For more information please visit the Privacy Technica Assistance Center: http://nces.ed.gov/ptac

Data Security Checklist

Overview

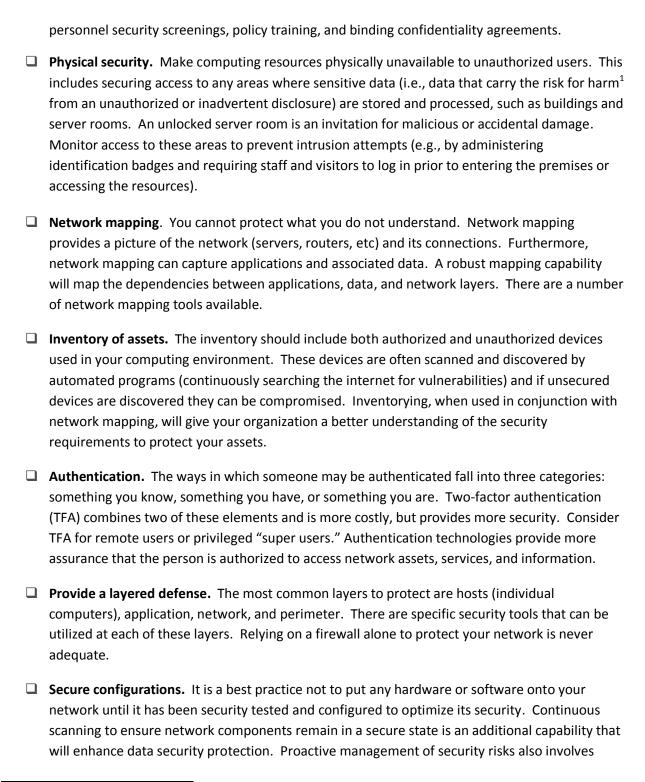
The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. PTAC provides timely information and 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.

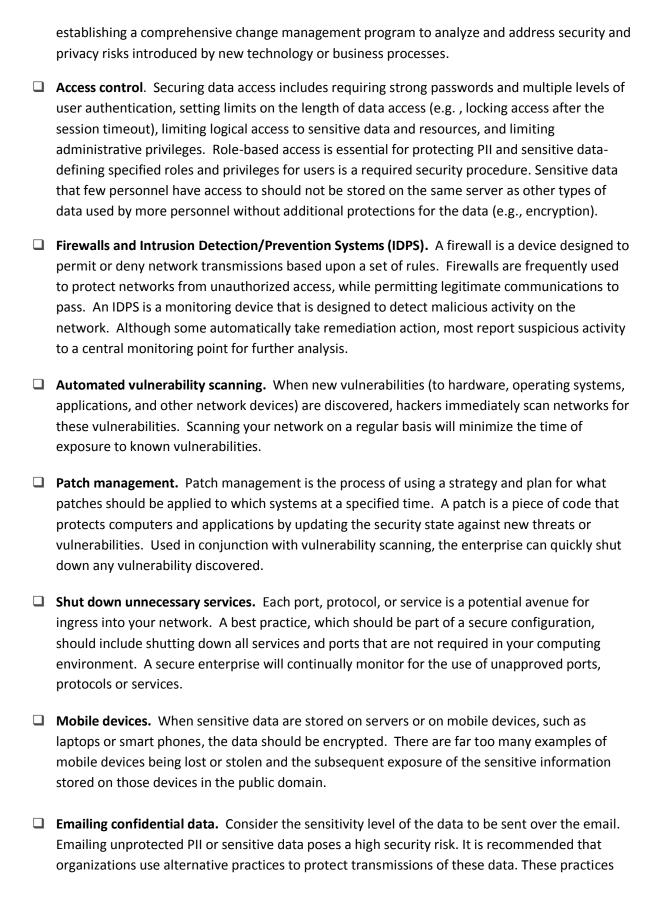
Data Security Checklist

- 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



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).

PTAC-CL, Dec 2011 Page 2 of 6



PTAC-CL, Dec 2011 Page 3 of 6

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, <u>34 CFR</u> §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 <u>Data Security: Top Threats to Data Protection:</u>
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