

# Information Security Fundamentals for DIAS Participants:

Learning to be Safe in an Insecure World

---

## Objectives:

- ✓ To increase the teachers' awareness of basic security issues.
- ✓ To provide basic techniques that teachers can implement into their classroom practices to increase information security.

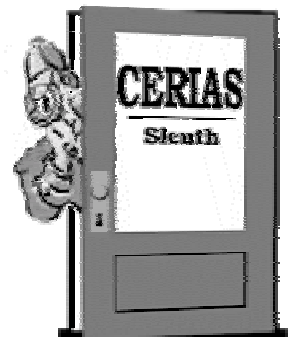


Center for Education and  
Research in Information  
Assurance and Security

Presented By:

**Judith L. Lewandowski**  
K-12 Outreach Coordinator  
CERIAS Purdue University  
1315 Recitation Bldg.  
West Lafayette, IN 47907  
(765) 496-6762

email: [judyL@cerias.purdue.edu](mailto:judyL@cerias.purdue.edu)  
<http://www.cerias.purdue.edu/K-12>



These materials may be reproduced in their original form for educational purposes. They may not be republished without express permission from CERIAS, Purdue University. Please contact the CERIAS K-12 Program for more information.

## Section#1: Information Security--- The Basics

### What is Information Security?

- **Information Security** refers to the protection of data, programs, and information stored on disks, networks, hard drives, etc. and includes within itself the issues of privacy, ethics, and loss prevention.

### How does I.S. impact teachers? (Why is this important to ME?)

- **Organizational Resources and Reputation:** Maintaining an effective security protocol is critical in order to sustain a credible reputation and protect an organization's resources. When a school system is not secure, the impact can negatively affect the viewpoint of parents, community leaders, and legislative officials. This negativity can, in turn, affect the overall well being of a school system.
- **Confidential School Records:** Educators have a responsibility to maintain the protection of confidential student information. Parents and students trust the educational system to protect these records. In addition, the federal government has established a series of legislation to hold school systems and officials accountable if this information is not properly maintained. Every teacher should be aware of the necessary precautions to protect this sensitive information from disclosure, and to protect themselves from a potential lawsuit.
- **Protecting Personal Work Files:** Most teachers have an abundance of self-generated materials that are stored electronically. If these materials were lost, deleted, or deleted by someone else, it would take a considerable amount of time to recreate the lessons for future use in the classroom. In addition, in the hands of the wrong person, these materials may lose their integrity and damage the assessment process of a course.
- **Increasing Rise of Alternative Assessment:** One of the most recent trends of evaluation has to do with the concept of "Alternative Assessment". Many educators are very excited about the possibility of evaluating students in a non-traditional manner. Although this new method of assessment is exciting, the logistical concerns of storage and access are quite overwhelming. Many schools are looking to technology to assist in this manner. As a result, school systems will need to thoroughly scrutinize the level of security surrounding the storage of these unique and personal student records.
- **Protecting Students While Working Online:** As lesson plans become increasingly influenced by the use of technology, it is important for teachers to understand the basic steps involved with protecting themselves and their students while in an online environment. The Internet offers many wonderful resources and supplements to the educational arena, but it also contains sites that are inappropriate for the K-12 environment. In order to fully use these resources, teachers must be aware of the potential dangers and pitfalls of using the Internet. Rather than focusing on the paranoia associated with the "unknown", school systems should promote an increased emphasis on security education and direct this awareness to the teachers, parents, and students involved with the online world.

## Section #2: Protecting Your Password---The Basics

### Reasons to protect your password:

- **Protects your documents from tampering.**  
Example: With the use of your password, an individual could modify important documents such as student records, classroom tests, or conference notes.
- **Protects your personal information.**  
Example: With the use of your password, an individual could access personal information and possibly use it to make purchases, abuse your personal accounts, or begin embarrassing gossip.
- **Prevents others from abusing your account.**  
Example: After pinpointing your password, an individual could easily send out threatening, inappropriate, or malicious emails that would be attributed to your account.

### General Guidelines to Protect YOUR Password:

1. Do **NOT** post your password or store it near your computer.
2. Require passwords to be at least **8** characters in length.
3. Require the use of non-alpha character and capitalization:  
Examples: Boiler\*Maker  
12girl#power  
Iam@Work
4. Do **NOT** use easy to guess selections.  
Examples: password  
123456  
computer
5. Use **NON-PERSONAL** selections.  
**Avoid:** your name  
spouse's name  
address  
birthday  
social security number
6. Maintain zero tolerance for password sharing at school.
7. Warn users not to type their passwords when someone may be watching.
8. Urge users to change their passwords frequently...especially if they feel theirs may have been compromised.
9. Always remember to log out!!
10. Constantly reinforce the importance of password security.



