Global Knowledge®

Expert Reference Series of White Papers

10 Essential Security Polices

10 Essential Security Polices

James Michael Stewart, Global Knowledge Instructor, CISSP, ISSAP, SSCP, MCT, CEI, CEH, TICSA, CIW SA, Security+, MCSE+ Security Windows 2000, MCSA Windows Sever 2003, MCDST, MCSE NT & W2K, MCP+I, Network+, iNet+

Introduction

Writing a corporate security policy might seem complex, but ultimately it is a collection of many small policies. By writing each of the essential sub-policies from this list, you are well on your way to creating (updating or revising) a corporate security policy. From firewalls, to backup, to personnel management, these are 10 common essential security policies your organization needs yesterday.

There are hundreds of sub-policies that a company eventually needs to construct in order to fully address and manage the security concerns of the organization. The focus on these ten does not imply that other policies are any less essential. This is an article not an exhaustive treatise, and the goal is to spur action toward writing or improving security guidelines. These ten security policies (or sub-policies) are essential to every organization, regardless of size, location, age, mission, or the product or service produced, and are presented here (in no particular order).

1. Acceptable Use Policy

The Acceptable Use Policy (AUP) defines what are and are not an allowed activities on company premises, with company equipment, and when using company resources. It often defines actions that are specifically prohibited, such as accessing pornography, pirated content, or running a side-business. These prohibitions are enforced with consequences in the event an employee is found in violation.

The AUP can also define activities that are allowed within reason or within specific boundaries. For example, it may be acceptable to surf the Internet, participate in chat and e-mail conversations, and even play games up to 10 minutes per hour, as long as it does not interfere with accomplishing work tasks.

The goal of the AUP is to guide employees toward working productively without burning out or putting the organization at risk due to risky or non-business behaviors. Employees should focus on work tasks while at work. Some downtime and distraction is expected, even necessary, but abusing Internet access to the detriment of work assignments is a choice and has consequences.

2. Privacy Policy

The privacy policy clearly defines what is and is not private when working on company equipment or when on company property. There are a variety of laws and regulations that address privacy. When privacy protection is

legally mandated, a company must enforce and protect privacy in compliance with the regulations. Some organizations choose to grant additional privacy beyond that mandated by law.

The privacy policy should include issues such as the use of security cameras, logging of user activity, recording of keystrokes, monitoring of Internet usage, etc. This policy defines what information is collected, what information is not collected, what can or cannot be disclosed, to whom information may be disclosed, and for what purposes the data was collected.

3. Password Policy

The password policy is directed toward improving the security of passwords. If the policy addresses topics beyond just passwords, it could be re-branded as an authentication policy.

A password policy defines the minimum length of a password, the types of characters allowed or required in the password, minimum and maximum age of the password, and the prevention of password re-use. The password policy might also include account lockout parameters that define the number of unsuccessful logon attempts granted before an account is temporarily or permanently disabled.

The password policy might also prescribe that password auditing or cracking be performed as a security assessment in order to discover weak passwords. Users should be trained on how to select more secure passwords. This would include selecting longer passwords and focusing on passphrases rather than individual words.

4. Disposal and Destruction Policy

The disposal and destruction policy defines when and how to get rid of stuff. There is always waste to be disposed of in every organization. Whether coffee grounds, sensitive printed documentation, or old storage devices, there needs to be a plan other than just tossing it in the bin.

Dumpster diving is a serious threat to security. Anything thrown away can be collected and examined by outsiders. Assume everything thrown out is obtained by your competitors, your enemies, and the government. With this in mind, define a procedure to properly dispose, destroy, and/or recycle everything.

Shredding and incineration are often solutions for both printed materials and storage devices. However, in today's green culture, companies seek to "zeroize" and re-use or recycle equipment whenever possible. (Note: to zeroize is to low-level format a storage device so that every single bit is reset to a zero value. This prevents all known concepts of data remnant recovery.)

5. Storage and Retention Policy

In addition to properly disposing of unwanted items, there is also a need for proper storage and retention of certain resources. Data, such as customer information, financial history, auditing data, etc., must often be retained for years or indefinitely. It is important to thoroughly plan out the technology, storage location, and security of the process of backing up and storing this information.

Often, law and regulations dictate what must be retained. Be sure to stay well within the lines of compliance. When in doubt, store more for longer under better security.

Often the storage and retention policy is interlinked with the privacy policy, especially when personally identifiable information is included in the retained data set. In such situations, disclosure about the personal data being stored may be necessary.

Keep in mind that secure storage is often offsite storage. Also, long-term storage can have unexpected consequences if the technology changes. Be sure to keep a working media device, backup software, and compatible OS software in storage along with all stored backup media. Consider whether you can still access those QIC or reel-to-reel backup tapes from the '90s or '80s. The situation is likely to repeat itself in the next 10 to 20 years.

6. Incident Response Policy

The incident response policy prepares the organization to respond properly when the inevitable security breach occurs. Here the adage "failing to plan is planning to fail" clearly holds true. If the company is not ready to respond to a security breach, then the loss will be greater, the recovery slower, and the risk of a complete company failure increased.

