Privacy and Security Risk Management

By

Tom Willard
Director of Technology Services
Alabama Commission on Higher Education
tom.willard@ache.alabama.gov

- This presentation serves as an example approach to developing a security program that follows federal guidelines.
- Every organization is different and must tailor its program to meet its specific requirements.
- This presentation does not include the upwards of 163 new policies, standards, and guidelines that correspond to each family/control/control enhancement from 800-53 under development at the Office of Information Technology.

Office of Information Technology

State of Alabama
Secretary of Information Technology Memorandum
State of Alabama Information Security Program
September 21, 2015

The security policies of the Office of Information Technology will establish the foundation for the Information Security Program within the State of Alabama based upon a formal adoption of the National Institute for Standards and Technology's (NIST) risk management framework, endorsed by the National Governor's Association and the National Association of State Chief Information Officers.

- The policies will set the ground rules under which the State will operate and safeguard its information and information systems

- Related procedures, standards and guidelines will support the management of information risks in daily operations

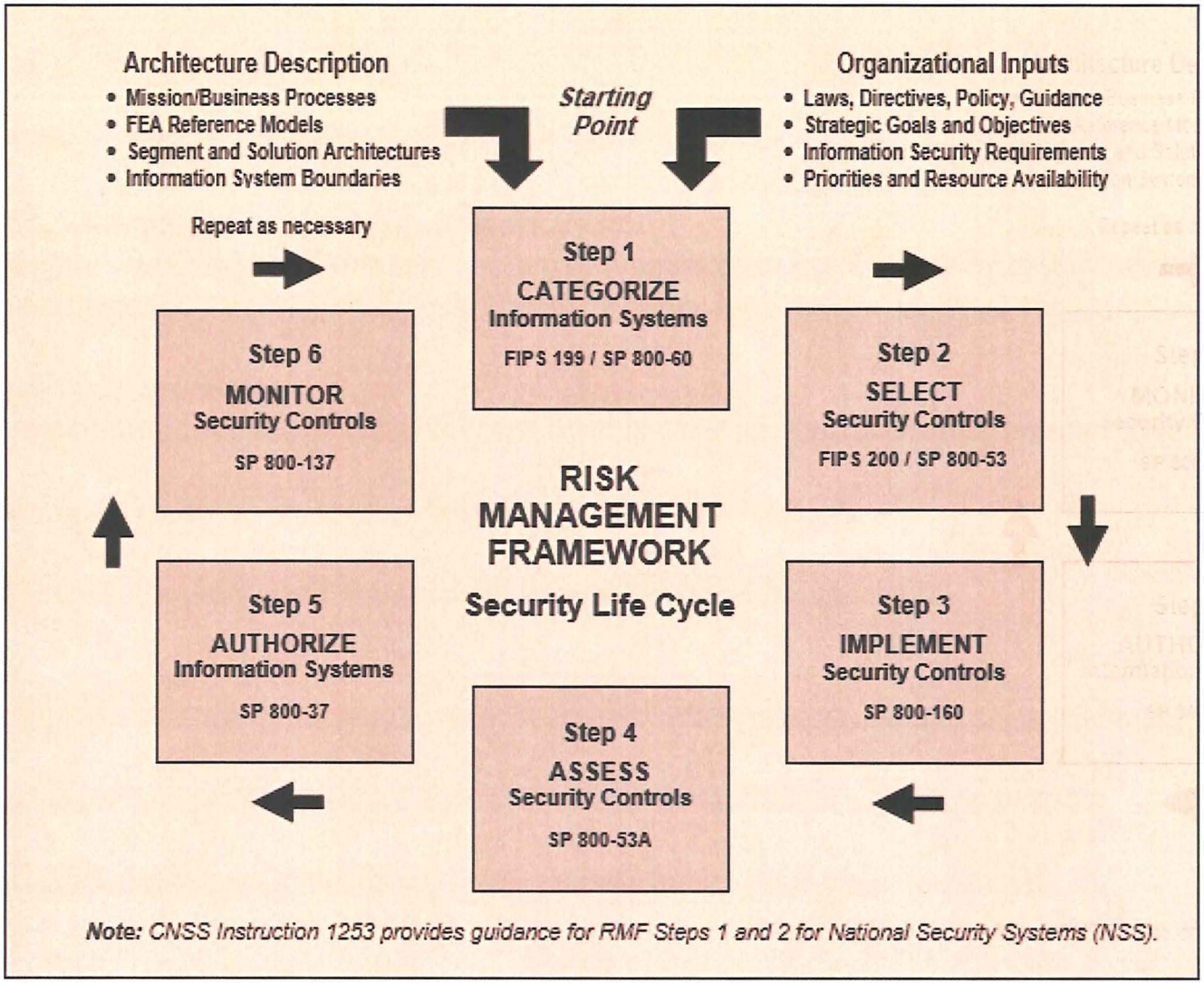
- Development of these concepts provides due care to ensure Alabama employees understand their day-to-day security responsibilities and the threats that could impact the state

