Global Information Assurance Certification Paper

SANS Institute

SANS Security Essentials
Practical Assignment
Version 1.2f

Congratulations to the New Security Manager

Practical

Nancy J. Carpenter
Original Submission
September 24, 2001

Congratulations to the New Computer Security Manager
N. J. Carpenter
September 24, 2001

CONGRATULATIONS!
You've been chosen to be the new
Computer Security Manager

Great! I can't wait to get started. I can defend the company against the hackers. What an opportunity to be in tune with the newest technology. This is going to be great! I can't wait learn all this great new high-tech stuff. I'll keep the company safe and be a hero!

What a shock the new Computer Security Manager is in for! The new manager may not realize the responsibility; potential pitfalls and risks that may be embedded in the new job!

- Does the company have a Security Policy?
- Is computer security important to your company? Does the security plan have executive support?
- Is there a security budget, or is a cost to be minimized?
- Was there a previous Security Manager? If so, what happened to the previous Security Manager?
- Do you understand computer and information security? Do you understand security in general?
- Do you understand the nature of the risks and consequences?
- Do you have a dedicated security staff? Is the staff's expertise adequate?
- Has the security function and responsibility been outsourced?
- Do you have trusted and experienced resources?
- Should you accept the current security policy?
- Is the current policy being properly executed?
- Have there been security incidents? What was the cause? How were they handled?
- What are the legal ramifications?
- What are the financial implications?
- Do you have any experience in Computer Security Management?
- Does the company have Security Procedures?

These scary questions are intended to help you determine your state of your readiness for your new position as well as the computer security readiness of your company. Many of these questions you can answer with the corporate knowledge you may

already have. Answer those first because they may lead to other questions. After you have answered the easy, corporate questions move on to the security questions.

If you are uncomfortable with any of your response to the questions dealing with Security Policy, you should waste no time in obtaining computer and information security training. Run don't walk. Make it a top priority. Becoming a Computer Security Manager with little or no background or experience will be akin trying to catch a speeding train on horseback. Oh, and don't forget you have to fend off the attackers at the same time.

> "The System Security Policy is the basis for the legitimate application of security measures designed to protect your network from both internal and external threats. Without the definition provided by the policy document there is a very good chance that a security measure that should be implemented will be missed or you will implement measures that are not required, expensive and the cost can outweigh the benefit."
>
> David Milford

Where to Start - Learn about Computer Security Policy

If you don't understand Computer Security Policies or what security includes, there are many excellent resources that are free or very low cost. Spend some time researching what is available. This paper will outline the general requirements, information resources and examples.

An extensive information resource is the Internet. Several powerful Internet search engine are http://www.google.com/ or http://www.dogpile.com/. Enter *Security Policy* in the window. Here you will find online resources, books, presentations, consultants, complete programs to purchase and full service companies that will complete the entire process for you.

Sans Institute Reading Room – Security Policies Issues – Here you find a lot of helpful reading. http://www.sans.org/infosecFAQ/policy/policy_list.htm

Evaluate Your Security Policy

Ask for your companies Security Policy and Procedures. Hopefully you will receive a copy of the policies and procedures, and not a long of string of excuses as to why they're not available or complete. With the policy now in hand, you can begin to evaluate the charter and responsibility of your new position. If you are unlucky enough to receive little or nothing, the following information will help you create a Security Policy.

With an understanding of Computer Security Policies, you can begin to evaluate the Security Policy that may already be in place.

Security polices can be lengthy and hard to understand, or short and to the point, but they should all contain some basic and essential points. The *Sans Security Essentials (*http://www.sans.org) training includes the *GIAC Basic Security Policy*, which may be used as a starting point of reference. The GIAC Basic Security Policy outlines basic points that should be covered in a basic policy:

- Purpose – The purpose will usually state the reason for the policy and the goals
- Policy Statement - Identify the guiding principles and what is to be done. This section should set forth actions that are prudent, expedient and advantageous to the organization.
- Responsibility – This section should describe who is responsible for the policy. This is usually a member(s) of the executive management. Other topics that may be included in this section are effective dates and update requirements.
- Background – This section may describe reasons why the policy was instituted or refer to other occurrences or documents.
- Scope – A statement that describes the range of the Security Policy is important. It should describe the depth and breadth of the policy.
- Cancellation or Revision Status – The status of the policy and what is in effect needs to be clearly stated. This may include new, revised or perhaps superseded policies. Dates and a short description of changes may be included.
- Related Documents – This is an important section that can reference higher-level policies, implementation guidelines or government documents.

