Global Information Assurance Certification Paper

“I Am The Gatekeeper”

A Company Security Handbook

Michael Mietlicki, MCSE, MCP+I, A+
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4 (amended April 8, 2002)

Contents

NOTE -- This handbook is intended as a template for security personnel who do not have such a handbook in place. The intended targeted audience is the general user community who may not be aware of security issues. Specifics may vary at your company but this will serve as a guide and covers the most common user security points.

Abstract (About This Handbook)

This handbook will help all employees protect the company and themselves from business interruptions and liability caused by inappropriate use of data and information technology assets. It describes employee responsibilities for safeguarding computer equipment and information from accidental or intentional unauthorized disclosure, modification or destruction. It also describes appropriate and inappropriate use of company computers and information. Employees may be disciplined for non-compliance with these policies.

This handbook does not address every possible security issue. It is your responsibility to always use sound judgment. Should you come across an issue or situation that you feel may be a possible security issue, please report it immediately to your manager, the company help desk or a member of the Information technology department.

A Message to the Employee

Information and information assets are critical resources. Security and information security is everyone's responsibility, so we must all be aware of what it takes to do this important part of our job. With rapidly changing technology and the increased use of the Internet, there is an increased potential for virus attacks, intrusion from unauthorized personnel and other security issues. It is essential for all employees to help reduce security risks, prevent unauthorized use of information assets and prevent compromise of business operations. Accordingly, you should become familiar with this handbook and incorporate these guiding principles into your daily activities. Direct any concerns about the protection of information to your manager, the company held desk, computer security management or designated members of the company's information technology department.

These efforts will ensure the confidentiality, integrity and availability of information system resources and result in increased customer confidence and ensure successful performance of organizational responsibilities

Internet Background (1)

The Internet is the global network of networks, which uses the TCP/IP protocols or are able to work together and trade information and files by means of TCP/IP networks. It provides users with electronic mail, file-transferring capabilities, news, the World Wide Web and other associated services and utilities.
The Internet began in the last 1960's and was originally known as ARPANET. The initial intention was to link military installations for protected information sharing. During the 1970's and 1980's it expanded to universities and commercial organizations were seen in the 1990's. Today, the Internet, as we know it, is comprised of millions of computers.

Computer Security: the basics

The Goal

The goal for computer security is to prevent the unauthorized disclosure, modification, corruption, degradation, or destruction of information and information technology assets, whether by accidental or intentional means.

Elements of computer security (2)
Effective computer security is based on four (4) essential elements:

Confidentiality, Integrity, Availability and Authentication

Confidentiality means assuring information will be kept limited to users who have a business need to know. The tides have shifted and a majority of security breaches come from within organizations, whether by intentional or unintentional means and these internal events can be prevented. While working at your computer, using a password protected screen saver on your system or pressing <CTRL>-<ALT>-<DEL> keys to lock the workstation before leaving your office is recommended.

Integrity means ensuring that information will not be accidentally or intentionally changed or deleted. The accuracy of information is paramount to goals of the organization and a sound business practice is to have the information always accurate and available should it need to be recovered from a tape backup or other method, such as a database dump or a drive device mirror configuration. These measures sometimes take place following an accidental file or folder deletion or unauthorized breach with the intent to alter data.

Availability addresses access to data and applications. Through measures implemented by the Information Technology staff, a "high availability" posture has been implemented to ensure that when a user or client needs to have the most current and accurate information, that information can be delivered when it is requested.

Authentication allows resources such as printers, designated directories or drives in a computer system or entire systems to be restricted to specific users. The most common form of authentication is a login and password combination that verifies user information. The following are three basic examples of authentication:

Something you have	Identification card, credit cards, ATM cards
Something you know	Passwords or personal identification numbers (PINs)
Something you are	Fingerprints, voiceprints or retinal scans

Unfortunately, these authentication items are common targets of individuals whom possess the intent of taking these from you. They are known as social engineers and will use all possible means to extract information under the guise of honesty and goodwill but have no intention of remaining that way once they have what they are after. Protect your authentication and identity items carefully and do not disclose them to anyone.

Employee responsibilities

You hold the key

Every employee is responsible for computer security. Management and the information technology organizations establish policies and guidelines but successful implementation of those guidelines are dependent on every employee. Employee responsibilities are:

- Maintaining confidentiality
- Managing your passwords
- Limiting access to shared files
- Backing up your files
- Locking your office and files
- Maintaining your equipment
- Communicating responsibly
- Protecting against viruses
- Respecting software licenses
- Monitoring security advisories

Each of these items is outlined in detail in the following sections.

