William T. Ainge
GSIO Practical Assignment
Version 1.3 (February 7, 2003)
Title: IT Security at a small corporation

GSIO Practical
Table of Contents

Title - **IT security at a small corporation**

Summary:

This practical is primarily a risk assessment on the IT Security at a small corporation that uses the Internet to conduct its business. It examines the IT Infrastructure, policies and staffing to identify the three most important security risks and the negative effects they could have on the corporation. To mitigate these risks the analysis documents actions to reduce or eliminate the vulnerability. It includes a review of an existing IT Use and Security Policies with correction of weak areas in revised policy. To ensure that the policy was implemented correctly a procedure was documented for one of the high-risk areas.

IT security at a small corporation

GIAC is a small automotive parts wholesaler who employs 28 management and staff personnel. They are located entirely in one building near Baltimore, MD. Their customers are primarily retail auto parts stores throughout the United States. GIAC relies on the Internet for its customers to purchase parts. Yearly sales for GIAC were approximately $4.0 million. GIAC has adopted a just in time inventory policy for its organization while offering the lowest cost. With this policy the minimum inventory is stored at GIAC warehouse to: prevent loss incurred in the event the item is not purchased; to retain needed funds by only purchasing what is required and; eliminate unnecessary warehouse costs. Emphasis on sales forecasting and timely procurements with GIAC suppliers and customers is of utmost importance. GIAC is responsible for the procurement, shipping, receiving, shipping, warehousing of auto parts for its customers. Management relies on their IT capabilities to plan, interact with its suppliers and customers to provide the lowest cost for automotive parts on Internet.

GIAC IT Infrastructure

GIAC IT network is used for processing both its internal and external applications functions required in a their business. The Internet and phone are used to purchase and sell parts. The mangers use the MSN email to send and receive email from the store managers and their suppliers. The IT department uses Windows 2000 servers and work stations for processing the resident Off the Shelf business applications used in GIAC's core business. When a sale is entered at the store level, it is done mostly through the Internet which when complete triggers an application program that updates the corporate database on the internal network. All of the traffic to GIAC from the Internet goes through a router and then into the DMZ-1 where the public web servers and the Auto Parts Catalog reside. Dial-in traffic into GIAC also is protected through the firewall into DMZ -2 through the Remote Access Server (RAS)

Router:
Netgear model RP334 router acts as interface between the ISP Internet protocol and the firewall Ethernet protocol. Used to block any traffic destined for restricted ports such as 135 Remote Program Control (RPC) and port 80 FTP Web sites. It also routes all outgoing traffic to the ISP. An identical Netgear router is maintained off line to use if the primary fails.

Firewall:
Nokia Firewall One Operating System is used to screen all traffic using deny by default, allow by exception. Traffic destined for specific ports not allowed is not allowed if it's on the denied port access list. Allows access to some company user IP addresses to port 21 FTP services. Remote access to Internal network is authenticated by logon password. The IT department maintains an identically configured Nokia Firewall off line to use in the event the primary one goes down.

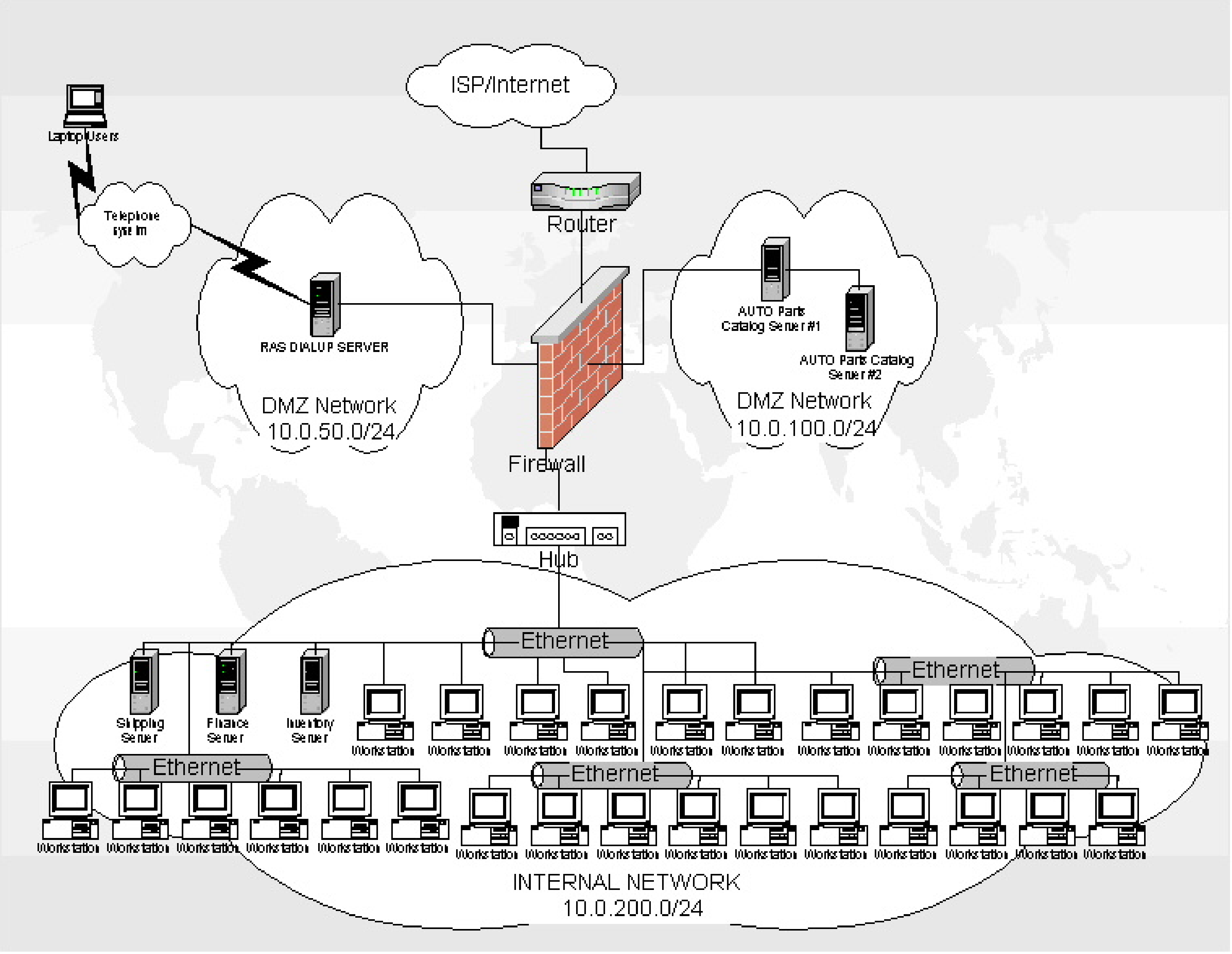
Plans exist to put this second firewall and the additional router on line to provide fail over capabilities and reduce down time.