### Section #3: Software Security

There are a variety of measures that you can follow to help ensure that your software use is done in a secure manner. We recommend the following:

- **Only install necessary and trusted software.** If you are using a school system computer, it is important to consider that your actions with downloading or installing software can impact other teachers, classrooms, and administrators. Before you install the software, reflect upon its use in the classroom. Will it improve your role as an educator? Will it help your students to learn? If you reply no to either of these questions, you may want to consider not using the software.
- **Beware of “free” games, screensavers, and graphics.** Many times these “freebies” contain unwanted programs or viruses that can damage your equipment or allow for your system to be an unwilling player in a cyber-attack.
- **Keep a printed version of all copyright agreements.** There are many items on the WWW that grant permission for use of their files, images, or content. It is a smart idea to keep a printed version in an effort to clear up any copyright discrepancies. If you were ever to be challenged on the legitimacy of the use of copyright-protected material, you could use this print out as evidence that you took “due care” to follow the copyright law.
- **Run and update your anti-virus software.** In order for your anti-virus software to work, you must routinely download the new virus definitions (.dat files). This is a fairly easy process that typically requires the user to visit the software vendors Website and follow a simple downloading procedure. (Check your product’s information for more detail!)

#### Types of Potentially Malicious Items:

- **Virus:** a computer program capable of attaching to disks or files and replicating itself repeatedly, typically without user knowledge or permission.
- **Trojan Horse:** a malicious program that pretends to be a benign application. These programs are not viruses due to the fact that they do not replicate.
- **Worm:** a reproducing program that runs independently and travels across network connections. Unlike a virus, a worm does not need a host file to survive.
- **Logic Bomb:** a program that executes itself when a specific condition occurs. Often times, these are a form of Trojan Horse as well.
- **Trapdoor:** a program that allows access to a system by skipping the usual login routine. This can be beneficial when used for troubleshooting or repair---but it can also be detrimental when used in a malicious way.

## Section #4: Classroom Management---Logistical Concerns

Before utilizing technology in your classroom, there are some basic concepts to consider related to classroom management and information security. By implementing these basic guidelines in your classroom, you will begin the process of protecting your students, information, and equipment.

- Place the computers in such a way that all screens can be easily seen from the center of the room.
- Increase the size of the display font so that you can more easily view the content on your students' screens. (This is also helpful by allowing you to answer "quick" questions from a considerable physical distance.)
  - Internet Explorer: Click on the "**View**" menu. Select "**Text Size**" and choose the desired size.
  - Netscape: Click on the "**View**" menu. Select "**Increase Font**" until the desired size is selected.
- Do not allow students access to the Internet when a substitute teacher is present.
- Utilize a software package that allows you to filter and monitor the students' access to the Internet.
- Maintain a secure physical environment:
  - Do NOT allow food or drink near the computers.
  - Lock all doors and windows when the room is unattended.
  - Do NOT advertise or draw attention to the location of important information such as grades, health files, discipline reports, etc.
- Practice proper file management:
  - Make a back-up copy of all files and documents on a **separate** disk. (Back-up frequently!!)
  - Store your back-ups in a different location. (home, department office, etc.)
  - Keep a hard (paper) copy of all important information.
  - Pay attention to the location you are saving documents. Avoid saving confidential information on a non-secured drive/disk.
  - Clearly label your disks and files. Use folders to organize information within these disks/drives.
  - Keep all magnets away from disks and computers.

## FERPA Fact Sheet

### Family Educational Rights and Privacy Act of 1974 (FERPA)

The Family Educational Rights and Privacy Act (FERPA) is a Federal law designed to protect the privacy of a student's education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student, or former student, who has reached the age of eighteen or is attending any school beyond the high school level. Students and former students to whom the rights have transferred are called eligible students.

- Parents or eligible students have the right to inspect and review all of the student's education records maintained by the school. Schools are not required to provide copies of materials in education records unless, for reasons such as great distance, it is impossible for parents and eligible students to inspect the records. Schools may charge a fee for copies.
- Parents and eligible students have the right to request that a school correct records believed to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record commenting on the contested information in the record.
- Generally, the school must have written permission from the parent or eligible student before releasing any information from a student's record. However, the law allows schools to disclose records, without consent, to the following parties:
  - School employees who have a **need-to-know**
  - Other schools to which a student is transferring
  - Certain government officials in order to carry out lawful functions
  - Appropriate parties in connection with financial aid to a student
  - Organizations doing certain studies for the school
  - Accrediting organizations
  - Individuals who have obtained court orders or subpoenas
  - Persons who need to know in cases of health and safety emergencies
  - State and local authorities, within a juvenile justice system, pursuant to specific state laws

Schools may also disclose, without consent, "directory" type information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendances. However, schools must tell parents and eligible students about directory information and allow parents or eligible students a reasonable amount of time to request that the school not disclose directory information about them.

Schools must notify parents and eligible students of their rights under this law. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school. For additional information or technical assistance, call (202) 260-3887 or TDD (202) 260-8956, or contact:

Family Policy Compliance Office  
U.S. Department of Education  
600 Independence Avenue, S.W.  
Washington, D.C. 20202-4605