

[Chapter 1](#) [Chapter 2](#) [Chapter 3](#) [Chapter 4](#) [Chapter 5](#) [Chapter 6](#) [Chapter 7](#) [Chapter 8](#) [Chapter 9](#) [Chapter 10](#)
[Table of Contents](#) [Glossary of Terms](#)

CHAPTER 5

Protecting Your System: Physical Security



CHAPTER 5 IN A NUTSHELL:

[Introduction to Physical Security](#)
[Commonly Asked Questions](#)
[Policy Issues](#)
[Physical Security Countermeasures](#)
[Physical Security Checklist](#)

Introduction to Physical Security

Most people think about locks, bars, alarms, and uniformed guards when they think about security. While these **countermeasures** are by no means the only precautions that need to be considered when trying to secure an information **system**, they are a perfectly logical place to begin. Physical security is a vital part of any security plan and is fundamental to all security efforts--without it, information security ([Chapter 6](#)), software security ([Chapter 7](#)), user access security ([Chapter 8](#)), and network security ([Chapter 9](#)) are considerably more difficult, if not impossible, to initiate. Physical security refers to the protection of building sites and equipment (and all **information** and **software** contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders.



Back to Top



Home Page



Commonly Asked Questions

Q. How can I implement adequate site security when I am stuck in an old and decrepit facility?

A. Securing your site is usually the result of a series of compromises-- what you need versus what you can afford and implement. Ideally, old and unusable buildings are replaced by modern and more serviceable facilities, but that is not always the case in the real world. If you find yourself in this situation, use the **risk assessment** process described in [Chapter 2](#) to identify your **vulnerabilities** and become aware of your preferred security solutions. Implement those solutions that you can, with the understanding that any steps you take make your system that much more secure than it had been. When it comes time to argue for new facilities, documenting those vulnerabilities that were not addressed earlier should contribute to your evidence of need.

Q. Even if we wanted to implement these physical security guidelines, how would we go about doing so?

A. Deciding which recommendations to adopt is the most important step. Your risk assessment results should arm you with the information required to make sound decisions. Your findings might even show that not every guideline is required to meet the specific needs of your site (and there will certainly be some variation based on need priorities). Once decided on, however, actually initiating a strategy is often as simple as raising staff awareness and insisting on adherence to regulations. Some strategies might require basic "handyman" skills to install simple equipment (e.g., key locks, fire extinguishers, and surge protectors), while others definitely demand the services of consultants or contractors with special expertise (e.g., window bars, automatic fire equipment, and alarm systems). In any case, if the organization determines that it is necessary and feasible to implement a given security strategy, installing equipment should not require effort beyond routine procedures for completing internal work orders and hiring reputable contractors.

Q. What if my budget won't allow for hiring full-time security guards?

A. Hiring full-time guards is only one of many options for dealing with security monitoring activities. Part-time staff on watch during particularly critical periods is another. So are video cameras and the use of other staff (from managers to receptionists) who are trained to monitor security as a part of their duties. The point is that by brainstorming a range of possible **countermeasure** solutions you can come up with several effective ways to monitor your workplace. The key is that the function is being performed. How it is done is secondary--and completely up to the organization and its unique requirements.

Determining countermeasures often requires creativity: don't limit yourself to traditional solutions.



Back to Top



Home Page

be found in [Chapter 3](#).

resource theft and destruction. To accomplish this, decision-makers must be concerned about building construction, room assignments, emergency procedures, regulations governing equipment placement and use, power supplies, product handling, and relationships with outside contractors and agencies.

The physical plant must be satisfactorily secured to prevent those people who are not authorized to enter the site and use equipment from doing so. A building does not need to feel like a fort to be safe. Well-conceived plans to secure a building can be initiated without adding undue burden on your staff. After all, if they require access, they will receive it—as long as they were aware of, and abide by, the organization's stated security policies and guidelines (see [Chapter 3](#)). The only way to ensure this is to demand that before any person is given **access** to your system, they have first signed and returned a valid Security Agreement. This necessary **security policy** is too important to permit exceptions.

