# Global Information Assurance Certification Paper

GIAC Enterprises – Security in a small consulting firm

GISO – Basic Practical Assignment, v1.0 (October 30, 2001)

Terry Miesse

# Table of Contents

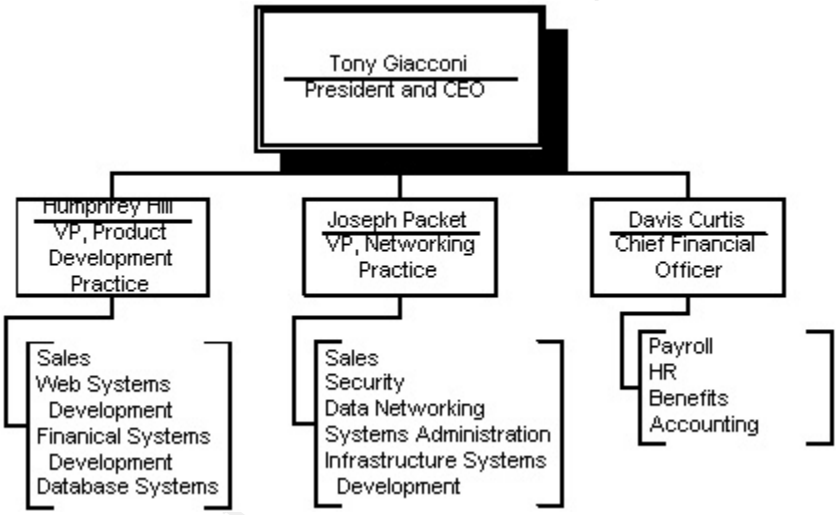
# Section 1 – Description of GIAC Enterprises

## *Company Overview*

Founded in May, 2001 by Tony Giacconi, GIAC Enterprises is a provider of outsourced IT services for small- to medium-sized businesses located in the Greater Cincinnati area. GIAC's typical customers are businesses of 50 employees or less who need assistance in establishing and maintaining a presence on the World Wide Web. GIAC provides fully outsourced IT functions, including desktop configuration and support, mail infrastructure support, and remote access support for several smaller clients. GIAC also provides web hosting services to a few smaller customers, but prefers to work with local hosting providers when the site becomes a significant source of income for the client.

## *Organizational Overview*

The organization of GIAC Enterprises is summarized in the following diagram;