Hot Lists identifying companies or individuals not allowed to access GIAC system are updated regularly and their access is blocked by the Firewall software.

FTP access is not allowed except for a small number of internal users.

Internal users requesting access to unapproved (inappropriate) web sites are blocked by use of a proxy server and software monitoring

Servers:
GIAC processes its IT business applications on its three Windows 2000 Servers. Transactions with customers are conducted using the Internet and two Web servers are located in one of two DMZ. These servers share the processing load and are configured to fail-over toach other as a contingency. The other DMZ is used to isolate Dial-up access. The GIAC network diagram is presented below:



Microsoft Windows 2000 operating system is used for all workstations, laptops and servers.

Laptops:

Dell Latitude, Pentium III with internal modems

Local Area Network:

Ethernet 100 MB LAN is providing connectivity for all GIAC users to shared applications and access to the Internet through the ISP.

Communication:

GIAC does use an ISDN line to an ISP for Internet Connectivity to purchase parts from any manufacture and receive orders from anywhere in the world.

Remote access:

Shiva – Remote Access System (RAS) for dial up remote communication from their sales personnel who were issued laptops.

GIAC IT Management Tools:

The GIAC IT team uses tools available for managing the network such as:

a) Retina software to scan the network for missing patches.
b) MS System Management System (SMS) for applying patches.
c) MS System Administrator functions
d) All servers are configured using guidelines found in Microsoft Security and Microsoft Security Toolkit http://www.microsoft.com/servers/techinfo/security.asp#2000 [6] before they are put into production.
e) Norton Anti Virus Corporate Edition software distributed first to server from Norton and to the workstations at log-on by the server.

Business Operations:

GIAC IT network is used for processing both its internal and external applications functions required in their business. The Internet and phone are used to purchase and sell parts. The mangers use the MSN email to send and receive email from the store managers and their suppliers. The IT department uses Windows 2000 servers and work stations for processing business applications used in GIAC's core business. When a sale is entered at the store level, it is done mostly through the Internet which when complete triggers an application program that updates the

[6]

corporate database on the internal network. All of the traffic to GIAC from the Internet goes through a router and then into the DMZ-1 where the public web servers and the Auto Parts Catalog reside. Dial-in traffic into GIAC also is protected through the firewall into DMZ -2 through the Remote Access Server (RAS).

GIAC maintains two public web servers on its DMZ that contains the complete catalog of auto parts it offers for sale. The firewall channels all valid traffic to the DMZ housing the two web servers used to manage customer sessions and transactions. The web server allows anyone on the Internet to access the catalog and browse for the item they desire. Customer sessions and purchase is accomplished using HTTPS with Secure Socket Layer (SSL) that provides encryption of personal data and credit numbers. The customer views the catalog selecting the desired item and then enters their credit card and shipping information to complete the transaction. Sale transactions are then passed through an interface program to the internal network containing financial, inventory, and shipping applications. These transactions update the internal files after each Internet application is completed. No customer or sales data remains on the web at the completion of the sale. GIAC processes about three hundred transactions that result in sales of $15.4 thousand per day. To compensate for the occasions when ISP circuits outages occur, GIAC displays a 800 number for customers to use when a problem occurs..

The IT department uses their Internal network for three Windows 2000 servers and workstations for processing the resident business applications used for GIAC's core business.

a) The Finance server includes a: Accounting application for accounts and monthly balance statements; Payroll; Sales Application where all sales are accounted for and selling price is established; Customers Lists for sending email to preferred customers (this data is considered to be critical or the crown jewels by GIAC management). Customer data base also contains a complete history of customer's sales, items purchased, sale total, date, name, email and street address.
b) Shipping server that includes: Information on where to ship purchase auto parts and the preferred method of shipping purchased by the customer; Warehouse applications used by warehouse workers to locate purchased parts; and email software.
c) Inventory server contains the current data base of all auto parts that GIAC offers for sale. This server also is used for the Catalog application where maintenance is performed before updating the Catalog servers in the DMZ.

The IT department performs a full backup of all files on a daily basis to allow for recovery in the event the files are corrupted or destroyed. On a weekly basis a copy of the most current back up is sent to an off site location for secure storage.

GIAC buyers use the Internet to access their suppliers systems and purchase parts. These purchases are also accomplished using SSL. To place reorders they depend heavily on the inventory reorder points established in the integrated sales and inventory application. These reorder points are dynamically calculated and provide sufficient lead team to avoid losing sales. All completed purchases must be updated to the sales application located on the private network. Buyers and management are the only users permitted access through their network logon and the secondary logon required by the application. The buyers also need to constantly use the Internet to shop for the lowest price available for the quality auto parts they offer in their catalog. Sales data is used to determine trends and what would be good items to feature in sales promotion. Again access to this application requires a separate logon and is restricted to Sales agent and management only. This data is also used to create mailing lists for emailing customers about promotional items not in the catalog. These mailings have produced highly successful sales for GIAC so the names and email addresses contained in the Sales file are the most valuable asset to GIAC. Loss of the Sales data would have a direct impact on the sales and future of GIAC.

The GIAC sales department also has ten Dell Laptops with Windows 2000 that they take with them on travel appointments with suppliers. They use these to dial into the SHIVA system first and then logon with a group logon provided with the Laptop. This logon procedure can also be completed beyond the standard three attempts. Once this is completed they have to sign on to the network and then they have full access to their desktop for the sales and other applications. This lack of control over the dial up presents the potential for a hacker to guess the general password making them one step closer to guess the GIAC network password.

New items are regularly added to the web catalog by GIAC staff personnel that requires them to update the internal Sales, Inventory server and the external web catalog. These tasks are performed by multiple staff personnel and facilitated by the file sever. Shipping of orders is accomplished by sending orders to the GIAC warehouse staff. This is done when the sale is completed and updated into the Shipping application. Next the warehouse staff then pulls and packages the parts, notifies the shipping company for pick-up and updates the shipping file.

