# Global Information Assurance Certification Paper

# GIAC Policy Analysis

**SANS GIAC**
**GISO Practical**
Version 1.2

**Neil R. McInnis**

## GIAC Policy Analysis

### Introduction

This paper will demonstrate how effective policies and procedures can be developed in order to mitigate security risks. To craft good policy, the author must first identify the risks that exist within the organization. This can only be achieved after gaining a thorough understanding of how the business operates. A significant amount of time will be spent describing the business of GIAC Enterprises, from its business model and daily operations to its IT (Information Technology) infrastructure. With this background to draw upon, an analysis of one of GIAC's current security policies will be conducted, and recommendations will be made that will help GIAC better protect its assets.

### The Nature of the business

GIAC Enterprises ("GIAC") is a privately held tax software vendor. GIAC develops, markets, ships, and supports its accounting package, "GIAC Pro Tax." Pro Tax is used by accounting professionals to streamline the tax form preparation process. The product includes a wide array of accounting and tax-related forms, templates, and reference data that are used by nearly every accounting practitioner in the United States. The vast majority of GIAC's customers are small accounting firms, which cannot afford the high-powered and expensive accounting software packages offered by most of GIAC's competitors. GIAC's marketing angle is to produce quality software that will get the job done for the small firms it caters to.

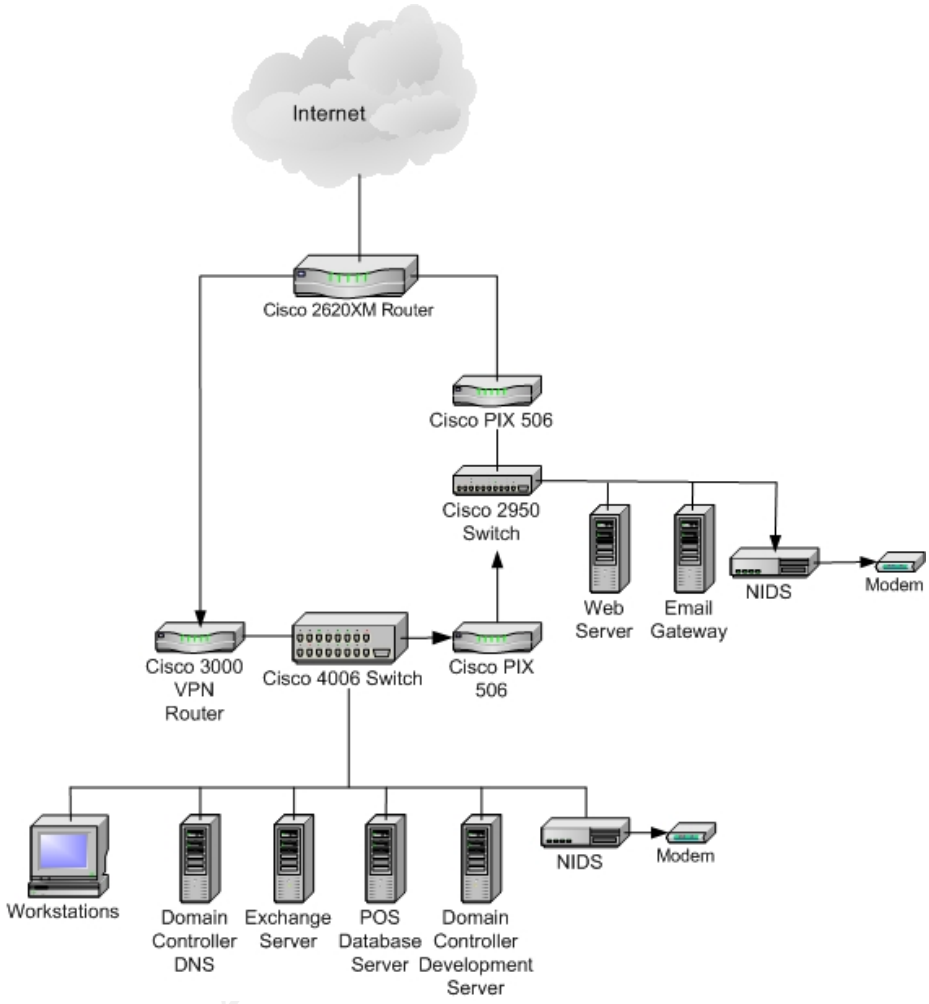
### IT Infrastructure - Network description

The chief duty of the IT department is to maintain the Point of Sale (POS) application and its associated databases, servers, and the supporting network infrastructure. Page 4 contains a network diagram that details the major components of GIAC's IT infrastructure. Unless otherwise noted, all of the servers at GIAC are Windows 2000 Server-based, and run on Dell Power Edge (PE) servers configured at RAID 10 (Redundant Array of Inexpensive Disks). The operating system segment of the RAID system is mirrored; the data storage area is striped with parity. All instances of Windows 2000 have had service pack 3 applied.