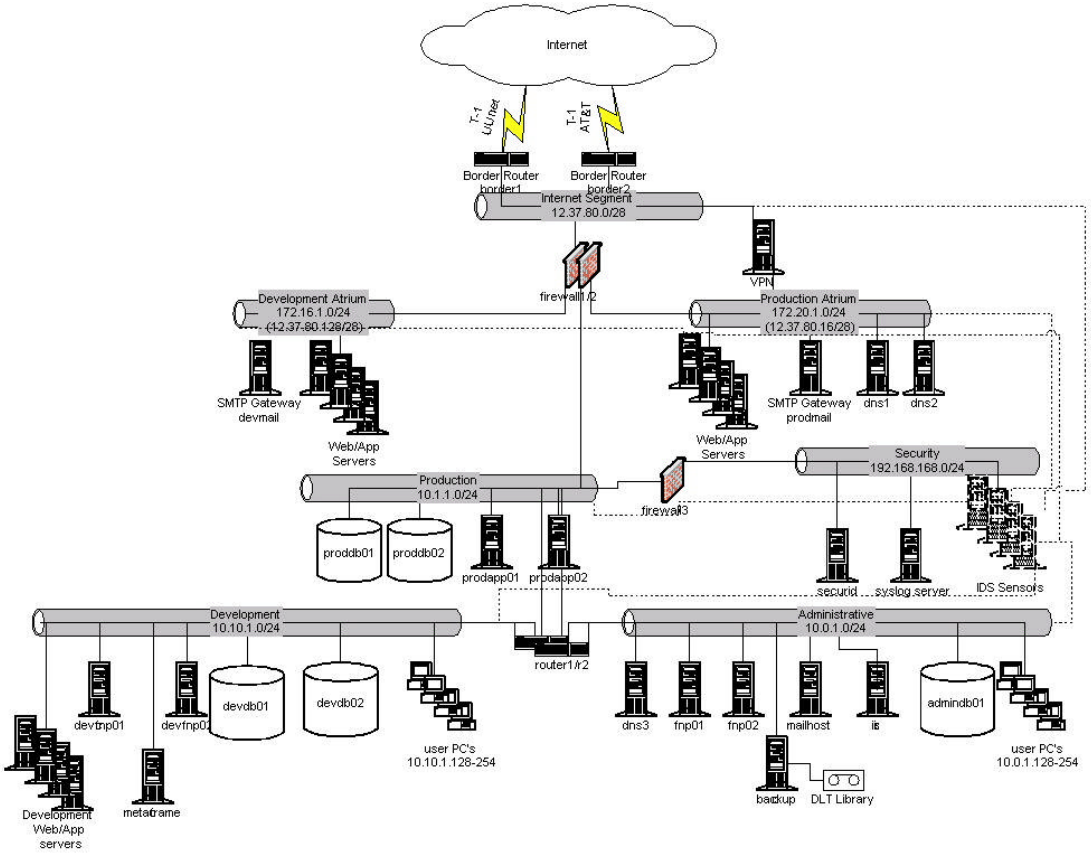



GIAC prefers to have the consultants in their Product Development practice work on software projects in-house as much as possible to facilitate the use of common toolsets. Occasionally, consultants will be required to work at a client's site for extended periods of time; during these engagements, they are expected to occasionally utilize GIAC's systems to access their email and record their time for billing back to their customer. The Product Development practice consists of 42 consultants and 2 account managers. The 31 consultants in the Networking practice are generally full-time at client's sites. The Networking Practice also has two systems administrators who are responsible for administration of GIAC's internal systems. These administrators are assisted by consultants who are "on the bench" between client assignments. There are also 2 account managers in the Networking Practice.

In addition to their customer-facing consulting practices, GIAC maintains the "classic" infrastructure functions reporting to their Chief Financial Officer. These 5 people provide administrative support to the executives as well as supporting the payroll, HR, benefits, and accounting functions.

## *IT Infrastructure*

The diagram below illustrates GIAC's internal network.




GIAC Enterprises utilizes 2 separate ISP's for redundancy. They have T-1 service from both AT&T and UUNet. They utilize a full class C network that has been delegated by AT&T. They also have their own ASN and have arranged with UUNet to have their routes propagated through UUNet for the times that the AT&T connection is unavailable. The two border routers (border1 and border2) are Cisco 3640 routers with sufficient memory to share full routing information with both ISP's. The routers have HSRP configured on the "inside" interface to provide redundancy for the default gateway. The UUNet router (border1) is configured as the HSRP primary, causing it to handle most of the outbound traffic. The AT&T router (border2) handles most of the inbound traffic since GIAC utilizes the AT&T address block. Both routers utilize both ingress and egress filtering to ensure that only specifically permitted traffic is passed in either direction.

GIAC utilizes two Nokia IP330 firewall appliances utilizing VRRP in a hot standby configuration. (The Security Team has submitted a request to purchase two PIX firewalls to provide separate internal and external firewalls. The funding has not yet been approved.) The Nokia appliances are running Checkpoint Firewall-1 2000. The firewalls permit only specified traffic in all directions. The class C delegated by AT&T has been

broken into subnets. This is so that the firewalls can route traffic to the various networks properly, rather than having to proxy arp for addresses being NAT'd.

GIAC prefers to use the term "atrium" for networks that provide services on the Internet. When designing their network, they found confusion around the use of the term "DMZ." "Classic" DMZ's refer to the network between the ISP border router and the outside interface of the firewall. "DMZ" is now often used to refer to a network that is protected by a firewall from both internal and external networks. While researching network designs, GIAC's consultants came across the term "atrium," and it was agreeable to all involved.

The Web Development team requested the establishment of a "development" atrium. This provides a network that is insulated from GIAC's "production" network, but is still Internet accessible. The servers on this network are used for presenting projects in process to clients. It is also helpful for the developers to deal with having a firewall between the front-end and back-end server in two- or three-tier applications. There is also an SMTP server in this atrium that the developers use to test sending and receiving email. Wherever possible, GIAC utilizes open source solutions. They utilize qmail and Linux for their SMTP gateways. All servers on this network utilize static IP addresses.