Risk Assessment

Based on a review of GIAC IT operations and security the following three areas present the most critical security risk:

Security Patches are not always applied:

GIAC system administrators access the Microsoft Web Site HTTP://WWW.MICROSOFT.COM/SECURITY [1]on an occasional basis to review current vulnerabilities. If the administrator has time, patches are downloaded for some vulnerabilities. Many of the available security patches, such as Internet Explorer are not downloaded because they take too long to apply to each of GIAC workstations. GIAC System Administrators contend they are too busy keeping the system and the users up and running. However, "Patching security vulnerabilities is a low-cost practice that can help prevent potentially high-cost damage" according to Patrick Evans in "Is patching a priority for your enterprise" http://www.itweb.co.za/office/symantec/0203140754.ht. [3]

No specific security policy and procedure exists at CIAC to ensure all security patches are applied in a timely manner. GIAC management is unaware of the great risk to their IT operations by not patching known vulnerabilities. GIAC is at risk on both their internal and external networks from hackers who prey on systems with open vulnerabilities. A good or even average hacker can obtain hacker software to exploit GIAC's unprotected software. GIAC employees may also attempt to obtain GIAC information and sell it to a competitor. Many vulnerabilities have been discovered in Windows software such as: Windows Buffer Overflow; Microsoft Internet Explorer Monthly Cumulative Patch and Microsoft RPC Vulnerability. Other Windows vulnerabilities can be manipulated to gain administrator rights to the entire system and databases at GIAC. Hackers develop or acquire software to take advantage of these vulnerabilities. The longer these systems remain uncorrected the greater the likelihood that GIAC's databases could then be compromised and its crown jewel customer information and credit card information stolen. The loss or unavailability of this information and lack of customer trust this would create would be damaging to GIAC.

The risk of this occurring at GIAC is high due to their lack of patches in place to protect them from hackers exploiting known vulnerabilities. No internal controls such as, Intrusion Detection System or performing regular scans exists at GIAC. So it is doubtful that an intrusion would even be noticed for some time. As a result it's only a matter of time before a hacker, customer, supplier or a GIAC employee takes advantage of this weaknesses. Financial loss to CIAC could be significant if their customer list is sold or obtained by a competitor. Theft of credit card numbers from CIAC databases would be very costly since CIAC would have to reimburse the credit card companies for the customers whose card numbers were stolen.
GIAC management needs to be made aware of the requirement to apply patches in a timely manner. Policies and procedures need to be developed that require system

[1]

[3]

administrators to place priority on applying security patches on a timely basis. The items below put a system of checks and balances between the System Administrator, Information Security Officer and GIAC management that will put controls in place to make sure systems are patched on time:

Steps to mitigate the risk:

a) If all of GIAC systems cannot be patched in a reasonable time then, disable software on user systems where it is not regularly used and enable when patched.
b) Develop policies and procedures requiring the System Administrator to obtain all applicable patches and record them on a database.
c) Require the System Administrator and Information Security Officer (when hired) to schedule the applying of these patches by their risk to the GIAC.
d) The System Administrator is required to apply all patches within 21 days.
e) Inform GIAC management weekly of vulnerabilities that are late so they can intercede have the IT department change priorities and patch the systems.
f) Require the Information Security Officer to verify patches have been successfully installed by running scanning software such as Retina.
g) Emergency patches may require the servers to be taken off line to apply the patch and safeguard the organization.
h) These items put a system of checks and balances between the System Administrator, Information Security Officer and GIAC management that did exist before.

Remote Access:

GIAC provides its sales personnel and management staff with laptops when traveling for dial access to their internal databases and web server. Dial-up access is necessary at GIAC for sales personnel inquires on auto parts availability, cost, sales statistics, and performing sales transactions for customers. However, dial-up access is not completely secure at GIAC because: users log-on to the Shiva device using a generic password; and the Shiva software is set to allow unlimited log-on attempts instead of the standard three attempts recommended.

Unauthorized users with war dialing software can guess the Shiva password. Beyond this the hacker will be presented with the GIAC network log-on screen that allows five attempts before disconnecting the IP address. With a software program and using a dictionary of frequently used passwords a determined hacker could attempt to guess any valid GIAC password. Once inside the system the hacker would have the same access rights as the person whose password they guessed. With the right access the hacker who may also be a competitor could download: GIAC customer lists: sales history, inventory and financial data. The unauthorized user could place a trap door in the web application to obtain credit card information. Once inside the internal network applications a destructive hacker could exploit known vulnerabilities or corrupt database records

The likelihood of this risk affecting GIAC's internal files is medium/high but exploiting the vulnerability would be difficult because of having to guess the password at two levels. However, it could be done because of the weak security controls over dial-up by allowing unlimited access attempts and not disconnecting the remote device. Contributing to this risk is that GIAC users don't change their passwords every 90 days. Another control weakness is that Network Logon allows sometimes unlimited attempts without disconnecting, it depends on system administrator since there is no policy. This is a critical risk at GIAC because even one incident could be very damaging. Compromise of GIAC's internal servers and highly valued customer lists is a risk GIAC does not need to take. Corruption of GIAC data could cause harm to GIAC reputation and loss of sales. Also there is the risk that any successful penetration would go undetected and be repeated by the hacker.

Steps to mitigate risk:

a) Set Shiva software to only allow 3 to 5 attempts before the system disconnects the device for at least 30 minutes.
b) Review access logs on the Shiva to determine if users are attempting to logon numerous times
c) Discontinue the use of generic passwords being assigned to authorized laptop remote users.
d) Require that the user generate their own password after the initial logon. If the software can't set up to do this obtain dialup software and or a device that can.
e) Because of the risk associated with dialup consider a call back procedure for dialup that only connects to systems with authorized token.
f) Determine if all remote users really need the capability and if they don't use it, notify them and remove their access.
g) Backup all of GIAC's files frequently in case a hacker were to gain access and corrupt valuable database

No dedicated IT security person exists at CIAC

As is the case with many small IT organizations GIAC does not have a dedicated person performing the IT security functions. The threat to GIAC is that no one is dedicated to overall IT security making them an easier target for hackers. An Information Security Officer (ISO) would not eliminate all risk but they should reduce the number of risks by: researching new vulnerabilities, verifying that old ones are corrected; implementing new security software; and creating and maintaining security policies. GIAC's IT department consists of a senior and junior System Administrator. Their primary responsibilities are keeping the servers, workstations and network up and running. They spend a very small portion of their time reviewing security logs or applying patches. GIAC needs to hire a full time ISO to perform the functions listed below which are not be performed now:

a) Reviewing server security logs for invalid logon attempts and other suspect entries are seldom reviewed or investigated.

b) Ensuring that all patches are applied in a timely manner to all systems.
c) Anti virus software is up to date on all systems.
d) Documenting all security incidents.
e) Training all users in security basis on an annual basis.
f) Keeping management aware of the need for security.
g) Running system scans to determine if they have vulnerabilities that haven't been patched.
h) Implementing Intrusion Detection Software
i) Developing security policy and procedures with management approval

The security officer is dedicated to protecting the organization against attacks of known vulnerabilities. Detection of attempted or successful intrusions is also a goal of the security officer whenever possible. Without a security professional in places at GIAC there is little assurance that they haven't been hacked already. Even in well-managed Information Assurance departments there is a constant risk of being hacked because of the number of vulnerabilities that exist in the software and the Internet. The risk of not having a full time IT security person is that GIAC IT information is not protected to the extend it could be.

