Data Security Checklist

Overview

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of longitudinal data systems. More PTAC information is available on http://ed.gov/ptac.

Purpose

The purpose of this checklist is to assist stakeholder organizations, such as state and local educational agencies, with developing and maintaining a successful data security program. A data security program is a vital component of an organizational data governance plan, and involves management of people, processes, and technology to ensure physical and electronic security of an organization's data. A comprehensive security program is critical to protecting the individual privacy and confidentiality of education records. Solutions and procedures supporting data security operations of education agencies should address their unique challenges, including the need to protect personally identifiable information (PII) while maintaining quality, transparency, and necessary access to the data. To ensure that all aspects of a security plan are executed properly, the program should offer clear guidance and tools for implementing security measures. The summary below lists essential components that should be considered when building a data security program. More information on terms discussed in this checklist is available on http://www2.ed.gov/policy/gen/guid/ptac/glossary.html.

Data Security Checklist

- ❑ **Policy and governance.** Develop a comprehensive data governance plan, outlining organizational policies and standards regarding data security and individual privacy protection. Such a plan should clearly identify staff responsibilities for maintaining data security and empower employees by providing tools they can use to minimize the risks of unauthorized access to PII. Refer to Governance Security Checklist for more information.

- ❑ **Personnel security.** Create policies and guidelines concerning personal and work-related use of Internet, Intranet, and Extranet systems. Incorporate security policies in job descriptions and specify employee responsibilities associated with maintaining compliance with these policies. Conduct regular checks and trainings to ensure employee understanding of the terms and conditions of their employment. Confirm the trustworthiness of employees through the use of

personnel security screenings, policy training, and binding confidentiality agreements.

- ❑ **Physical security.** Make computing resources physically unavailable to unauthorized users. This includes securing access to any areas where sensitive data (i.e., data that carry the risk for harm[1] from an unauthorized or inadvertent disclosure) are stored and processed, such as buildings and server rooms. An unlocked server room is an invitation for malicious or accidental damage. Monitor access to these areas to prevent intrusion attempts (e.g., by administering identification badges and requiring staff and visitors to log in prior to entering the premises or accessing the resources).

- ❑ **Network mapping**. You cannot protect what you do not understand. Network mapping provides a picture of the network (servers, routers, etc) and its connections. Furthermore, network mapping can capture applications and associated data. A robust mapping capability will map the dependencies between applications, data, and network layers. There are a number of network mapping tools available.

- ❑ **Inventory of assets.** The inventory should include both authorized and unauthorized devices used in your computing environment. These devices are often scanned and discovered by automated programs (continuously searching the internet for vulnerabilities) and if unsecured devices are discovered they can be compromised. Inventorying, when used in conjunction with network mapping, will give your organization a better understanding of the security requirements to protect your assets.

- ❑ **Authentication.** The ways in which someone may be authenticated fall into three categories: something you know, something you have, or something you are. Two-factor authentication (TFA) combines two of these elements and is more costly, but provides more security. Consider TFA for remote users or privileged "super users." Authentication technologies provide more assurance that the person is authorized to access network assets, services, and information.

- ❑ **Provide a layered defense.** The most common layers to protect are hosts (individual computers), application, network, and perimeter. There are specific security tools that can be utilized at each of these layers. Relying on a firewall alone to protect your network is never adequate.

- ❑ **Secure configurations.** It is a best practice not to put any hardware or software onto your network until it has been security tested and configured to optimize its security. Continuous scanning to ensure network components remain in a secure state is an additional capability that will enhance data security protection. Proactive management of security risks also involves

[1] Here, harm refers to any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII (NIST, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* 2010 Special Publication 800-122, p. 3-1, 2). Harm to an individual includes any negative or unwanted effects (i.e., that may be socially, physically, or financially damaging).

establishing a comprehensive change management program to analyze and address security and privacy risks introduced by new technology or business processes.

- **Access control**. Securing data access includes requiring strong passwords and multiple levels of user authentication, setting limits on the length of data access (e.g. , locking access after the session timeout), limiting logical access to sensitive data and resources, and limiting administrative privileges. Role-based access is essential for protecting PII and sensitive data-defining specified roles and privileges for users is a required security procedure. Sensitive data that few personnel have access to should not be stored on the same server as other types of data used by more personnel without additional protections for the data (e.g., encryption).

