (EDU)

Enrollment		**ADM-EDU-04**	**CP**	**5**	**Retain 5 years after completion then destroy**		**No**
91-194	*Student Enrollment Report*						
	Retain 1 year, microfilm and destroy. (Supersedes AR-1 #8978)						
National Records		**ADM-EDU-16**	**CYE**	**25**	**Retain 25 years after calendar year end then destroy**		**No**
09-013	*ACT Historical Documents*						
	Retain 25 years, then destroy.					*25*	
Programs		**ADM-EDU-09**	**CP**	**5**	**Retain 5 years after completion then destroy**		**Yes**
08-004	*State Program Records*						
	Retain 3 years. Then evaluate for legal, administrative, and historical value for transfer to the State Archives. Destroy remaining records.					*3*	
08-080	*School Foundation Program*						
	Retain 5 years. Then evaluate for legal, administrative, and historical value for transfer to the State Archives. Destroy remaining records.					*5*	
Student Records		**ADM-EDU-12**	**CP**	**5**	**Retain 5 years after completion then destroy**		**No**
00-188	*School for the Deaf Student Records*						
	Retain the Individual Education Plan (IEP), front page of student evaluations, report cards for all years attended, special tests, medical records including shot records, hearing evaluations, and the last three years of student assessments permanently. Destroy all other records five years after the last year of documented attendance. (Supersedes AR# 91-240)					*0*	
01-162	*Court-Ordered Placement Records*						
	Retain 5 years, then destroy. (Supersedes AR# 97-232)					*5*	
02-279	*Gifted and Talented Records*						
	Retain 5 years, then evaluate for legal, administrative and historical value for transfer to Stat Archives. Destroy remaining records at discretion.					*5*	
Training Materials		**ADM-EDU-14**	**SUP**	**2**	**Retain 2 years after superseded then destroy**		**No**
99-158	*Open Response Scoring Guides*						
	Retain until superseded, then destroy. Transfer 1 copy to State Archives.						
99-161	*Test Booklet (Blank)*						
	Retain until superseded, then destroy. Transfer 1 copy to State Archives.						

Administration and Business Support (ADM)

Equipment and Vehicle Management (EVM)

Maintenance and Repairs	**ADM-EVM-02**	**CP**	**5**	**Retain 5 years after completion then destroy**		**No**
93-039	*School Bus Safety Inspection Reports*					
	Retain 10 years, then destroy.				*10*	

General Management (GMT)

Correspondence - Elected Officials	**ADM-GMT-04**	**PERM**		**Retain permanently**		**No**
91-189	*Superintendent of Public Instruction's Correspondence*					
	Permanent or transfer to State Archives.				*0*	
91-190	*Deputy Superintendent of Public Instruction's Correspondence*					
	Permanent or transfer to State Archives.				*0*	
Correspondence - General	**ADM-GMT-05**	**CR**	**3**	**Destroy 3 years after create date**		**Yes**
07-145	*District Superintendent Memos*					
	Retain 5 years. Then evaluate for legal, administrative, and historical value for transfer to the State Archives. Destroy remaining records. Any records transferred to State Archives will be evaluated. Records deemed not worthy of permanent retention will be destroyed by the State Archives.				*5*	
08-003	*General Correspondence*					
	Retain 1 year. Then evaluate for legal, administrative, and historical value for transfer to the State Archives. Destroy remaining records.				*1*	
Planning and Development	**ADM-GMT-17**	**CR**	**5**	**Destroy 5 years after create date**		**Yes**
91-191	*School District Reorganization Plans and Related Records*					
	Retain 1 year, then microfilm and destroy. (Supersedes AR-1 #5455)					
Reports - Annual Agency	**ADM-GMT-28**	**PERM**		**Retain permanently**		**Yes**
08-001	*Federal Program Final Report*					
	Permanent or transfer to State Archives.					
Reports - General	**ADM-GMT-22**	**CR**	**5**	**Destroy 5 years after create date**		**No**
02-039	*Assurances Reports (WDE Forms 604 and 605)*					
	Retain 5 years, then destroy.				*5*	
04-047	*Monthly Video Utilization Report*					
	Retain 6 years, then destroy					