- Every employee and agency must know these policies and must conduct their activities accordingly

OIT Memorandum cited the following NIST Risk Management Framework document:

http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

- A set of industry standards and best practices to help organizations manage cyber security risk
- Created through collaboration between government and the private sector
- Uses a common language to address and manage cyber security risk
- Helps the organization align its cyber security activities with its business requirements, risk tolerances, and resources
- Enables organization – regardless of size, degree of cyber security risk, or cyber security sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure



Note: *CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS).*

Ground Rules

- Policies and plans must be understood by non IT personnel
- There must be organizational ownership
- Use best business practices to offset threats to an acceptable risk
- Use FIPS 199, NIST 800-53, and 800-122
  - ✓ PII, FERPA, HIPPA, IRS 1075, and etc.
  - ✓ State policies, plan, standards, guidelines, and procedures
  - ✓ Obtain any audit checklists that may apply to your agency
- There is going to be a significant organizational impact
  - ✓ Resources to develop a comprehensive security program
  - ✓ Resources to implement improvements

Security Program Development Steps

1. Determine FIPS 199 risk levels for confidentiality, integrity, and availability
2. Review the NIST documents and select the appropriate controls
3. Group the selected controls into categories/activities
4. Draft the privacy and security policy
5. Write a compliance document that describes in detail how each control is met
6. Include any State policies, plans, standards, guidelines, and procedures that apply
7. Determine SAOP and CPO duties that ensure organizational ownership and governance
8. Draft the privacy and security plan
9. As required, obtain State and Federal level approval (coordination should occur throughout the previous steps)

Step 1 – Determine FIPS 199 levels for confidentiality, integrity, and availability

FIPS 199 Categories – Security of data and information systems must offset possible threats, while ensuring the following:

- Confidentiality – Preserves authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- Integrity – Assures that sensitive data has not been modified or deleted in an unauthorized and undetected manner
- Availability – Ensures timely and reliable access to and use of information

Levels:

- Low – Limited impact
- Moderate – Serious impact
- High – Severe or catastrophic impact

FIPS – Federal Information Processing Standards, issued by NIST, pursuant to The Information Technology Reform Act of 1996 and Federal Information Security Management Act of 2002

Step 2 – Review the NIST documents and select the appropriate controls

NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations (Apr 2013)

Special Publication 800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (Apr 2010)

Security Controls:

- Selected through a process of categorization using FIPS Publication 199
- Tailored for application to agency information system architecture and mission needs
- Adopted from NIST guidance as they apply to PII to meet both data and physical security requirements

Controls selected in the following order:

- NIST SP 800-53 Appendix J Privacy Control Catalog (18)
- NIST SP 800-122 Guide to Protecting the Confidentiality of PII (17)
- NIST SP 800-53 Appendix D Security Control Baseline and Appendix F Security Control Catalog (23)

AC-11 SESSION LOCK **Standard 662S2-03: Client Systems Security – No more than 15 minutes**

Control: The information system:

a. Prevents further access to the system by initiating a session lock after *[Assignment: organization-defined time period]* of inactivity or upon receiving a request from a user; and
b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7.

Control Enhancements:

(1) SESSION LOCK | PATTERN-HIDING DISPLAYS

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Supplemental Guidance: Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.