This presents a high risk to GIAC that could result in financial loss and public embarrassment and legal consequences. Hiring a person to perform the IT Security functions would reduce some of the vulnerabilities at GIAC and keep management better informed of what is required to even be mildly secure.

Steps to mitigate risk:

a) Take immediate steps to hire an experienced Information Security Officer (ISO) justifying it based on
b) The potential loss that could likely occur at GIAC. Use a contractor until one is hired to focus on the basic items such as patches and server logs.
c) Develop a position description for ISO based on best practices by SANS and other Security organizations.
d) Provide continual security to the ISO so they can be reasonably up to date with IT security
e) Place the ISO so they can be organizationally independent reporting to the CEO or Managing Director of GIAC
f) Require the ISO to develop security policies and procedures that will be effective in your organization.
g) Contract out for an IT Risk Assessment so high risk areas can be corrected first.

Security Policy:

GIAC did not have a written security policy. The following IT security policy was obtained from http://www.usm.edu/security/policy.html [2]

Information Technology Resource
Use and Security Policies

Introduction

The USM Faculty Handbook, Employee Handbook and Student Handbook address the rights and responsibilities of the corresponding segments of the university population. However, none of these documents directly address the additional responsibilities and issues introduced by the increasing use of electronic communication and data storage. This document is intended to supplement the previously mentioned documents and applies to all members of the university community utilize university-owned Information Technology Resources.

General Responsibilities

Users of university information technology resources:
must use these resources in a manner consistent with the University's mission
must limit use to levels that will not reduce the availability of resources for other users
must take steps to ensure that resources remain secure
must comply with any reasonable requests made by authorized system, network or security administrators
must abide by all applicable laws and regulations
must not attempt to access any resource which is not publicly available and for which the user has not been given prior authorization
must not attempt to misrepresent their identity in any electronic communications or while trying to access resource

Information Technology Resource Availability

The networks and servers on the USM campuses all have finite capacity and are shared by multiple users. As such, it is necessary for all users to limit their use of these resources to reasonable levels. Any activity that limits the ability of other users to access resources, whether intentional or accidental, is a violation of this policy. Accidental or unintentional disruption of network services may result from a poorly configured computer or from the use of applications that generate significant amounts of network traffic. Incidents that are determined to be accidental will be treated as such and no action will be taken beyond those necessary to resolve the situation. Incidents determined to be unintentional, but that occurred due to excessive use by the responsible individual will result in a warning and repeated incidents will be treated as intentional attacks on University resources. If it is determined that the network traffic was generated for the sole purpose of limiting

[2]

access to the affected resource (often referred to as a Denial of Service (DoS) attack), appropriate action will be taken by the University.

Illegal Activities

Copyrighted software/files The use of university information technology resources to collect, store, or distribute copyrighted materials (without proper authorization) is a violation of this policy. Such materials include movies, audio files, electronic documents, and software.

Possession

Some materials are illegal to possess even in electronic format. The most common examples of this category are child pornography and obscenity. The use of university information technology resources to collect, store or distribute this type of content is a violation of this policy.

Hacking

Any attempt to gain unauthorized access to information technology resources, whether they belong to the university or other entities on the Internet, is a violation of this policy. This includes, but is not limited to, scanning remote machines for the purpose of profiling running services, unauthorized scanning for vulnerabilities, execution of any script or exploit designed to grant elevated privileges on a target system, execution of any script, exploit, or tools designed to disable or overwhelm a target system, and obtaining or attempting to obtain other user's data or credentials by any means.

Misrepresentation

Any attempt by an individual to misrepresent or hide his or her identity in electronic communications is a violation of this policy. If such actions also violate any state or federal laws, the incident will be referred to the appropriate authorities. Any other illegal activities will also be considered a violation of this policy. Any violations of this policy that occur as a result of illegal activities will result in disciplinary action against the responsible individual. The incident will be reported to the appropriate authorities.

Unacceptable Use

Since the activities of the university's faculty, staff and students reflect on the university itself, actions that could tarnish the reputation of the university or expose it to liability are prohibited. Such actions include the actions listed in preceding sections of this document and the following:

- viewing, storing, collecting, or distributing pornography without a legitimate academic purpose
- generating any threatening or harassing electronic communications using university information technology resources for personal financial gain or profit

This list will be appended as other inappropriate activities are identified.

Rights of The University

Under routine conditions, the content of electronic communications is not monitored and network connectivity will not be revoked without informing affected parties prior to the interruption of service. However, the university has the authority to:

- monitor network traffic, including e-mail and Web browsing patterns
- impound university-owned computers for any reason
- disconnect any computer from the network for the purpose of isolating it for analysis or to protect other resources from attacks originating on the computer

Information Technology Resource Security

Maintaining the integrity of information stored in University systems is a responsibility shared by all users of those systems. As such, all users have certain security related responsibilities. Failure to properly implement these steps may lead to unauthorized access to confidential data, corruption of essential data or irreversible damage to university systems. If any of these events occur as a result of a failure to abide by these recommendations, the individual(s) responsible will be held accountable.

Passwords

All users are required to have their own username and password in order to access university systems. This is necessary to ensure resources are only being accessed by authorized individuals and to provide a mechanism for tracking unauthorized actions if they occur. It is never permissible for multiple individuals to share the same username and password.

In many cases, the only protection the university's computers and data have from unauthorized users is the password chosen by the individuals using the system. If users on systems are not using sufficiently complex passwords it becomes a fairly simple task for malicious individuals to gain access to systems by either guessing passwords or employing utilities designed to perform "brute force" password guessing until they gain access. For this reason, it is necessary for all users of University systems to use sufficiently complex passwords. As of the publication of this document, the minimum requirements for passwords on university systems are:

- they must be at least eight characters long
- they must not be based on a dictionary word
- they should consist of characters from at least three of the following four categories:
    - lowercase letters
    - uppercase letters
    - numbers and special characters (punctuation and mathematical symbols)
- In those rare situations where the software does not permit these requirements to be met, the user should satisfy as many password construction requirements as possible.
- For examples of appropriate passwords and for suggestions on how to generate good passwords for your accounts, please visit http://www.usm.edu/security/goodpasswords.html

Confidential Data

This policy strongly discourages the storage of any confidential or sensitive data on any computer or network-attached device that has not been explicitly approved by university information security personnel. Individuals working in areas that routinely deal with sensitive data are encouraged to store such data on removable media and to only insert the media in the computer while the data is actively needed. Strict adherence to this recommendation would significantly reduce the risk of data being inadvertently leaked as a result of a system mis-configuration, virus infection, or other mishap.

