Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Information Security Officer Training
GISO–Basic Practical Assignment
Version 1.1 (December 12, 2001)
SANS Boot Camp, San Diego, CA October 2001

I'm Not Big Brother – I'm Short Sister

Information Assurance Security Policy
For GIAC Enterprises

© SANS Institute 2000 - 2002, Author retains full rights.

Presented by:
Dawn M. Stanko
24 December 2001

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ASSIGNMENT 1: DESCRIBE GIAC ENTERPRISES

1.0 Introduction

Assignment 1 introduces GIAC Enterprises by briefly describing GIAC Enterprises and its business, providing a diagram of its Information Technology (IT) infrastructure, listing its major IT components and describing its operational IT requirements.

1.1 Description of GIAC Enterprises

GIAC Enterprises is a "growing internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings. They have recently acquired an established fortune cookie sayings company China Sayings, Inc."[1] GIAC Enterprises has approximately 300 employees.

1.2 My Role in GIAC Enterprises

I am the new Information Systems Security Officer (ISSO) of GIAC Enterprises. Since I'm a staff of one, I have to rely on a matrix organization to accomplish security tasks. I've been the ISSO for approximately 3 months.

1.3 Information Technology (IT) Infrastructure

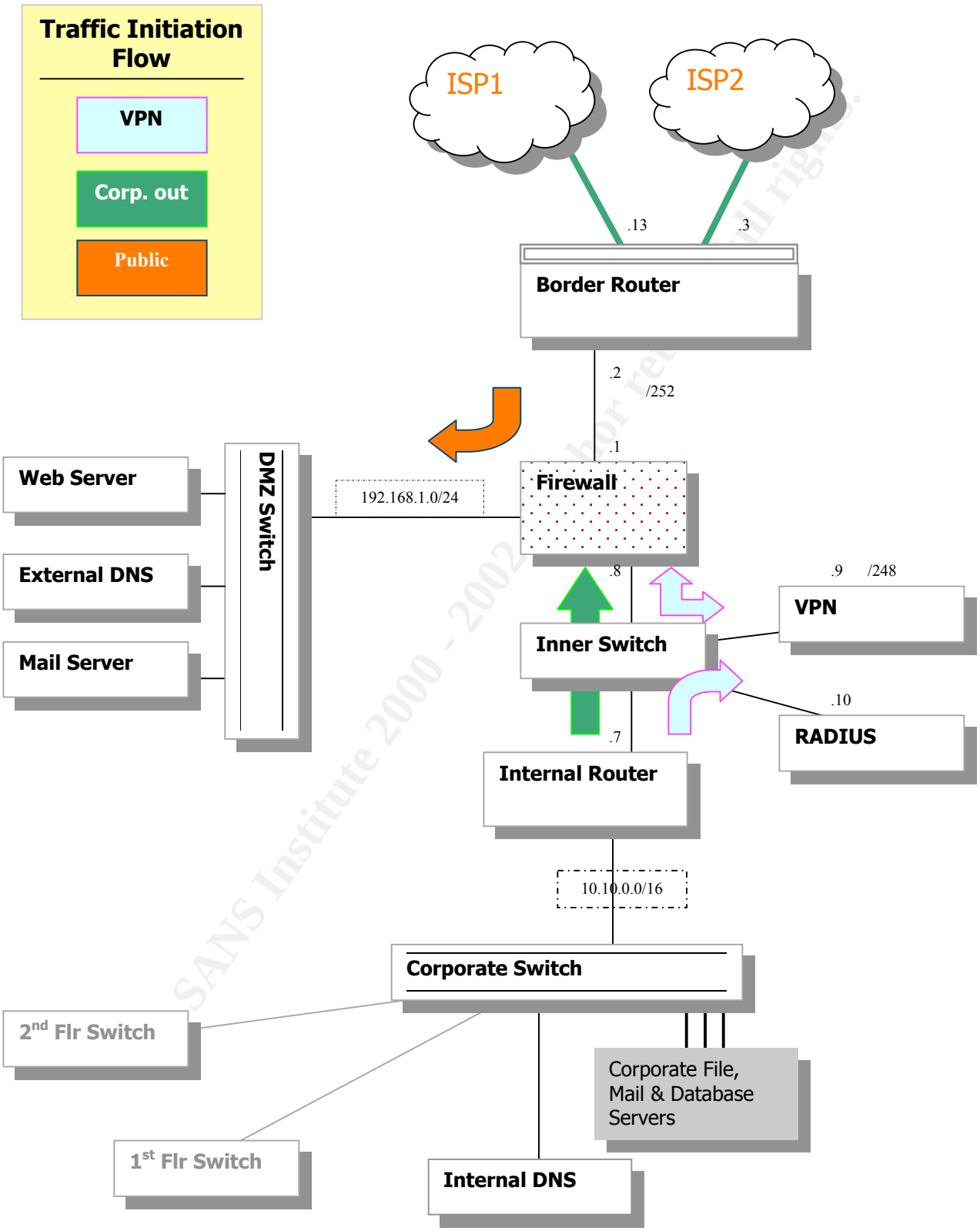
The Information Technology (IT) infrastructure supports 600 nodes. The infrastructure has recently migrated from Windows NT to Windows 2000 architecture. The Network Manager provided me the network diagram of GIAC Enterprises Information Technology Infrastructure in Figure 1.

© SANS Institute 2000 - 2002, Author retains full rights.