References: OMB Memorandum 06-16.

P3	**LOW Not Selected**	**MOD AC-11 (1)**	**HIGH AC-11 (1)**

National Institute of Standards and Technology (NIST):

Selected controls are as follows:

NIST SP 800-53 Appendix J – AP-1, AP-2, AR-1, AR-2, AR-4, AR-5, AR-7, AR-8, DI-1, DM-1, DM-2, DM-3, IP-1, SE-1, SE-2, TR-1, UL-1, UL-2

NIST SP 800-122 – AC-3, AC-5, AC-6, AC-17, AC-19, AC-21, AU-2, AU-6, IA-2, MP-2, MP-3, MP-4, MP-5, MP-6, SC-8, SC-28, SI-4

NIST SP 800-53 Appendix D/F – AC-7, AC-11, AC-12, CM-4, CP-2, CP-4, CP-6, CP-9, CP-10, PE-2, PE-3, PE-4, PE-5, PE-6, PE-9, PE-11, PE-12, PE-13, PE-14, PE-15, PE-16, SI-2, SI-3

800-53 Appendix J Privacy Control Catalog

AP-1 Authority to Collect

AP-2 Purpose Specification

AR-1 Governance and Privacy Program
- SAOP, CPO, technology leaders, and data stewards

AR-2 Privacy Impact and Risk Assessment
- SAOP and CPO duties
- Privacy Impact Assessment (PIA)
- Policy 606-00: Risk Management and Guideline 606G1-00: Risk Assessment and Mitigation

AR-4 Privacy Monitoring and Auditing
- SAOP and CPO duties

AR-5 Privacy Awareness and Training
- Policy 610-02: Cyber Security Awareness and Training

AR-7 Privacy-Enhanced System Design and Development
- Multi-factor authentication
- Roles and permissions management
- Separation of applications and data
- Anti-virus and malware protection

AR-8 Accounting of Disclosures

- Policy 604-01: Cyber Security Incident Response
- Procedure 604P1-00: Cyber Security Incident Reporting
- Procedure 604P2-02: Cyber Security Incident Handling
- Policy 685-00: Data Breach Notification

DI-1 Data Quality

- Edit system to validate all input data

DM-1 Minimization of PII

DM-2 Data Retention and Disposal

- Procedure 681P1-00: Equipment Disposal
- Standard 681S3-00: Media Sanitization

DM-3 Minimization of PII Used in Testing, Training, and Research

IP-1 Consent

IP-2 Individual Access

IP-3 Redress

IP-4 Complaint Management

SE-1 Inventory of PII
- Listing of all programs and information systems identified as collecting, using, maintaining, or sharing PII

SE-2 Privacy Incident Response
- AR-8

TR-1 Privacy Notice

TR-2 System of Records Notices and Privacy Act Statements
- TR-1

TR-3 Dissemination of Privacy Program Information
- TR-1

UL-1 Internal Use
- AP-1 – PII used internally for authorized legal purposes

UL-2 Information Sharing With Third Parties
- MOUs/Interagency Agreements

800-122 Guide to Protecting the Confidentiality of PII (Apr 2010)

AC-3 Access Enforcement
- AR-7

AC-5 Separation of Duties
- System administrators, programmer, and users have different roles and responsibilities for access

AC-6 Least Privilege
- Role Based Access Control and Discretionary Access Control

AC-17 Remote Access

AC-19 Access Control for Mobile Devices

AU-2 Auditable Events
- Anti-virus, malware, and event logs

AU-6 Audit Review, Analysis, and Reporting
- Results of daily log reviews

IA-2 Identification and Authentication (Organizational Users)
- AR-7 and AC-5

MP-2 Media Access
- Restrict digital and non-digital media to authorized users

MP-3 Media Marking

MP-4 Media Storage

MP-5 Media Transport

MP-6 Media Sanitization

SC-8 Transmission Confidentiality
- SSL, SFTP, and VPN

SC-28 Protection of Information at Rest
- Encryption
- Multi-factor authentication
- Role Based Access Control