Furthermore, data of this type should never be transmitted via e-mail or other electronic communication protocols without taking specific actions to ensure that the content is encrypted. Many electronic communication protocols are inherently insecure, which may provide malicious individuals the opportunity to eavesdrop on your electronic “conversations.”

Virus Protection

All university-owned computers must have current anti virus software installed (where applicable; this does not apply to any systems for which anti virus software is unavailable). It is the responsibility of computer users to routinely verify that their anti virus software has been updated with the latest program version and that the virus detection database is the most current available. For additional information, see http://antivirus.usm.edu.

Software Updates

Individual departments are responsible for keeping the software installed on its computers properly maintained. Most software ships with a number of bugs that are later fixed with patches and service packs. If a computer does not have current patches and service packs installed, there is a fairly high probability that it will not run properly and a smaller probability that it will be vulnerable to remote attacks via the network. It is the responsibility of individual departments to keep its software updated to current levels. In the event that a department does not have access to individuals with the necessary technical expertise, the OTR Help desk (266-HELP) can arrange for technicians to help with the evaluation and installation of necessary patches. Generally, patches of this nature are provided by software vendors free of charge. In the event that patches are needed, but are not freely available, the affected department will be responsible for purchasing the updates. If this is not possible, OTR technicians can provide help in minimizing the risk associated with running the unpatched product(s), but they cannot guarantee that the product will run stable or securely.

Computer Access

All of the above steps are meaningless if unauthorized users can gain physical access to your computer. For this reason it is strongly recommended that unattended computers be stored behind locked doors and that all computers should be configured such that a password protected screen saver will initialize after a minimal period of inactivity (usually 5-10 minutes).

Contact Information

Violations of this policy may be reported to the Office of Technology Resources Security Services Administrator 24 hours a day/seven days a week at 266-5561 or via e-mail to security@usm.edu.

Additional Responsibilities for System Administrators

Any individual(s) responsible for the administration of server(s) has additional responsibilities as outlined below:

Server Registration

Effective September 1, 2002, in order for servers to be available from off campus, system administrators are required to register their server(s), including the services it (they) will be running and contact information, with university information security administrators. If at any time it is determined that the provided contact information is no longer valid, remote access to the server will be disabled until such time as security administrators are provided with updated information.

Discovered Vulnerabilities

Information security administrators will periodically scan the university's network looking for services vulnerable to remote attack or exploitation. In the event that vulnerable services are discovered, the system's administrator will be contacted with details about the vulnerability and a deadline for re-mediation. Under extreme circumstances, as in cases where active attacks are observed, the system will be immediately removed from the network and the system's administrator contacted. If the deadline passes without the issue being resolved, the affected system will be disconnected from the network until such time as the re-mediation has been completed.

Encryption

All remote authentication, remote sessions, and sensitive data transfers must be encrypted to minimize the risk that such information can be intercepted by malicious devices on the network. As such, network protocols that do not support encryption may only be used for "anonymous" communication of non-sensitive data (such as anonymous FTP and Web browsing). Other commonly used unencrypted protocols such as telnet, pop3, non-anonymous FTP, etc. are being phased out. This implementation will began October 2002 and continued through January 2003. During this implementation period, protocols were blocked at the perimeter firewall and any devices that were detected that communicate via these unencrypted protocols will be considered to be in violation of this policy and were treated as a security risk (i.e. as stated above, the system administrator will be contacted with a deadline for re-mediation and if the problem is not resolved prior to the deadline the machine will be removed from the network.) In cases where encrypted alternatives are not available, network and security administrators are working with the system administrator to take any steps necessary to minimize the risks inherent in unencrypted communications.

Logging

As a minimum, all servers should be logging both successful and unsuccessful login attempts to enable identification of brute force password guessing attacks and other anomalous usage patterns, as well as any attempts to modify critical system or application files. Where possible, these logs should not be stored locally on the logging machine, to protect them from any malicious users who might gain access to the machine. Where this is not possible, logs should be reviewed more frequently than indicated in the auditing section below.

Auditing

The logs for most devices should be reviewed on a weekly basis. However, any devices that contain sensitive data or that are essential to the proper functioning of the university should have their logs reviewed on a more frequent basis. Where possible, automated processes should be used to supplement manual log review to alert system administrators when unexpected conditions occur.

Patches

System administrators must apply operating system and application patches in a timely manner. The urgency with which these patches must be applied depends on the problem that the patch is designed to remedy. In the event that the patch is designed to increase performance or stability, the system administrator may apply it as his or her leisure. However, if the patch is security related and is designed to prevent malicious access to the server, it must be applied as soon as possible. In all cases, vulnerabilities enabling the remote compromise of servers should be patched within 10 hours of the patch becoming available. Failure to comply with this policy may lead to the server being removed from the network until such time as appropriate patches have been applied.

Evaluating the IT Resource use and Security Policy

The **purpose** of this policy is to inform all users of the University Computer resources on the acceptable use rules and security in place. The Introduction and General Responsibilities paragraph make it clear that this policy sets the rules for using university IT resources. The purpose would have had impact if contained a statement, Improper use of IT by some university members and increased hacker activity brought about the need for the policy.

The **scope** of this policy is the use and security of all university computer resources and it stated that it applies to all members of the university community.

Use **policy statements** for users concerning: General Responsibilities; Information Technology Resource Availability; Copyrighted software; Possession; Hacking; Misrepresentation; Unacceptable Use and Rights of the University were excellent items to include with the security policy. They state very specifically what users can and can't do with University IT resources. This coupled with warning banners negates the user excuse that they didn't know such things as using a system for personal use was against policy. The policy on Hacking did not clearly spell out the consequences that either GIAC or other entities would incur. This use portion of the policy is put in the revised policy for GIAC with minor changes.

Security policy statements included areas that should be part of any effective security policy. Since GIAC has no written security policy all the areas listed were reviewed and corrected if needed for the revised policy:

Passwords: This is a good policy because it goes into sufficient detail how easily passwords can be hacked if not a formulated in a complex manner. Also the password policy provides how your password must be formatted and provides a web site to go to for assistance. It does not however, say how frequently passwords should be changed or if the password will be edited for adherence to format.

Confidential Data: Agree with policy not to store confidential data on any network device that isn't certified by having extra protection. Also sensitive data should always be protected by using encryption such as PKI or PGP.

Virus Protection: Agree that all systems should have current anti-virus software but it should be a joint responsibility between IT and the security department. By this I mean the IT department should use software that updates the signature files at log-on. If they are still sending a script to go to the sever supplying the updates they risk users not performing the update and becoming infected.