[1] Loring_Rose_GCFW.zip URL: http://www.giac.org/GCFW.php/

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Figure 1: GIAC Enterprises Information Technology (IT) Infrastructure[2]



[2] Tracy_Thurston_GCFW.zip URL: http://www.giac.org/GCFW.php/

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1.4 List of Major IT Components

The Network Manager also provided a list of the major IT components used at GIAC Enterprises in Table 1.

Device	Hardware	Software
Border Router	Cisco 3620	12.2.3
Firewall	Cisco PIX 515	6.0.1
VPN	Cisco VPN 5002	6.0.19
External DNS	Dell Pentium 4	Windows 2000 Server (SP2)
Internal DNS	Dell Pentium 4	Windows 2000 Server (SP2)
Internal Router	Cisco 3620	12.2.3 fw/ipsec plus
RADIUS	Cisco Secure ACS	Cisco Secure ACS v2.6 Windows 2000 Server (SP2)
DMZ Switch	Cisco 2924	12.1.9
Web / SSL Server	Dell Pentium 4	Windows 2000 Server (SP2) IIS5
Corporate Switch	Cisco 2948	12.1.9
Mail Servers	Dell Poweredge, Pentium 4	Window 2000 Server (SP2) Microsoft Exchange 5.5 (SP4)
Database Servers	Dell Pentium 4	Windows 2000 Server (SP2), MS SQL Server 2000 (SP2)

Table 1: GIAC Enterprises List of Major IT Components[3]

[3] Tracy_Thurston_GCFW.zip with modifications from Loring_Rose_GCFW.zip URL: http://www.giac.org/GCFW.php/

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1.5 Operational IT Requirements

This section describes the IT applications, services, and access GIAC Enterprises needs to conduct its mission. The operational IT requirements depend on the needs of four user groups: customers, employees, partner China Sayings and suppliers to GIAC Enterprises, and remote and mobile users. The primary operational IT requirements are summarized in Table 2.

1.5.1 Customers

Customers require access to the public web site to learn about the company's products. They must be able to place secure orders with GIAC Enterprises. [4] Internet customers must be able to contact GIAC Enterprises by email for customer service issues. GIAC Enterprises must provide customers with web, Secure Socket Layer (SSL), Domain Name Service (DNS) and public email to meet these operational requirements. Customers reach these services via the Internet with SSL-enabled browsers.

1.5.2 Employees

Employees require access to Internet, corporate email, public email, and corporate servers and applications. [5] In addition, employees need to access SSL, DNS, Secure Shell (SSH), Virtual Private Network (VPN) to China Sayings and suppliers, and SQL. Employees reach these services via GIAC Enterprises IT infrastructure.

1.5.3 China Sayings and Suppliers

China Sayings and suppliers need to exchange sensitive business data with GIAC Enterprises over Internet and email. [6] These users also need to access SSL, DNS, Secure Shell (SSH), Virtual Private Network (VPN) to GIAC Enterprises, and SQL. China Sayings and suppliers reach these services over an encrypted VPN.

1.5.4 Remote and Mobile Users

Remote and mobile users require access Internet, corporate email, public email, and corporate servers and applications. These users require the same services as on-site employees. Remote and mobile users access these services through a VPN with VPN client software.

[4] Loring_Rose_GCFW.zip URL: http://www.giac.org/GCFW.php/
[5] Loring_Rose_GCFW.zip URL: http://www.giac.org/GCFW.php/
[6] Loring_Rose_GCFW.zip URL: http://www.giac.org/GCFW.php/

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

SERVICE Direction	Customers	Employees	China Sayings and GIAC Enterprises' Suppliers	Remote and Mobile Users
Web Inbound	X	X	X	X
Web Outbound		X		X
SSL Inbound	X	X	X	X
SSL Outbound	X	X	X	X
DNS Inbound	X	X	X	X
DNS Outbound	X	X	X	X
Email SMTP Inbound	X	X	X	X
Email SMTP Outbound	X	X		X
SSH Inbound		X	X	X
SSH Outbound		X	X	X
VPN Inbound		X	X	X
VPN Outbound		X	X	X
Database (SQL) Inbound		X	X	X
Database (SQL) Outbound		X	X	X

Table 2: Operational IT Requirements for GIAC Enterprises

Inbound: From Internet to GIAC Enterprises
Outbound: From GIAC Enterprises to Internet

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ASSIGNMENT 2: AREAS OF RISK AND SECURITY POLICIES FOR GIAC ENTERPRISES

2.0 Introduction

Assignment 2 has two parts. The first part defines areas of security risk to GIAC Enterprises. An informal risk assessment revealed five (5) areas of significant security risk. These risks are:

- Risk 1: Sufficient Security Awareness and Training for Users
- Risk 2: Security of Remote and Mobile Users
- Risk 3: Protecting Critical Data
- Risk 4: Rapid Detection of Intrusions
- Risk 5: Securing the Perimeter

Each risk area addresses the concern to GIAC Enterprises, the threats, the consequences, and proposed actions to mitigate the risk. In this discussion, a threat is defined as "any unwanted or unplanned event that causes disruption, damage to the computing infrastructure or loss in data integrity."[7] If any of the vulnerabilities are successfully exploited, consequences range from lost customers and revenues to potential legal issues. Recommended actions to mitigate these risks are based on Defense in Depth strategies. Defense in Depth strategies are successive layers of protection throughout the GIAC Enterprises IT infrastructure.[8]

