Data Security Protocol for Protecting Electronic Educational Records

By

Jennifer Radecki & Candace Elliott Person
for the I.A.S.E.P. project

Introduction

- What is I.A.S.E.P.?
- What is the IASEP Data Security Protocol?
- Who is its audience?
- What information can be found in the IASEP Data Security Protocol?
- How is this Protocol being developed as a web site?

What is I.A.S.E.P.?

- I.A.S.E.P. stands for the Indiana Assessment System of Education Proficiencies.

- It is an integrated computer-based documentation system to be used with mentally handicapped students in elementary school through twelfth grade to fulfill state and Federal assessment requirements.

I.A.S.E.P. Security Web Site Staff

- Professor Deborah Bennett: I.A.S.E.P. Principal Investigator

- Candace Elliott Person: Protocol Author/Web Site Coordinator

- Jennifer Radecki: Graduate Research Assistant/Web Site Designer

A Definition of Protocol

- A set of rules, laws or recommendations governing the treatment and formatting of data in an electronic communications system. This includes policy samples and suggestions for overall treatment of data security in individual school districts.

The Audience

- The document provides information for policy makers, administrators and school boards to help them create organization-specific policies to protect and secure their organization’s data access, storage and transmission.

- Teachers can use the protocol to develop specific classroom interventions to protect data.

I.A.S.E.P. Data Security Protocol

- As data is collected from this system, it will be transmitted via the Internet to I.A.S.E.P. for research.

- To insure the confidentiality and safety of student data, I.A.S.E.P., in cooperation with CERIAS, is developing a data security protocol to distribute to those who use this system.

Protocol Objective 1

- Identify current education-related and general data security policies, procedures, guidelines and standards. Make this information available to IASEP constituents through a protocol document.

Protocol Objective 2

- Identify current education-related and general data security state, federal and private laws and regulations. Make this information available to IASEP constituents through a protocol document.

Protocol Objective 3

- Develop a protocol that will assist IASEP constituents to formulate their own data security policies in order to affect how data is entered, accessed, stored, transmitted and reported in Indiana.

Protocol Objective 4

- Coordinate with CERIAS, state education and legal consultants to facilitate the architectural security work underway with the IASEP system. Use the protocol document to supplement the architectural activities.

Protocol Objective 5

- Develop a set of schematics to assist readers and practitioners to readily visualize how the protocol elements fit together and how they can be used to develop and implement individual school district data security policy plans.

Protocol Objectives 6

- Develop a training protocol to disseminate critical information.

Research on Existing Security Documentation

- Jennifer Radecki, a part-time Purdue graduate assistant, researched state and education-based data, physical, software and e-mail security policies currently on the web.

- Shelly Shinevar, a part-time paralegal student in Lansing, Michigan, researched federal, state and education-based data security laws and statutes.

The Research Process

- Web sites and legal resources were examined for state, federal and education-based security documents to use as a model in the creation of our own protocol.

- E-mail was then sent out to all contact persons listed on the examined Web sites with a request for additional information.

Research Findings

- Most State-level Information Security Web sites contained some security plans on the site or under construction.
- Very few education-specific data security policies were found on the WWW.
- Most education-based technology plans focused on acquisition and set up, as well as curriculum creation.

Research Findings

- Internet and Network Acceptable Use Policies were the most prevalent security documents found on the Web on both state and education-based sites.

- Response to our e-mail request for additional resources was limited, but a number of states expressed a need for information related to compiling data security policies.