GIAC's production atrium is used for hosting a few web sites for smaller customers, as well as GIAC's own web site. They are implemented on open source platforms, utilizing Apache on Linux for serving static HTML. PHP and JSP are both used for dynamic web content. (Apache Tomcat is used for processing JSP.) GIAC's DNS servers also reside in this atrium. All servers on this network utilize static IP addresses.

GIAC also utilizes a Nortel Contivity 400 VPN device for external access to their internal network. The external interface of the Contivity is on the Internet segment. The internal interface is in the production atrium. This allows GIAC to apply access controls to traffic into the network via the VPN. (The Contivity switch provides access controls as well, but GIAC decided to centralize this control within the firewalls.)

The database and application servers used for the applications hosted in the production atrium are on an internal production network. These servers were placed on a separate network to enable more stringent change control processes on systems that directly impact customers. Changes to servers on this network are performed outside of business hours. All servers on this network utilize static IP addresses. GIAC utilizes Oracle running on Linux servers for their production applications. While the use of Oracle contradicts the company's support of open source products, it does ease transition of the applications to customers' environments when that becomes appropriate. GIAC utilizes one of the database servers as the primary server, with the second being available for failover should that become necessary. Nightly backups and hourly journal files are copied from the primary to the backup server to reduce the loss of data should a recovery become necessary.

The desktops for all members of the Product Development practice, as well as all of their servers, are on the development network. This segregation was implemented to accommodate the developers' request to have full control over all development servers. Segregating them to a separate network reduces the risk to production and administrative systems. The routers that are used to interconnect the production, development, and administrative networks contain ACL's to ensure that the only traffic that passes between these networks has a specific business reason. (These routers are Cisco 3640's running HSRP on all interfaces for high availability.) The CVS server (used for source code control) is also configured to provide DHCP services to the desktops on this network. All servers utilize static IP addresses. The developers also have a dedicated Oracle server for their use. A second database server is used for Microsoft SQL Server to meet certain customers' requirements.

All other employees' desktops are on the administrative network. All servers providing "infrastructure" services, such as accounting, HR, email, and file and print are also on this network. GIAC utilizes POP and IMAP for all email. Because they have a small number of internal meetings, they have not yet had a need for a calendaring solution. Microsoft Exchange was considered, but its overhead was considered excessive since calendaring would be underutilized. There is a small Microsoft Windows2000 server to support HR and financial applications that require IIS. A second small Windows2000 database server houses SQL Server for these applications. The internal DNS server also resides on this network. This server provides DNS for all machines on internal (non-atrium) networks. It also serves as the DHCP server for desktops on the administrative network. All servers utilize static IP addresses. GIAC's backup server also resides on this network. It utilizes ARCServe and a 7-tape DLT library to back up servers on the development and administrative networks, as well as the production database servers and the central syslog server. The SQL Server database server is currently set up as a domain controller to provide centralized authentication for the file and print servers.

Recently, the security consultants in the Networking Practice implemented a segregated security network. This network is "attached" to the production network via a Linux-based firewall utilizing iptables for packet filtering. The SecurID server, the centralized syslog server, and the command and control interfaces for the snort IDS sensors are on this network. The SecurID server is utilized for authentication and authorization by the Contivity VPN device and all four of the routers. The security consultants are experimenting with integrating SecurID with ssh for access to the snort IDS sensors and the Linux firewall. The syslog server is used to centralize logging from all routers and switches, as well as the syslog output from the firewalls and IDS sensors. Each network has a corresponding snort IDS sensor. The "sniffing" interface is configured as a "stealth" interface with no IP address.

## *Business Operations*

### *Product Development Practice*

As mentioned previously, the Product Development Practice prefers to perform development work for their customers in-house wherever possible. While this generally

makes product development less complicated by enabling use of common development tools, it also introduces some issues. Occasionally, customers will require specific software or configurations that are unique for their project. In these cases, either an existing available server is reconfigured to meet the requirements, or a new server is purchased and configured as necessary. If the requirement involves desktop software, the desktops for the consultants working on the project are reconfigured as necessary. At the end of the engagement, any machines whose configurations are modified are reloaded using Symantec's Ghost imaging software and GIAC's standard image for that platform. In-house development also requires stringent backup procedures of all source code and data owned by customers. Consultants may also occasionally require VPN access to the client's network, which is accommodated on a case-by-case basis. GIAC company policy requires any machine that has client-provided software installed, including VPN client software, to be re-imaged following the conclusion of the customer engagement.