Physical Threats (Examples)

Examples of physical **threats** include:

As discussed more completely in [Chapter 2](#), a threat is any action, actor, or event that contributes to risk

- Natural events (e.g., floods, earthquakes, and tornados)
- Other environmental conditions (e.g., extreme temperatures, high humidity, heavy rains, and lightning)
- Intentional acts of destruction (e.g., theft, vandalism, and arson)
- Unintentionally destructive acts (e.g., spilled drinks, overloaded electrical outlets, and bad plumbing)



Physical Security Countermeasures

A countermeasure is a strp planned and taken in opposition to another act or potential act.

The following countermeasures address physical security concerns that could affect your site(s) and equipment. These strategies are recommended when risk assessment identifies or confirms the need to counter potential breaches in the physical security of your system.

Countermeasures come in a variety of sizes, shapes, and levels of complexity. This document endeavors to describe a range of strategies that are potentially applicable to life in education organizations. In an effort to maintain this focus, those countermeasures that are *unlikely* to be applied in education organizations are *not* included here. If after your risk assessment, for example, your security team determines that your organization requires high-end countermeasures like retinal scanners or voice analyzers, you will need to refer to other security references and perhaps even need to hire a reliable technical consultant.



Create a Secure Environment: Building and Room Construction:¹⁷



- *Don't arouse unnecessary interest in your critical facilities:* A secure room should have "low" visibility (e.g., there should not be signs in front of the building and scattered throughout the hallways announcing "expensive equipment and **sensitive information** this way").
- *Maximize structural protection:* A secure room should have full height walls and fireproof ceilings.
- *Minimize external access (doors):* A secure room should only have one or two doors—they should be solid, fireproof, lockable, and observable by assigned security staff. Doors to the secure room should never be propped open.
- *Minimize external access (windows):* A secure room should not have excessively large windows. All windows should have locks.
- *Maintain locking devices responsibly:* Locking doors and windows can be an effective security strategy as long as appropriate authorities maintain the keys and combinations responsibly. If there is a breach, each compromised lock should be changed.
- *Investigate options other than traditional keyhole locks for securing areas as is reasonable:* Based on the findings from your risk assessment (see [Chapter 2](#)), consider alternative physical security strategies such as window bars, anti-theft **cabling** (i.e., an alarm sounds when any piece of equipment is disconnected from the system), magnetic key cards, and motion detectors.

Select only those countermeasures that meet perceived needs as identified during risk assessment ([Chapter 2](#)) and support security policy ([Chapter 3](#)).



Recognize that some countermeasures are ideals and may not be feasible if, for example, your organization is housed in an old building.

- *Be prepared for fire emergencies:* In an ideal world, a secure room should be protected from fire by an automatic fire-fighting system. Note that water can damage electronic equipment, so carbon dioxide systems or halogen agents are recommended. If implemented, staff must be trained to use gas masks and other protective equipment. Manual fire fighting equipment (i.e., fire extinguishers) should also be readily available and staff should be properly trained in their use.
- *Maintain a reasonable climate within the room:* A good rule of thumb is that if people are comfortable, then equipment is usually comfortable—but even if people have gone home for

when they thaw out.

- *Be particularly careful with non-essential materials in a secure computer room:* Technically, this guideline should read "no eating, drinking, or smoking near **computers**," but it is quite probably impossible to convince staff to implement such a regulation. Other non-essential materials that can cause problems in a secure environment and, therefore, should be eliminated include curtains, reams of paper, and other flammables.

Security is measured not by its effect on theory, but by its effect on reality!



Guard Equipment:



Locking critical equipment in secure closet can be an excellent security strategy findings establish that it is warranted.