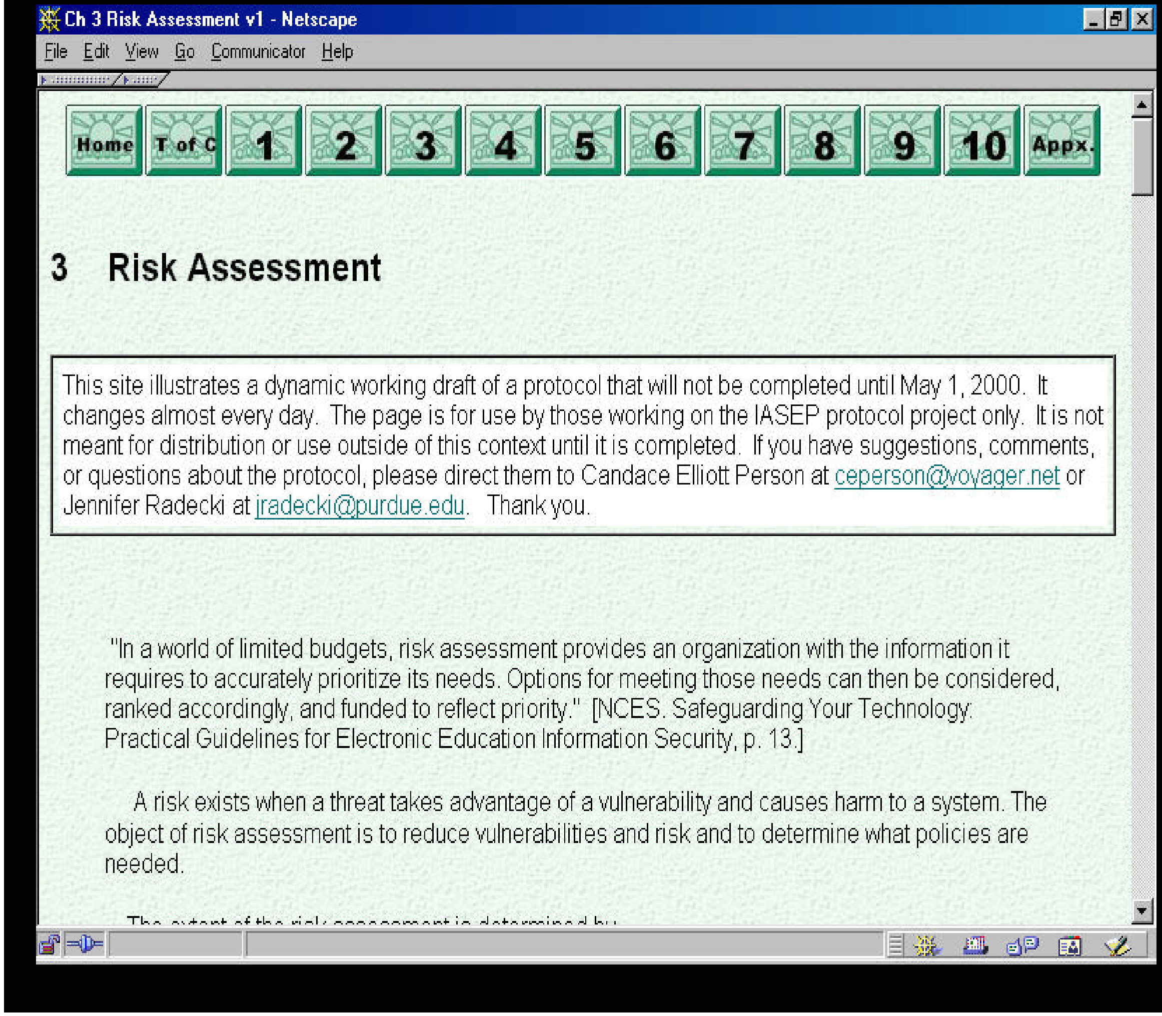
Web site Development

- A Web Site is currently being developed in order to better disseminate the protocol to constituents.

- The site: http://www.soe.purdue.edu/projects/iasep/protocol/home_page/home_page.htm

- The site currently contains the protocol draft chapters, several appendices of state, federal and educational policy and a glossary.

Web Site Specifics


Ch 3 Risk Assessment v1 - Netscape
File Edit View Go Communicator Help
Home
T of C
1
2
3
4
5
6
7
8
9
10
Appx.

3 Risk Assessment

This site illustrates a dynamic working draft of a protocol that will not be completed until May 1, 2000. It changes almost every day. The page is for use by those working on the IASEP protocol project only. It is not meant for distribution or use outside of this context until it is completed. If you have suggestions, comments, or questions about the protocol, please direct them to Candace Elliott Person at ceperson@voyager.net or Jennifer Radecki at jradecki@purdue.edu. Thank you.

"In a world of limited budgets, risk assessment provides an organization with the information it requires to accurately prioritize its needs. Options for meeting those needs can then be considered, ranked accordingly, and funded to reflect priority." [NCES. Safeguarding Your Technology: Practical Guidelines for Electronic Education Information Security, p. 13.]