The second part of Assignment 2 takes three (3) areas of risk and develops security policy to address each risk area. The policies and primary areas of risk they address are:

Name of Policy	Primary Risk Area the Policy Addresses
Acceptable Use Policy	Risk 1: Sufficient Security Awareness and Training for Users
Remote Access Policy	Risk 2: Security of Remote and Mobile Users
Password Policy	Risk 3: Protecting Critical Data

2.1 Areas of Significant Security Risk To GIAC Enterprises

2.1.1 Risk 1: Sufficient Security Awareness and Training for Users

2.1.1.1 Why the Concern?

Sufficient security awareness is necessary so employees understand and support the connection between IA and the success of GIAC Enterprises. "Security education also

[7] Guel, Michele. Proven Practices for Managing the Security Function. SANS Institute, 2001. Pg. 72.
[8] Kerby, Fred. Defense In Depth. SANS Institute, 2001. Pgs. 3-4.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

reinforces the corporate and team nature of the security requirement and stops it appearing irrelevant to other corporate activities."[9] However over the past 6 months GIAC Enterprises has experienced a rash of incidents to indicate security awareness isn't at acceptable levels:

- NIMDA infection due to unpatched web server.
- W32.Badtrans.B@mm infection because a user didn't have updated anti-virus software on their PC.[10]
- W32.Goner.A@mm infection because the user really wanted to see the screen saver and opened the attachment.[11]
- Firewall logs showed three (3) new hires accessing pornographic web sites during working hours.

2.1.1.2 Threats and Associated Consequences

The table below lists the major threats and associated consequences of Risk 1: Sufficient Security Awareness and Training for Users.

What are the threats?	What are the consequences?
Users have anti-virus software installed, but the update cycles are different from user to user.	Malicious code infection. Lost revenue due to server downtime. Lost productivity containing and cleaning malicious code infection.
Inappropriate use of Internet and Email.	Possible legal issues; lost employee productivity. Lost Internet bandwidth for business functions. Email system congested with unnecessary traffic. Lost or compromised data.
Server and host patches not up to date.	Data compromise. Hacker able to steal corporate or customer data such as credit card numbers, ID's, etc. GIAC Enterprises sued for breach of privacy.
Policies aren't known or understood, so employees circumvent policies.	Possible legal actions. Malicious code infection. Lost revenue, lost customers and lost productivity from data compromise.
Backdoor connection into GIAC Enterprises.	GIAC Enterprises could be attacked or infected through this backside connection. Lost or corrupted data. Host, server or data compromise.

2.1.1.3 How to Mitigate the Risk?

[9] Caelli, William; Longley, Dennis; Shain, Michael. Information Security Handbook. Stockton Press, 1991. Pg. 53.
[10] http://securityresponse.symantec.com/avcenter/venc/data/w32.badtrans.b@mm.html
[11] http://securityresponse.symantec.com/avcenter/venc/data/w32.goner.a@mm.html

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Update Policy. Review and clarify the Information Assurance (IA) policies and procedures for the organization. Create IA web site to promulgate policies and procedures to employees. Establish user forum on IA web site to address user's policy questions.

- Training. Develop and implement an Information Assurance training program at GIAC Enterprises. Address security awareness for management, system administrators, network administrators, and general users. Have users take awareness training via the IA web site. Have the Information System Security Officer (ISSO) meet and brief new hires in security practices. Require each user to sign a User Agreement prior to receiving an account. The User Agreement lists the user's fundamental IA responsibilities. Have the ISSO periodically brief managers on security issues and concerns.

- Develop Metrics. Test users on training and produce training metrics. Have the ISSO periodically send managers security metrics: lost revenues from server downtime due to virus attacks, intrusion attempts, training and audit results. Consider posting metrics to IA web site (internal only).

- Perform Audits. Perform regular system and desktop audits. Perform internal scans for vulnerabilities on servers and desktops. Use wardialing to detect unauthorized modem connections.

- Monitor Internet Use. Implement Internet management software like Net Nanny or Surf Control to monitor Internet use. Block access to inappropriate web sites.

- Implement Anti-virus Management Server. Implement anti-virus management server to automatically update virus definitions for all computer assets.

- Filter Email. Implement virus wall and email filters on internal and external mail servers to check incoming and outgoing emails. Block certain email attachment types known to be dangerous: .bat, .cmd, .com, .dll, .eml, .exe, .pif, .scr, .shs, .vbs, .vbe.[12]

- Provide Rewards. Give security kudos and rewards to deserving employees and their supervisors. Rewards can be modest cash awards, movie tickets or free lunches. Reward System Administrators whose servers consistently pass security audits.

2.1.2 Risk 2: Security of Remote and Mobile Users

[12] "The 60 Minute Network Security Guide." Version 1.0. Oct, 16, 2001. http://nsa2.www.conxion.com/support/download.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.1.2.1 Why the Concern?

GIAC Enterprises has recently completed acquisition of China Sayings. GIAC Enterprises must securely exchange sensitive data with China Sayings and suppliers over the Internet. In addition, mobile and remote users need to securely connect to GIAC Enterprises to conduct company business.

2.1.2.2 Threats and Associated Consequences

The table below lists the major threats and associated consequences of this Risk 2: Security of Remote and Mobile Users.