Maintaining confidentiality

During the course of your employment, you may have access to or become familiar with confidential or proprietary information regarding business operations and those of our clients. This information may include customer lists, subscription lists, contracts, policies, financial statements, projections, plans, strategies, methods and so on. It is every employee's responsibility to not disclose any confidential information, directly or indirectly and to avoid using the information except as required in the course of your employment.

Managing your passwords [3]

Passwords are your personal "something you know" means of authentication. It is important that you choose appropriate passwords and change them on a regular basis. Here are some guidelines to help you:

- Use a password that is easy to remember and difficult to guess (i.e. – pokeywasthehorse) – all one word.
- Use a password with a mixture of alphabetic and non-alphabetic characters (digits and punctuation). (i.e. – X21b!u@s9)
- Use a password of at least 8 characters (i.e. – M!k1Ew@sh37e)
- Change your passwords at regular intervals. Contact your company help desk or designated Information Technology representative for the suggested interval and assistance, if required.
- Change all vendor-supplied or default passwords on a computer prior to connecting to the network. Many "hackers" will use the built-in accounts and their default passwords on operating

systems to breach computer systems. Once they have access to a computer, they have access to whatever network connections and information the user has access.
- Change your password immediately if it has been disclosed (or if you suspect it has been disclosed) to anyone.

Additionally, there are several things you should not do when managing passwords:

Do not:
- use your login name in any form as a password (i.e. – reversed, capitalized, doubled and so on)
- use your first or last name in any form (i.e. – Michael01)
- use other personal information that can be easily obtained. This includes license plate numbers, birth dates, names of spouses, children or pets, telephone or social security numbers, zip code, your street name and/or address.
- use a password of all digits or all the same letter (i.e. – 77777777)
- use a single word contained in English or foreign language dictionaries, spelling lists or other word lists. Password cracking programs use standard dictionary words and combinations thereof as their points of reference in attempts to uncover passwords.
- write down your password and leave it where unauthorized personnel might have access to it. The most common mistake is writing down your system password on a "post-it" note and sticking it in plain site, usually on the edge of the monitor and under the keyboard where it is "hidden" is the 2nd most common place where anyone who is in the building having the intent of breaching your system will look. If you must write it down to remember it, keep it on your person at all times.
- share your passwords with anyone. There should never be a need for an administrator to request disclosure of your password over the phone. Such requests should come on a one to one basis, where you can verify the identity of the person.

Limiting access to shared files

Microsoft Windows file sharing features allow you to share part or all of your hard drive over a network. While this facilitates collaborative work, it can also result in a significant security exposure. If you share "read access" to your entire C drive, everything on your drive is at risk of disclosure. If you share "full access" to your entire C drive everything on your drive is at risk of disclosure, modification or deletion. Additionally, software is widely available on the Internet that allows anyone with access to the LAN (local area network) to hack into password-protected files. Some recent viruses can identify unprotected, writeable shares on a network and delete the related files or infect the machine.

It is strongly encouraged that you implement the following precautions:
Password protect or limit user/group access to shared directories and files, share only directories and files that must be shared, allow read only where possible, never share your entire C drive with "full control" granted to everyone… not even for a few moments.

(Contact your user support group for directions and/or assistance)

Backing up your files

Any file that contains business information should be backed up. If your files are saved to a file server then it is likely that they are already being backed up. If you save to your local hard drive, you should also save to your network home directory. Files can also be backed up onto floppy disk or other removable media backup, which should then be locked in your desk drawer or overhead cabinet. (See the following section)

Locking your office and files

Physical security measures play an important part in the overall information security scheme. Diskettes and other removable media containing sensitive information should never be left on your desk or anywhere in the open. All removable media should be secured behind a locked drawer or cabinet. Do not leave this key in the office, take it home with you. A copy of the key may also be left with your manager. Sensitive information should be secured anytime you leave the office, not just when you go home.

Locking your computer when leaving the office is another practice that should become habit. In Windows NT, 2000 and XP press the <CTRL> <ALT> <DEL> keys to display the windows security dialogue box and select "Lock Workstation" or "Lock Computer". You can now leave your area knowing the system is secure. On Windows 95 and 98 machines, you can set a password lock on your screensaver and adjust the activation time for a few minutes.

Maintaining your equipment

It is very important to keep your computer in good working condition. Do not leave liquid near your keyboard or computer even if it is in a sealed or spill-proof container. Do not eat close to your keyboard or mouse… crumbs can be as damaging as liquids.

Diskettes that you use on a regular basis should be retired after six months. Copy the information, verify the copy was successful and then erase and discard the old floppy. Any diskette that begins to show errors in reading should be immediately copied verified and destroyed. Under no circumstances should you discard a diskette that contains data in the trash. CDs that are being discarded should be snapped in half before being discarded.

If your hard drive begins to give you trouble, immediately report the trouble to your company help desk or user support group and then back up your data to your network home directory.