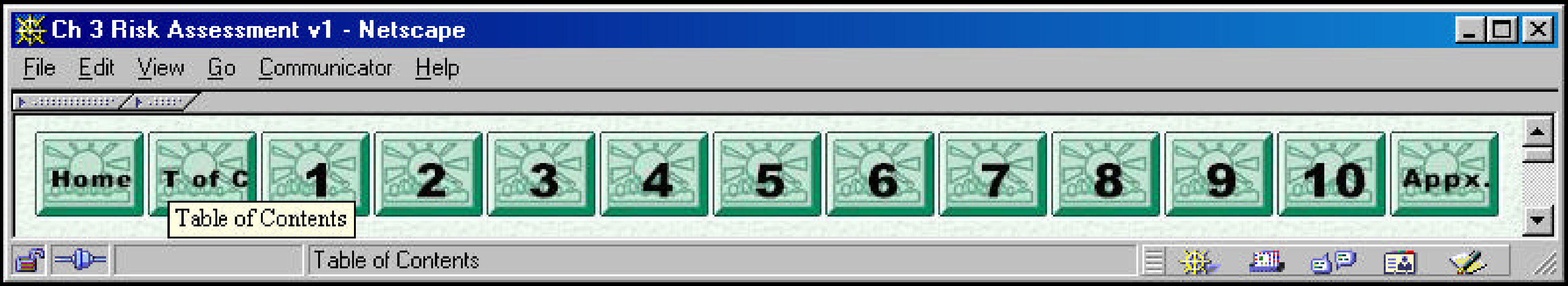
A risk exists when a threat takes advantage of a vulnerability and causes harm to a system. The object of risk assessment is to reduce vulnerabilities and risk and to determine what policies are needed.

The extent of the risk assessment is determined by:

- The protocol is divided into 10 chapters.
- Appendices include listings of the federal, state and education laws, statues and policies, and a glossary.

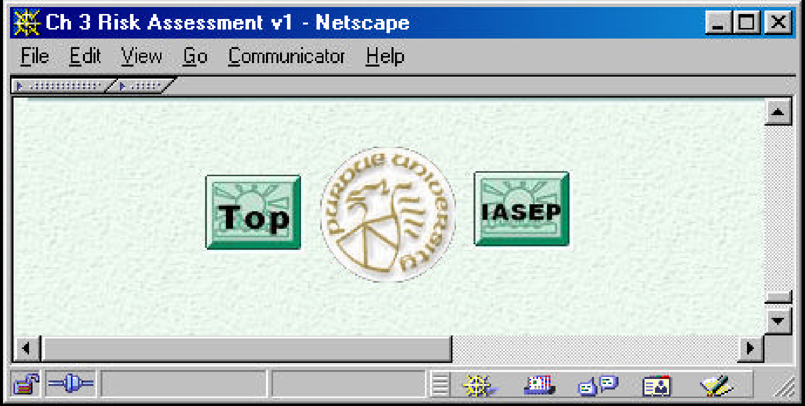
Web Site Design

- A navigation bar composed of separate buttons for each chapter is included at the top of every web page.



Web Site Design (con’t)

- Navigation buttons at the bottom of each Web page for movement to the Top of the Page, to the Purdue Home page, and to the I.A.S.E.P. Home page.


Ch 3 Risk Assessment v1 - Netscape
File Edit View Go Communicator Help
Top
IASEP

Web Site Accessibility

- The web site was designed for accessibility to all users.
- While designing the site, we often referred to the World Wide Web Consortium’s Web Content Accessibility Guidelines found at http://www.w3c.org

Web Site Progress

- The web site is continually being updated.
- The web site should be ready for public use in May of 2000.
- Currently, only I.A.S.E.P. constituents have viewing access to the site while it is being developed.

Protocol Chapters

- Chapter 1: Introduction
- Chapter 2: General Protocol & Policy Statements
- Chapter 3: Risk Assessment
- Chapter 4: Physical Security Policies

Protocol Chapters (con't)

- Chapter 5: Information Security Policies
- Chapter 6: Software Security Policies
- Chapter 7: User Access Security Policies
- Chapter 8: Network & Internet Security Policies

Protocol Chapters (con't)

