DATA GOVERNANCE MANUAL

AMERICAN SAMOA
DEPARTMENT OF EDUCATION

CONTENTS

B. POLICIES AND PROCEDURES

The establishment of data policies and processes is a critical component of the ASDOE Data Governance program for it will consistently ensure the protection and confidentiality of student educational records throughout the information lifecycle in support of the Data Governance program objectives. To protect confidential data, adherence to FERPA guidelines will be strictly monitored.

General Principles for Data Security and Privacy

- *Minimalism*-Records and notes created during the data collection process – whether electronic or paper –should contain only the minimum necessary personally identifiable information.

- *Exclusivity*-Access to data should be strictly limited to personnel with specific responsibility for each data
  element or a "legitimate educational interest". Electronic databases should be password and login-protected and personally identifiable information should be accessible only when necessary for a specific reporting purpose.

- *Awareness*-Staff training should include building an understanding of Federal laws and their application to ongoing data collections.

- *Documentation*-Develop a written list of policies and practices related to data security and privacy and ensure that it is disseminated to all personnel involved in data collection, entry, and reporting.

- *Comprehensiveness*-Statewide system-generated identifiers should be created for all individual student
  records. Using a statewide system will allow tracking of students as they move between schools and districts. Social security numbers should not be used as student identifiers.

AMERICAN SAMOA DEPARTMENT OF EDUCATION

Area: Data Privacy and Security	**Policy #001:** Confidentiality of Individual Information	**Final Draft:** 11/14/21 **By:** Data Governance Committee
Version 1.1	**Approved By**: ASDOE Leadership Team	**Effective Date:** 7/1/22

Purpose: To provide guidance in understanding the importance of protecting the Personal Identifiable Information (PII) and Personal Health Information (PHI) of students and personnel pursuant to the Family Educational Rights and Privacy Act (FERPA).

Scope: Applies to all ASDOE employees, including part-time employees, volunteers, contractors, and temporary workers.

Policy: Safeguarding data from inappropriate use is critical and must be maintained at the highest level of security. ASDOE will comply with the requirements of FERPA and protect against unauthorized disclosure of any and all PII and PHI contained in student and personnel records. Parameters are established to ensure the confidentiality of such data.

- **Electronic Protection of Student Identifiers and Information**
  - A unique number is assigned to each student upon registration and information is maintained in the ASDOE PowerSchool Student Information System (SIS)
- **Identifiable Individual Data**
  - Not allowed outside of the ASDOE server environment. (i.e.no laptops, downloads, cloud storage, etc.) except in rare, approved exceptions.
  - Exceptions will be handled on a case-by-case basis with documented approval by the ASDOE Executive Policy Committee.
- **Data may be exported to requestors in de-identified or aggregate formats**
  - De-identification is the process used to prevent a person's identity from being connected to the information.
  - The export of de-identified data will be based on an agreement between ASDOE and all the involved data owners, as well as approval by the ASDOE Executive Policy Committee.
- **All ASDOE employees, part-time employees, volunteers, temporary workers, and contractors**
  - Access to the ASDOE Student Information System(SIS) requires a signed Confidentiality Agreement Form and an approved Data Request Form for research purposes.
- **ASDOE Account**:
  - All ASDOE employees are responsible for anything done under their accounts.

Responsibilities: All individuals identified in the scope of this policy are responsible for abiding by the terms and guidelines set forth by this policy

ASDOE Assistant Directors and Program Directors are responsible for ensuring all employees under their supervision have signed and dated the Confidentiality Agreement form, which is to be renewed annually.

Compliance: All individuals stated under the scope of this policy that fail to comply with this or any other security policy, will result in disciplinary actions set forth by the Director of Education. Legal actions may also, be taken for violation of applicable regulations outlined under FERPA.

Form(s): ASDOE Confidentiality Agreement

References and Related Policies:

- ASDOE Data Governance Policy #2 Data Access and Management
- ASDOE Data Governance Policy #7 Information Classification
- ASDOE Data Governance Policy #4 Data Security
- ASDOE Data Governance Policy #8 Security Awareness and Training
- ASDOE Data Governance Policy #9 Security Incident Procedures
- ASDOE Data Governance Policy #10 Data Breach
- ASDOE Data Governance Policy #11 Data Breach Management

Area: Data Access	**Policy #002:** Data Access and Management	**Final Draft:** 11/17/21 **By:** Data Governance Committee
Version 1.1	**Approved By:** ASDOE Leadership Team	**Effective Date:** 7/1/22

AMERICAN SAMOA DEPARTMENT OF EDUCATION

Purpose: To assure security & confidentiality parameters are adhered to and only authorized individuals are allowed access to student data.