Communicating responsibly

Email guidelines

E-mail has rapidly become the principal means of communication, is a strategic company resource and should be treated as such. E-mail servers are normally backed up on a regular basis however if you save or archive messages locally, such as to an offline folder, you should back up the folder in the same manner as any other sensitive information (see "Backing up your files" on page 7).

E-mail is also a tactical resource and, as such, produces many documents of limited life span (project related e-mail). Periodically, you should go through your inbox and remove messages that have exceeded their usefulness. Some can be simply deleted; others may have historical importance, in which case you should archive them.

E-mail may sometimes be used as a personal resource… this is recognized. A certain amount of personal (non-business related) e-mail may be acceptable in accordance with local company policies. Please use good judgment on this, keeping in mind that your computer is a company resource, not a personal one, you are on company time and correspondence may be subject to monitoring and review.

E-mail can also be time consuming. There is a tool available to help you deal with email efficiency – filtering. Filtering lets you set up rules and the system will automatically filter messages according to those rules. Example: "spam" (unsolicited email messages) can be deleted before you ever see it. Messages can be sorted by sender or other criteria and place specific messages into various folders that you can read based upon your own priorities.

Appropriate Use

Employees are expected to use electronic and telephonic communications equipment and facilities for legitimate business purposes in a manner that is consistent with company policies and procedures. While respecting your privacy and understanding that employees should have a reasonable expectation of privacy, communications may, from time to time, be monitored or intercepted and a review of the use of electronic communications may follow to ensure that usage is consistent with legitimate business interests.

Inappropriate use [4]

All users are expected to conduct themselves professionally and are to refrain from using office equipment, the Internet and e-mail systems for activities that are inappropriate, which includes, but not limited to: Use that could cause congestion, delay, or disruption of service to any system or equipment, i.e. -- Greeting cards, videos or other large file attachments can degrade the performance of the network. Continuous data streams (i.e. – Internet radio and ticker tape banners such as weather and stock information) can also degrade network performance.
Creating, transmitting or forwarding chain letters or other unauthorized mass mailings, regardless of subject matter.
Any illegal or offensive activity that is offensive to fellow employees, clients, contractors or the public. This includes any messages that deride others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
Creating, downloading, viewing, saving or transmitting sexually explicit or sexually oriented materials.

Gambling, weapons, terrorist activities and any other illegal activities.
Use for profit or outside employment or outside business activity.
Any outside fundraising activity without authorization or endorsing any product or service.
Posting company information to newsgroups or other public forum without authority.
On-line games, false self-representation, interfering with any employee's duties or the operation of Internet gateways and any type of personal solicitation.

Protecting against viruses

You are connected to the Internet. You can exchange documents with others. You have e-mail. Therefore, you are vulnerable to viruses. You are required to run the company standard anti-virus program on any machine that contains company documents, email and that connects to the network, whether locally or remote. (Further detail on this will be provided in an upcoming section).

Viruses are becoming more prevalent and virulent every day. While technology can do a great deal to keep resources safe, it is still up to you to follow a few simple best practices:

Do not download software from questionable sites. This particularly applies to games, screensavers, backgrounds, icons and other "cool stuff" that is widely available.

Never open e-mail attachments from someone you do not know. Additionally, do not open an attachment from someone you DO know if you cannot verify that the person intended to send you that attachment and that it is work related. Be suspicious of attachments that will show you something cute, funny or exciting and spicy.
Never double click the attachment. This has been known to be the easiest way to unwittingly infect your own workstation system and spread malicious code from your machine. Instead, save the attachment to a known local location (your hard drive), open the program that is normally associated with the type of file and then open the attachment through the program.

Respecting software licenses

It may be the policy of your company to not accept or use hardware, software, data or other information belonging to another company without that company's written consent. Additionally, software that is not properly licensed may not be allowed nor copying of software for use at home except as expressly stated in the license agreement and your company's software usage policy.

Monitoring security advisories

Most likely, there is a method of posting security and virus advisories and practices. You should monitor these posting on a regular basis to avoid a potential unnecessary threat and protect your computer.

Security outside of the office

Telecommuting

Before you telecommute, you must make your computer secure from other who may have access to that system. Any time you are connected to the Internet, you are vulnerable to attacks by hackers attempting to take over your machine for their own purposes or a greater cause.

If you are dialing into a company modem pool, you are most likely protected. If you are connecting via a cable modem or a DSL connection or dialing into a public Internet Service Provider (ISP), you will require a firewall. This is either hardware or software that filters out attacks, blocking them before they can harm your computer or hijack your secure session. Any computer-to-computer communication over the network must conform to individual company security requirements. This may include connecting via a Virtual Private Network (VPN) connection. User support, security administration or network administration personnel should have information on the company requirement.