- Chapter 9: Administrative Policies & Procedures

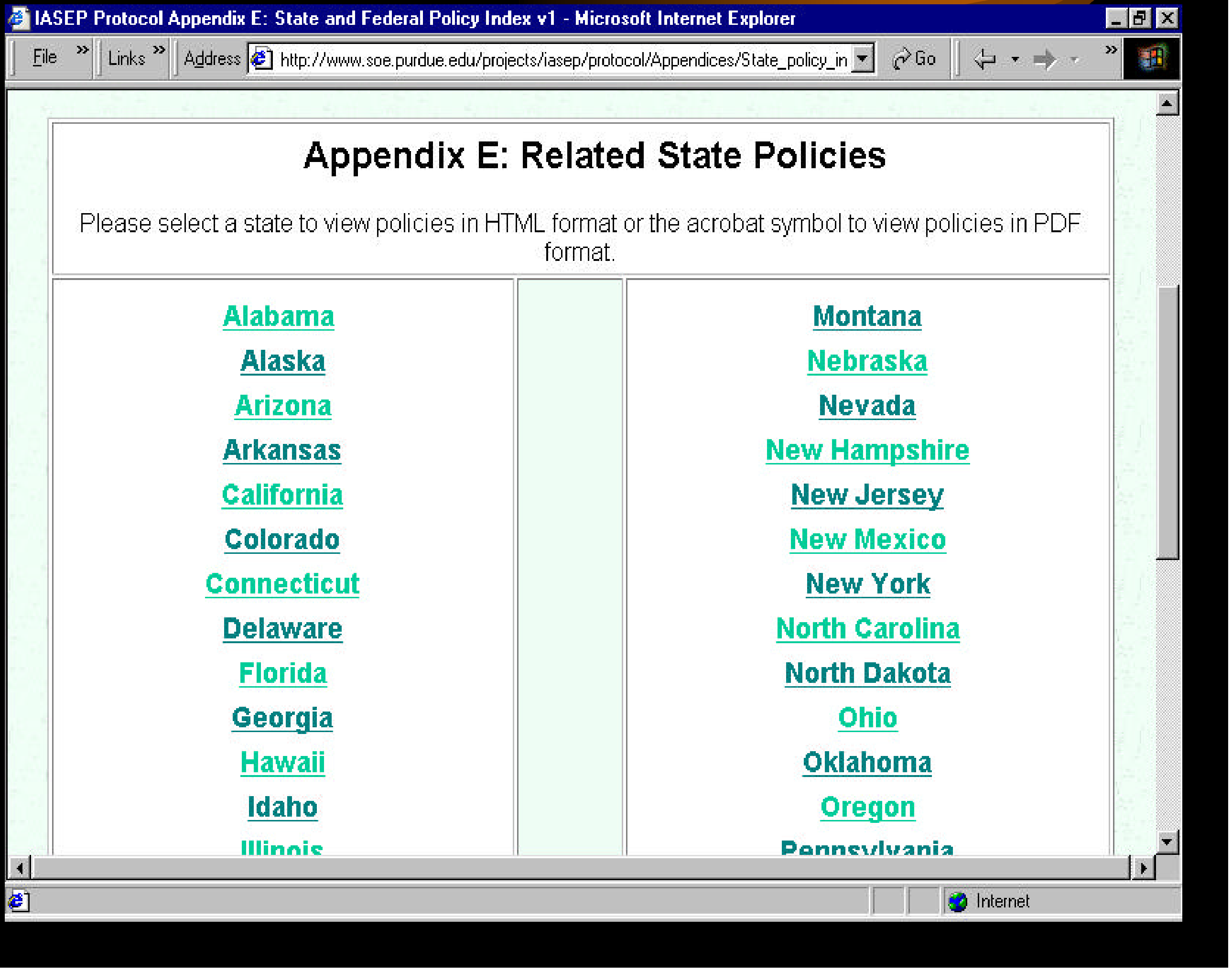
- Chapter 10: Training Protocol

Protocol Appendices

- Appendix A: Glossary
- Appendix B: Related Federal Laws & Policy Implications
- Appendix C: Related State Laws
- Appendix D: Related Federal Data Security Policies

Protocol Appendices (con't)

- Appendix E: Related State Data Security Policies



IASEP Protocol Appendix E: State and Federal Policy Index v1 - Microsoft Internet Explorer