What are the threats?	**What are the consequences?**
A backside connection from China Sayings, supplier or remote user.	GIAC Enterprises could be attacked or infected through this backside connection. Lost or corrupted data. Possible legal issues.
Data is compromised in transit to/from GIAC Enterprises and remote users.	User ID compromise enabling a hacker to gain access to sensitive internal information by stealing the identity of a valid user. Compromise of personal customer data such as credit card info, SSN, financial data. Sensitive business data made available over the Internet.
Laptop lost or stolen	Sensitive information will be compromised or altered and the information will be known to a competitor or announced to the general public

2.1.2.3 How to Mitigate the Risk?

- Establish Memorandums of Agreement with China Sayings and each supplier detailing security responsibilities among parties. Establish VPN with China Sayings and suppliers.

- Remote access will be over a VPN client rather than Remote Access Server (RAS) with dial up modems. Telecommuters and remote users can access GIAC Enterprises data with company-owned laptops as opposed to privately owned PCs. The laptop will have a standard software load: VPN client, managed anti-virus, etc. Use encrypted drives on laptops.

- Use SSL for customer transactions over the Internet.

- Use public key/private key for remote and mobile users.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.1.3 Risk 3: Protecting Critical Data

2.1.3.1 Why the Concern?

As an Internet start-up selling on-line the information contained in our web and data base servers constitute our business operation. Protecting these assets is critical if GIAC Enterprises is to generate profit.

2.1.3.2 Threats and Associated Consequences

The table below lists the major threats and associated consequences of Risk 3: Protecting Critical Data.

What are the threats?	What are the consequences?
System Administrator inexperienced or untrained in securing systems.	Default installations and scripts left intact. Unused ports left opened. GIAC Enterprises exposed to attack and compromise of data.
Hackers deface the web sites or compromise sensitive customer data.	Lost revenue while rebuilding server. Lost customers. Damaged company reputation. Embarrassment to company
While regular backups occur and the backup procedures are well documented, restore procedures are untested.	Restore procedure may not work when data must be restored from in event of a contingency (earthquake, flood, massive power hit, data compromised, etc)
Improper permissions set in web server or database.	Granting unauthorized access to user or hacker.
Server and host patches not up to date. Servers not hardened with latest patches.	Leaves servers open to vulnerabilities and data compromise. Hacker is able to steal corporate or private customer data such as credit card numbers, ID, etc. GIAC sued for breach of privacy.
Weak passwords. The ISSO ran a basic dictionary password cracker against the network. She cracked the password of the Chief Financial Officer and one hundred sixty (160) other users in less than five (5) minutes.	Host and server compromise. Compromise of sensitive company and customer data.
Insider or disgruntled employee compromises data.	GIAC Enterprises exposed to attack and compromise of data.

2.1.3.3 How to Mitigate the Risk?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Utilize Principle of Least Privilege when granting access to all users. Establish the minimum level of access necessary for the user to do their job.[13]

- Follow the Windows 2000 Security Recommendation Guides from National Security agency.[14] Follow vendor guidelines in securing systems and applications.

- Automatically push patches to servers and desktops.

- Send System Administrators (SA's) to training to learn how to secure and harden their systems. Audit server configuration with SA before server is allowed to connect to the network.

- Install password checking software to help users develop strong passwords. Run password cracking software to identify weak passwords.

- Routinely check for unused or outdated accounts. Notify SA's when users no longer require access to computer resources. Put SA on employee checkout list.

- Run internal scans for vulnerabilities for servers, user workstations and desktops. Scan for open ports. Disable unused services.

- Post and test backup and recovery procedures.

- Develop and test server contingency plans.

- Test patches on test server to determine if patch causes server failure.

- Place publicly accessible servers in DMZ.

- Use SSL for public Internet transactions.

- Use VPN for China Sayings and suppliers. Establish extranet for China Sayings and supplies.

- Use VPN for remote and mobile users.

2.1.4 Risk 4: Rapid Detection of Intrusions

2.1.4.1 Why the Concern?

Rather than detecting and containing intrusions as they occur, we've been reacting after the intrusion has happened. In Figure 1 of Assignment 1, GIAC Enterprises has two ISPs

[13] Kerby, Fred. Defense In Depth. SANS Institute, 2001. Pg. 7.
[14] http://nsa2.www.conxion.com/win2k/download.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

and no Intrusion Detection System (IDS). This configuration contributed to the following known intrusion incidents at GIAC Enterprises:

- Hackers penetrated GIAC Enterprises and defaced two web sites. We had to take both servers off line and rebuild them. Customers were unable to place orders, so we lost revenues.

- Now GIAC Enterprises is listed on hacker web sites. Since the hack occurred over the weekend, the Computer Emergency Response Team (CERT) called us and told us about the defacements.

2.1.4.2 Threats and Associated Consequences

The table below lists the major threats and associated consequences of this Risk 4: Rapid Detection of Intrusions.

What are the threats?	What are the consequences?
Rely on firewall and server logs to detect intrusions. Due to limited staff the logs are spot checked as opposed to being checked daily.	The servers end up being the IDS if the hacker feels like bragging. Find intrusions after the fact – too late. Compromised data. Lost customer confidence and revenues. GIAC Enterprises embarrassed.
Install an IDS. Due to limited staff the IDS is only spot checked.	Still find intrusions after the fact, but the forensics data is better. Compromised data. Lost customer confidence and revenues. GIAC Enterprises embarrassed.

2.1.4.3 How to Mitigate the Risk?

- Install two network-based IDS's in DMZ and internal network. Use Snort (Win32) Windows 2000 Professional (SP2).