SI-4 Information System Monitoring
- Anti-virus, malware, and event logs (intrusion events)

Other 800-53 Appendix D Controls

AC-7 Unsuccessful Logon Attempts

AC-11 Session Lock

AC-12 Session Termination

CM-4 Security Impact Analysis

- OS, software, hardware upgrades and security updates

CP-2 Contingency Plan

CP-4 Contingency Plan Testing

CP-6 Alternate Storage Site

CP-9 Information System Backup

CP-10 Information System Recovery and Reconstitution

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-9 Power Equipment and Cabling

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

SI-2 Flaw Remediation

- Minor and major updates

SI-3 Malicious Code Protection

- Parameterized variables, input data validation, stored procedures, and server side code
- Anti-virus and malware protection

Step 3 – Group the selected controls into categories/activities

Core set of cyber security activities

- Decision-Making Authority
- Standard Policies and Procedures
- Data Inventories
- Data Content Management
- Data Records Management
- Data Quality
- Data Access
- Data Security and Risk Management

Decision-Making Authority:

- Designate the Senior Agency Official for Privacy (SAOP) and the Chief Privacy Officer (CPO)
- Establish data governance activities, which include identifying data stewards responsible for coordinating data governance

AR-1

Checklist:
Assigning appropriate levels of authority to data stewards and proactively defining the scope and limitations of that authority is a prerequisite to successful data management.

1. Has an organizational structure with different levels of data governance (e.g., executive, judicial, legislative, administrative, etc.) been established, and roles and responsibilities at various levels specified (e.g., governance committee members, technology leaders, data stewards, etc.)?

2. Have data stewards (e.g., program managers) responsible for coordinating data governance activities been identified and assigned to each specific domain of activity?

3. Are data stewards' roles, responsibilities, and accountability for data decision making, management, and security clearly defined and communicated (to data stewards themselves as well as other relevant stakeholders)?

4. Do data stewards possess the authority to quickly and efficiently correct data problems while still ensuring that their access to personally identifiable information (PII) is minimized in order to protect privacy and confidentiality?

Standard Policies and Procedures:

- Establish data governance rules and requirements and determine roles for key personnel
- Develop procedures to ensure that all collected, managed, stored, transmitted, used, reported, and destroyed records containing PII are handled in a way that preserves privacy and ensures confidentiality and security
- Develop procedures for monitoring compliance
- Post governance policies and practices and purposes for which PII is collected
- Duties within agency shall be separated to minimize the risk of malevolent activity
- No external network connection other than the state network is allowed for PII
- No computer devices may be connected to the state network that have been connected to any other network
- Security controls shall be assessed and corrected on a continuous basis to eliminate vulnerabilities

AC-5, AR-1, IP-1, TR-1

Checklist:
Standard Policies and Procedures

Adopting and enforcing clear policies and procedures in a written data stewardship plan is necessary to ensure that everyone in the organization understands the importance of data quality and security—and that staff are motivated and empowered to implement data governance.

1. Have policy priorities affecting key data governance rules and requirements been identified, and has agreement (either a formal agreement or a verbal approval) on priorities been secured from key stakeholders?

2. Have standard policies and procedures about all aspects of data governance and the data management lifecycle, including collection, maintenance, usage and dissemination, been clearly defined and documented?

3. Are policies and procedures in place to ensure that all data are collected, managed, stored, transmitted, used, reported, and destroyed in a way that preserves privacy and ensures confidentiality and security (this includes, but is not limited to maintaining compliance with the Family Educational Rights and Privacy Act [FERPA])?

4. Has an assessment been conducted to ensure the long-term sustainability of the proposed or established data governance policies and procedures, including adequate staffing, tools, technologies, and resources?

5. Does the organization have a written plan outlining processes for monitoring compliance with its established policies and procedures?

6. Have data governance policies and procedures been documented and communicated in an open and accessible way to all stakeholders, including staff, data providers, and the public (e.g., by posting them on the organization's website)?