Software Updates: Good warning that software is often shipped with bugs and should be patched. This would consist of applying the latest service pack and missing patches. The policy falls short on actually keeping the system out of production until its patched. Also the policy applies to each department, At GIAC the IT department will be responsible.

Computer Access: Policy on locking the computer up will not be used because GIAC systems are protected by a screen saver and timeout feature after 5 minutes of inactivity.

Server Registration: Is good practice to remind IT personnel because it provides an additional level of security for systems with remote user access.

Discovered Vulnerabilities: this policy should be listed near the patching policy. The good part about it is a system missing patches can be disconnected from the network. Also a deadline for correcting the system has to be set.

Encryption: A policy requiring encryption for sensitive data transmission is good rule because it protects the owners in the event that transmission is intercepted. This is extremely important since GIAC is entrusted with credit card numbers of its customer. It also stops the often-used practice of sending sensitive or confidential data over the non-secure Internet.

Logging and Auditing: Are required to have effective security. For GIAC I would combine these two areas into one because the logs are being kept for the audit review. Policy states that any system critical to the university must be reviewed more frequently then weekly. However, it doesn't t state, how often two times or three times per week?

Patches: does document the requirement for applying patches in a timely manner and attempts to define patches as either performance or security related. However most patches are security related and this policy fails to define what is a timely manner. The one exception is for applying patches within 10 hours for patches affecting vulnerabilities of remote access to servers. This policy relies on System Administrator judgement to determine what is a critical patch which even industry has trouble at times determining. Patches not determined to be critical are not scheduled for applying and no reporting to management is discussed. Accountability for ensuring all patches issue by Microsoft and other software are applied is not even discussed. More importantly no mention of oversight of patching by an information security officer is described.

Responsibility: The university stated that they have the right to alter, modify, or amend this policy at any time (subject to the approval of the University's Information Security Policy Review Committee). This leaves one guessing as to whom in the university wrote the policy. Was it written by the university IT and security personnel? No further details were provided on how the policy can be corrected or improved based on new technologies.

Action: Listed below are the primary actions/responsibilities for the IT use and security policy:

- All University Users – must abide by rules forbidding Hacking, possession of pornography, using computer resources for personal gain, harassment of others, etc. continuous - Users
- Passwords: mandatory format – Users but no requirement to change the password was provided.
- Server registration: complete by 9/2/02 – Systems Administrator
- Discovered Vulnerabilities – Immediate review – System Administrator
- Encryption: 10/2/02 – System Administrator
- Logging and Auditing- Weekly – System Administrator
- Patches – 10-hour period for applying patches for vulnerabilities affecting remote access to servers. For everything else the policy does not provide time parameters - System Administrator.

Revised GIAC IT Use and Security Policy:

1.0 Purpose:

This policy is intended to inform all GIAC employees of their user responsibilities and what GIAC considers as unacceptable use of GIAC computer resources. Included in this policy are the primary Security policies necessary to protect computer resources and who is required to maintain these policies. The need for this policy was brought about due to increased instances of unacceptable use by GIAC personnel and external hackers. It is important to GIAC integrity that its data especially customer data be accurate and completely confidential

2.0 Scope:

Specifically, the policy encompasses what GIAC users and IT staff must do to ensure that GIAC computer resources are used in acceptable manner. It applies to GIAC personnel either working at company facilities or communicating remotely. To a lesser extent it applies to GIAC customers who may attempt some form of unauthorized use. A major portion of the policy includes the security policies that users, IT personnel, system administrators and security personnel must adhere to.

3.0 Policy:

General Responsibilities

Users of GIAC information technology resources must:

a) Use these resources in a manner consistent with the GIAC's mission.
b) Limit use to levels that will not reduce the availability of resources for other users.
c) Take steps to ensure that resources remain secure.
d) Comply with any reasonable requests made by authorized system, network or security administrators.
e) Abide by all applicable laws and regulations.

f) Not attempt to access any resource which is not publicly available and for which the user has not been given prior authorization.
g) Misrepresent their identity in any electronic communications or while trying to access resource.

Information Technology Resource Availability

The networks and servers at GIAC all have finite capacity and are shared by multiple users. As such, it is necessary for all users to limit their use of these resources to reasonable levels. Any activity that limits the ability of other users to access resources, whether intentional or accidental, is a violation of this policy. Accidental or unintentional disruption of network services may result from a poorly configured computer or from the use of applications that generate significant amounts of network traffic. Incidents that are determined to be accidental will be treated as such and no action will be taken beyond those necessary to resolve the situation. Incidents determined to be unintentional, but that occurred due to excessive use by the responsible individual will result in a warning and repeated incidents will be treated as intentional attacks on GIAC resources. If it is determined that the network traffic was generated for the sole purpose of limiting access to the affected resource (often referred to as a Denial of Service (DoS) attack), appropriate action will be taken by the University.

Illegal Activities

Copyrighted software/files The use of GIAC information technology resources to collect, store, or distribute copyrighted materials (without proper authorization) is a violation of this policy. Such materials include movies, audio files, electronic documents, and software.

Possession

Some materials are illegal to possess even in electronic format. The most common examples of this category are child pornography and obscenity. The use of GIAC information technology resources to collect, store or distribute this type of content is a violation of this policy.

Hacking

Any attempt to gain unauthorized access to GIAC information technology resources, whether they belong to the GIAC or other entities on the Internet, is a violation of this policy. Any incident where GIAC employees or entities outside of GIAC are found to have attempted or gained unauthorized access could result, in dismissal; notification of authorities for prosecution; and removal of the individuals access rights to the system. This includes but is not limited to: scanning remote machines for the purpose of profiling running services; unauthorized scanning for vulnerabilities; execution of any script or exploit designed to grant elevated privileges on a target system; execution of any script; exploit, or tools designed to disable or overwhelm a target system; and obtaining or attempting to obtain other user’s data or credentials by any means.

Misrepresentation

Any attempt by an individual to misrepresent or hide his or her identity in electronic communications is a violation of this policy. If such actions also violate any state or federal laws, the incident will be referred to the appropriate authorities. Any other illegal activities will also be considered a violation of this policy. Any violations of this policy that occur as a result of illegal activities will result in disciplinary action against the responsible individual. The incident will be reported to the appropriate authorities.

Unacceptable Use

Since the activities of the GIAC personnel reflect on the GIAC itself, actions that could tarnish the reputation of the GIAC or expose it to liability are prohibited. Such actions include the actions listed in preceding sections of this document and the following:

- viewing, storing, collecting, or distributing pornography without a legitimate academic purpose
- generating any threatening or harassing electronic communications using university information technology resources for personal financial gain or profit

This list will be appended as other inappropriate activities are identified.