- *Keep **critical systems** separate from **general systems**:* Prioritize equipment based on its criticality and its role in processing sensitive information (see [Chapter 2](#)). Store it in secured areas based on those priorities.
- *House computer equipment wisely:* Equipment should not be able to be seen or reached from window and door openings, nor should it be housed near radiators, heating vents, air conditioners, or other duct work. Workstations that do not routinely display sensitive information should always be stored in open, visible spaces to prevent covert use.
- *Protect cabling, plugs, and other wires from foot traffic:* Tripping over loose wires is dangerous to both personnel and equipment.
- *Keep a record of your equipment:* Maintain up-to-date logs of equipment manufacturers, models, and serial numbers in a secure location. Be sure to include a list of all attached **peripheral equipment**. Consider videotaping the equipment (including close-up shots) as well. Such clear evidence of ownership can be helpful when dealing with insurance companies.
- *Maintain and repair equipment:* Have plans in place for emergency repair of critical equipment. Either have a technician who is trained to do repairs on staff or make arrangements with someone who has ready access to the site when repair work is needed. If funds allow, consider setting up **maintenance contracts** for your critical equipment. Local computer suppliers often offer service contracts for equipment they sell, and many workstation and **mainframe vendors** also provide such services. Once you've set up the contract, be sure that contact information is kept readily available. **Technical support** telephone numbers, maintenance contract numbers, customer identification numbers, equipment serial numbers, and mail-in information should be posted or kept in a log book near the system for easy reference. Remember that computer repair technicians may be in a position to access your **confidential information**, so make sure that they know and follow your policies regarding outside employees and contractors who access your system.



Rebuff Theft:¹⁸



- *Identify your equipment as yours in an overt way:* Mark your equipment in an obvious, permanent, and easily identifiable way. Use bright (even fluorescent) paint on **keyboards**, **monitor** backs and sides, and computer bodies. It may decrease the resale value of the components, but thieves cannot remove these types of identifiers as easily as they can adhesive labels.

Losing a computer to theft has both financial

(the files contained on the hard drive).

Laptops and other expensive equipment that leave the office often never return.

- ***Make unauthorized tampering with equipment difficult:*** Replace regular body case screws with Allen-type screws or comparable devices that require a special tool (e.g., an Allen wrench) to open them.
- ***Limit and monitor access to equipment areas:*** Keep an up-to-date list of personnel authorized to access sensitive areas. Never allow equipment to be moved or serviced unless the task is pre-authorized and the service personnel can produce an authentic work order and verify who they are. Require picture or other forms of identification if necessary. Logs of all such activity should be maintained. Staff should be trained to always err on the cautious side (and the organization must support such caution even when it proves to be inconvenient).



Attend to Portable Equipment and Computers:¹⁹

- ***Never leave a laptop computer unattended:*** Small, expensive things often disappear very quickly—even more quickly from public places and vehicles!



While the X-ray conveyor belt is the preferred way of transporting a laptop through airport security (compared to subjecting the computer to the magnetic fields of walk-through or wand scanners), it is also a prime place for theft. Thieves love to "inadvertently" pick up the wrong bag and disappear while passengers are fumbling through their pockets to find the loose coins that keep setting off the metal detectors. Use the X-ray conveyor belt, but never take your eyes off your laptop!

Require laptop users to read the recommended travel guidelines that should come with the equipment's documentation.

- ***Store laptop computers wisely:*** Secure laptops in a hotel safe rather than a hotel room, in a hotel room rather than a car, and in a car trunk rather than the back seat.
- ***Stow laptop computers appropriately:*** Just because a car trunk is safer than its back seat doesn't mean that the laptop won't be damaged by an unsecured tire jack. Even if the machine isn't stolen, it can be ruined all the same. Stow the laptop and its battery safely!
- ***Don't leave a laptop computer in a car trunk overnight or for long periods of time:*** In cold weather, condensation can form and damage the machine. In warm weather, high temperatures (amplified by the confined space) can also damage **hard drives**.

It Really Happens!

Jack's briefcase was his life. Well, maybe it wasn't his whole life, but it definitely contained the better part of his professional life. It held his grade book, his lesson plans, his master's thesis—all very important things in the world of a middle school teacher.

And it wouldn't be an exaggeration to say that Jack sure was surprised when his life (the briefcase) went up in flames one afternoon in the school cafeteria. He couldn't explain it, but nonetheless he found himself sitting in front of the district technologist trying to do exactly that—explain why his briefcase caught on fire and ruined, among more important things to him, the spare battery he was carrying for the school's laptop computer.

"So," the technologist asked, "you're saying that you're surprised that your briefcase caught on fire? Well, let me tell you, I'm glad that it was only your bag that was damaged. Didn't you know that the exposed terminals of a battery can cause a spark? Didn't you know that any piece of metal, even a paper clip, can serve as the conduit? That's all it takes: an improperly stored battery, a paper clip and anything combustible—and wham, you've got yourself a fire. Your home could have gone up in flames last night because of it. Or your school could have this afternoon. Didn't you know that?"