Data Inventories:

- Establish a current inventory of all computer equipment, software, and data files
- Maintain a list of all data elements that are PII and update this list based on programmatic changes
- All security controls must protect PII at the "MODERATE" level

SE-1

Checklist:
Conducting an inventory of all data that require protection is a critical step for data security projects. Maintaining an up-to-date inventory of all sensitive records and data systems, including those used to store and process data, enables the organization to target its data security and management efforts. Classifying data by sensitivity helps the data management team recognize where to focus security efforts.

1. Does the organization have a current inventory of all computer equipment, software, and data files?
2. Does the organization have a detailed, up-to-date inventory of all data elements that should be classified as sensitive (i.e., data that carry the risk for harm from an unauthorized or inadvertent disclosure), PII, or both?
3. Have data records been classified according to the level of risk for disclosure of PII?
4. Does the organization have a written policy regarding data inventories that outlines what should be included in an inventory and how, when, how often, and by whom it should be updated?

Data Content Management:

- In performance of duties only specific data elements that contain PII to accomplish lawful duties shall be collected
- PII data must be protected, both at rest and in motion
- Also, system-related data at rest must be protected
- Connections to and from data systems will only be allowed from trusted servers, controlled by firewalls and/or network address filtering

AP-1, AP-2, DM-1, SC-8, SC-28

Checklist:
Closely managing data content, including identifying the purposes for which data are collected, is necessary to justify the collection of sensitive data, optimize data management processes, and ensure compliance with federal, state, and local regulations.

1. Does the organization have a clearly documented set of policy, operational, and research needs that justify the collection of specific data elements (e.g., what PII needs to be collected to successfully monitor a student's participation in and progress through the education system)?

2. Does the organization regularly review and revise its data content management policies to assure that only those data necessary for meeting the needs described above are collected and/or maintained?

Data Records Management:

- All data components will operate in an organization controlled data center or in a highly secure cloud infrastructure
- Media shall not be transported outside controlled areas and shall not be stored on local workstations. Only approved software can be installed on any device
- Media (servers, hard drives, DVD's, etc.) containing PII must be physically protected, checked, and destroyed as soon as not needed
- This includes lockable file cabinets and a secure data center
- Output devices, including printers shall be monitored to ensure PII is protected and properly stored
- Records used for production, testing, training, and research that involves PII shall only be retained for a time period to fulfill the purposes identified in the authority to collect

AR-4, DM-2, DM-3, MP-2, MP-3, MP-4, MP-5, MP-6, PE-2 to PE-6, PE-9, PE-11 to PE-16

Checklist:
Specifying appropriate managerial and user activities related to handling data is necessary to provide data stewards and users with appropriate tools for complying with an organization's security policies.

1. Have mechanisms been put in place to de-identify PII data whenever possible (e.g., by removing all direct and indirect identifiers from PII)?

2. Has the organization established and communicated policies and procedures for handling records throughout all stages of the data lifecycle, including acquiring, maintaining, using, and archiving or destroying data?

Data Quality:

- A change control system must be maintained to ensure that data is accurate, relevant, timely, and complete for the intended purpose

- An edit system must be incorporated to ensure accuracy of inputted data

DI-1

Checklist:
Ensuring that data are accurate, relevant, timely, and complete for the purposes they are intended to be used is a high priority issue for any organization. The key to maintaining high quality data is a proactive approach to data governance that requires establishing and regularly updating strategies for preventing, detecting, and correcting errors and misuses of data.

1. Does the organization have policies and procedures in place to ensure that data are accurate, complete, timely, and relevant to stakeholder needs?

2. Does the organization conduct regular data quality audits to ensure that its strategies for enforcing quality control are up-to-date and that any corrective measures undertaken in the past have been successful in improving data quality?

Data Access:

- All PII data must be transmitted over secure connections
- Access must be limited based on role based permissions with limited unsuccessful login attempts
- Access control for mobile devices is not allowed
- The user list and permissions must be reviewed on a periodic basis
- User accounts must be kept up-to-date and accounts no longer in use are to be disabled or deleted
- Strong/complex passwords must be used
- Multi-factor authentication for roles regarding direct access to the student data base is required
- All access must be logged, maintained, and audited for unauthorized access and suspicious activity affecting PII
- Security screening, training and confidentiality/accountability statements must be accomplished

AC-3, AC-6, AC-7, AC-12, AC-17, AC-19, AC-21, AR-5, AR-7, AU-2, AU-6, IA-2, SC-8, SC-28, UL-1

Checklist:
Data Access

Defining and assigning differentiated levels of data access to individuals based on their roles and responsibilities in the organization is critical to preventing unauthorized access and minimizing the risk of data breaches.