Rights of GIAC

Under routine conditions, the content of electronic communications is not monitored and network connectivity will not be revoked without informing affected parties prior to the interruption of service. However, the GIAC has the authority to:

- monitor network traffic, including e-mail and Web browsing patterns
- impound university-owned computers for any reason
- disconnect any computer from the network for the purpose of isolating it for analysis or to protect other resources from attacks originating on the computer

Information Technology Resource Security

Maintaining the integrity of information stored in GIAC systems is a responsibility shared by all users of those systems. As such, all users have certain security related responsibilities. Failure to properly implement these steps may lead to unauthorized access to confidential data, corruption of essential data or irreversible damage to GIAC systems. If any of these events occur as a result of a failure to abide by these recommendations, the individual(s) responsible will be held accountable.

Passwords

All users are required to have their own username and password in order to access university systems. This is necessary to ensure resources are only being accessed by authorized individuals and to provide a mechanism for tracking unauthorized actions if they do occur. It is never permissible for multiple individuals to share the same username and password.

In many cases, the only protection the GIAC computers and data have from unauthorized users is the password chosen by the individuals using the system. If users on systems are not using sufficiently complex passwords it becomes a fairly simple task for malicious individuals to gain access to systems by either guessing passwords or employing utilities designed to perform "brute force" password guessing until they gain access. For this reason, it is necessary for all users of GIAC systems to use sufficiently complex passwords. As of the publication of this document, the minimum requirements for passwords on university systems are:

a) they must be at least eight characters long
b) they must not be based on a dictionary word
c) they should consist of characters from at least three of the following four categories:
   - lowercase letters
   - uppercase letters
   - numbers and special characters (punctuation and mathematical symbols)

d) The software will edit the password you enter to determine if it is formatted correctly and to ensure the same password as before is not used.
e) In rare situations where the software does not permit these requirements to be met, the user should satisfy as many password construction requirements as possible.
f) All GIAC employees will be required to change their password every 90 days. Employees will be prompted daily at log-on and given the opportunity to change their password ten days prior to end of the 90 days.
g) Passwords not changed will expire after the 90 days and employees will have to reapply for access.

Confidential Data

This policy strongly discourages the storage of any confidential or sensitive data on any computer or network-attached device that has not been explicitly approved by GIAC information security personnel.

a) Individuals working in areas that routinely deal with sensitive data are encouraged to store such data on removable media and to only insert the media in the computer while the data is actively needed.
b) Strict adherence to this recommendation would significantly reduce the risk of data being inadvertently leaked as a result of a system's poor configuration, virus infection, or other mishap.

c) Furthermore, data of this type should never be transmitted via e-mail or other electronic communication protocols without taking specific actions to ensure that the content is encrypted. Many electronic communication protocols are inherently insecure, which may provide malicious individuals the opportunity to eavesdrop on your electronic "conversations."

Virus Protection

All GIAC-owned computers must have current anti virus software installed (where applicable; this does not apply to any systems for which anti virus software is unavailable). It is the responsibility of computer users to routinely verify that their anti virus software has been updated with the latest program version and that the virus detection database is the most current available

Software Updates

GIAC IT department is responsible for keeping the software installed on their computers properly maintained. Most software is shipped with a number of bugs that are later fixed with patches and service packs. If a computer does not have current patches and service packs installed, there is a fairly high probability that it will not run properly and a smaller probability that it will be vulnerable to remote attacks via the network.

a) It is the responsibility of GIAC IT department to keep software updated to current levels. Generally, patches of this nature are provided by software vendors free of charge.
b) Systems missing critical patches will not be installed on the network until patched.

Computer Access

All of the above steps are meaningless if unauthorized users can gain physical access to your computer. For this reasons users should perform use the Task Manager and lock the computer from access. All computers should be configured such that a password protected screen saver will initialize after a minimal period of inactivity for (usually 5-10 minutes).

Additional Responsibilities for System Administrators

Any individual(s) responsible for the administration of server(s) has additional responsibilities as outlined below:

Server Registration

Effective September 1, 2002, in order for servers to be available for remote access, system administrators are required to register their server(s), including the services it (they) will be running and contact information, with GIAC administrators. If at any time it is determined that the provided contact information is no longer valid, remote access to the server will be disabled until such time as security administrators are provided with updated information.

Discovered Vulnerabilities

a) Information security administrators will periodically scan GIAC's network looking for services vulnerable to remote attack or exploitation.
b) In the event that vulnerable services are discovered, the system's administrator will be contacted with details about the vulnerability and a deadline for re-mediation.
c) Under extreme circumstances, as in cases where active attacks are observed, the system will be immediately removed from the network and the system's administrator contacted.
d) If the deadline passes without the issue being resolved, the affected system will be disconnected from the network until such time as the re-mediation has been completed.

Encryption

All remote authentication, remote sessions, and sensitive data transfers must be encrypted to minimize the risk that such information can be intercepted by hackers on the network.

a) As such, network protocols that do not support encryption may only be used for "anonymous" communication of non-sensitive data (such as anonymous FTP and Web browsing). Other commonly used unencrypted protocols such as telnet, pop3, non-anonymous FTP, etc. are being phased out.
b) This implementation will began October 2002 and continued through January 2003.
c) During this implementation period, protocols were blocked at the perimeter firewall and any devices that were detected that communicate via these unencrypted protocols will be considered to be in violation of this policy. They will be treated as a security risk (i.e. as stated above, the system administrator will be contacted with a deadline for re-mediation. If the problem is not resolved prior to the deadline the machine will be removed from the network).
d) In cases where encrypted alternatives are not available, network and security administrators are working with the system administrator to take any steps necessary to minimize the risks inherent in unencrypted communications.

Logging and Auditing

a) As a minimum, all servers should be logging both successful and unsuccessful login attempts to enable identification of brute force password guessing attacks and other anomalous usage patterns, as well as any attempts to modify critical system or application files.
b) Where possible, these logs should not be stored locally on the logging machine, to protect them from any malicious users who might gain access to the machine. Where this is not possible, logs should be reviewed more frequently than indicated in the auditing section below.
c) The logs for most devices should be reviewed on a weekly basis. However, any devices that contain sensitive data or that are essential to the proper functioning of GIAC should have a sample of these logs reviewed at least daily.

d) Where possible, automated processes should be used to supplement manual log review to alert system administrators when unexpected conditions occur.