Administration and Business Support (ADM)

General Management (GMT)

Transitory Records		**ADM-GMT-26**	**OBS/SUP**	**Destroy when obsolete or superseded.**	**No**
04-045	*Video Conference Request Form*				
	Retain (6) months from document date, then destroy.				
04-046	*Video Credit Course Application*				
	Retain until event has taken place, then transfer to the Department of Administration and Information, Division of Information Technology, Telecommunication Section, Video Conferencing Program, WENVIDEO Program				
04-049	*Video Conference Authorization Form*				
	Retain until event has taken place, then destroy.				
04-162	*Video Conference Request Form*				
	Retain until event has taken place, then transfer to the Department of Administration and Information, Division of Information Technology, Telecommunications Section, WENVIDEO Program (Supersedes AR#04-045)				
08-079	*Certified Welding and Trade School Records*				
	Straight Destruction.				*0*
5335	*Isolation Report*				
	Retain 2 years, then destroy.				*2*
91-192	*Daily Mail Log*				
	Retain 1 year, then destroy.				*1*
91-230	*Leave Slips, Annual & Sick*				
	Retain 1 year, then destroy.				*1*
91-231	*Information Files - Communication Services*				
	Retain 1 year. Evaluate for audit, legal, administrative, and historical value for transfer to State Archives. Destroy remaining records at discretion of director. (Supersedes AR-1 #5296)				*1*
91-239	*School for the Deaf Administrative Files*				
	Retain 4 years, then review for audit, legal, historical, and administrative value and retain permanently or transfer to State Archives. Destroy at discretion remaining correspondence. (Supersedes AR-1 #14601)				*3*
99-159	*Standard Setting Working Documents*				
	Retain 6 months, then destroy.				

Administration and Business Support (ADM)

General Management (GMT)

Transitory Records		**ADM-GMT-26**	**OBS/SUP**		**Destroy when obsolete or superseded.**	**No**
99-160	*Student Response Booklet (copy)*					
	Retain 1 year, then destroy.				*1*	
99-180	*Item Review Documents (Working Papers)*					
	Destroy after the review committees have met.					

Employee Services (EMP)

Employer and Labor Services (ELS)

Training and Rehabilitation		**EMP-ELS-04**	**CP**	**5**	**Retain 5 years after completion then destroy**	**No**
91-238	*Visually Handicapped Services Client File*					
	Retain 1 year, then destroy. (Supersedes AR-1 #5358)				*1*	

Personnel Management (PER)

Awards		**EMP-PER-01**	**CYE**	**3**	**Retain 3 year after calendar year end then destroy**	**No**
08-117	*Teacher of the Year Program*					
	Retain 3 years. Then evaluate for legal, administrative, and historical value for transfer to the State Archives. Destroy remaining records. Any records transferred to State Archives will be evaluated. Records deemed not worthy of permanent retention will be destroyed by the State Archives.				*3*	

Staffing and Recruiting (SAR)

Staff Planning		**EMP-SAR-05**	**SUP**	**3**	**Retain 3 years after superseded then destroy**	**No**
02-280	*Professional Staffing Lists (PSL)*					
	Retain 5 years, then destroy.				*5*	
08-067	*Staff Work Requests*					
	Retain 3 years, then evaluate for legal, administrative, and historical value for transfer to State Archives. Destroy remaining records.				*3*	

Financial and Accounting (FIN)

Accounting Management (ACC)

Reports - Accounting		**FIN-ACC-10**	**FYE**	**5**	**Retain 5 years after the fiscal year end then destroy**	**No**
02-201	*Career Technical Student Organization (CTSO) Fiscal Report*					
	Retain 4 years, then destroy.				*4*	