The incident response policy should define various levels of incidents and, generally, how to handle each. Low-level incidents might be managed automatically by the security infrastructure with minimal response from a human administrator. Mid-level incidents may require an internal corporate investigation. High-level incidents may require the involvement of law enforcement, legal evidence collection, and prosecution in court.

The incident response policy should address six key areas: preparation, detection, containment, eradication, recovery, and post-mortem review. The goal or purpose of this policy is to minimize downtime, reduce loss, and improve availability.

7. Classification Policy

Not every organization is a government or military agency or contractor, but every business can benefit from the use of a classification system. A classification system sorts and labels every resource with its value, importance, sensitivity, cost, and other concerns in order to guide the implementation of security and prescribe processes of management and use.

Assigning classification labels, such as public, private, sensitive, internal only, confidential, proprietary, etc., helps workers understand how to use and handle resources properly. Those resources with moderate to high value and sensitivity require greater control, tighter security, and stricter authentication.

Often classification can improve the organizations defense against social engineering and other information leakage attacks. If workers know that certain information cannot be communicated via instant message, e-mail, or over the phone, then most socially guided attacks through those mediums will fail.

8. Human Resource Policy

A human resource (HR) policy is often multiple policies tied together. HR issues include almost everything that directly relates to people, whether employees or not. HR policies should address hiring practices, such as how to seek out new workers; what level or depth of background investigation to perform; and the minimal education, experience, and capability requirements of each job position. The goal is to find ethical, reliable workers.

The HR policy should address ongoing supervision and management. How are employees monitored? What is used to measure their performance and/or success? What resources are made available for the employee to learn and improve? Are regular assessments performed? What are the consequences for violating a policy – whether accidental, due to ignorance, or intentional? This policy should also cover cross-training, job rotation, educational services, mandatory vacations, and other forms of auditing and oversight.

The HR policy should address termination. What must occur to legally justify termination? What is the process used to fire someone, disable their electronic access, and remove them from the facility? What evidence or records are retained in order to support the firing in the event of a wrongful termination suit?

An HR policy should also include a code of ethics. This is a general guideline for employees to follow whenever they face any sort of ethical dilemma. In most cases, the recommended action is to respond and perform in a manner that is legal. However, other considerations might include maintaining public opinion, benefiting the customer, and avoiding business loss. A code of ethics also prescribes a general minimal expected behavior, such as avoiding tardiness, completing tasks on deadline, and minimizing waste and loss.

9. Change Management Policy

One of the biggest threats to security is change or, at least, unknown, unmanaged, and uncontrolled change. Change can often result in a reduction of security. Change includes installation of new software, updating device drivers, application of patches, modifying configuration, and even physical reorganizations.

When change is not controlled and monitored, then security is at risk. A change management policy imposes a procedure to evaluate, test, and approve changes before they are allowed into the production environment. Organizations should adopt the rule that no software is ever installed before it has been tested and approved. This stance alone will prevent most internal causes of downtime and security failures.

10. Firewall Policy

Firewalls are essential components in a complete security structure. No security implementation is complete without integrated firewalls. The firewall policy dictates and defines how firewalls are to be implemented throughout the infrastructure.

A firewall should be considered mandatory on each and every host. Then, appliance firewalls should be deployed at strategic locations throughout the network at choke points, risk/trust level changes, and at any point where remote connectivity or external communication is possible. The firewall policy should dictate that a Deny by

Default stance be implemented. The policy should prescribe the rules set to limit activities to only those that support business activities.

Summary

Proper security exists only when it is written down. A written security policy, in fact, a large collection of individual written sub-policies, is the foundation upon which a viable real-world security infrastructure is based. Take the time, make the effort, and write it down. A written security policy serves as a guide, a measuring stick, and decision tool for not only security, but many other business decisions. Solid security starts with a written document.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:

Security+ Prep Course

Certified Ethical Hacker

CISSP Prep Course

For more information or to register, visit **www.globalknowledge.com** or call **1-800-COURSES** to speak with a sales representative.

Our courses and enhanced, hands-on labs and exercises offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 1,200 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and business training needs.

About the Author

James Michael Stewart has been working with computers and technology for over 25 years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses, such as CISSP, CEH, and Security+. He is the primary author on the CISSP Study Guide 4th Edition and the Security+ 2008 Review Guide. Michael has also contributed to many other CISSP- and Security+-focused materials, including exam preparation guides, practice exams, DVD video instruction, and courseware.

In addition, Michael has co-authored numerous books on other security and Microsoft certification, and administration topics. He has developed certification courseware and training materials and has presented these materials in the classroom. Michael holds the following certifications: CISSP, ISSAP, SSCP, MCT, CEI, CEH, TICSA, CIW SA, Security+, MCSE+ Security Windows 2000, MCSA Windows Sever 2003, MCDST, MCSE NT & W2K, MCP+I, Network+, and iNet+. Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in Philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of the-pants, hands-on, "street smarts" experience. You can reach Michael by e-mail at michael@impactonline.com.