- Assign IDS duties to one of the network engineers. Start recruiting effort with management to devote 0.25 workyear toward checking IDS and logs.

- Install tripwire on all components in Table 1 of Assignment 1 and critical servers in the network.

- Evaluate for purchase NetIQ product for security management of Windows 2000 systems. The goal is to automate this function to reduce workload on the ISSO and IT staff.

2.1.5 Risk 5: Securing the Perimeter

2.1.5.1 Why the Concern?

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

"Perhaps the biggest security challenge businesses face today is the disappearing perimeter…there was a clear perimeter between what was perceived as the anarchic, hacker-ridden Internet and the carefully controlled internal network. No more."[15]

2.1.5.2 Threats and Associated Consequences

The table below lists the major threats and associated consequences of Risk 5: Securing the Perimeter.

What are the threats?	What are the consequences?
Incorrectly configured access control list on border router or firewall.	Allow hacker direct internal access.[16]
Unpatched or incorrectly configured DMZ servers.	If a DMZ server is compromised, allow internal access to hacker.[17]
Unknown, unauthorized backdoor into network	GIAC Enterprises could be attacked or infected through this backside connection. Lost or corrupted data. Possible legal issues.
Unnecessary TCP/IP services allowed through the border router and firewall.	Leak information about internal network to hacker and cause compromise.[18] GIAC Enterprises exposed to attack.

2.1.5.3 How to Mitigate the Risk?

Employ the following recommendations from The 60 Minute Network Security Guide:[19]

- Scan for open ports perimeter router and firewall. Eliminate unnecessary TCP/UDP services. Limit access to required TCP/UDP services only to administrators.
- Disable unused router and firewall interfaces.
- Use wardialing to detect unauthorized modem connections.
- Use strong passwords on the perimeter router and firewall.
- Filter TCP/IP services inbound and outbound based on Operational IT Requirements.

---

[15] Erlanger, Leon. "21st Century Security." Internet World. December 2001: 24-25.
[16] Scambray, Joel; Mcclure, Stuart; Kurtz, George. Hacking Exposed. Berkley, California: Osborne/McGraw-Hill, 2001. Pg. 661.
[17] Scambray, Joel; Mcclure, Stuart; Kurtz, George. Pg. 661.
[18] Scambray, Joel; Mcclure, Stuart; Kurtz, George. Pg. 661
[19] "The 60 Minute Network Security Guide." Version 1.0. Oct, 16, 2001. http://nsa2.www.conxion.com/support/download.htm

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.2 Security Policies for GIAC Enterprises

2.2.1 Acceptable Use Policy[20]

Name of Policy	Primary Risk Area the Policy Addresses
Acceptable Use Policy	Risk 1: Sufficient Security Awareness and Training for Users

Acceptable Use Policy
For GIAC Enterprises
21 December 2001

1.0 Purpose

The purpose of this policy is to outline the acceptable use of computer networks and computer equipment at GIAC Enterprises. These rules are in place to protect the employee and GIAC Enterprises. Inappropriate use exposes GIAC Enterprises to risks including virus attacks, compromise of network systems and services, and legal issues.

2.0 Background

The start of an Information Assurance (IA) program is to inform users of their privileges and responsibilities when using company information, computer networks, and computer assets. Policies and procedures form the basis for IA awareness and training. GIAC Enterprises is committed to protecting their employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Effective Information Assurance is a team effort involving the participation and support of every GIAC Enterprises' employee and affiliate who deals with information and/or information systems.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at GIAC Enterprises, including all personnel affiliated with third parties. This policy applies to all computer networks and equipment owned or leased by GIAC Enterprises.

4.0 Policy

4.1 General Use and Ownership

[20] http://www.sans.org/newlook/resources/policies/Acceptable_Use_Policy.doc

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1. All information, computer networks, and computer assets are the property of GIAC Enterprises. Users should be aware that the data they create on the corporate systems remains the property of GIAC Enterprises. Due to the need to protect GIAC Enterprises' network, management cannot guarantee the confidentiality of information stored on any network device belonging to GIAC Enterprises.
2. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.
3. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Limited personal use is allowed. Employees are recommended to limit personal use to before/after work and during lunch or break periods. Employees are advised to keep personal use short and infrequent. Personal use should be no more disruptive than a brief personal phone call.
4. Information that users consider sensitive or vulnerable must be encrypted. For guidelines on information classification, see GIAC Enterprises' Information Sensitivity Policy. For guidelines on encrypting email and documents, go to GIAC IA web site under the Awareness Initiative.
5. For security and network maintenance purposes, authorized individuals within GIAC Enterprises may monitor equipment, systems and network traffic at any time.
6. GIAC Enterprises reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
7. Access to GIAC Enterprises' computer or network assets constitutes the user's consent to monitoring.