Backup procedures are as important at home as they are in the office. Make sure you have duplicate copies of any work … one on your hard drive and one on floppy or other removable media option.

Approved anti-virus programs and updated virii pattern files must be run on any home system that will be connecting to the network.

Traveling

Always hand-carry your laptop. Pay strict attention when passing through airport security scanners, especially when you have to put your laptop, PDA or other device o the x-ray scanner. Thieves often work in pairs… while one stalls you, the other is scooping up your equipment. Remain alert. Similarly, always carry your laptop yourself. Never let anyone else carry it for you, even if the seem to be airport employees. This has changed a bit since 9/11 but again, remain alert. Use the security features on PDA's and laptops so unauthorized use may be prevented if they are lost or stolen and report losses and thefts immediately.

Awareness and ongoing training [5]

Delivery of awareness programs

It only takes a single lapse to put the organization's data and information resources at risk. Therefore, ideally, staff would develop their awareness of Information Security risks so that it almost becomes second nature. The task of developing the awareness program and providing ongoing training to the user community is part of the responsibilities of the information security staff and designated information technology personnel.

Through the implementation of this program, the potential for critical impact on data and information assets is lessened by the following actions as part of an overall comprehensive awareness program.

As part of an overall comprehensive security awareness package, the information security staff will ensure that a focus on information security issues is maintained by providing the distribution of regular security notifications, appropriate 'change of function' training prior to commencing new duties, a mandatory receipt of Information Security Education for you to initial, Information Security awareness training products and programs to ensure that information security issues are in mind. Further attention will be presented by briefing all personnel and contractors who will have access to sensitive company systems, information, or assets, training using available multi-media (classes, web pages, on-line documents and video), [6] regular training intervals and as part of your new employee orientation program, training to support staff, users and managers, on appropriate levels. Additionally, the IS staff will review its security training procedures regularly to ensure they are up to date and relevant.

All associates will be scheduled for the mandatory annual security training. Upon conclusion of this instruction, managers will make certain that the proper documentation indicating the completion of the training is sent to HR for insertion in the individual's personnel file. [7]

These measures are an element of the information security training you will receive and at unannounced intervals, periodic testing of security issues and standards will be conducted to maintain the level of focus and awareness of current issues and best practices.

Contacts and resources

If you need help…

The following is a template for your use and presents some of the resources through which you can get more information or solve specific security related issues. Maintaining this list and knowing who to contact can reduce the impact of a possible breach of security.

Resource	Contact Information	Description
Your Manager	Name _____ Phone _____ E-mail _____	Immediate Supervisor
Company help desk	Phone _____ E-mail _____ URL _____	To report potential security issues, acquire software, hardware and technical assistance
Information Technology Personnel	Networking _____ E-mail Admin _____ Backups _____ Security _____	Possible escalation point for security events if help desk personnel are not available
Computer Security Management Staff	Name _____ Phone _____ E-mail _____	Designated security staff personnel
Security Director	Name _____ Phone _____ E-mail _____	Director or Manager of Security

References

(1) - Internet Background
Internet Security Policy: A Technical Guide – 1. Introduction
http://secinf.net/info/policy/isptg.en/ISPTG-1.html#Heading5

(2) - Elements of Computer Security
Excerpts and definitions based upon and extracted from:
Information Security Policy and Standards Information Systems and Technology
University of Waterloo
http://dcs.uwaterloo.ca/security/bcp/info.html

(3) - Managing passwords - Concepts based upon:
"Managing Windows NT Logons" By Kathy Ivens 1st Edition January 2000 ISBN# 1-56592-637-4
Chapter 2 – Password Problems
http://www.oreilly.com/catalog/ntlogon/chapter/ch02.html

(4) - Inappropriate Use
Excerpts from:
United States Department of Agriculture – Natural Resources Conservation Service
National Information Security Handbook
PART 602 - INTERNET USAGE AND E-MAIL GUIDELINES
Section 602.5 – Inappropriate Usage
http://public.nrcs.usda.gov/scripts/lpsiis.dll/H/h_270_602.htm
(Information and items used as a template. Portions changed to reflect non-government terminology)

(5) - Awareness and ongoing training
Concepts and excerpts from:
RUSecure Evaluation Security Online Support Evaluation
Information Security Policies .... full policy evaluation copy

(6) - Portions excerpted from SANS Institute Network Security Roadmap Poster:
http://www.sans.org/newlook/publications/roadmap.htm

(7) - Information Security Policy Manual
by Edmond D. Jones ISBN# 1-931-332-09-6
Published by The Rothstein Catalog On Disaster Recovery
EXCERPT - SAMPLE POLICY: SECURITY AWARENESS AND TRAINING PROGRAM
http://www.disastercenter.com/Rothstein/cd524a.htm

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event