The Department of Energies *Cyber Security Policy Management Policy* is illustrative of the basic security policy discussed above. This policy can be found at http://www.directives.doe.gov/pdfs/doe/doetext/neword/205/p2051.pdf

Not that you've taken the first steps toward learning about Security Policy or reviewing your own Security Policy, you're ready for the next step of Implementation or the 'How To'.

Security Procedures – The 'How To' Implement the Security Policy

> "Having a security policy document in itself is not enough.... the contents MUST be implemented to be effective. This is often easier said than done! The fundamental question is how to deploy the policies - how to deliver them. This is critical, as undelivered or badly delivered policies might as well not exist. "
>
> Information Security Policy World

Security Procedures are the 'how to' tools used to implement a Security Policy. A

Security Policy without Security Procedures is like making an apple pie, without a recipe – you may forget the spices. The Policy and Procedures go hand in hand.

For example, your Security Policy may specify a requirement for 'Controls to Protect Assets' or user authentication. Password protection is one way to protect assets. It's not enough to simply specify password protection, you must specify in detail how this is to be implemented in the Security Procedure for Password Protection. The Password Procedure may specify:

- Minimum Password Length
- Character requirements
    - Upper and lower case requirement
    - Requirement for numeric character
    - Requirement for special character
    - Positional requirements, i.e. special character in first and last positions
- Maximum and Minimum age of password
- Password Uniqueness – The user can't reuse the last x number of past passwords
- Account Lockout – The number tries does the user get before lockout
- Maximum number of days a password is valid
- The use of dictionary words

Examples of Basic Security Policy and Procedures

A Security Policy and Procedures handbook is being developed by the Site Security Policy Handbook Working Group (SSPHWG) and is a combined effort of the Security Area and User Services Area of the Internet Engineering Task force (IETF). RFC2196 is the current issue. The previous issue, RFC1244, contained an excellent of basic security policies and procedures in the table of contents. The table of contents from the RFC1244, Site Security Handbook, is reproduced in Appendix 1 as an illustrative example of basic Security Policy and Procedures. This RFC1244 is a first attempt at providing Internet users guidance on how to deal with security issues in the Internet.

Careful examination of this table of contents demonstrates most of the Security Policy is Sections 1, 2 and other sections at the end of the table of contents. Sections 3-6 outline the procedures used to implement the Security Policy.

The Sans Institute provides online downloadable Security Police and Procedure templates that can be used as a starting point for your security policy. This is an excellent resource for samples of 'how to' implement many aspects of a Security Procedures. http://www.sans.org/newlook/resources/policies/policies.htm

As you can see, Security Policy and Procedures range from high-level corporate policy

to very detailed implementations.

Baselining Security Policy and Procedure Effectiveness

Now you have a complete and comprehensive set of Security Policies and Procedures you can relax. Wrong! Would you feel comfortable if your credit card company told you that it never makes mistakes and you can always trust their statements? Would you feel comfortable with a rescue organization that never trains? You should feel the same way about your Security Policies and Procedures.

> "All too often, security policy and similar documentation becomes shelfware; that is, it fulfills the organization's requirement that it have a policy, without achieving acceptance as a functional tool. So, if asked, the security manager can say, "yes, I have a security policy" (or contingency plan or incident response plan, etc.), "and there it is on my bookshelf." But when tasked with making a security decision or responding to a crisis, this manager will rely on his own expertise, rather than referring to the written documentation."
>
> Gary Desilets

As the new Computer Security Manager it is prudent to baseline your Security Policies and Procedures.

- Are they shelfware?
- Are they current? An annual review and update is usually sufficient unless major changes occur in your system or technology.
- Have the responsibilities changed? They have. You are the new Security Manager.
- Do they provide enough detail? For instance, is the Incident Response list up to date?
- Have they been tested? Testing the procedures during an emergency may not be the approach you want to take.

The baseline can be accomplished through System Security Audits. (Note section 4.1 in the table of contents of the Site Security Handbook, Appendix 1). Your Security Procedures should contain the details and requirements for System Security Audits. In many companies internal auditing is an ongoing activity. For some government agencies and contractors this is a requirement.