4.2 Security and Proprietary Information

1. The user interface for information contained on GIAC Enterprises' computer systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Prior to receiving an account, each user must sign a User Agreement Form describing the user's fundamental IA responsibilities.
3. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Authorized users are responsible for actions taken under their accounts. System level passwords should be changed quarterly. User level passwords should be changed every six months.
4. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by locking the workstation (control-alt-delete for Win2K users) when the host will be unattended.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5. Use encryption of information in compliance with the Acceptable Encryption Use policy.
6. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
7. Postings by employees from a GIAC Enterprises email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of GIAC Enterprises, unless posting is in the course of business duties.
8. All hosts used by the employee that are connected to the GIAC Enterprises, whether owned by the employee or GIAC Enterprises, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.
9. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code. When employees receive e-mail from unknown senders or e-mail containing unknown attachments, employees should delete the suspect e-mail without opening it. Use SHIFT+DELETE in your e-mail application to permanently delete suspect email.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of GIAC Enterprises authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing GIAC Enterprises-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.
2. Installing or distributing "pirated" software products that are not appropriately licensed for use by GIAC Enterprises.
3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

4. Installing of any copyrighted software for which GIAC Enterprises or the end user does not have an active license.
5. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
6. Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
7. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
8. Using a GIAC Enterprises computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
9. Using a GIAC Enterprises computing asset to engage in on-line gambling, day-trading, or running a second personal business interest.
10. Making fraudulent offers of products, items, or services originating from any GIAC Enterprises account.
11. Effecting security breaches or disrupting network communication. Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
12. Accessing data when the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties
13. Scanning for vulnerabilities or port usage without prior approval from the ISSO.
14. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
15. Circumventing user authentication or security of any host, network or account.
16. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
17. Hacking any computer system or network within or connected to GIAC Enterprises.
18. Providing information about, or lists of, GIAC Enterprises employees to parties outside GIAC Enterprises.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within GIAC Enterprises' networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by GIAC Enterprises or connected via GIAC Enterprises' network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Responsibilities

5.1 GIAC Enterprises Management is responsible for

1. approving Information Assurance policy and revisions
2. ensuring employees receive Information Assurance training and annual refresher training
3. acting on policy violations in coordination with the Human Resources Office.
4. providing final interpretation of policy

5.2 The Information Systems Security Officer (ISSO) is responsible for

1. developing reviewing, updating and disseminating this policy
2. developing employee training programs for new employees and refresher training for current employees
2. auditing policy compliance and developing compliance metrics
3. forwarding policy violations to management for action
4. acting as consultant to management and users on policy questions.

5.3 Employees are responsible for

1. knowing this policy
2. conducting their use of GIAC Enterprises' computer networks and assets according to this policy
3. taking the required annual training in Information Assurance on the IA web site
4. reporting known violations to their manager or ISSO.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.2.2 Remote Access Policy[21]

Name of Policy	Primary Risk Area the Policy Addresses
Remote Access Policy	Risk 2: Security of Remote and Mobile Users

Remote Access Policy
For GIAC Enterprises
21 December 2001

1.0 Purpose

The purpose of this policy is to define standards for connecting to GIAC Enterprises's network from any host. These standards are designed to minimize the potential exposure to GIAC Enterprises from damages that may result from unauthorized use of GIAC Enterprises resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical GIAC Enterprises internal systems, etc.

2.0 Scope

This policy applies to all GIAC Enterprises employees, contractors, vendors and agents with a GIAC Enterprises-owned computer or workstation used to connect to the GIAC Enterprises network. This policy applies to remote access connections used to do work on behalf of GIAC Enterprises, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

1. Remote access connections are an extension of GIAC Enterprises' corporate network. Users with remote access privilege are responsible for ensuring their remote access connection is given the same security consideration as the user's on-site connection to GIAC Enterprises.
2. Users with remote access privileges are allowed to connect to GIAC Enterprises' corporate network with a GIAC Enterprises' owned computer using a Virtual Private Network (VPN).

[21] http://www.sans.org/newlook/resources/policies/Remote_Access_Policy.doc

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of GIAC Enterprises's network:
    a. *Acceptable Encryption Policy*
    b. *Virtual Private Network (VPN) Policy*
    c. *Wireless Communications Policy*
    d. *Acceptable Use Policy*
4. For additional information regarding GIAC Enterprises's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any GIAC Enterprises employee provide their login or email password to anyone, not even family members.
3. GIAC Enterprises employees and contractors with remote access privileges must ensure that their GIAC Enterprises-owned personal computer which is remotely connected to GIAC Enterprises's corporate network, is not connected to any other network at the same time.
4. GIAC Enterprises employees and contractors with remote access privileges to GIAC Enterprises's corporate network must not use non-GIAC Enterprises email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct GIAC Enterprises business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the GIAC Enterprises network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. The Information Systems Security Officer (ISSO) must approve non-standard hardware configurations. The ISSO must approve security configurations for access to hardware.
9. All hosts that are connected to GIAC Enterprises internal networks via remote access technologies must use the most up-to-date anti-virus software. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Organizations or individuals who wish to implement non-standard Remote Access solutions to the GIAC Enterprises production network must obtain prior approval from the ISSO.

4.0 Enforcement

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Responsibilities

5.1 GIAC Enterprises Management is responsible for

1. approving Information Assurance policy and revisions
2. acting on policy violations in coordination with the Human Resources Office
3. providing final interpretation of policy

5.2 The Information Systems Security Officer (ISSO) is responsible for

1. developing reviewing, updating and disseminating this policy
2. auditing policy compliance and developing compliance metrics
3. forwarding policy violations to management for action
4. acting as consultant to management and users on policy questions.

5.3 Employees are responsible for

1. knowing and complying with this policy
2. reporting known violations to the ISSO.