Scope: Applies to all ASDOE workforce members including part-time employees, trainees, volunteers, contractors, and temporary workers.

Policy: Access to sensitive information is contingent on a "need to know" basis and job descriptions are reviewed to determine access privileges.

- **Use of Student Data at the Local School Level**: Procedures will be followed to ensure the confidentiality of student records maintained in ASDOE's data system and student files.
- **Disclosure of Statistical Data:** To prevent student identification, when the student population is less than 10 per grade or 5 per subgroup, Data will be suppressed to protect student privacy.

ASDOE Staff Access to Student Records: Specific student data fields are assigned an access level between 1 and 3:

- ***Level 1 Access*** allows read/write access to all records and fields in the ASDOE PowerSchool Student Information System. Permission is only allowed to a minimal number of ASDOE-authorized technical staff members who operate or manage the data warehouse or are responsible for maintaining the accuracy, security, and audit corrections in the performance of their duties. Authorization is required from the Director of Education.

- ***Level 2 Access*** limits access to student data contained within the ASDOE PowerSchool Student Information System. The only access to individual-level data if necessary, to perform a specific function of their job and is permitted under FERPA. Authorization is required from the Deputy Director who supervises the requestor's office or division.

- ***Level 3 Access*** allows read-only access for public viewing of standard reports and data tables in aggregated formats.

Intended Use of Data by ASDOE Staff: Authorization will only be granted to certain personnel who have a legitimate need to access specific student information in order to fulfill their job duties as agents of the Department and in accordance with current Department policy and FERPA regulations.

Responsibilities: All Assistant Directors will review and assign security level access for staff and ascertain level access is aligned with the individual's job role or functions.

Compliance: All individuals stated under the scope of this policy that fail to comply with this or any other security policy, will result in disciplinary actions set forth by the Director of Education. Legal actions may also be taken for violations of applicable regulations outlined under the Family Educational Rights and Privacy Act (FERPA).

Form(s): System Access Form

References and Related Services

- ASDOE Data Governance Policy #2 Data Access and Management
- ASDOE Data Governance Policy #7 Information Classification
- ASDOE Data Governance Policy #4 Data Security
- ASDOE Data Governance Policy #8 Security Awareness and Training
- ASDOE Data Governance Policy #10 Data Breach
- ASDOE Data Governance Policy #11 Data Breach Management
- ASDOE Data Governance Policy #1 Confidentiality of Individual Information

Area: Data Request	**Policy #003:** Data Request	**Final Draft:** 11/17/21 **By:** Data Governance Committee
Version 1.1	**Approved By:** ASDOE Leadership Team	**Effective Date:** 7/1/22

AMERICAN SAMOA DEPARTMENT OF EDUCATION

Purpose: The ASDOE PowerSchool Student Information System (SIS) contains an array of confidential student and staff information. Parameters need to be in place to safeguard any or all data requests.

Scope: Applies to all ASDOE employees, part-time employees, temporary workers, volunteers, contractors, and external agencies.

Policy: All ASDOE confidential data must be protected at all costs, but non-confidential data is made accessible on its data systems for public use. Requests for specific data not accessible in the public domain may be submitted. Any individual(s) who request student, staff, or program data must abide by the guidelines set forth within this policy.

Responsibilities: TIS Assistant Director and Integrated Data Services(IDS) Program Director ensure all submitted requests are thoroughly vetted before approval is granted and forwarded to the Director of Education or Deputy Directors for final approval.

Compliance: All individuals stated under the scope of this policy that fail to comply with this or any other security policy will result in disciplinary actions set forth by the Director of Education. Legal actions may also be taken for violations of applicable regulations outlined under the Family Educational Rights and Privacy Act (FERPA).

Form(s): Data Request Form, Confidentiality Form

References:

- ASDOE Data Governance Policy #2 Data Access and Management
- ASDOE Data Governance Policy #7 Information Classification
- ASDOE Data Governance Policy #4 Data Security
- ASDOE Data Governance Policy #8 Security Awareness and Training
- ASDOE Data Governance Policy #9 Security Incident Procedures
- ASDOE Data Governance Policy #10 Data Breach
- ASDOE Data Governance Policy #11 Data Breach Management

Guidelines for requesting access to confidential student or staff data for research purposes.

Procedures

1. Download the ASDOE Data Request Form and complete all pages before submission. An incomplete form will not be accepted and delay the request.

2. Submit the completed form(s) electronically(martym@doe.as) or hard copy to the IDS office and a ticket number assigned.

3. Responsible IDS staff will review and ensure all areas have been addressed and determine-if the data requested is public or confidential. ASDOE reserves the right to deny any request.

4. If requested data is available on the public reporting portal, the requestor will be directed to the ASDOE or SLDS website, and the ticket closed.