At the core of GIAC's operation is the POS system. Since practically all of its processing is back-end, the server must be powerful and reliable. The hardware chosen as a platform for the POS system is a Dell PE 6650, with dual Intel Xeon processors. The system stores its data in Microsoft's SQL Server 2000 databases, which reside on this same computer. POS is accessible to its users via web browser, and Microsoft Internet Explorer version 6 is the standard browser at GIAC. The system requires each user to log in for access. Access for each user and group is determined according to the organization's access and permissions policy, which assumes a deny-by-default posture. POS users are given only the access levels needed to perform their duties. For example,

personnel in the shipping department are able to access customer names and addresses, but have no ability to access credit card information.
For its email system, GIAC uses Microsoft's Exchange 2000 server, which integrates with the company's Active Directory domain infrastructure. The Exchange system runs on a PE 2650. All GIAC employees have their own email accounts, and use Microsoft Outlook 2002 to access data from the email server.
GIAC has two Windows 2000 domain controllers.
One of these servers is configured as an Active Directory-integrated Dynamic DNS (Domain Name System) server as well. This machine is a PE 1650, and uses RAID 1 (mirroring) because as a network services system, it does not house critical data and a RAID 5 array is unnecessary. It performs internal DNS duties, and forwards DNS resolution requests for non-GIAC resources to specified Internet DNS servers. It is not able to accept DNS queries from outside the trusted LAN (Local Area Network).
The other domain controller server also doubles as a file server for the development department. This machine performs much more file storage than the other domain controller and is configured with a RAID 10 array, and has plenty of hard drive space available. The development team writes GIAC Pro Tax using Microsoft's Visual Basic, and uses Microsoft Visual Source Safe to manage version control. The master program code resides on this server, along with all of the other miscellaneous files that the development team uses.

**GIAC Enterprises**
Network Diagram




In the DMZ (DeMilitarized Zone or DeMarcation Zone) is where GIAC's public-access web server is located. This server uses Microsoft's Internet Information Server (IIS) version 5.0 to render the company's web site. The web server is not a member of any Windows domain; it is a standalone server. The hardware itself is a Dell PE1650, at RAID 1. IISLockdown has been implemented on the web server. According to Microsoft, this tool works by disabling unnecessary IIS features, thus providing a smaller avenue of attack for hackers.[i]
GIAC uses another similarly configured server as its Internet email gateway. The major difference between the two DMZ servers is that the SMTP (Simple Mail Transport Protocol) gateway does not have the World Wide Web Publishing service running; instead it has Microsoft SMTP service running. The SMTP server has been configured to disallow open relaying. With open relaying disabled, GIAC is helping to preserve its reputation by not letting those with ill intent use the server to forward "spam" or UCE (Unsolicited Commercial Email). Also located in the DMZ is one of GIAC's two Network Intrusion Detection Systems (NIDS). The other NIDS computer is located on the trusted network, and is plugged into a span tree port on the company's Cisco 4006 network

switch. This configuration allows the NIDS to analyze all of the traffic on the LAN, not just traffic from a single switched segment. The NIDS computers are both Dell PE350 servers, which use Microsoft Windows 2000 Professional as their operating system. Snort version 1.9.0 has been chosen as the company's intrusion detection program. In the case of both NIDS machines, the Network Interface Card (NIC) has been configured to run in promiscuous mode and with no protocols bound. This renders the NICs incapable of transmitting any data, but able to "hear" all traffic that is transmitted to them. Each NIDS has an external modem, each set to dial out only, and each with its own dedicated analog phone line. The result of this configuration is that the computers are not addressable via the Ethernet network, and are highly resistant to compromise unless the attacker has physical access.

GIAC's workstations consist of three different models of Dell computers, all running Microsoft Windows 2000 Professional. Eight members of GIAC's marketing department are road warriors, and have Dell Precision laptops with Windows 2000 Professional.

The Local Area Network (LAN) infrastructure at GIAC consists of purely Cisco brand networking devices. The core switch is a Cisco Catalyst 4006, which runs Cisco IOS version 12.1. Virtually all data on the GIAC network travels through this switch. Attached to this 4006 is a Cisco 3000 VPN (Virtual Private Networking) concentrator. While traveling, marketing department personnel connect to the network through the VPN device, using Cisco's VPN client, version 3.6.3. They connect to the network mainly so they can correspond with other GIAC employees via email in a secure manner. When necessary, they can also access the POS system through the VPN. All the servers and workstations are connected to the 4006 (via patch panel) as well.

Moving from the trusted LAN toward the DMZ is a Cisco PIX 506 firewall running PIX 6.2.2 software. Egress filtering for the trusted LAN is performed by this firewall. The only traffic allowed inbound through this firewall is SMTP from the email gateway server on the DMZ.

Connected to the interior PIX firewall is a Cisco Catalyst 2950-12 switch, at IOS version 12.1. This serves as the DMZ switch. The SMTP gateway, the web server, and the DMZ NIDS machines are all connected directly to this switch.

Traveling outbound from here, the next device is the external Cisco PIX 506, also running PIX 6.2.2. Besides a limited amount of traffic filtering performed by the border router, this firewall constitutes GIAC's first line of defense from Internet attackers. The rules on this firewall severely restrict egression from the nodes on the DMZ network. In fact, the only traffic allowed out from the DMZ network is DNS and SMTP.