6.0 Definitions

Term	Definition
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function.
DLCI	Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

	into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a GIAC Enterprises-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into GIAC Enterprises and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
Remote Access	Any access to GIAC Enterprises's corporate network through a non-GIAC Enterprises controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-GIAC Enterprises network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into GIAC Enterprises's corporate network via a VPN tunnel.
VPN	Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

2.2.3 Password Policy[22]

Name of Policy	Primary Risk Area the Policy Addresses
Password Policy	Risk 3: Protecting Critical Data

Password Policy
For GIAC Enterprises
21 December 2001

1.0 Purpose
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2.0 Background
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. Weak passwords may result in the compromise of GIAC Enterprises's entire corporate network. As such, all GIAC Enterprises employees (including contractors and vendors with access to GIAC Enterprises systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

3.0 Scope
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any GIAC Enterprises facility, has access to the GIAC Enterprises network, or stores any non-public GIAC Enterprises information.

4.0 Policy
4.1 General

- All system-level passwords (e.g., root, enable, Windows 2000 admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the global password management database. The Information Systems Security Officer administers the global password management database.
- All router, switch, firewall, and Simple Network Management Protocol (SNMP) passwords must not be left in default settings. Network infrastructure passwords must also follow the Password Policy.
- All user-level passwords must be changed at least every six months. User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.

[22] http://www.sans.org/newlook/resources/policies/Password_Policy.doc

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Users should not use weak passwords. Weak passwords have the following characteristics:

- The password contains less than eight characters.
- The password is the same as your user account.
- The password contains obscenities and vulgarities.
- The password contains or is the word “password.”
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "GIAC Enterprises", “GIAC”, “Enterprise” or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, abcdefgh,123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z).
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'?,./).
- Are at least eight alphanumeric characters long.
- Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1Wr~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for GIAC Enterprises accounts as for other non-GIAC Enterprises access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various GIAC Enterprises access needs. For example, select one password for the Engineering systems and a separate password for IT systems.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Do not share GIAC Enterprises passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential GIAC Enterprises information.

Here is a list of "dont's":

- Don’t write down your password or store them on-line.
- Don’t post your password on your monitor, under your keyboard, under your mousepad, or in your office space.
- Don't reveal a password over the phone to ANYONE, including Help Desk or PC Maintenance personnel.
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly).

If an account or password compromise is suspected, report the incident to the Information Systems Security Officer and change all passwords.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Access to the GIAC Enterprises Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases
Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Auditing Compliance

Password cracking will be performed on a periodic by the ISSO. Your password must be able to withstand an 8 hour dictionary scan without being deciphered. If a password is guessed or cracked during one of these scans, the user will be required to change it.

6.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7.0 Responsiblities

7.1 GIAC Enterprises Management is responsible for

- approving Information Assurance policy and revisions
- ensuring employees receive Information Assurance training and annual refresher training
- acting on policy violations in coordination with the Human Resources Office.
- providing final interpretation of policy

7.2 The Information Systems Security Officer is responsible for

- acting as consultant to management and users on policy questions.
- developing reviewing, updating and disseminating this policy
- auditing policy compliance by performing password scans on the network

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- reporting audit results to management
- forwarding policy violations to management for action
- acting as consultant to management on policy questions.

7.3 Employees are responsible for

- creating and using passwords according to this policy
- reporting known or suspected password compromises to their manager or ISSO.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ASSIGNMENT 3: DEFINE SECURITY PROCEDURE FOR GIAC ENTERPRISES

3.0 Introduction

Assignment 3 is a procedure to implement a policy in Assignment 2. This procedure starting on the next page implements a Norton Anti-Virus management server to meet the requirement established in the Acceptable Use Policy, Section 4.2, Item 8.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

3.1 Managed GIAC-NORTON Installation Procedure

MANAGED GIAC-NORTON INSTALLATION PROCEDURE
23 December 2001

1.0 Purpose.

The procedure in Figure1 instructs users on how to install managed Norton Anti-virus Corporate Edition 7.5 on their desktop, laptop, or workstation. You will find detailed installation instructions at http://www.giac-norton/install/instructions/

2.0 Importance.

GIAC Enterprises' Acceptable Use Policy requires that users run anti-virus software on their desktops and keep the virus definitions current. Current anti-virus definitions are critical to protecting GIAC Enterprises against Internet viruses, worms and other malicious code. GIAC Enterprises has installed a new Norton Anti-Virus Management server called GIAC-NORTON to automatically update your anti-virus signatures and scan your drives. GIAC-NORTON also automatically notifies the Information Assurance (IA) staff of any virus infection on GIAC-NORTON clients. This enables faster quarantine, containment, and cleans up of virus infections.

3.0 Scope.

This procedure applies to all desktops, laptops, and workstations attached to GIAC Enterprises Information Technology Infrastructure.

4.0 Responsibility.

Each user is responsible for ensuring their desktop, laptop, and workstation is a GIAC-NORTON client. The person with administrator rights on the desktop, laptop, or workstation should perform this procedure. If you do not have administrator rights, please contact your System Administrator to perform this procedure.