5. If requested data is confidential, the ticket number will be assigned to a designated IDS staff member to ensure the request follows the ASDOE and FERPA policies before data is compiled.

6. A one-week process turnaround for review and approval by the IDS Program Director, who submits to the Director of Education for final approval and release.

7. The requestor will be contacted and the data requested will be provided electronically.

Responsibilities: TIS Assistant Director and IDS Program Director are to ensure all procedures are followed and Director's approval is obtained before the release of any data to the requestor.

AMERICAN SAMOA DEPARTMENT OF EDUCATION

Area: Data Privacy and Security	**Policy #004:** Data Security	**Final Draft:** 11/17/21 **By:** Data Governance Committee
Version 1.1	**Approved By:** ASDOE Leadership Team	**Effective Date:** 7/1/22

Purpose: To secure the ASDOE Data Systems designed to store and manage student and staff data.

Scope: Applies to all ASDOE employees, including part-time employees, temporary workers, volunteers, and contractors.

Policy: All data contained within the ASDOE Student Information Systems (SIS) will be securely maintained through safeguard parameters to ensure all confidential information such as student and staff Personal Identifiable Information (PII) and Personal Health Information (PHI), plus the intended use of such data, is not compromised.

Security parameters include the technical measures to ensure records are not lost, stolen, vandalized, or illegally accessed; a high level of protection of electronic data through secure firewalls, socket layers, passwords, and restricted server room access.

(1) Secure user authentication protocols include:

(a) Direct access to ASDOE databases, servers, and stand-alone computers through active directory authentication

(b) Requirement of a Single Sign-On (SSO) to access ASDOE web-based systems

(c) Control of passwords to ensure they are kept in a location and/or format that does not compromise the security of the data they protect

(d) Managing user access to applications; and

(e) Blocking access to users after multiple unsuccessful attempts;

(2) Secure access control measures that:

(a) Restrict access to records and files containing personal information to those who need such information to perform their job duties; and

(b) Assign different security roles to each person for system access to maintain the integrity of the security of the access controls.

(3) Apply different end-user levels of ‘encryption’ for transmission of specific files or records containing confidential information

(4) Monitor systems for unauthorized use of or access to personal information;

(5) Install up-to-date firewall protection and operating system security patches, designed to maintain the integrity of personal information;

(6) Train employees as needed on the proper use of the computer security system and the importance of personal information security.

Responsibilities: TIS Assistant Director and IDS Program Director to ensure security measures and safeguards specified in this policy are functional, operating, and shared with all individuals noted under the scope of this policy

Compliance: All individuals stated under the scope of this policy that fail to comply with this or any other security policy, will result in disciplinary actions set forth by the Director of Education. Legal actions also may be taken for violations of applicable regulations outlined under FERPA.

Reference and Related Policies:

- ASDOE Data Governance Policy #1 Confidentiality of Individual Information
- ASDOE Data Governance Policy #2 Data Access and Management
- ASDOE Data Governance Policy #7 Information Classification
- ASDOE Data Governance Policy #8 Security Awareness and Training
- ASDOE Data Governance Policy #9 Security Incident Procedures
- ASDOE Data Governance Policy #10 Data Breach
- ASDOE Data Governance Policy #11 Data Breach Management

AMERICAN SAMOA DEPARTMENT OF EDUCATION

Area: Data Privacy and Security	**Policy #005:** E-mail Security	**Final Draft:** 11/17/21 **By**: Data Governance Committee
Version 1.1	**Approved By:** ASDOE Leadership Team	**Effective Date:** 7/1/22

Purpose: To protect and minimize risks associated with transmitting or receiving sensitive material such as Personal Identification Information (PII) or Personal Health Information (PHI).

Scope: Applies to all ASDOE employees, including part-time employees, volunteers, contractors, and temporary workers.

Policy: ASDOE recognizes that using email without an encryption mechanism is an insecure means of transmitting and receiving messages. Until such an encryption mechanism is implemented, ASDOE will utilize the following guidelines when sensitive information is electronically sent:

- Emails containing sensitive information are permitted only when the sender and receiver are members of ASDOE's workforce and the e-mail stays within the confines of ASDOE's local network. That is, both email addresses must end with " doe.as "

ASDOE-provided e-mail system is intended for official and authorized purposes only. All e-mail messages are considered ASDOE property. When an e-mail is not in use, users are to exit the software to prevent unauthorized access.

Electronic information about students or staff in an organized format should be protected to the extent that a hard copy record is protected and disclosed only when required for authorized purposes.

E-mail system administrators and those with special system-level access privileges are prohibited from reading electronic messages of others unless authorized by appropriate ASDOE officials. Only the ASDOE Director and Deputies are authorized to access e-mail messages when there are a legitimate purpose, e.g., technical or administrative problems.