GIAC also provides remote access to internal resources for their consultants who are working at the customer's site or working from home. Access to the internal network is provided via the Nortel Contivity VPN gateway. Access via the VPN gateway is restricted to accessing email (via POP or IMAP) and the internal web-based time-tracking application (via HTTPS). Consultants are also able to utilize the VPN gateway to map drives to the internal fileservers, although not to individual desktops. Access via other protocols (such as the use of a database client) is currently not supported via the VPN gateway. Some consultants also utilize ssh clients to access GIAC's internal servers while connected via VPN.

To address the shortcomings merely providing VPN connectivity, GIAC is currently conducting a pilot test to provide remote access to internal applications via Citrix MetaFrame. This eases software support concerns, allowing standard development tools to be loaded on the MetaFrame server rather than on individual desktops or laptops. The use of MetaFrame also allows access to GIAC's systems from client locations where the use of VPN software is not possible due to the client's firewall configuration. Because the MetaFrame server is on a trusted network and available to the Internet, GIAC's network security policy requires the use of the encryption features of the MetaFrame client, as well as the use of SecurID for strong authentication.

The Web Development team maintains the applications in the Development atrium. GIAC's systems administrators support the hardware, operating system, and "infrastructure" software (such as Apache and Tomcat). While change control procedures are followed for these servers, changes are permitted during business hours.

### *Networking Practice*

Due to the nature of their work, the consultants in the Networking Practice generally perform their work at the customer's site. They utilize the Nortel VPN gateway for remote access to GIAC's network as described above. The consultants in this practice are also testing remote access to their internal email by using IMAP tunneled within SSL (also referred to as SIMAP). Once again, GIAC's network security policy requires the use of SecurID for authentication in this situation.

### *Administrative Functions*

The servers and desktops on the administrative network are isolated from the rest of the corporate network via ACL's (Access Control Lists) on the core routers. These routers ensure that only developer's desktops (on the Development network) have access to the file and print servers. Access from the Production network and the atrium networks is specifically blocked, in case the other security measures on these networks are compromised. The ACL's allow the backup server to provide backup services as described above. It was also initially used to back up the Internet-facing DNS servers, but the decision was made to keep all DNS configurations under source code control, utilizing the Product Development practice's CVS server. It is GIAC's policy that any configuration files on the development servers are kept in source control, and also that no data is stored on any production servers other than the two production database servers. Therefore, backups of servers in the production environment are not required.

GIAC has not yet had a need to allow customers access to any internal systems. All customers to date have required paper invoices. Consultants enter their time tracking information into the web-based time tracking system either from their internal desktop or utilizing the remote access methods described above. However, should remote access by clients become a requirement, GIAC is confident this can be accommodated by utilizing the VPN and ACL functionality of the VPN gateway in combination with the facilities provided by the Nokia Firewall-1 appliances.

### *Hosting*

GIAC Enterprises provides web hosting for a few of their smaller clients. GIAC also occasionally provides temporary hosting services until a client can make arrangements with other hosting providers. All services in the production atrium, as well as on all internal non-development servers, are monitored by the system administrators using Big Brother. The system administrators are notified immediately of any service outages.

Projects under development are made available to clients in the Development atrium. Systems under development utilize some level of authentication, depending upon the sensitivity of the application and the client's requirements, to prevent public access to pre-release sites. Authentication may range from IP-based authentication, ensuring that only traffic from the client's site is permitted to the application, to SecurID authentication for sites that may either require it once it is in production at the client's site or when requested by the client. Servers in this atrium are also monitored by Big Brother, with notifications going to the Web Development team.

# Section 2 – Define GIAC Enterprise's Security Policy

## *Areas of Risk*

GIAC Enterprises has identified the following five areas as representing their most significant security-related concerns.