http://www.soe.purdue.edu/projects/iasep/protocol/Appendices/State_policy_in

Appendix E: Related State Policies

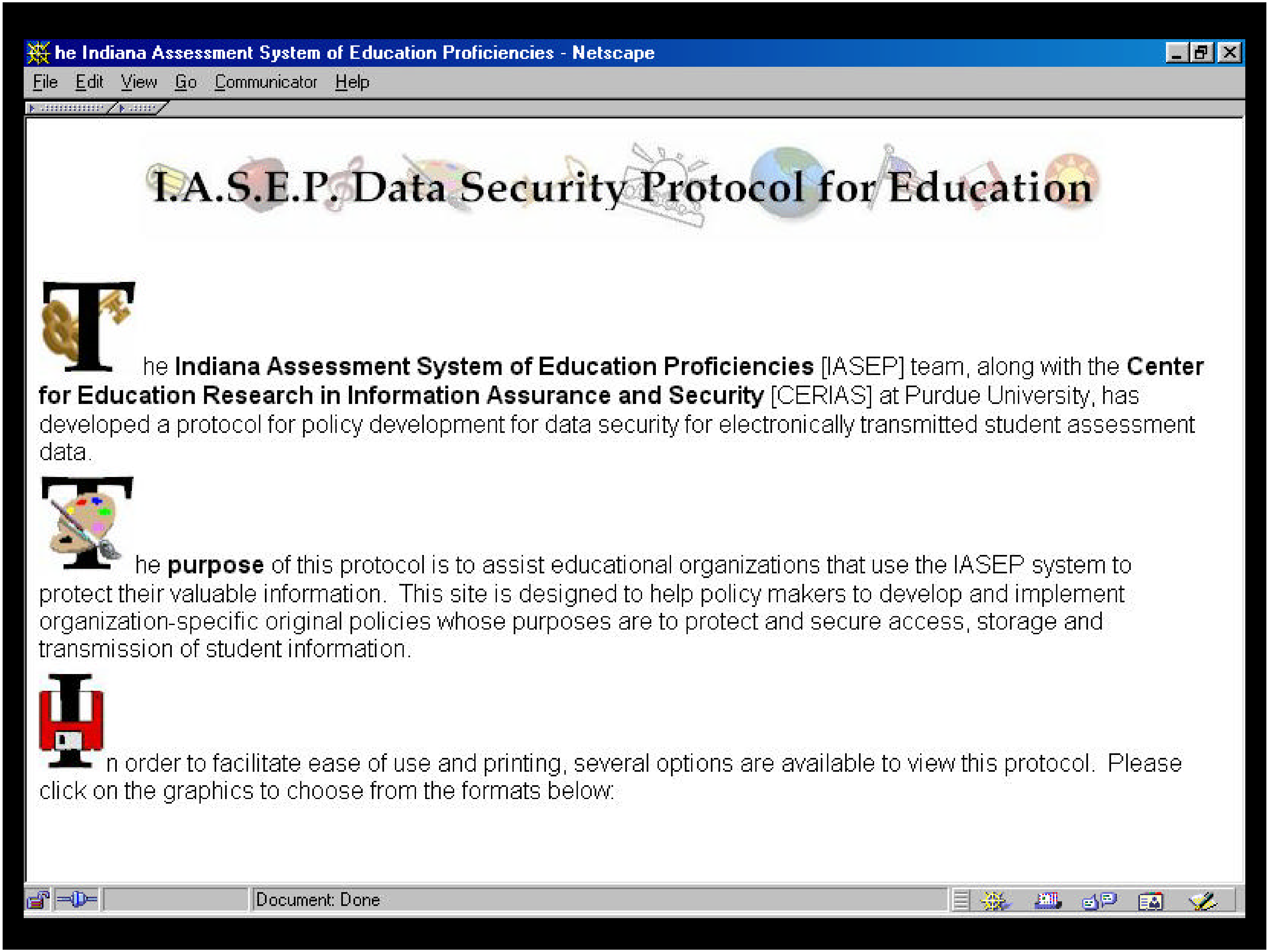
Please select a state to view policies in HTML format or the acrobat symbol to view policies in PDF format.

Alabama
Alaska
Arizona
Arkansas
California
Colorado
Connecticut
Delaware
Florida
Georgia
Hawaii
Idaho
Illinois

Montana
Nebraska
Nevada
New Hampshire
New Jersey
New Mexico
New York
North Carolina
North Dakota
Ohio
Oklahoma
Oregon
Pennsylvania

Protocol Appendices (con’t)

- Appendix F: Technology Resources
- Appendix G: Model Policies
- Appendix H: Bibliography & Policy Resources


he Indiana Assessment System of Education Proficiencies - Netscape
File Edit View Go Communicator Help
Document: Done

I.A.S.E.P. Data Security Protocol for Education

The **Indiana Assessment System of Education Proficiencies** [IASEP] team, along with the **Center for Education Research in Information Assurance and Security** [CERIAS] at Purdue University, has developed a protocol for policy development for data security for electronically transmitted student assessment data.