1. Are there policies and procedures in place to restrict and monitor staff data access, limiting what data can be accessed by whom, including assigning differentiated levels of access based on job descriptions and responsibilities? Are these policies and procedures consistent with applicable local, state, and federal privacy laws and regulations (including FERPA)?

2. Have internal procedural controls been established to manage user data access, including security screenings, training, and confidentiality agreements required for staff with PII access privileges?

3. Are there policies and procedures in place to restrict and monitor data access of authorized users (e.g., researchers) to ensure the conditions of their access to data in the system are consistent with those outlined in the data governance plan, including which data elements can be accessed, for what period of time, and under what conditions?

Data Security and Risk Management:

- Establish a plan to mitigate the risks associated with intentional and inadvertent data breaches, a contingency plan to ensure the continuity of data services in the event of a breach, loss, or other disaster, and an incident response plan
- Shut down services outside normal business hours
- Establish policies for data exchange
- Other than data correction, ensure that only summary level reports are generated
- Programming must be accomplished using methods that create secure code and provide malicious code protection
- Monitor logs for potential attacks
- All systems must be kept updated, including all security updates
- All systems must be running anti-virus and malware software, updated daily for new definitions, and continuously scanned

AR-2, AR-8, CM-4, CP-2, CP-4, CP-6, CP-9, CP-10, IP-1, SE-2, SI-2, SI-3, SI-4, UL-2

Checklist:
Data Security and Risk Management

Ensuring the security of sensitive and personally identifiable data and mitigating the risks of unauthorized disclosure of these data is a top priority for an effective data governance plan.

1. Has a comprehensive security framework been developed, including administrative, physical, and technical procedures for addressing data security issues (such as data access and sharing restrictions, strong password management, regular staff screening and training, etc.)?

2. Has a risk assessment been undertaken, including an evaluation of risks and vulnerabilities related to both intentional misuse of data by malicious individuals (e.g., hackers) and inadvertent disclosure by authorized users?

3. Is a plan in place to mitigate the risks associated with intentional and inadvertent data breaches?

4. Does the organization regularly monitor or audit data security?

5. Have policies and procedures been established to ensure the continuity of data services in an event of a data breach, loss, or other disaster (this includes a disaster recovery plan)?

Data Security and Risk Management (Contd.)

6. Are policies in place to guide decisions about data exchanges and reporting, including sharing data (either in the form of individual records containing PII or as de-identified aggregate reports) with educational institutions, researchers, policymakers, parents, and third-party contractors?

7. When sharing data, are appropriate procedures, such as sharing agreements, put in place to ensure that any PII remains strictly confidential and protected from unauthorized disclosure? Make certain that any data sharing agreements are allowed under local, state, and federal privacy laws and regulations, such as FERPA.

8. Are appropriate procedures, such as rounding and cell suppression, being implemented to ensure that PII is not inadvertently disclosed in public aggregate reports and that the organization's data reporting practices remain in compliance with applicable local, state, and federal privacy laws and regulations (e.g., FERPA)?

9. Are stakeholders, including eligible students or students' parents, regularly notified about their rights under applicable federal and state laws governing data privacy?

Step 3 – Draft the privacy and security policy

Protecting student privacy is paramount to the effective implementation of FERPA. All personnel must act responsibly and be held accountable for safeguarding students' personally identifiable information (PII) from education records.

Objective: Policy establishes the procedures that must be followed to ensure compliance with FERPA.

Scope: This policy applies to all personnel and includes policies and procedures to ensure that all student data is collected, managed, stored, transmitted, used, reported, disclosed and destroyed in a way that preserves privacy and ensures confidentiality and security.