The last device before the Internet is a Cisco 2620XM router, which serves as GIAC's border router.

Wherever possible, nodes on the GIAC internal network communicate through Ethernet on Category 5E network cable. All nodes communicate at least at 100Mb, full duplex. All servers and many workstations are equipped with Gigabit Ethernet NICs.

Nightly backups are performed automatically by software and a tape backup device on the Network Administrator's workstation. This machine is locked in an office, and only the Network Administrator, the CEO (Chief Executive Officer), and the IT Manager have keys. On Monday mornings, the Friday night full backup tape is placed in a lock box and picked up by a data storage contractor, then returned to GIAC a month later. GIAC has chosen to use a combination of incremental and full backups, with a one month tape rotation scheme. Backup tapes that remain onsite are stored in a fire safe in the server room. The Backup Operator, the IT Manager, and the CEO have the combination.

The main antivirus product in use is Trend Antivirus. The workstations all use Trend Office Scan version 6.15, and the servers use Trend Server Protect version 5.0. Additionally, the email gateway server uses Symantec Antivirus for SMTP Gateways, version 3.0. The internal Exchange server scans with Sybari Antigen 7.0. Antigen is configured to use updated pattern files from both Symantec and Trend.

Each employee wears a photo identification badge with a magnetic stripe on the back. These cards are used to gain access to various areas of the GIAC office building. The server room is locked at all times, and is access-controlled by magnetic stripe card readers. Each workstation is set to activate a password-protected screen saver after 10 minutes of nonuse. Additionally, employees are instructed to lock their workstations while they are away. GIAC cyber security policy dictates that passwords will not be shared with others, and that they will not be written down, as they could be compromised easily. All passwords must be at least 12 characters in length, use a combination of upper case, lower case, digits, and special characters, and must be changed at least every 60 days. This password policy is enforced by Windows 2000 domain policy. In the server room, each server and workstation is subject to the same policy as the workstations outside the server room; they are locked when not in use, and have password-protected screensavers implemented. Light-duty paper shredders are located in each office or cubicle; heavy duty shredders can be found in copy rooms.

**Business Operations - How does GIAC Conducts Business**

The flow of business at GIAC is fairly straightforward. The firm is made up of about 200 employees divided into six separate departments: Development, Marketing, Sales, Support, Shipping, and Information Technology (IT). The entire operation is housed in a single facility in an urban office park. GIAC is the only occupant of the building.

Due to the nature of the business of its customers, GIAC operates based on an annual product development cycle. Accounting and tax laws change from year to year, and in order to stay competitive, GIAC's software must keep pace with these changes.

The business cycle at GIAC begins on the first of May each year, immediately after the surge in demand created by the dreaded April 15th tax filing deadline in the United States. This is known as the development phase. It is during this

time that the development team studies changes in tax and accounting laws, and incorporates the changes into the software model before its release date, at the beginning of the next tax season. The Programmers on the development team stay busy updating and debugging the code throughout the development phase. "Tax season" is from approximately January first through the end of April. This phase is marked by sharply increased volume in sales, as well as increased workload for the Customer Support staff.

The sales cycle at GIAC typically begins at an industry trade show. GIAC's marketing team attends these trade shows nationwide throughout the year. They operate an information booth with a live demonstration of GIAC Pro Tax for the potential customers to watch. Customers take brochures, business cards, etc. back to the office with them.

When the customer calls GIAC to discuss purchasing their copy of the software, the call is answered by a member of the sales team. (GIAC chooses not to sell its product directly over the Internet in the traditional e-commerce manner because the final price varies depending on the outcome of negotiations between the sales staff and the customer. The GIAC website is merely an informational site.) When the sales representative closes the deal with the customer, the customer's information is entered into GIAC's POS (Point Of Sale) application. The sales person also enters the customer's credit card information into a browser-based credit card processing application. This process involves an SSL-protected (Secure Socket Layer) communication between GIAC and its online credit card processing service. The transaction is processed within seconds of submission. When the credit card information is approved, the sales person finalizes the transaction in the POS system.

Throughout the day as sales are finalized, the shipping department's portion of the POS application extracts customer shipping information and prints the required mailing labels. The shipping crew boxes the product, attaches the shipping label, and places the outbound packages in the shipping queue for delivery. The sales process ends when the customer receives the software in the mail. If the customer has problems or questions regarding the software, a call to the support staff is in order. The support staff handles the majority of its calls during tax season, as all the customers are busy preparing tax forms for their clients. For support phone calls that require the customer to purchase support, the same credit card billing procedure is followed as with the sales process. Support-related data is maintained in the POS database, and is used for trend analysis, troubleshooting reference for the support staff, as well as product improvement information for the development staff.

In the context of business operations, the most critical points on GIAC's network are the POS database server, the Cisco 4006 switch, and the Cisco 2620XM border router. The POS server maintains all customer and sales data. Without this service available, the company would not be able to sell product efficiently. The border router helps provide GIAC's Internet connection, which enables GIAC to process credit cards. The 4006 switch enables all the components to communicate with each other.