Financial and Accounting (FIN)

Accounting Management (ACC)

Reports - Accounting		**FIN-ACC-10**	**FYE**	**5**	**Retain 5 years after the fiscal year end then destroy**	**No**
02-202	*Career Technical Student Organization (CTSO) Program Records*					
	Retain 5 years, then evaluate for legal, administrative, and historical value for transfer to State Archives. Destroy remaining records at discretion of agency.				*5*	
04-050	*Video Conferencing Billing File*					
	Retain 6 years from document date, then destroy					

Grant and Scholarship Management (GRM)

Grant Files		**FIN-GRM-01**	**CP**	**10**	**Retain 10 years after completion then destroy**	**Yes**
00-126	*State Grant Program Files*					
	Retain 3 years from the date the final expenditure report is submitted to the awarding agency, then destroy. If the grant is open ended, retain 3 years from last expenditure report for that period, then destroy.				*3*	
04-035	*State Grant Records*					
	Retain 5 years from date of the final expenditure report, then destroy provided the records have been audited. If records have not been audited, retain until audited or 5 years from date of final expenditure report, whichever is later, then destroy.				*5*	
04-036	*Federal Grant Records*					
	Retain 5 years from date of the final expenditure report, then destroy provided the records have been audited. If records have not been audited, retain until audited or 5 years from date of final expenditure report, whichever is later, then destroy.				*5*	
06-021	*Montgomery Trust Fund Grants*					
	Retain 11 years from date of approval or denial, then destroy				*11*	
09-014	*Hathaway Scholarship Program*					
	Retain 10 years, then destroy.				*10*	
Scholarships		**FIN-GRM-03**	**CP**	**3**	**Retain 3 years after completion then destroy**	**Yes**
91-202	*Wyoming Legislative Scholarship File*					
	Retain until loan repaid or 2 years after the state auditor has directed that the debt be discharged and extinguished, then destroy. (Supersedes AR-1 #5478)				*2*	

Governance and Compliance (GAC)

Accreditation and Certification (AAC)

Schools		**GAC-AAC-04**	**EXP**	**25**	**Retain 25 years after expiration then destroy**	**No**
02-038	*School Accreditation Reports*					
	Retain 25 years, then destroy. (Supersedes AR-1 # 94-486)				*25*	

Audit, Oversight and Compliance (AOC)

Federal Programs and Reporting		**GAC-AOC-03**	**CP**	**5**	**Retain 5 years after completion then destroy**	**Yes**
08-002	*Federal Programs Records*					
	Retain 5 years or until completion of any audit in progress, then destroy.				*5*	
5307	*Federally Impacted Areas (Form #PL874)*					
	Retain 4 years, then destroy.				*4*	
94-672	*Child Nutrition Programs/Financial Summary Reports*					
	Retain 20 years, then destroy.				*20*	
General		**GAC-AOC-05**	**CP**	**5**	**Retain 5 years after completion then destroy**	**Yes**
00-187	*Desk Audit Records (District and School)*					
	Retain 10 years, and then destroy. (Supersedes AR-1 #94-487)				*10*	

Governance (GOV)

Minutes and Agendas		**GAC-GOV-03**	**PERM**		**Retain permanently**	**Yes**
91-187	*State Board of Education Minutes*					
	Permanent or transfer to State Archives. (Supersedes AR-1 #5290)				*0*	
91-188	*State Committee on Reorganization Minutes*					
	Permanent or transfer to State Archives. (Supersedes AR-1 #5291)				*0*	

Policy and Standards Management (PSM)

Standards		**GAC-PSM-03**	**SUP**		**Destroy when superseded**	**Yes**
03-253	*State Standards*					
	Retain 25 years, then transfer to the Sate Archives for evaluation of legal, administrative, and historical value. Records deemed not worthy of permanent retention will be destroyed by State Archives.				*25*	

Appendix C (References)