5.0 Compliance.

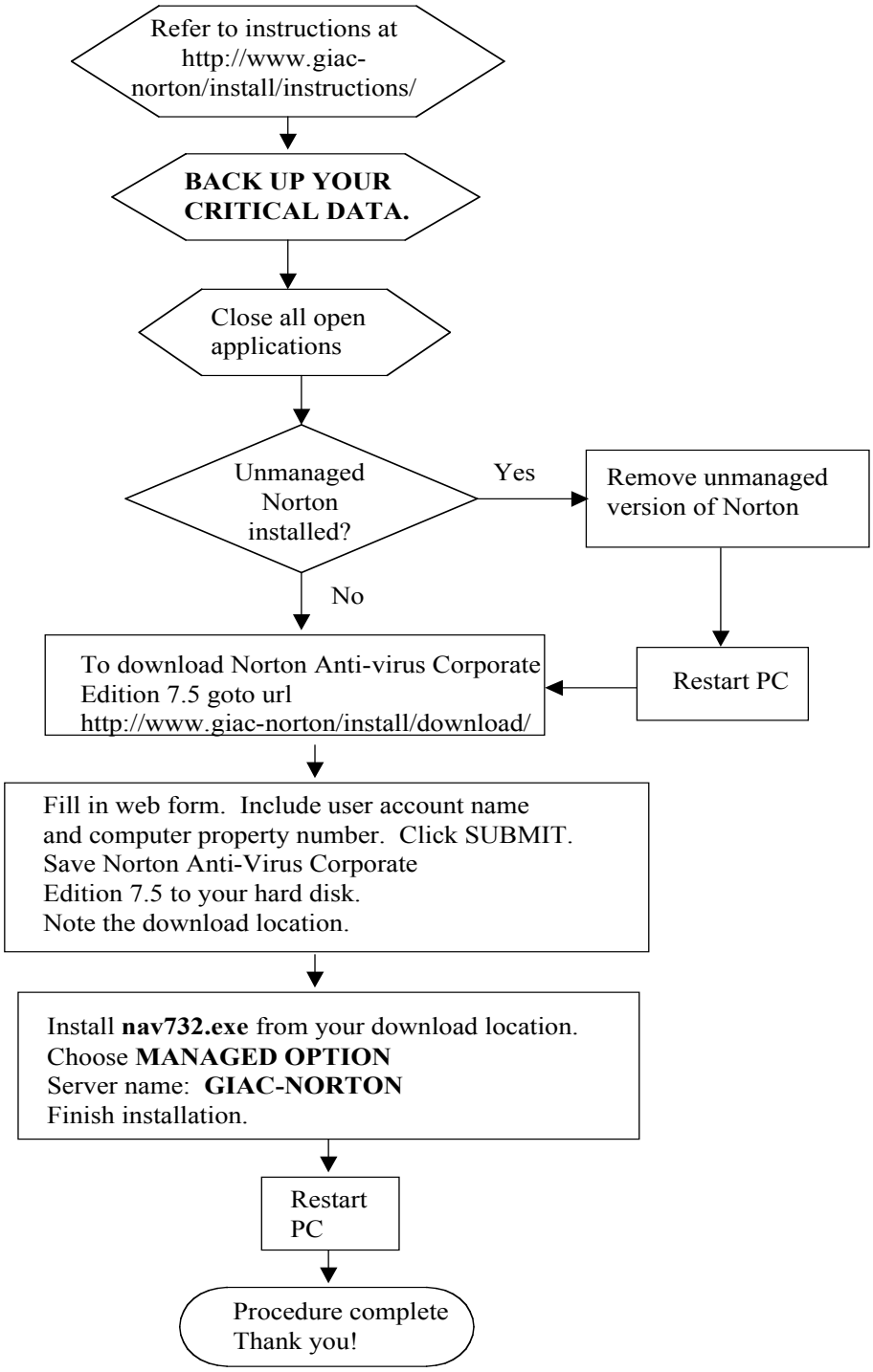
GIAC-NORTON maintains a list of clients for distribution and auditing purposes. The procedure directs users to fill in a form on the web site with their account name and computer property number. The GIAC-NORTON client list will be compared to the account and computer database to verify compliance. The Information Systems Security Officer will also check for GIAC-NORTON compliance on periodic Information Security desktop audits.

6.0 Help Desk.

If you require assistance with this procedure, please contact the Help Desk at 3-5481.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

FIGURE 1: MANAGED GIAC-NORTON INSTALLATION PROCEDURE



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

List of References

Caelli, William; Longley, Dennis; Shain, Michael. Information Security Handbook. Stockton Press, 1991. Pg. 53.

Erlanger, Leon. "21st Century Security." Internet World Magazine. December 2001: 24-25.

Guel, Michele. Proven Practices for Managing the Security Function. SANS Institute, 2001. Pg. 72.

http://nsa2.www.conxion.com/win2k/download.htm

http://securityresponse.symantec.com/avcenter/venc/data/w32.badtrans.b@mm.html

http://securityresponse.symantec.com/avcenter/venc/data/w32.goner.a@mm.html

http://www.sans.org/newlook/resources/policies/Acceptable_Use_Policy.doc

http://www.sans.org/newlook/resources/policies/Password_Policy.doc

http://www.sans.org/newlook/resources/policies/Remote_Access_Policy.doc

Kerby, Fred. Defense In Depth. SANS Institute, 2001. Pgs. 3-7.

Loring_Rose_GCFW.zip URL: http://www.giac.org/GCFW.php/

Scambray, Joel; Mcclure, Stuart; Kurtz, George. Hacking Exposed. Berkley, California: Osborne/McGraw-Hill, 2001. Pg. 661

The 60 Minute Network Security Guide." Version 1.0. October 16, 2001. URL: http://nsa2.www.conxion.com/support/download.htm

Tracy_Thurston_GCFW.zip URL: http://www.giac.org/GCFW.php/

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.