How to Check Compliance with your Security Policy, by Krishni Naidu, is another excellent source of information on the subject of verifying Security Policy compliance.

Internal audit teams can perform security audits. Contracted resources can perform audits. And last, but not least, your client or customer may perform surprise audits. The basis for the audit will be the current Computer Security Policies and Procedures.

Some areas that may be of particular interest to auditors are:

- Access and Perimeter Control – May include
  - Firewalls
  - Physical access to servers, network and workstations.
- User Authentication
  - Password verification
- Vulnerabilities & Configuration Control
  - Vulnerability scanning, servers and workstation
  - Latest Security patches installed
  - Latest upgrades and service packs installed
- Continuity of Service
  - Operating System Hardening
    - Security Parameters Set
  - Incident Response
    - Response list current
    - Response details appropriate for current threats
  - Backup and Recovery
    - Backup instructions
    - Backup media marked and properly stored
    - Restoration test
- Security Monitoring
  - Host security controls
  - Intrusion detection
  - Firewall logs
  - System security logs
  - Syslogs are monitored
  - Access logs are monitored
- Training
  - User Training
    - Security policy / procedure requirements
    - Incident Response
    - User signed acknowledgement of requirements
- Malicious Code
  - Virus update procedures
  - E-mail monitoring
  - System scanning
  - Latest Virus Protection is installed
    - Servers

        - Workstations
- Hardware & Software Control
    - All hardware is identified and inventoried
    - All software is identified and inventoried
- Internal Audits & Results

Maintaining Current Security Policies and Procedures

Section 6 of RFC2196, Site Security Handbook, lists activities that can aid in keeping your Security Polices and Procedures up to date. The list from RFC2196 follows:

1. Subscribe to advisories that are issued by various security incident response teams, like those of the CERT Coordination Center, and update your systems against those threats that apply to your site's technology.

2. Monitor security patches that are produced by the vendors of your equipment, and obtain and install all that apply.

3. Actively watch the configurations of your systems to identify any changes that may have occurred, and investigate all anomalies.

4. Review all security policies and procedures annually (at a minimum).

5. Read relevant mailing lists and USENET newsgroups to keep up to date with the latest information being shared by fellow administrators.

6. Regularly check for compliance with policies and procedures. This audit should be performed by someone other than the people who define or implement the policies and procedures.

Summary

Welcome to your new job! As you may have realized by now, the job of a Computer Security Manager is very complex, and ever changing. This is a role that is evolving as our technology advances. The problems and challenges that you face today will be quickly replaced by tomorrow problems. Keep your eye on evolving technology and your backdoor. There will always be someone new at the backdoor as long as you are connected to the outside world.

Find the best possible resource possible to assist and guide you. You will find the job very rewarding, challenging, and at times nearly impossible. Good Luck!

APPENDIX 1.

1991-11-08 IETF RFC 1244 - Site Security Handbook
http://csrc.nist.gov/secplcy/rfc1244.txt

This handbook is the product of the Site Security Policy Handbook Working Group (SSPHWG), a combined effort of the Security Area and User Services Area of the Internet Engineering Task Force (IETF). This FYI RFC provides information for the Internet community

The text following is the Table of Contents for the RFC 1244 Site Security Handbook. Note: RFC 1244 has been replaced by RFC 1296. The Table of Contents presented for illustration of Security Policy details.

Finally, we intend for this FYI RFC to grow and evolve. Please send comments and suggestions to: ssphwg@cert.sei.cmu.edu.