Federal

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99); http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
Higher Education Opportunity ACT; http://www.gpo.gov/fdsys/pkg/PLAW-110publ315/pdf/PLAW-110publ315.pdf
PL 107-110, No Child Left Behind Act of 2001; http://www2.ed.gov/policy/elsec/leg/esea02/index.html
PL 107-279, Education Sciences Reform; http://www.gpo.gov/fdsys/pkg/PLAW-107publ279/pdf/PLAW-107publ279.pdf
PL 110-134, Head Start Act; http://eclkc.ohs.acf.hhs.gov/hslc/standards/law/HS_ACT_PL_110-134.pdf
Individuals with Disabilities Education act (IDEA); http://www.gpo.gov/fdsys/pkg/BILLS-108hr1350enr/pdf/BILLS-108hr1350enr.pdf
HIPAA, 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf
Uninterrupted Scholars Act https://www.govtrack.us/congress/bills/112/s3472/text

State

W.S. § 9-2-405 through 9-2-413; http://legisweb.state.wy.us/statutes/statutes.aspx?file=titles/Title9/T9CH2AR4.htm
Wyoming Department of Enterprise Technical Services, Reference, http://ets.wyo.gov/resources/policies-and-standards
Enrolled Act No. 29, Senate; Sixty-First Legislature of the State of Wyoming 2012 Budget Session; http://legisweb.state.wy.us/2012/Bills/SF0001.pdf
Enrolled Act No. 66, Senate; Sixty-Second Legislature of the State of Wyoming, 2014 Budget Session; http://legisweb.state.wy.us/2014/Enroll/SF0079.pdf

General

Privacy Technical Assistance Center, U.S. Department of Education; http://ptac.ed.gov/
National Institute of Standards and Technology; http://csrc.nist.gov/publications/PubsSPs.html
Data Quality Campaign; http://dataqualitycampaign.org/

Appendix D (Glossary)

Advanced Encryption Standard definition. (**AES**) The NIST's replacement for the Data Encryption Standard (DES). The Rijndael /rayn-dahl/ symmetric block cipher, designed by Joan Daemen and Vincent Rijmen, was chosen by a NIST contest to be AES. AES is Federal Information Processing Standard FIPS-197.

Access Controls limit entry to information system resources to authorized users, programs, processes, or other systems. Components of an access control system include, for example, physical access (e.g., locks on doors to a server room), authentication systems that verify the identity of a user or client machine attempting to log into a system, and file encryption that makes data unreadable to anyone who does not possess the cipher key or encryption algorithm.

Data Breach is the intentional or unintentional release of secure information to an untrusted environment.

Data Loss Prevention solutions encompass a spectrum of software and hardware solutions, employed to protect sensitive data at rest and in motion from being stored, moved, or accessed in an unauthorized manner through the application of identification and filtering mechanisms.

Data Owner is a term that can be used in many ways, depending on the context. For the purposes of this document, it is used to refer to an individual within an organization who is in direct control of the data and is responsible for authorizing access to or dissemination, integrity, and accuracy of the data.

Data Security is the means of ensuring that data are kept safe from corruption and that access to it is suitably controlled. The primary goal of any information and technology security system is to protect information and system equipment without unnecessarily limiting access to authorized users and functions.

Disclosure means to permit access to or the release, transfer, or other communication of Personally Identifiable Information (PII) by any means. Disclosure can be authorized, such as when a parent or an eligible student gives written consent to share education records with an authorized party (e.g., a researcher). Disclosure can also be unauthorized or accidental. An unauthorized disclosure can happen due to a data breach or a loss. An accidental disclosure can occur when data released in public aggregate reports are unintentionally presented in a manner that allows individual students to be identified.

Disclosure avoidance refers to the efforts made to reduce the risk of disclosure, such as applying statistical methods to protect PII in aggregate data tables. These safeguards, often referred to as disclosure avoidance methods, can take many forms (e.g., data suppression, rounding, recoding, etc.).