**Risk Identification**

Like any organization with a network, GIAC is able to identify many risks to its electronic resources. For the purposes of this paper, three of these risk areas will be addressed.

GIAC's most valuable information asset is the Pro Tax source code. The greatest risk concerning the source code is theft. If the Pro Tax source code were compromised, GIAC's competition could gain detailed knowledge about how the program works, and then sell essentially the same product to the public for a much lower price. GIAC has focused much of its energy on protecting its data from insiders as opposed to concentrating on the threat of outside attack, since the primary threat to computer systems has traditionally been the insider attack, according to Lawrence E. Bassham and Timothy Polk in their composition *Threat Assessment of Malicious Code and Human Threats*.[ii]

Several different measures have been taken to secure this data from such attacks. The data resides on a server that has been well hardened, and it sits behind both firewalls. The server's file systems are on NTFS (NT File System) volumes with RAID redundancy. Access lists are in place in the Active Directory system. Other measures include logon hours enforcement and deny-by-default file system permissions. Only those developers who have a legitimate business need to access the source code are allowed to do so. Additionally, not all developers have access to all the code. Each programmer or developer can only access the module(s) for which he or she is responsible. Developers who have access to the code are by policy not allowed to take uncompiled code off GIAC property. To give this policy weight, the server and development workstations are denied access to the Internet by ACLs (Access Control Lists) on the interior PIX firewall. This keeps a thief from simply sending the code offsite via FTP, for instance. To prevent developers from taking the code off the premises on removable media, the workstations do not have CD burners, Zip drives, LS-120 drives, etc. and padlocks are used on the computers' cases. Developers are not granted VPN access from outside the network. Integrity of the source code is protected by strict file permission settings and the version control system. Availability is enhanced by housing the data on a server with UPS (Uninterruptible Power Supply) protection, redundant disks, as well as through daily tape backups.

In addition to these methods, GIAC has chosen to use legal means to help protect its code. Each person who has access to the code must sign a nondisclosure agreement as a condition of employment. This agreement holds the employee legally liable if compromise is traced back to him or her.

Merely getting access to the code is of course not difficult for developers. The difficulty a thief would face would be obtaining *all parts* of the necessary data to compile the entire program. (Only the lead developer has this level of access). First, a copy of each separate module would have to be obtained. This would require the cooperation of several different programmers, or the compromise of several of their passwords. Even after a rogue employee obtained all the code, he would still face the problem of getting it offsite. There is no such thing as

perfect security, but GIAC is comfortable with the level of risk that remains with these measures in place.

GIAC has identified laptop computer compromise as another area of risk that must be dealt with. As mentioned earlier, several of GIAC's employees spend a great deal of their time traveling. Because these employees spend so much time in airports, on trains, and in other unfamiliar places, the threat of laptop theft is very high. The major problem is that the laptops are set up to allow remote access into GIAC's network. Anyone who has access to one of these laptops could conceivably use it to do grave damage to the company. Also, email messages found on these computers frequently contain sensitive information that could be used against the company by its competitors. In the worst case scenario, an evil-doer could use a GIAC laptop to log into the company's network, find a way to browse (or alter or destroy) the company's sacred databases, and send email to customers or competitors that could damage GIAC's reputation. There would be no trace of any intrusion if legitimate login credentials were used. The only person to blame would be the employee who did not keep an eye on his laptop at the airport.

Mitigating the risks associated with mobile networking requires several steps. Since employees must have access to corporate data from the road, GIAC has implemented a VPN solution as discussed earlier. This provides encryption of sessions between the remote users and the home network. With VPN encryption, sniffing and session hijacking risks are reduced. Laptop users are given normal user permissions on their machines, as opposed to local administrative rights. This helps prevent users from installing unauthorized hardware such as 802.11b wireless cards, USB hard drives, etc.

The threats remaining are mainly those which require physical access or possession of the laptop itself. Employees already are good about following the common sense rules of laptop use; don't leave the computer unattended, don't write down or share passwords, etc. Probably the best way to further prevent compromise is by encrypting the entire hard drive. This would prevent anyone who did manage to steal the computer from simply copying all of its data onto another machine and misusing it. Employees are instructed to contact the IT department immediately if their laptop is stolen, or if they for any reason suspect that their account has been compromised. The IT staff can then disable the user's VPN and Windows domain accounts in order to limit the scope of potential damage.

A third risk identified is that the potential introduction of malicious code such as Trojan horses, viruses, and worms to GIAC's network via the Internet. This is the risk area I will concentrate on for the policy section of this paper. A current policy will be presented, critiqued, and rewritten to be more effective. Additionally, one procedure will be presented, which will aid in the enforcement of the new policy. In real life, each policy could have many procedures in place to support it, but for the purpose of this composition, only one procedure will be written.