Jack almost replied that, of course, he hadn't known about all of those dangers, and that the technologist should have warned him about them before he had borrowed the laptop and extra battery. But instead he just shook his head sheepishly. After all, along with his grade book, lesson plans, and master's thesis, he had just burned a \$200 dollar laptop battery that didn't belong to him.

Regulate Power Supplies:



Pay attention to the manufacturer's recommendations for storing portable computer batteries—they carry live charges and are capable of igniting fires if not handled properly.

- ***Be prepared for fluctuations in the electrical power supply:*** Do so by (1) plugging all electrical equipment into surge suppressors or electrical power filters; and (2) using Uninterruptible Power Sources (UPSs) to serve as auxiliary electrical supplies to critical equipment in the event of power outages.
- ***Protect power supplies from environmental threats:*** Consider having a professional electrician design or redesign your electrical system to better withstand fires, floods, and other disasters.
- ***Select outlet use carefully:*** Although little thought generally goes into plugging equipment into an outlet, machines that draw heavily from a power source can affect, and be affected by, smaller equipment that draws energy from the same outlet.
- ***Guard against the negative effects of static electricity in the office place:*** Install anti-static carpeting and anti-static pads, use anti-static sprays, and encourage staff to refrain from touching metal and other static-causing agents before using computer equipment.

are very powerful tools for disseminating information--so powerful, in fact, that their use must be monitored.

- **Assign printers to *users* with similar security clearances:** You don't want employees looking at sensitive financial information (e.g., staff salaries) or confidential student information (e.g., individual records) while they are waiting for their documents to print. It is better to dedicate a **printer** to the Director of Finance than to have sensitive **data** scattered around a general use printer. Don't hesitate to put printers in locked rooms if that is what the situation demands.
- **Label printed information appropriately:** Confidential printouts should be clearly identified as such.
- **Demand suitable security procedures of common carriers when shipping/receiving confidential information:** Mail, delivery, messenger, and courier services should be required to meet your organization's security standards when handling your confidential information.
- **Dispose of confidential waste adequately:** Print copies of confidential information should not be placed in common dumpsters unless shredded. (Comparable requirements for discarding electronic copies of confidential information can be found in [Chapter 6](#).)

It Really Happens!

Dr. Hamilton was everything that a school district could ask for. She was a great visionary, a trusted leader, and an excellent superintendent... but she was terrible with the piles of paper she kept on her desk. Luckily for her and the district, she had an equally competent secretary. Lucy was always one step ahead of Dr. Hamilton with the paperwork. She knew where to find the latest draft of the letter to the Board. She knew which form needed to be completed by when. She knew how many copies of the monthly report needed to be run off.

One afternoon, Dr. Hamilton came running out of her office to Lucy's desk, "You haven't shredded those papers I gave you this morning yet, have you?"

As was always the case, Lucy had, of course, completed the task shortly after it had been handed to her. She told Dr. Hamilton so, and asked what was the matter.

"I think that I accidentally gave you my only copy of the speech I'm giving to the Chamber of Commerce tonight," the distraught woman replied, knowing that she'd never be able to reproduce the outline in time for the meeting.

"Don't worry," Lucy said, beaming with pride that her forethought was about to again pay off, "I make backup copies of every sheet of paper you give me before I turn on that paper shredder. Let's look in my filing cabinet."

Dr. Hamilton let out a deep sigh of relief--Lucy had again saved the day. Suddenly, however, the astute superintendent paused, "What do you mean you make copies of everything I give you before you turn on the paper shredder?"

Don't throw a
monkey-wrench into
the machinery.
—Philander Johnson


[Back to Top](#)

[Home Page](#)

Physical Security Checklist

While it may be tempting to simply refer to the following checklist as your security plan, to do so would limit the effectiveness of the recommendations. They are most useful when initiated as part of a larger plan to develop and implement security policy throughout an organization. Other chapters in this document also address ways to customize policy to your organization's specific needs--a concept that should not be ignored if you want to maximize the effectiveness of any given guideline.

Security Checklist for Chapter 5

The brevity of a checklist can be helpful, but it in no way makes up for the detail of the text.