Patches

Patches are provided by vendors to correct security vulnerabilities in their software. Once identified these vulnerabilities become new targets for hackers both inside and outside the organization. Failure to apply patches in a reasonable amount of time puts GIAC at an unnecessary risk for attack and compromise by hackers. A report by the CERT Coordination Center at Carnegie Mellon estimates that 99% of all reported intrusions “result through exploitation of known vulnerabilities or configuration errors, for which countermeasures were available” by Patrick Evans in “Is patching a priority for your enterprise?” http://www.itweb.co.za/office/symantec/0203140754.htm [3].

At GIAC the following policy will be followed to keep our software up to date against attacks on known vulnerabilities:

System Administrator will access Microsoft Security / Downloads Web site [1] and Carnegie Mellon Cert Coordination Center (CERT/CC) [4] to obtain all security patches.

a) A database will be maintained by System Administrator for all security patches downloaded with date obtained, scheduled, tested and applied. The System Administrator and Information Security Officer will review the database daily and schedule the most critical patches followed by least critical ones.
b) Software that can’t be patched immediately during the day because it could adversely affect production will be scheduled for off peak production times.
c) For those system with vulnerabilities deemed as a high risk to GIAC and needing patched immediately in the judgment of the System Administrator and Information Security Officer. Inform GIAC management immediately that the system performance may be degraded or that it may have to be taken off line till patched.
d) System Administrator will test and apply the patches by the scheduled date or submit a report to management stating when they will be patched.
e) The System Administrator will use automated processes such as SMS whenever possible to apply. If time permits patches should be applied anytime and not wait for the scheduled date.
f) On a weekly basis GIAC Management and Information Security will review all late items justification and determine if the new date for completion is acceptable. If it’s not acceptable they will change the scheduled date and notify the System Administrator.
g) System Administrator and Information Security Officer will audit a
h) sample of the systems patched to determine that the patch actually was applied.

[3]

[1]

[4]

4.0 Enforcement:
Any GIAC employee or external user who violates this policy may be subject to disciplinary action, up to termination and/or criminal prosecution.

5.0 Responsibility of this Policy:
The Information Security Officer (ISO) and IT Department are responsible to ensure this policy is being adhered to properly. The System Administrator is to assist (ISO) in documenting all security incidents affecting this policy or other IT security areas. Review and updating of this policy is to be performed by ISO at least yearly or as required by significant changes in technology. All changes must be approved by GIAC management and the IT department prior to publication. Violations of this policy will be reported by the ISO to GIAC management and or local law enforcement personnel.

6.0 Action:

a) Users must change their password every 90 days.
b) System Administrators must be registered for remote access by 9/1/02.
c) System Administrators unencrypted protocols such as Telenet will be phased out by 1/1/03.
d) System Administrators and ISO will review server logs daily if they contain sensitive data or weekly if they don't contain sensitive data.
e) New vulnerabilities will be reviewed on a daily basis
f) Security patches will be installed by the scheduled date or reported to GIAC management.

Develop Security Procedures

GIAC Applying Security Patch Procedures

Purpose:
These procedures are to ensure that all Security Patches for vulnerabilities are reviewed, obtained, recorded, scheduled, tested, applied and verified in a timely manner. The procedures intent is have the most secure computer system possible at GIAC and not be needlessly exposed to attacks on known vulnerabilities.

Who:
The System Administrator, Information Security Officer, GIAC management and to a limited extent GIAC users.

When:

The procedure is performed on a daily basis by the System Administrator and reviewed by the Information Security Officer and on a weekly or as needed basis by GIAC management.

How:

a) The System Administrator logs on to the Microsoft Security Web site [1] and reviews those vulnerabilities listed to determine which ones are applicable to GIAC Windows 2000 environment. Also review Carnegie Mellon, Cert coordination Center (CERT/CC) web site at http://www.cert.org/meet_cert/meetcertcc.html [4] to determine if vulnerabilities exist that weren't mentioned in the Microsoft web site. Also this site offers a best practice guide to protect IT infrastructure reference System and Network Security Practice http://www.kb.cert.org/vuls [5].

b) System Administrator downloads all the applicable patches and related documentation containing the complete description of the vulnerability and creates the required fields such as patch number description and applicable GIAC hardware.

c) The System Administrator and the Information Security Officer will then review the items in the Database and schedule by prioritizing the most critical first and according to the amount of patches that can be applied by GIAC in one day.

d) If the description of the vulnerability describes that if the software is not patched GIAC systems could be accessed or damaged by personnel then patch implementation should be considered a critical task.

e) Those security patches determined not to be critical will be scheduled so as to not exceed 21 days until applied.

f) All patches for application to GIAC systems will be downloaded by the System Administrator who will stage the patch to accomplish applying the patch to all servers, workstations, laptops.

g) The completed schedule will be provided to GIAC management and the Information Security Officer at least weekly or when items are late being applied. Include in this report will be an explanation of why the item is late being patched and what is being done to mitigate the risks and a projected date for completion.

h) All patches for application to GIAC systems will be downloaded by the System Administrator who will stage the patch to accomplish applying the patch to all servers, workstations, laptops.

i) Users are not allowed to download or apply patches because of the risk associated with mobile code.

j) Laptops not connected to the system because of traveling will be patched as soon as the user returns.

k) The System Administrator will test the downloaded patch on a test machine to determine if it doesn't cause unintended problems.

[1]

[4]

[5]

l) The System Administrator applies multiple patches to all workstation and servers affected where possible using SMS software. Update the schedule to reflect the number of systems patched.
m) The Information Security Officers audits the updated database on a daily basis to ensure it's accurate.
n) Information Security Officer performs scans on all GIAC systems to verify if appropriate patches were applied. The System Administrator is informed of any that where not patched.

References:

1. Microsoft Corporation, Continuous "Security and Downloads" URL: HTTP://WWW.MICROSOFT.COM/SECURITY (3/29/03)

2. The University of Southern Mississippi, 2/11/03 Information Technology Resource "Use and Security Policy" Pages 1through 8 URL:http://www.usm.edu/security/policy.html (3/2/03)

3. Patrick Evans, 3/14/2002 " Is Patching a priority for your enterprise" Page 1, paragraph 3&4 URL: http://www.itweb.co.za/office/symantec/0203140754.htm (3/15/03)

4. Carnegie Mellon Cert Coordination Center (CERT/CC) continuous entire site and Vulnerabilities, Incidents and fixes URL: http://www.cert.org/meet_cert/meetcertcc.html (3/14/03)

5. Carnegie Mellon Cert Coordination Center (CERT/CC) continuous entire site " Vulnerability Notes Database. URL : http://www.kb.cert.org/vuls (5/4/03)

6. Microsoft Corporation, Continuous, 5/4/04 "Microsoft Security" and "Microsoft Security Toolkit" URL: http://www.microsoft.com/servers/techinfo/security.asp#2000 (5/4/04)