The risk of "malware" (malicious software) is particularly high at GIAC due to the fact that the company uses several of the technologies listed as having vulnerabilities among the "SANS / FBI Top Twenty"[iii]

(http://www.sans.org/top20/). Examples of these technologies include Microsoft Internet Explorer, Microsoft SQL Server, NETBIOS, and others. Exploitation of vulnerabilities associated with these technologies could lead to the compromise of GIAC's crown jewels, the POS databases. To compound matters, GIAC currently uses a somewhat lax "*Acceptable Use of the Internet"* policy. Employees are able to visit any website they wish to, as there is no enforcement mechanism in place to prevent access to unauthorized Internet resources. The email system does employ several layers of antivirus protection, as discussed earlier. GIAC believes that its email-born virus/worm/Trojan risk is at a manageable level as a result of these protective measures. A significant risk remains however, of GIAC's Internet users visiting websites that employ malicious Active X controls, Java applets, VBScript, etc. that could potentially exploit one or more of the vulnerabilities associated with the technologies mentioned above, or other vulnerabilities that are not currently known. Some malicious websites exploit vulnerabilities in Internet Explorer, for example, and all these sites require from a victim is that the victim's browser "surf" to the site. Other malware is at least polite enough to ask the user's permission to install itself on the victim computer. Viruses, Trojans, back doors, keystroke loggers, and Denial of Service clients are ready and willing to infect GIAC's network. All it takes is for one user to simply visit certain malicious websites. If a GIAC network user were to become the victim of one of the myriad website-based threats, the resulting damage to GIAC's entire network and business could be severe. For example, security bulletin MS02-005 located on Microsoft's security website, describes six vulnerabilities in Internet Explorer, the worst of which can lead to an attacker running his code of choice on the victim's computer.[iv] "Code of Choice" is a broad term, and could certainly include unauthorized manipulation of GIAC's sensitive databases. To help mitigate the risk of malicious code as described above, I would recommend a 3-pronged approach. This approach would involve training, technology, and policy.

To help reduce GIAC's risk of contracting Internet-born pathogens from a training aspect, I would suggest the implementation of an end-user training program. Such a program might include a "Network Driver's License" testing program, semi-annual security awareness sessions, videos, mandatory online security knowledge testing, or any combination of these methods. Another recommendation would be to produce a handbook for all the users to reference. This should be written in plain language with examples of what bad things can happen as a result of unauthorized use of company resources. For example, "Opening unexpected email attachments is bad because the attachment could actually be a virus that will destroy all the data on your computer" or "Don't ignore warnings from your browser or antivirus software. Here's why…" Care should be taken in composing this manual; it must remain in fidelity with GIAC's policies.

From a technology aspect, I would recommend either of two solutions to help prevent malware from entering the organization through web browsers or other Internet vectors: 1) Removing the internal PIX firewall and replacing it with a Microsoft ISA 2000 server and a web filtering suite such as SurfControl's SuperScout for ISA Server; 2) Installing WebSense Enterprise v4.4.1, Cisco PIX

Firewall Edition. According to a description found on Microsoft's web site at http://www.microsoft.com/ISAServer , the ISA server acts as a proxy server and as an application-level firewall.[v] In GIAC's case, it would be used as a proxy server with the SuperScout software installed, and as the firm's internal firewall in the DMZ. (ISA Server and SuperScout would be installed on a multi-homed server-class Windows 2000 computer.) SuperScout is an add-on module for ISA server that allows an administrator to specify which web sites are allowed and disallowed by using rule sets similar to those in a firewall. Web sites or types of web sites known to be risky could be blocked, which would reduce the risk of malicious code entering GIAC's network via web browser. As an added feature, this method would deepen GIAC's defense posture by introducing a second type of firewall into the DMZ. In other words, a vulnerability that allowed an attacker to penetrate the external PIX firewall would probably not exist on an ISA server. The attacker would then have to start from scratch in order to penetrate a second type of firewall.

The WebSense method would work in conjunction with the existing PIX firewall to intercept traffic that is bound for an off-limits website. The internal PIX firewall "asks permission" of the WebSense server to allow each unique outbound request. If the destination host or domain is found in the Web Sense "black-list" the request is denied, and the user's browser is rerouted to an internal web page informing them that the site they have requested is off-limits. Like SuperScout, Web Sense depends on administrator input and optionally, a subscription service in order to keep its black-list current. Web Sense offers an added feature for blocking Spyware[vi] as well.

The IT staff would set the included rules on either product to deny access to hacking and other known malicious sites, and other unauthorized content. Either solution will make it possible for the IT staff to prevent users from visiting unauthorized websites, thus reducing the chance of introducing malicious code via that avenue. Access to Internet email websites such as Yahoo, AOL, and others could be blocked with WebSense or ISA/SurfControl as well. (POP [Post Office Protocol] traffic is already blocked by the external firewall.) Both solutions will provide the IT group with enhanced logging and reporting functionality, which can help enforcement efforts.