- **Firewalls and Intrusion Detection/Prevention Systems (IDPS).** A firewall is a device designed to permit or deny network transmissions based upon a set of rules. Firewalls are frequently used to protect networks from unauthorized access, while permitting legitimate communications to pass. An IDPS is a monitoring device that is designed to detect malicious activity on the network. Although some automatically take remediation action, most report suspicious activity to a central monitoring point for further analysis.

- **Automated vulnerability scanning.** When new vulnerabilities (to hardware, operating systems, applications, and other network devices) are discovered, hackers immediately scan networks for these vulnerabilities. Scanning your network on a regular basis will minimize the time of exposure to known vulnerabilities.

- **Patch management.** Patch management is the process of using a strategy and plan for what patches should be applied to which systems at a specified time. A patch is a piece of code that protects computers and applications by updating the security state against new threats or vulnerabilities. Used in conjunction with vulnerability scanning, the enterprise can quickly shut down any vulnerability discovered.

- **Shut down unnecessary services.** Each port, protocol, or service is a potential avenue for ingress into your network. A best practice, which should be part of a secure configuration, should include shutting down all services and ports that are not required in your computing environment. A secure enterprise will continually monitor for the use of unapproved ports, protocols or services.

- **Mobile devices.** When sensitive data are stored on servers or on mobile devices, such as laptops or smart phones, the data should be encrypted. There are far too many examples of mobile devices being lost or stolen and the subsequent exposure of the sensitive information stored on those devices in the public domain.

- **Emailing confidential data.** Consider the sensitivity level of the data to be sent over the email. Emailing unprotected PII or sensitive data poses a high security risk. It is recommended that organizations use alternative practices to protect transmissions of these data. These practices

include mailing paper copies via secure carrier, de-sensitizing data before transmission, and applying technical solutions for transferring files electronically (e.g., encrypting data files and/or encrypting email transmissions themselves).

- **Incident handling.** When an incident does occur it is critical to have a process in place to both contain and fix the problem. Procedures for users, security personnel, and managers need to be established to define the appropriate roles and actions. Outside experts may be required to do a forensics investigation of the incident, but having the correct procedures in place initially will minimize the impact and damage.

- **Audit and compliance monitoring.** Audits are used to provide an independent assessment of your data protection capabilities and procedures (see Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records) and should be performed periodically. Auditors that are familiar with Family Educational Rights and Privacy Act statutory and regulatory requirements can further assist you in determining whether your systems are in compliance.

Glossary

Education Agency or Institution refers to any public or private agency or institution to which funds have been made available under any program administered by the Secretary, if the educational institution provides educational services or instruction, or both, to students; or the educational agency is authorized to direct and control public elementary or secondary, or postsecondary educational institutions. For more information, see the Family Educational Rights and Privacy Act regulations, 34 CFR §99.1.

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.

Personally identifiable information (PII) refers to information, such as a 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, Family Educational Rights and Privacy Act regulations, 34 CFR §99.3, for a complete definition of PII specific to education data, and for examples of education data elements that can be considered PII.

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) 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 NIST, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* 2010 Special Publication 800-122, for more information.

Additional Resources

Below are several links that provide more detailed discussions on building a data security program and the components that should be considered.

The international ISO 177799 standard: http://17799.denialinfo.com/

National Institute of Standards and Technology (NIST), NIST SP 800-14 (Generally Accepted Principles and Practices for Securing Information Technology Systems): http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

System Administration, Networking, and Security Institute, 20 Critical Security Controls (Version 2.3): http://www.sans.org/critical-security-controls/guidelines.php

PTAC Issue Brief Data Security: Top Threats to Data Protection:
http://www2.ed.gov/policy/gen/guid/ptac/pdf/issue-brief-threats-to-your-data.pdf

Statewide Longitudinal Data Systems (SLDS) Technical Brief 2. Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records (NCES 2011-602):
http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2011602