Impact: The Federal Information Processing Standard (FIPS 199) was adopted as a tool to ascertain and categorize the potential impact of negative events to information systems as Low, Moderate or High in three areas of concern: Confidentiality, Integrity and Availability. Through this process, it was determined that the potential impact of loss of confidentiality, integrity, and availability for the purposes of this policy is to be considered "MODERATE".

Education Records: An education record is any record from which a student can be personally identified. Records may be in any form and include, but not limited to: written documents, computer media, and electronic files. This includes communications and documents distributed or received by e-mail or other systems, which are retained in organization information systems.

National Institute of Standards and Technology (NIST): List selected controls.

Activities: List core set of cyber security activities with the controls that apply to your organization.

List the activities that apply to your organization using the following examples:

Decision-Making Authority:

- Designate the Senior Agency Official for Privacy (SAOP) and the Chief Privacy Officer (CPO)
- Establish data governance activities, which include identifying data stewards responsible for coordinating data governance

AR-1

Standard Policies and Procedures:

- Establish data governance rules and requirements and determine roles for key personnel
- Develop procedures to ensure that all collected, managed, stored, transmitted, used, reported, and destroyed records containing PII are handled in a way that preserves privacy and ensures confidentiality and security
- Develop procedures for monitoring compliance
- Post governance policies and practices and purposes for which PII is collected
- Duties within agency shall be separated to minimize the risk of malevolent activity
- No external network connection other than the state network is allowed for PII
- No computer devices may be connected to the state network that have been connected to any other network
- Security controls shall be assessed and corrected on a continuous basis to eliminate vulnerabilities

AC-5, AR-1, IP-1, TR-1

and etc.

Step 5 – Write a compliance document that describes in detail how all the selected NIST security controls are met.

Step 6 – Include any State policies, plans, standards, guidelines, and procedures that apply.

- Every control must be discussed in detail – Risk Management Framework

  1. CATEGORIZE Information Systems based on FIPS 199
  2. SELECT Security Controls - SP 800-53 / 800-122
  3. IMPLEMENT Security Controls – Document the design, development, and implementation details
  4. ASSESS Security Controls – Determine the extent to which the controls are implemented correctly, operating as intended, and providing the desired outcome with respect to meeting security requirements
  5. AUTHORIZE Information Systems – Authorize the system based on acceptable risk
  6. MONITOR Security Controls – Monitor based on control effectiveness, changes, and compliance with changing requirements

- Describe how the organization will meet its privacy and security commitments

- Becomes the reference document for the Privacy and Security Plan

Step 7 – Determine SAOP and CPO duties that ensure organizational ownership and governance.

Step 8 – Draft the privacy and security plan, as outlined below.

Reference the compliance document, as an appendix

Reference the State policies, plans, procedures, and standards used as an appendix

Describe the duties of the SAOP and CPO in the following areas:

- Leadership
- Privacy Risk Management
- Information Security
- Incident Management
- Notice
- Privacy Training and Awareness
- Accountability

Add a conclusion

Leadership

The SAOP/CPO, in consultation with the ISD Chief Information Security Officer (CISO), and others as appropriate:

- Ensures the development, implementation, and enforcement of privacy policies, plans, and procedures
- Defines roles and responsibilities for protecting PII
- Determines the level of information sensitivity with regard to PII holdings
- Identifies the laws, regulations, and internal policies that apply to the PII
- Monitors privacy best practices
- Monitors/audits compliance with identified privacy controls

Privacy Risk Management

- Evaluates new technologies, programs, online activities, contracts, regulations, and legislation for potential privacy impacts, and advising other members of senior leadership on implementation of corresponding privacy protections

- Holds regular meetings with other organization officials to discuss new initiatives and how privacy should be addressed

- Acts as subject area experts for reviews of new programs and IT systems to identify privacy compliance issues

- Performs risk assessments to determine if an existing or new activity involves PII or otherwise may impact privacy and to oversee compliance efforts to mitigate the risks while maintaining transparency, mission support, and effective operations

- Uses the Privacy Impact Assessment (PIA) to identify and reduce the risk of the organization's activities