Responsibilities: All individuals identified in the scope of this policy are responsible for abiding by the terms and guidelines set forth by this policy

EdTech and TIS Assistant Directors and IDS Program Director are responsible for:

- Evaluating, on a periodic basis, emerging encryption solutions for email and implementing them when one is found that meets the criteria described in the policy section of this document
- Maintaining procedures and forms in support of this policy
- Monitoring and enforcing workforce compliance with this policy

Compliance: All individuals stated under the scope of this policy that fail to comply with this or any other security policy, will result in disciplinary actions set forth by the Director of Education. Legal actions may also be taken for violations of applicable regulations outlined under the Family Educational Rights and Privacy Act (FERPA).

References and Related Resources:

- ASDOE Data Governance Policy #4 Data Security
- ASDOE Data Governance Policy #1 Confidentiality of Individual Information
- ASDOE Data Governance Policy #7 Information Classification

- ASDOE Data Governance Policy #2 Data Access and Management

Area: Data Privacy and Security	**Policy #006:** System User Access	**Final Draft:** 11/15/21 **By:** Data Governance Committee
Version 1.1	**Approved By:** ASDOE Leadership Team	**Effective Date:** 7/1/22

AMERICAN SAMOA DEPARTMENT OF EDUCATION

Purpose: To safeguard access to the ASDOE Student Information System(SIS), ASDOE Google Workspace, and assist in identifying and tracking user identity.

Scope: Applies to all ASDOE employees

Policy: All individuals approved for access to sensitive information within the ASDOE SIS will be provided a User Single Sign-On (SSO). At no time will any workforce member allow anyone else to use his or her password.

- ASDOE will develop a standard convention for assigning user access.
- ASDOE will maintain a secure record of user access.
- ASDOE will track individual activities and record events as required by policies established by the IDS office
- All ASDOE staff are required to read and sign the ASDOE Confidentiality Agreement Form before receipt of user access.
- All ASDOE employees' access will be reviewed on a quarterly basis.

Responsibilities: The IDS Program Director, TIS, and EdTech Assistant Director will be responsible for ensuring the implementation of the requirements for this policy.

Compliance: All individuals stated under the scope of this policy that fail to comply with this or any other security policy, will result in disciplinary actions set forth by the Director of Education. Legal actions may also be taken for violations of applicable regulations outlined under the Family Educational Rights and Privacy Act (FERPA).

Form(s): Confidentiality Agreement, PowerSchool System Access Request

References & Related Resources:

- ASDOE Data Governance Policy #1 Confidentiality of Individual Information
- ASDOE Data Governance Policy #2 Data Access and Management
- ASDOE Data Governance Policy #7 Information Classification
- ASDOE Data Governance Policy #4 Data Security
- ASDOE Data Governance Policy #8 Security Awareness and Training
- ASDOE Data Governance Policy #9 Security Incident Procedures
- ASDOE Data Governance Policy #10 Data Breach
- ASDOE Data Governance Policy #11 Data Breach Management

AMERICAN SAMOA DEPARTMENT OF EDUCATION

Area: Data Privacy and Security	**Policy #007:** Information-Classification	**Final Draft:** 11/21/21 **By:** Data Governance Committee
Version 1.1	**Approved By:** ASDOE Leadership Team	**Effective Date:** 7/1/22

Purpose: To provide clarity regarding all ASDOE information that may or may not be released to the public or disclosed to any individual(s) outside of the department.

Scope: Applies to all ASDOE workforce members including part-time employees, temporary workers, volunteers, and contractors.

Policy: All ASDOE information will be organized into two main classes, "Public" and "Confidential."

Public information can be shared freely with anyone in the department without the possibility of negative consequences.

Public information includes, but is not necessarily limited to:

- Calendar of school events, activities, courses, grading scale, etc.
- Parent notifications, PTA announcements, etc.
- ASDOE initiatives, announcements, staff responsibilities, budget, etc.

Internal Data Information is information regarding the day-to-day operations primarily for employee use.

Confidential information includes all other information (when shared or disclosed, could possibly have a negative consequence). There are varying levels of sensitive information, and the lengths employees should go to protect the information depends on the sensitivity.

Confidential information includes, but is not necessarily limited to:

- Business information(hiring process, employee records, etc.)
- Financial information (salaries, leave, pay stubs, etc.)
- Operational information (ECO grievances, compensation, incident reports, etc.)
- Personnel information (date of birth, social security number, phone number, medical, etc.)
- Student personal information (date of birth, social security number, medical, etc.)

Anyone who is unsure of the relative sensitivity of a piece of information is required to contact their immediate supervisor for clarification.