**Security Policy Evaluation**

The area of focus for the policy analysis segment of this paper is the risk of malicious code being introduced to GIAC's systems via the Internet. GIAC's "*Policy for Electronic Mail and Appropriate use of the Internet*" will be evaluated. This policy was taken from the author's place of employment, and is effective policy at the time of this writing. There are no procedures currently in place to support the enforcement of this policy:

Policy for Electronic Mail and Use of the Internet GIAC P 564.1 09-29-00

1. Cancellation: Cancels Electronic Mail Policy *GIAC* P 564.1, of 11-8-95

2. Electronic mail (E-Mail) and the Internet at *GIAC* are provided as communications and research tools for official *GIAC* business only.
3. *GIAC* employees and contractors do not have a right, nor should they have any expectation of privacy when using *GIAC* resources at any time, including *GIAC's* E-Mail system and accessing the Internet for personal E-Mail systems or other purposes.
4. All messages and attachments produced or received through *GIAC's* E-Mail system and/or the Internet are the property of *GIAC.*
5. Unauthorized uses of E-Mail technology and/or the Internet include, but are not limited to, those that: (1) result in a loss of productivity or impair the performance of *GIAC's* network; (2) are unlawful, abusive or potentially abusive to fellow employees or the public (e.g. gambling, hate speech or material that ridicules on the basis of race, creed, religion, color, sex, national origin, disability, or sexual orientation); (3) transmit sexually explicit or sexually oriented material; or (4) allow unauthorized access to controlled information (e.g., computer software, privacy information, classified or other non-public data, copyright, trademark or other intellectual property rights).
6. Misuse of *GIAC* resources is a violation of the law and can result in disciplinary action. Incidents of unauthorized use should be reported to *GIAC's* IT Manager. EEO-related incidents should be reported to the Diversity Programs Manager. In either case, the responsible supervisor should be notified.
7. E-Mail will be purged from the online E-Mail system 60 days after creation.
8. E-Mail and attachments that meet the definition of a GIAC record should be retained in accordance with established Record Management procedures.
9. E-Mail messages and Internet usage logs will be randomly reviewed to manage these GIAC resources.

*John Doe,* Vice President GIAC Enterprises

While the policy is weak overall, it does have a few strong points. It is concise; the entire policy fits on one printed page, which increases the likelihood that the employees will read it and be able to remember it. The policy begins with a cancellation statement, which prevents any ambiguity regarding which policy version is in effect. The policy states clearly that employees have no expectation of privacy when dealing with email or Internet resources. This serves as a sort of "catch-all" rule, which can work in the company's favor should it need to investigate employee resource usage for any unforeseen reason. The policy states concisely that every email message and any attachment(s) are the property of the company. This policy element reinforces the previous one by making it clear that not only does the employee have no right to expectation of privacy, but the company owns all of the employees' email in the first place. These two policy statements are very significant, as they establish the foundation

for the use of GIAC's Internet and email resources. The fifth bullet in the policy attempts to name each type of potential abuse that an employee might be tempted to perpetrate. It is a good idea to spell out as many unacceptable activities as possible, as this leaves little room for confusion. Number 6 gives the employee guidance as to whom he or she should report incidents of policy violation. This increases the likelihood that incidents will actually be reported. The last policy element says that email messages and Internet usage logs will be randomly reviewed to manage corporate resources. This type of control is necessary if the policy is to be enforced.

The problems with this policy begin with the fact that it is largely an unenforceable policy. It is unenforceable because it relies on the cooperation of the network users, and does not contain any meaningful enforcement language. Bullet 2 states that "Electronic mail and the Internet at GIAC are provided … for official GIAC business only." With no technology (e.g. SurfControl or WebSense) solution in place, and no verification procedures, this portion of the policy is unenforceable. A "limited judicious personal use" style of policy is much more realistic than an "official business only" policy.

Bullet number 6 states that "Misuse of *GIAC* resources is a violation of the law and can result in disciplinary action." This statement is extremely broad, and not necessarily true. The policy would be more realistic if it said "Misuse of GIAC resources *could be* a violation of the law. Policies tend to be taken more seriously when they state to what extent the company is willing to pursue action against violators. For example the term "disciplinary action" alone is not necessarily very specific. The phrase "disciplinary action including termination" has more of a bite to it.

Item 6 also makes liberal use of the word "should". Strong policy will use strong words to specify action – "should" sounds more like a suggestion.

There is no purpose for the policy stated at the beginning. The purpose is fairly obvious to those who deal in policy and security on a daily basis, but for the new employee in the shipping department, no statement of purpose might serve only to confuse. Policy is best written so that it is understandable by the people who are subjected to it. This includes that new shipping clerk, who has had very little exposure to computers or the security mindset.

The scope of the policy is not defined as clearly as it could be. By not spelling out the scope of the policy, there is potentially room for employees to exclude themselves. For example, the PC Technician might say to herself "This policy probably doesn't include IT staff, it's ok for me to visit hacking websites at work."

The responsibility for this policy is not defined. The policy is signed by the Vice President of the firm, which may imply responsibility, but implication of responsibility is not adequate. The policy would carry more weight if it would spell out by title or position, whom is responsible for its execution and for its maintenance.

Item 9 in the policy says that "E-Mail messages and Internet usage logs will be randomly reviewed to manage these GIAC resources." This portion of the policy fails to name the person or group who will perform these random reviews, and when and how the reviews will be carried out.

The action item listed for this policy is the "random reviews" discussed above. Again, the policy does not associate names or times with actions. The problem with this is that nobody will take ownership for any aspect of the policy unless they are held accountable for specific actions.