- Oversees the issuing of privacy statements

Information Security

- Responsible for implementing comprehensive privacy policies, plans, and procedures to ensure the confidentiality, integrity, and availability of PII data and is responsible for establishing requirements, including the use of appropriate technologies for privacy-related data management

- Ensures the security of PII is a top priority

- Works closely with State security offices to ensure that information security is made a priority at every level

Incident Management

- Reporting suspected or confirmed incidents to the ISD Customer Services Center Help Desk as the first line of defense and the primary point of contact for all suspected cyber security incidents (State of Alabama Information Technology Procedure 604P1-00: Cyber Security Incident Reporting). Depending on the incident, this may activate the State Cyber Security Incident Response Team (CSIRT)

- Assisting the designated ISD Customer Services Center Help Desk point of contact or CSIRT to determine the appropriate course of action in the event of a privacy incident

To determine whether notification is required in the event of a data breach or similar event, the incident response team assesses the likely risk of harm caused by the breach and then assesses the level of risk based on several factors:

- The nature of the data elements breached
- The number of individuals affected
- The likelihood that the information is accessible and usable
- The likelihood the breach may lead to harm
- The organization's ability to mitigate the risk of harm

By careful analysis and the assessment of these factors, notification is only given in those instances where there is a reasonable risk of harm to affected individuals. Incidents that pose little risk may not be publicly notified because they could create unnecessary concern and confusion.

Notice

- Ensure that the organization provides notice to the public through the organization's Privacy Statement

Privacy Training and Awareness

- Ensure that all employees and contractors receive annual training and review the privacy policy and plan documents, and sign a Statement of Confidentiality / Accountability

- Ensure specific security training is provided at the individual employee level based on specific job duties and level of access to ensure protection of PII, including specific role and permission based training by the database administrator, as roles and permissions change

Accountability

- Accountable for compliance with all applicable privacy protection requirements, including all legal authorities and established policies and procedures that protect privacy and govern the collection, use, dissemination, and maintenance of PII

- Ensures auditing of the use of PII to demonstrate compliance with established privacy controls

- Responsible for performing self-assessments of activities involving PII to ensure compliance with privacy laws, regulations, internal policies, and any other established privacy controls on a periodic basis based on system, policy, and procedure changes involving PII

- Reviews software upgrades for implementation and hardware is for replacement on a schedule that keeps abreast of technology and obsolescence

- Responsible for conducting periodic governance reviews with the stakeholders to ensure that policies and procedures are still relevant, reflect the ground truth of what is happening, and provide appropriate guidance on procedures, roles, and responsibilities

Conclusion

- Issues surrounding the protection of information and information systems will continue to be a factor as technologies advance and programs that require the collection, use, storage, dissemination, and destruction of PII are proliferated

- The elements discussed can serve as an example for implementation of a robust privacy program

- The SAOP/CPO responsibilities discussed ensure privacy protection and compliance with applicable privacy laws, regulations, internal policies, and any other established privacy controls

- Organizations are responsible for providing information security protections and complying with security standards and guidelines

- Maintaining the public's trust greatly depends on an organization's procedures for detecting, reporting, and responding to privacy incidents involving the suspected or confirmed breach of PII

- Even with the implementation and monitoring of privacy and security controls, it is impossible to prevent all risks associated with government operations and it is inevitable that organizations will experience privacy incidents

- Being prepared to respond to and mitigate these risks before substantial damage is done is critical to the success of a privacy program

Step 9 – As required, obtain State and Federal level approval

Summary

Security Program Development Steps

1. Determine FIPS 199 risk levels for confidentiality, integrity, and availability
2. Review the NIST documents and select the appropriate controls (800-53 & 800-122)
3. Group the selected controls into categories/activities (Compliance Checklists)
4. Draft the privacy and security policy
5. Write a compliance document that describes in detail how each control is met
6. Include any State policies, plans, standards, guidelines, and procedures that apply
7. Determine SAOP and CPO duties that ensure organizational ownership and governance
8. Draft the privacy and security plan
9. As required, obtain State and Federal level approval (coordination should occur throughout the previous steps)

Every employee and agency must know these policies and must conduct their activities accordingly