The **purpose** of this protocol is to assist educational organizations that use the IASEP system to protect their valuable information. This site is designed to help policy makers to develop and implement organization-specific original policies whose purposes are to protect and secure access, storage and transmission of student information.

In order to facilitate ease of use and printing, several options are available to view this protocol. Please click on the graphics to choose from the formats below:

Chapter 2

- **Chapter 2: General Protocol and Policy Statements**
  - Describes the distinctive characteristics of an effective security policy.
  - Describes the usefulness and uses for security policy.

Chapter 3

- **Chapter 3: Risk Assessment**
  - A Risk exists when a threat takes advantage of a vulnerability and causes harm to a system.
  - Risk assessment provides the impetus and the information necessary to construct an effective tailored security plan around perceived priorities.

Chapter 3 (con’t)

- Five steps for effective risk assessment:

(1) Inventory all information assets: hardware, software, automated files, databases and data communication links

(2) Categorize all data, based on its sensitivity to loss. Categories include sensitive, confidential, private and public information.

Chapter 3 (con’t)

- Risk assessment steps (continued):

  (3) Inventory all information systems: hardware, software, automated files, databases and data communication links.

  (4) Create a Risk Profile Matrix rating threats, visibility, consequences and sensitivity of data to determine priority of protection.

  (5) Assess Network Vulnerabilities and Defenses.

Chapter 4

- **Chapter 4: Physical Security Policies & Procedures**
  - The National Center for Education Statistics (NCES) says that “[p]hysical security refers to the protection of building sites and equipment (and all other information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes and accidental damage . . .

Chapter 4 (con't)

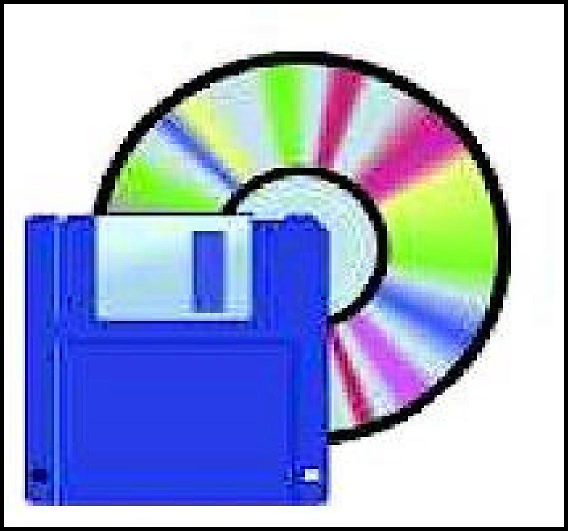
- Thinking about Physical Security:
  - Building and Classroom Security
  - Equipment Security
  - Equipment Usage
  - Anti-virus program instillation
  - Equipment maintenance and labeling
  - System Backup
  - Power Supply regulation
  - Careful addition of new users to the system

Chapter 5

- **General Data Protection Policy Formulation involves policies related to:**
  - Data classification: sensitive, confidential, private and public
  - Transmission of information
  - Identification, Authentication, and Integrity

Chapter 6

- **Software Security Policies relate to**:
  - Protection against viruses
  - Software licensing
  - Encryption
  - Intellectual property protection



Chapter 7

- **User Access Security Policies relate to:**
  - System access controls
  - Login process and monitoring
  - Password & User ID process
  - Privileges levels

Chapter 8

- **Network & Internet Security Policies relate to**:
  - System security, integrity, documentation, and incident handling
  - Firewall administration
  - Authenticating
  - Logs & audit trials
  - Internet & Email use policies

Chapter 9

- **Administrative Policies & Procedures Stress**:
  - The importance of administrative involvement and endorsement of all data security storage, access, and transmission policies.
  - The need for periodic compliance reviews and contingency plans.

Chapter 10

- **Training protocols address:**
  - Responsibilities of Educational Administrators and School Board Members to assure that Systems and Data are secure.
  - How to develop applicable specific school district policies, procedures, and guidelines.

Conclusion

- Top educational administrators and school boards are ultimately responsible for the integrity and security of school property.
- They need to understand and use sound security strategies, and ensure that valuable equipment and information, such as private student and staff records, are adequately protected.
- The purpose of this protocol is to assist administrators to achieve those goals.