**Policy Revision**

The improved version of the policy was written with help from the Acceptable Use Policy template from the SANS Institute website, at http://www.sans.org/resources/policies/Acceptable_Use_Policy.doc, as well as from the US Office of Personnel Management's Policy on Personal Use Of Government Office Equipment, located at http://www.opm.gov/extra/itusepolicy.htm.
Below is the policy rewritten to better serve GIAC's needs:

Policy for Electronic Mail and Use of the Internet GIAC P 564.1 01-30-03

A. Cancellation: Cancels Electronic Mail Policy *GIAC* P 564.1 09-29-00.
B. Purpose: The purpose of this policy is to outline the acceptable use of Internet and email resources at GIAC. These rules are in place to protect GIAC and its employees. Unauthorized use of email and Internet resources exposes GIAC to risks including virus attacks, compromise of network systems and services, and legal liability.
C. Scope: This policy applies to employees, contractors, consultants, temporaries, and other workers at GIAC, including all personnel affiliated with third parties, who use GIAC assets to access email and/or the Internet.
D. Responsibility: This policy is maintained by the IT Manager, who will review this policy at least annually and make changes as appropriate. The IT Manager is responsible to ensure GIAC-wide compliance with this policy. The IT Manager will ensure that all procedures supporting this policy are followed by appropriate personnel, and in a timely manner as described by each procedure. All employees of GIAC and all others who use GIAC Internet and email resources are responsible for following the policies set forth in this document. The Personnel department will maintain a signed acknowledgement of receipt of this policy in each person's file. This will be verified by the IT staff member responsible for creating the user's network login account, prior to granting network access to the user.
E. Policy
    1. While GIAC's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems, including email, remains the property of GIAC. Because of the need to protect GIAC's network, management cannot guarantee the confidentiality of information stored on any network device belonging to GIAC. GIAC employees and contractors do not have a right, nor should they have any

expectation of privacy when using *GIAC* resources at any time, including GIAC's email system and accessing the Internet for any purpose.

2. Electronic mail (E-Mail) and Internet access at *GIAC* are provided as communications and research tools for business. However, GIAC does permit limited judicious personal use of its email and Internet resources. Limited personal use is authorized if it involves minimal additional expense to the company. Limited personal use of Internet and email resources is authorized during non-work hours. This use must not reduce productivity or interfere with official business. GIAC reserves the right to further restrict personal use based on the needs of the organization or problems with unauthorized use.
3. Unauthorized uses of E-Mail technology and/or the Internet include, but are not limited to, those that: (1) result in a loss of productivity or impair the performance of GIAC's network; (2) are unlawful, abusive or potentially abusive to anyone (e.g. gambling, hate speech or material that ridicules on the basis of race, creed, religion, color, sex, national origin, disability, or sexual orientation); (3) transmit sexually oriented material; or (4) allow unauthorized access to controlled information (e.g., proprietary code, private personnel information, copyright, trademark or other intellectual property, licensed software, or unauthorized access to any other GIAC electronic resources).
4. All messages and attachments produced or received through GIAC's E-Mail system and/or the Internet are the property of GIAC. For security and network maintenance purposes, authorized individuals within GIAC may monitor network traffic, including email and Internet access, at any time. Access to outside (non-GIAC) email accounts from a GIAC-owned computer is prohibited. GIAC reserves the right to monitor its network and systems to ensure compliance with this policy.
5. Users of GIAC's Internet access resources are strictly forbidden from engaging in any activity which may be perceived as disruptive. For purposes of this section, "disruptive" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes. Unless it is part of an employee's job duties, port scanning any internal or external host(s) using GIAC resources is strictly prohibited without written permission from the IT Manager.
6. Users of GIAC's email resources are strictly forbidden from engaging in any activity which may be perceived as disruptive. For purposes of this section, "disruption" includes, but is not limited to: sending unsolicited email messages, including "junk mail" or other advertising material to individuals who did not specifically request such material; Any form of harassment via email, whether through

language, frequency, or size of messages; Unauthorized use, or forging, of email header information; Creating or forwarding "chain letters" or "pyramid" schemes of any type; Transmission of data that are abusive or potentially abusive to anyone (e.g. gambling, hate speech or material that ridicules on the basis of race, creed, religion, color, sex, national origin, disability, or sexual orientation); Transmission of sexually explicit or sexually oriented material; Allowing unauthorized access to controlled information (e.g., proprietary code, private personnel information, copyright, trademark or other intellectual property, licensed software, or unauthorized access to any other GIAC electronic resources).