Check Points for Physical Security

Create a Secure Environment: Building and Room Construction

1. Does each secure room or facility have low visibility (e.g., no unnecessary signs)?

[Click for more info.](#)
[Click for more info.](#)

3. Has the room or facility been constructed with a fireproof ceiling?
4. Are there two or fewer doorways?
5. Are doors solid and fireproof?
6. Are doors equipped with locks?
7. Are window openings to secure areas kept as small as possible?
8. Are windows equipped with locks?
9. Are keys and combinations to door and window locks secured responsibly?
10. Have alternatives to traditional lock and key security measures (e.g., bars, anti-theft cabling, magnetic key cards, and motion detectors) been considered?
11. Have both automatic and manual fire equipment been properly installed?
12. Are personnel properly trained for fire emergencies?
13. Are acceptable room temperatures always maintained (i.e., between 50 and 80 degrees Fahrenheit)?
14. Are acceptable humidity ranges always maintained (i.e., between 20 and 80 percent)?
15. Are eating, drinking, and smoking regulations in place and enforced?
16. Has all non-essential, potentially flammable, material (e.g., curtains and stacks of computer paper) been removed from secure areas?

Guard Equipment

17. Has equipment been identified as critical or general use, and segregated appropriately?
18. Is equipment housed out of sight and reach from doors and windows, and away from radiators, heating vents, air conditioners, and other duct work?
19. Are plugs, cabling, and other wires protected from foot traffic?
20. Are up-to-date records of all equipment brand names, model names, and serial numbers kept in a secure location?
21. Have qualified technicians (staff or vendors) been identified to repair critical equipment if and when it fails?
22. Has contact information for repair technicians (e.g., telephone numbers, customer numbers, maintenance contract numbers) been stored in a secure but accessible place?
23. Are repair workers and outside technicians required to adhere to the organization's security policies concerning sensitive information?

Rebuff Theft

24. Has all equipment been labeled in an overt way that clearly and permanently identifies its owner (e.g., the school name)?
25. Has all equipment been labeled in a covert way that only authorized staff would know to look for (e.g., inside the cover)?
26. Have steps been taken to make it difficult for unauthorized people to tamper with equipment (e.g., by replacing case screws with

☒ Click for more info.

27. Have security staff been provided up-to-date lists of personnel and their respective access authority?

Click for more info.

28. Are security staff required to verify identification of unknown people before permitting access to facilities?

Click for more info.

29. Are security staff required to maintain a log of all equipment taken in and out of secure areas?

Click for more info.

Attend to Portable Equipment and Computers

Click for more info.

30. Do users know not to leave laptops and other portable equipment unattended outside of the office?

Click for more info.

31. Do users know and follow proper transportation and storage procedures for laptops and other portable equipment?

Click for more info.

Regulate Power Supplies

Click for more info.

32. Are surge protectors used with all equipment?

Click for more info.

33. Are Uninterruptible Power Supplies (UPSs) in place for critical systems?

Click for more info.

34. Have power supplies been "insulated" from environmental threats by a professional electrician?

Click for more info.

35. Has consideration been given to the use of electrical outlets so as to avoid overloading?

Click for more info.

36. Are the negative effects of static electricity minimized through the use of anti-static carpeting, pads, and sprays as necessary?

Click for more info.

Protect Output

Click for more info.

37. Are photocopiers, fax machines, and scanners kept in open view?

Click for more info.

38. Are printers assigned to users with similar security clearances?

Click for more info.

39. Is every printed copy of confidential information labeled as "confidential"?

Click for more info.

40. Are outside delivery services required to adhere to security practices when transporting sensitive information?

Click for more info.

41. Are all paper copies of sensitive information shredded before being discarded?

Click for more info.

Back to Top

Home Page

Previous Chapter

Next Chapter

Explore the Institute of Education Sciences

IES

Home
About
Publications
Data
Funding
News

IES Centers

NCEE
NCER
NCES
Home
About
Programs
Publications
Data
Data Training
School Search
News

IES Policies and Standards

Public Access Policy
Privacy and Security Policies
NCES Statistical Standards
Peer Review Process
ED Data Inventory
Fed Stats

Contact Us

U.S. Department of Education

Additional Resources

ERIC
Sitemap
Organizational Chart