Responsibilities: Assistant Directors and Program Directors will ensure all ASDOE employees under their supervision, including part-time employees, trainees, volunteers, contractors, and temporary workers follow security-related policies and procedures.

Compliance: All individuals stated under the scope of this policy that fail to comply with this or any other security policy will result in disciplinary actions set forth by the Director of Education. Legal actions may also be taken for violations of applicable regulations such as federal rules including FERPA.

References and Related Policies

- ASDOE Data Governance Policy #1 Confidentiality of Individual Information

- ASDOE Data Governance Policy #2 Data Access and Management
- ASDOE Data Governance Policy #4 Data Security
- ASDOE Data Governance Policy #8 Security Awareness and Training
- ASDOE Data Governance Policy #9 Security Incident Procedures
- ASDOE Data Governance Policy #10 Data Breach
- ASDOE Data Governance Policy #11 Data Breach Management
- ASDOE Data Governance Policy #14 Parent Notification

AMERICAN SAMOA DEPARTMENT OF EDUCATION

Area: Data Privacy and Security	**Policy #008:** Security Awareness Training	**Final Draft:** 11/17/21 **By:** Data Governance Committee
Version 1.1	**Approved By**: ASDOE Leadership Team	**Effective Date:** 7/1/22

Purpose: It is understood that "people", not necessarily technology, are often the largest threat to the security of sensitive information, and justifies the need for security awareness training to ensure such data is protected.

Scope: Applies to all ASDOE employees, including part-time employees, temporary workers, volunteers, and contractors.

Policy: All individuals under the scope of this policy are mandated to complete training on security policies and procedures for protecting student and staff data, and how to identify, report, and prevent potential security incidents.

Training mandate for ALL

- Must complete FERPA 101: For Local Education Agencies online training at:
    - https://studentprivacy.ed.gov/training/ferpa-101-local-education-agencies
    - Complete the 40minute Course and Test
    - Print, Sign, and Submit the Certificate of Completion to the Supervisor

The following must be implemented;

- Periodic security reminders to keep employees up to date with new threats, such as computer viruses or "scams"; security-related flyers or posters in offices, emails, and verbal updates at staff meetings. The frequency and form these reminders take will be determined by the *IDS Program Director along with TIS and EdTech Assistant Director*s.
- Bi-annual review of security awareness training

Responsibilities: *Deputy Directors, IDS Program Director along with EdTech and TIS Assistant Director need to;*

- Ensure all ASDOE workforce members understand and follow security-related policies and procedures
- Maintain a year-round security awareness program for the ASDOE
- Identify and coordinate activities to bring ASDOE into compliance with regulatory requirements

Compliance: All individuals stated under the scope of this policy that fail to comply with this or any other security policy, will result in disciplinary actions set forth by the Director of Education. Legal actions may also be taken for violations of applicable regulations outlined under FERPA.

References and Related Resources:

- ASDOE Data Governance Policy #2 Data Access and Management
- ASDOE Data Governance Policy #7 Information Classification
- ASDOE Data Governance Policy #4 Data Security
- ASDOE Data Governance Policy #9 Security Incident Procedures
- ASDOE Data Governance Policy #10 Data Breach
- ASDOE Data Governance Policy #11 Data Breach Management

- ASDOE Data Governance Policy #1 Confidentiality of Individual Information

AMERICAN SAMOA DEPARTMENT OF EDUCATION

Area: Data Privacy and Security	**Policy #009:** Security Incident Procedures	**Final Draft:** 11/17/21 **By:** Data Governance Committee
Version 1.1	**Approved By**: ASDOE Leadership Team	**Effective Date:** 7/1/22

Purpose: To ensure an efficient approach to identifying and reporting all real and potential violations of data privacy and security policies.

Scope: Applies to all ASDOE workforce members including part-time employees, temporary workers, volunteers, and contractors.

Policy: ASDOE will maintain procedures for responding to serious and non-serious security incidents in order to prevent the escalation of the incident and to prevent future incidents of a similar nature. A security incident is any breach of security policy or any activity that could potentially put sensitive student or staff information at risk of an unauthorized use, disclosure, or modification.

Responsibilities: All individuals identified in the scope of this policy are required to:

- Be aware of and identify potential security incidents
- Report any suspected security incident
- Assist in addressing the security incident if possible

IDS Program Director, TIS and EdTech Assistant Directors:

- Maintain all security incident-related policies and procedures
- Characterize all reported security incidents as "serious" or "non-serious" as per guidelines and document all incidents on Security Incident Documentation Log, along with the incident outcome(s).

Director and Deputy Directors:

- Mitigate, to the extent possible, any harmful effects of reported security incidents.

Compliance: All individuals stated under the scope of this policy that fail to comply with this or any other security policy, will result in disciplinary actions set forth by the Director of Education. Legal actions may also be taken for violations of applicable regulations outlined under the Family Educational Rights and Privacy Act (FERPA).