7. Misuse of *GIAC* resources in any way that violates Federal, State, or Local law, is strictly prohibited, and can result in disciplinary and/or legal action. Disciplinary action can involve appropriate measures up to and including termination. Incidents of unauthorized use will be reported to *GIAC's* IT Manager. In cases where a confidential report is made, every effort will be made by GIAC to protect the privacy of the notifying party. EEO-related (Equal Employment Opportunity) incidents should be reported to the Personnel Manager. In any case of violation of this policy, the employee's supervisor will also be notified.[vii]
8. In accordance with GIAC's Records Management Policy, email will be permanently deleted from the email system 60 days after creation. Email and attachments that meet the definition of a GIAC corporate record should be retained in accordance with GIAC's Records Management Procedures.
9. Email messages and Internet usage logs will be reviewed by the Network Administrator, in compliance with GIAC's auditing procedures.
10. Procedures in support of this policy include the following:
    1) Procedure for Audit of Internet usage, Malware GIAC P 564.11 01-30-03
    2) Procedure for Audit of Email, Proprietary Code GIAC P 564.12 01-30-03
    3) Procedure for Audit of Email, Unauthorized Personal Use GIAC P 564.13 01-30-03
    4) Procedure for Audit of Internet, Unauthorized Personal Use GIAC P 564.14 01-30-03

*John Doe,* Vice President GIAC Enterprises

**Procedures**

Several procedures are needed in order to properly enforce the new policy. For the purposes of this paper, I will detail only one of these procedures. The

procedure I have chosen to develop is one that will instruct the Network Administrator in an audit of email usage by GIAC network users, with the purpose of monitoring the policy's effectiveness at preventing proprietary code from being transmitted via email.

Procedure for Audit of Email Usage, Proprietary Code,
GIAC P 564.12 01-30-03

A. Cancellation: None
B. Purpose: The purpose of this procedure is to provide instruction pertaining to the audit of GIAC's email resources. The procedure will provide verification that GIAC's email access resources are not being used for the unauthorized transmission of proprietary code.
C. Scope: This procedure is applicable to all systems within the control of GIAC Enterprises and is intended to be executed in support of GIAC's Policy *for Electronic Mail and Use of the Internet,* GIAC P564.1 01-30-03.
D. Responsibility: This procedure is maintained by the IT Manager. The IT Manager will review this procedure at least annually, and make changes as appropriate. This procedure will be followed by the Network Administrator or other designee as assigned by the IT Manager.
E. Procedure:
    1. This procedure shall be executed once per calendar month by the Network Administrator, or when requested by the IT Manager.
    2. The contents of electronic mail (email) will be inspected for signs of the unauthorized transmission of proprietary code, as required by GIAC P564.1 01-30-03, policy section 6.
    3. The Network Administrator will notify the IT Manager of any unauthorized data found, to include the name of the user, the date(s) and time(s) the violation(s) occurred, and the details of the violation(s).
    4. Steps:
        a. The IT Manager will provide the Network Administrator with a list of keywords to be searched for. The list will consist of a comma-separated list of key text strings, as provided by the Lead Developer.
        b. Login to the email server as "giac\administrator".
        c. Run the ExMerge utility on the server in two-step mode, searching for all the keywords in the list provided by the IT Manager.
        d. Import the .pst file with messages containing keyword hits into Outlook on a workstation in the server room.
        e. In Outlook, open the .pst file.
        f. Messages containing the keywords will display. Open each message and verify that the message does appear to be in violation of GIAC P564.1 01-30-03 policy section 6.

g. If apparent proprietary code is found, record the name of the account being audited, the information in the "to", "from", "subject", "sent", etc. fields, and the entirety of the code string.
h. Report findings to the IT Manager for appropriate action.

The procedure presented above is only one example. Many more could be written to assist GIAC enforce its policy. For example, Bullet 4 in the policy states that "authorized individuals within GIAC may monitor network traffic, including email and Internet access, at any time." A procedure might be put in place that explains the method for monitoring network traffic. Policy stating that actions will be taken, where no supporting procedure is in place, often leads to the implementation of an unenforceable policy.

**Conclusion**

This paper has presented the reader with a view of the policy situation of a fictional company, but the same principles of policy evaluation and improvement can be carried over to real organizations of any type or size. I would again stress the importance of knowing the business as intimately as possible before attempting to create policy; no policy template will fit every organization without modification. Good policy can serve as a foundation for good security.

## Endnotes

[i] "IIS Lockdown Tool"
URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp
02 FEB 2003.

[ii] Bassham, Lawrence E. and Polk, Timothy. "Threat Assessment of Malicious Code and Human Threats." 10 MAR 1994.
URL: http://csrc.nist.gov/publications/nistir/threats/subsection3_4_1.html#SECTION000410.
09 JAN 2003.

[iii] "The SANS Institute Top 20 List. 'The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus'." Version 3.21. 17 OCT 2002. URL: http://www.sans.org/top20/. 21 JAN 2003.

[iv] "Microsoft Security Bulletin MS02-005". 11 FEB 2002.
URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-005.asp.
13 JAN 2003.

[v] "Microsoft Internet Security and Acceleration Server". 09 JAN 2003.
URL: http://www.microsoft.com/ISAServer/. 10 JAN 2003.

[vi] Webopedia online encyclopedia "Spyware" 02 OCT 2002.
URL: http://www.webopedia.com/TERM/S/spyware.html 06 FEB 2003.

[vii] U.S. Office of Personnel Management. "Policy on Personal Use of Government Office Equipment." MAY 1999.
URL: http://www.opm.gov/extra/itusepolicy.htm. 21 JAN 2003.