Education Records include those records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations, 34 CFR §99.3.

Encryption is the process of transforming information using a cryptographic algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as an encryption/decryption key. “One way” encryption is a data destruction technique which makes use of encryption techniques to render data unusable by first encrypting the data and then destroying the key used to encrypt the data initially.

Enterprise the state infrastructure managed by ETS (i.e. Servers, switches, routers, firewalls, etc)

Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Health Insurance Portability and Accountability Act (HIPAA) 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 ad help the healthcare industry control administrative costs

Incident manager is a key leadership role within an incident response process, typically filled by a senior level manager. The incident manager activates the incident response team, appropriates the necessary resources to investigate and

manage the incident, and acts as a bridge between executive leadership (e.g., institution president, superintendent, provost, chancellor, principal, etc.), legal counsel, and information technology and law enforcement, when appropriate.

Incident response plan is a document, which establishes specific procedures for detecting, responding, mitigating, and recovering from incidents affecting organization's information systems.

Incident response team is a group of key people within an organization who are responsible for responding to computer security-related incidents.

Internet Message Access Protocol (IMAP), a protocol for retrieving email messages.

Intrusion Detection/Prevention System is a software and hardware system, which automates monitoring of computer systems and networks for indications of security violations.

Metadata a set of data that describes and gives information about other data.

National Institute of Standards and Technology (NIST), is a non-regulatory Federal agency under the Department of Commerce headquartered in Gaithersburg, Maryland.

Personally Identifiable Information (PII) refers to information, such student's name or identification number that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See

Post Office Protocol 3, a protocol for receiving e-mail by downloading it to your computer from a mailbox on the server of an Internet service provide

Principle of Least Privilege (PoLP), where minimal system access privileges are granted in order to perform assigned duties.

Protection of Pupil Rights Amendment (PPRA), a Federal law that affords certain rights to parents of minor students with regard to surveys that ask questions of a personal nature.

Protected Health Information (PHI), is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

Risk Assessment is the process of identifying: (1) all assets an organization possesses, (2) all potential threats to those assets, (3) all points of vulnerability to those threats, (4) the probability of potential threats being realized, and (5) the cost estimates of potential losses. Risk assessment enables an organization to at least consider the range of potential threats and vulnerabilities it faces, and is the first step in effectively securing an information and technology system.

Role Based Access, restricting system access based on an authorized users job duties within the organization.

Sanitization of the media is a process which is applied to data or storage media to make data retrieval unlikely for a given level of effort. Clear, purge, and destroy are actions that can be taken to sanitize data and media.

Secure Sockets Layer (SSL), is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser; or a mail server and a mail client (e.g., Outlook).

Sensitive data are data that carry the risk for adverse effects from an unauthorized or inadvertent disclosure. This includes any negative or unwanted effects experienced by an individual whose personally identifiable information (PII) from education records was the subject of a loss of confidentiality that may be socially, physically, or financially damaging, as well as any adverse effects experienced by the organization that maintains the PII. See Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), 2010, NIST Special Publication 800-122, for more information.

Simple Mail Transfer Protocol (SMTP), a protocol for sending email messages between servers.

Transport Layer Security (**TLS**) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communication security over the Internet.

Triple DES (**3DES**) is the common name for the Triple Data **Encryption** Algorithm (TDEA or Triple DEA) symmetric-key block **cipher**, which applies the Data **Encryption** Standard (DES) **cipher** algorithm three times to each data block.

Virtual Private Network (**VPN)** is a private network that uses a public network (usually the Internet) to connect remote sites or users together. The **VPN** uses "virtual" connections routed through the Internet from the business's private network to the remote site or employee.

WISER ID, The Wyoming Integrated Statewide Education (WISE) Student Record ID (WISER ID) is a unique, non-personally identifiable, Statewide student identifier that connects a student's data across districts and Institutions.