Procedure(s): ASDOE Security Incident Procedures

Form(s): Security Incident Documentation Log

References and Related Services:

- ASDOE Data Governance Policy #2 Data Access and Management
- ASDOE Data Governance Policy #7 Information Classification
- ASDOE Data Governance Policy #4 Data Security
- ASDOE Data Governance Policy #8 Security Awareness and Training
- ASDOE Data Governance Policy #10 Data Breach
- ASDOE Data Governance Policy #11 Data Breach Management
- ASDOE Data Governance Policy #1 Confidentiality of Individual Information

Guidelines for Notification of Security Incidents

Purpose:
Guidelines provide a required course of action upon discovery of a security breach of personal information within and from the American Samoa Department of Education (ASDOE). These guidelines address breaches of personally sensitive information covered by the Family Educational Rights and Privacy Act (FERPA).

Information Security Breaches include but are not limited to:

- Computers/laptops
- Electronic Storage Devices (e.g. USB/flash drives, CDs, DVDs, etc.)
- Email (e.g., sent unsecured to an unauthorized recipient, hacked email inbox, etc.)
- Electronic documents (e.g., access to an unsecured computer by an unauthorized individual, failure to destroy files as required, hacked computer, website, server, or database, etc.)
- Paper Documents (e.g., loss, unauthorized duplication or theft of hardcopy, failure to destroy hard copy as required, etc.)

Procedures:
Upon discovery of a known or potential security breach of personal information, the following steps shall be taken:

1. Personnel immediately report the incident to the Principal or Supervisor
2. The principal/supervisor is responsible for reporting all incidents to IDS and EdTech who will determine the type of incident if:

   a. Non-serious-generally has the following characteristics:
      - Determined there was no malicious intent (or attack was not directed specifically at an individual(s) or DOE and
      - Determined no sensitive information was used, disclosed, or damaged in an unauthorized manner OR

   b. Serious-generally has the following characteristics:
      - Determined that malicious intent and/or an attack was directed specifically at an individual(s) or ASDOE and
      - Determined that sensitive information, may have been used, disclosed, or damaged in an unauthorized manner or that this incident may be construed as a data breach
3. Incidents characterized as 'serious' will be reported immediately by IDS and EdTech to the DOE Director or Deputy Director(s).
4. IDS and EdTech will document the incident, and incident outcome(s)and continue to monitor the incident and minimize data breaches until resolved.
5. Any or all personnel involved in a 'serious' incident will be subject to suspension or termination depending upon the severity of the incident.

AMERICAN SAMOA DEPARTMENT OF EDUCATION

Area: Data Privacy and Security	**Policy #010:** Data Breach	**Final Draft:** 11/17/21 **By:** Data Governance Committee
Version 1.1	**Approved By:** ASDOE Leadership Team	**Effective Date:** 7/1/22

Purpose: To provide guidance in identifying potential data breaches of confidential information, such as Personal Identifiable Information (PII) or Personal Health Information (PHI).

Scope: Applies to all ASDOE workforce members including part-time employees, temporary workers, volunteers, and contractors.

Policy: *A breach is defined as* Any unlawful or unauthorized access, use, or disclosure of student or staff confidential personal, educational, or health records.

Common examples of data breach incidents include, but are not limited to, any of the following:

- Successful attempts to gain unauthorized access to the ASDOE PowerSchool Student Information System (SIS), student or educator PII, or PHI regardless of where such information is located
- Changes to the ASDOE PowerSchool SIS system hardware or software characteristics without the Director's approval
- Loss or theft of equipment that stores Confidential Information, PII, or PHI
- Human error involving the loss or mistaken transmission of Confidential Information, PII, or PHI
- Public display of student or staff PII or PHI through electronic or hard copy format

A breach does not include:

- Any unintentional, access, or use of protected information by an employee or individual acting under the authority of ASDOE;
- Access, or use of data made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual;
- Any inadvertent disclosure from an individual who is otherwise authorized to access student data and/or PII at the ASDOE;
- Any such information received as a result of inadvertent disclosure;
- Information rendered unusable, unreadable, or indecipherable i.e. encrypted data

Responsibilities: IDS Program Director, EdTech, and TIS Assistant Directors are to oversee and ensure all security-related policies and procedures are followed.

Compliance: All individuals stated under the scope of this policy that fail to comply with this or any other security policy, will result in disciplinary actions set forth by the Director of Education. Legal actions may also be taken for violations of applicable regulations outlined under the Family Educational Rights and Privacy Act (FERPA).