Table of Contents

1. Introduction..... 3
1.1 Purpose of this Work..... 3
1.2 Audience..... 3
1.3 Definitions..... 4
1.4 Related Work..... 4
1.5 Scope..... 4
1.6 Why Do We Need Security Policies and Procedures?..... 5
1.7 Basic Approach..... 7
1.8 Organization of this Document..... 7
2. Establishing Official Site Policy on Computer Security..... 9
2.1 Brief Overview..... 9
2.2 Risk Assessment..... 10
2.3 Policy Issues..... 13
2.4 What Happens When the Policy Is Violated..... 19
2.5 Locking In or Out..... 21
2.6 Interpreting the Policy..... 23
2.7 Publicizing the Policy..... 23
3. Establishing Procedures to Prevent Security Problems..... 24
3.1 Security Policy Defines What Needs to be Protected..... 24
3.2 Identifing Possible Problems..... 24
3.3 Choose Controls to Protect Assets in a Cost-Effective Way..... 26
3.4 Use Multiple Strategies to Protect Assets..... 26
3.5 Physical Security..... 27
3.6 Procedures to Recognize Unauthorized Activity..... 27
3.7 Define Actions to Take When Unauthorized Activity is Suspected.. 29
3.8 Communicating Security Policy..... 30
3.9 Resources to Prevent Security Breaches..... 34
4. Types of Security Procedures..... 56
4.1 System Security Audits..... 56
4.2 Account Management Procedures..... 57

4.3 Password Management Procedures..... 57
4.4 Configuration Management Procedures..... 60
5. Incident Handling..... 61
5.1 Overview..... 61
5.2 Evaluation..... 65
5.3 Possible Types of Notification..... 67
5.4 Response..... 71
5.5 Legal/Investigative..... 73
5.6 Documentation Logs..... 77
6. Establishing Post-Incident Procedures..... 78
6.1 Overview..... 78
6.2 Removing Vulnerabilities..... 78
6.3 Capturing Lessons Learned..... 80
6.4 Upgrading Policies and Procedures..... 81
7. References..... 81
8. Annotated Bibliography..... 83
8.1 Computer Law..... 84
8.2 Computer Security..... 85
8.3 Ethics..... 91
8.4 The Internet Worm..... 93
8.5 National Computer Security Center (NCSC)..... 95
8.6 Security Checklists..... 99
8.7 Additional Publications..... 99
9. Acknlowledgements.....101
10. Security Considerations.....101
11. Authors' Addresses.....101

Sources Cited:

GIAC Basic Security Policy, 1.35, September 5, 2000 – SANS Security Essentials Certification I

Gary Desilets. *Shelfware: How to Avoid Writing Security Policy and Documentation That Doesn't Work, April 20, 2001*
URL http://www.sans.org/infosecFAQ/policy/shelfware.htm

David Milford. *A System Security Policy for You*, April, 25,2001
URL http://www.sans.org/infosecFAQ/policy/sys_sec.htm

Krishni Naidu. *How to Check Compliance with your Security Policy*, January 30, 2001
URL http://www.sans.org/infosecFAQ/policy/compliance.htm

Information Security Policy World
URL http://www.information-security-policies-and-standards.com/

INFOSYSSEC – The Security Portal for Information System Security Professionals
URL http://www.infosyssec.org/infosyssec/secpol1.htm

James G. Natoli. Role of the Information Security Officer, February 26, 1999
URL http://www.irm.state.ny.us/policy/99-2.htm

RFC 1244 – Site Security Handbook, Network Working Group, July 1991
UFL http://www.cis.ohio-state.edu/htbin/rfc/rfc1244.html

RFC 2196 – Site Security Handbook, Network Working Group, September 1997
URL http://www.faqs.org/rfcs/rfc2196.html

Business Security Advisors Magazine, Dr. Bruce V. Hartley. You Need a Corporate Security Policy, June 1998
URL: http://www.advisor.com/Articles.nsf/aidp/HARTB03

The Threat of 'Infowar' – Secure your Online Assets Dimension Data – Industry View
URL http://www.didata.com/thoughtleadership/showresult.asp?QuesID=39

CERT Coordination Center, Carnegie Mellion
URL http://www.cert.org/nav/index_main.html

Department of Energy – Unclassified Computer Security Program, DOE N-205-1, dated 7/26/1999, extended to 12/31/2001
URL http://www.directives.doe.gov/pdfs/doe/doetext/neword/205/n2051.pdf

Department of Energy, Cyber Security Architecture Guidelines, March 8, 2001
URL http://www.directives.doe.gov/pdfs/doe/doetext/neword/205/g2051-1.pdf

SANS Institute:
URL http://www.sans.org
SANS Institute, Information Security Reading Room
URL http://www.sans.org/infosecFAQ/policy/policy_list.htm
SANS Model Security Policies
URL http://www.sans.org/newlook/resources/policies/policies.htm

Search Engines:
URL http://www.google.com/
URL http://www.dogpile.com/

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
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 Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 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 Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 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	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	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