Procedure(s): Data Breach Management Procedures

References and Related Policies:

- ASDOE Data Governance Policy #2 Data Access and Management
- ASDOE Data Governance Policy #7 Information Classification
- ASDOE Data Governance Policy #4 Data Security
- ASDOE Data Governance Policy #8 Security Awareness and Training
- ASDOE Data Governance Policy #9 Security Incident Procedures
- ASDOE Data Governance Policy #11 Data Breach Management

AMERICAN SAMOA DEPARTMENT OF EDUCATION

Area: Data Privacy and Security	**Policy #011:** Data Breach Management	**Final Draft:** 11/17/21 **By:** Data Governance Committee
Version 1.1	**Approved By:** ASDOE Leadership Team	**Effective Date:** 7/1/22

Purpose: To safeguard all ASDOE confidential information through proper management of breach-related activities,

Scope: Applies to all ASDOE workforce members including part-time employees, temporary workers, volunteers, and contractors.

Policy: ASDOE will minimize any loss or destruction of data, mitigate the weakness that was exploited and restore all computing and other impacted services through lawful and fair handling of the breach and implement preventative measures. If and when the data breach is discovered, the following will be adhered to;

- Breach identification per Data Breach Policy #010
- Security Incident Procedures Policy #009 is required to be followed
- All meeting minutes, technical documentation, and handwritten notes of the breach are to be compiled within 72 hours of the breach
- Appropriate levels of management are involved in the response
- Evaluation of response to incidents is reviewed for improvement
- Containment and recovery process
- Assessment of risks

Responsibilities: EdTech Assistant Director and IDS Program Director are responsible for the proper management of all security incidents.

- All information users are responsible for reporting actual suspected potential information incidents and for assisting with investigation as necessary particularly urgent action must be taken to prevent further damage.

All workforce members are responsible for:

- Understanding and following all security-related policies and procedures

The ASDOE Deputies and Assistant Directors are responsible for:

- Ensuring all workforce members understand and follow security-related policies and procedures

Compliance: All individuals stated under the scope of this policy that fail to comply with this or any other security policy, will result in disciplinary actions set forth by the Director of Education. Legal actions may also be taken for violations of applicable regulations outlined under the Family Educational Rights and Privacy Act (FERPA).

References and Related Resources:

- ASDOE Data Governance Policy #1 Confidentiality of Individual Information
- ASDOE Data Governance Policy #2 Data Access and Management
- ASDOE Data Governance Policy #7 Information Classification
- ASDOE Data Governance Policy #4 Data Security
- ASDOE Data Governance Policy #8 Security Awareness and Training
- ASDOE Data Governance Policy #9 Security Incident Procedures
- ASDOE Data Governance Policy #10 Data Breach

AMERICAN SAMOA DEPARTMENT OF EDUCATION

Area: Data Privacy and Security	**Policy #012:** Workstation Security	**Final Draft:** 11/17/21 **By:** Data Governance Committee
Version 1.1	**Approved By:** ASDOE Leadership Team	**Effective Date:** 7/1/22

Purpose: To safeguard all workstations such as desktops, laptops, phones, and mobile devices owned or operated by ASDOE.

Scope: Applies to all ASDOE workforce members including part-time employees, temporary workers, volunteers, and contractors.

Policy: Physical safeguards will be implemented for all workstations that access sensitive information and to restrict access to authorized users only.

- All members of the workforce will be trained on the appropriate and authorized use of workstations as part of the security awareness training.
- Workstations will be positioned such that the monitor screens and keyboards are not within view of unauthorized individuals.
- Users will log off before leaving the workstation. Users will store any written passwords in secure locations only – under no circumstance must any password information be accessible on the workstation or its vicinity.

All workstations must be operated in a manner that ensures:

- Confidentiality of sensitive information.
- Display of an appropriate warning banner before gaining operating system access.
- Employment of a password-protected screen saver and/or workstation locking mechanism when the workstation is unattended.
- Proper logoff and shut down of workstations at the end of the business day.
- Routine backup of all critical data on Google Workspace Team Shared Drive
- Virus scanning of media before use on any workstation.
- Only approved software may be used on ASDOE systems.
- Workstations and said software are used in accordance with contract agreements and copyright laws.
- Users are responsible for maintaining workstation security outside of ASDOE.

Responsibilities: All individuals identified in the scope of this policy are responsible for:

- Using ASDOE computing devices only for work-related purposes
- Following all procedures implemented by IDS and EdTech related to this policy.

ASDOE IDS Program Director, TIS, and EdTech Assistant Directors are responsible for:

- Maintaining procedures and compliance required to support this policy

Compliance All individuals stated under the scope of this policy that fail to comply with this or any other security policy, will result in disciplinary actions set forth by the Director of Education. Legal actions may also be taken for violations of applicable regulations outlined under the Family Educational Rights and Privacy Act (FERPA).

References and Related Resources:

- ASDOE Data Governance Policy #1 Confidentiality of Individual Information
- ASDOE Data Governance Policy #2 Data Access and Management
- ASDOE Data Governance Policy #7 Information Classification
- ASDOE Data Governance Policy #4 Data Security
- ASDOE Data Governance Policy #8 Security Awareness and Training
- ASDOE Data Governance Policy #9 Security Incident Procedures
- ASDOE Data Governance Policy #10 Data Breach
- ASDOE Data Governance Policy #11 Data Breach Management

AMERICAN SAMOA DEPARTMENT OF EDUCATION

Area: Data Privacy and Security	**Policy #013:** User Access Termination Procedures	**Final Draft:** 11/17/21 **By:** Data Governance Committee
Version 1.1	**Approved By:** ASDOE Leadership Team	**Effective Date:** 7/1/22

Purpose: To safeguard accessibility to ASDOE data systems from all individuals no longer a member of the ASDOE workforce.

Scope: Applies to all ASDOE employees, including part-time employees and temporary workers.

Policy: Any termination, resignation, retirement, and separation of a workforce member immediately result in the ASDOE Personnel Office, Education Technology, and Integrated Data Systems (IDS) areas implementing the following to ensure:

- Any and all access to workspace or office is prohibited
- User Access, Request, and Deletion Goggle form is completed by the Supervisor and submitted EdTech and IDS
    - Password is immediately invalidated
    - Access to all systems and applications is suspended
    - Any keys and IDs provided are returned

IDS and EdTech will conduct quarterly user access review reports and provide them to all ASDOE divisions and offices for user access confirmation.

Responsibilities: EdTech Assistant Director and IDS Program Director are responsible for ensuring all activities identified within this policy are followed and implemented.

Compliance: All individuals stated under the scope of this policy that fail to comply with this or any other security policy, will result in disciplinary actions set forth by the Director of Education. Legal actions may also be taken for violations of applicable regulations outlined under the Family Educational Rights and Privacy Act (FERPA).

Form(s): Deletion Google Form (IDS)

References & Related Resources:

- ASDOE Data Governance Policy #1 Confidentiality of Individual Information
- ASDOE Data Governance Policy #2 Data Access and Management
- ASDOE Data Governance Policy #7 Information Classification
- ASDOE Data Governance Policy #4 Data Security
- ASDOE Data Governance Policy #8 Security Awareness and Training
- ASDOE Data Governance Policy #9 Security Incident Procedures
- ASDOE Data Governance Policy #10 Data Breach

- ASDOE Data Governance Policy #11 Data Breach Management

AMERICAN SAMOA DEPARTMENT OF EDUCATION

Area: Data Privacy and Security	**Policy #014:** Parent and Student Annual Notification	**Final Draft:** 6/2/22 **By:** Data Governance Committee
Version 1.1	**Approved By:** ASDOE Leadership Team	**Effective Date:** 7/1/22

Purpose: To inform and educate parents and students about their privacy and security rights under the federal statute, the Family Educational Rights and Privacy Act (FERPA), and ASDOE Data Governance Policies.

Scope: Applies to all ASDOE employees involved with student registration and maintenance of student records at all following locations: Central Office, Elementary and Secondary Divisions and Schools, Office of Student Records, Special Education Division, Early Childhood Education Division, and Centers.

Policy: ASDOE will provide all parents and students at the beginning of every school year and for every new student who enrolls in the ASDOE system the following documents:

- Parent Notification: Quick Guide to Student Information Privacy (FERPA)

- Notice to Parents, Guardians, and Eligible Students: Directory Information

- Notification of Rights Under the Protection of Pupil Rights Amendment (PPRA)

- Notification of Rights Under FERPA for Schools

Responsibilities: Deputy Directors of Instruction and Instructional Support, Assistant Directors, and Office heads noted under the scope of this policy will ensure the appropriate documents are made readily available for distribution and access for parents and students.

Compliance: All individuals stated under the scope of this policy that fail to comply with this or any other security policy, will result in disciplinary actions set forth by the Director of Education. Legal actions may also be taken for violations of applicable regulations outlined under the Family Educational Rights and Privacy Act (FERPA).

References and Related Resources:

- ASDOE Data Governance Policy #1 Confidentiality of Individual Information
- ASDOE Data Governance Policy #2 Data Access and Management
- ASDOE Data Governance Policy #7 Information Classification
- ASDOE Data Governance Policy #4 Data Security
- ASDOE Data Governance Policy #8 Security Awareness and Training
- ASDOE Data Governance Policy #9 Security Incident Procedures
- ASDOE Data Governance Policy #10 Data Breach
- ASDOE Data Governance Policy #11 Data Breach Management