1. The need for a secure network perimeter
2. Confidentiality, integrity, and availability of customer-owned code and data
3. Anti-virus protection
4. Integration of security with all products and service offerings
5. Prompt creation and deactivation of user accounts

These risks were determined based on identified threats, GIAC's vulnerability to those threats, and the impact of the threat upon GIAC's business. Each of these risks is described in greater detail below, along with the steps that have been identified to address each risk.

### *1. The Need for a Secure Network Perimeter*

As with many companies, GIAC Enterprises has defined the need for a secure network perimeter as their primary security concern. The integrity of internal systems cannot be ensured unless unauthorized users are kept out – not only out of the systems, but out of the internal networks entirely. GIAC has realized that, sadly, the threat of "hacking" faced by any entity that connects to the Internet is increasing, and will continue to do so for the foreseeable future.

Many of the other risks identified above cannot be fully addressed unless the company's network perimeter is secure. If the perimeter is not secure, internal systems may be easily and repeatedly compromised. This may cause not only financial loss due to system downtime and administrator overtime, but would have a direct impact on GIAC's revenues. As a small consulting company, GIAC relies heavily on their reputation among local companies. GIAC also heavily markets its security expertise, not only within the Networking Practice, but also in applications developed by the Product Development Practice. Word of a compromise of GIAC's network would quickly spread among the local small business that comprise GIAC's main client base, potentially causing grave damage to their reputation.

GIAC has implemented the steps below to address this risk. Further details are provided in GIAC's Network Security Policy.

a. *Identify the network perimeter.* In order to secure the perimeter, that perimeter first had to be defined. GIAC has defined their perimeter as anything "outside" the outside interface of their firewalls and VPN gateway for their data network.

b. *Secure non-Internet connectivity.* GIAC currently has no incoming dialup or private network connections; however, their policy defines the inside interface of those connections as forming the perimeter should they be added in the future.

c. *Secure modems.* Any modem that is utilized must be configured to not accept incoming calls, and modems cannot be attached to phone lines that accept incoming calls. GIAC has not yet taken any steps to secure their voice network; however, they recognize that the public telephone network should be treated as an untrusted network, and hope to specifically address the security of their PBX in the near future. In the meantime, they have ensured that remote access to any control or configuration functions of the PBX is disabled.

d. *Utilize ingress and egress filtering on border routers.* ACL's are used as the first layer of defense against unwanted traffic entering GIAC's internal networks, and as the last layer of defense against any unwanted outbound traffic.

e. *Install firewalls at all perimeter interfaces.* GIAC's network security policy states that all connectivity between "untrusted" networks and GIAC's networks must be controlled via a firewall. In the future, should GIAC install a private network connection to an external business partner, that connection would also be required to be "behind" a firewall. The firewalls are used to filter traffic in both directions. Only services that are specified in GIAC's network security policy or approved by GIAC's management (with strong input from the Networking Practice) are permitted outbound through the firewall. Likewise, only the necessary ports are enabled to specific servers in the Production and Development atria.

f. *Deploy intrusion detection systems on all networks.* GIAC has realized that, as SANS' Eric Cole uses as an incantation, prevention is important but detection is essential. GIAC utilizes snort, an open-source network-based intrusion detection tool, to monitor the traffic on their networks and alert them of possible attack attempts. The snort IDS sensors are configured to log all alerts to the centralized syslog server, where Psionic Software's logwatcher then sends notifications to the system administrators. The Security Team of the Networking Practice has spent considerable time in tuning each IDS sensor to detect possible attacks or other network compromises based on the specific network the sensor is monitoring, and continue to make changes as new threats are published and new applications are deployed.

g. *Insulate trusted networks from untrusted networks.* GIAC's security policy prohibits any connections that initiate on an untrusted network, such as the Internet, from terminating on a server on a trusted network, such as an internal web server, unless both strong encryption and strong authentication are utilized. All traffic from an untrusted network must terminate in an atrium, after first passing through a firewall. Connections from an atrium server to internal servers are allowed, as long as they once again pass through a firewall. GIAC utilizes the VPN gateway and Citrix Metaframe to ensure strong encryption for all traffic that goes directly to trusted servers, and SecurID for strong authentication of these connections.

h. *Segment internal networks based on role.* GIAC has segmented their internal network to provide another layer of security. This has allowed them to isolate all servers that directly affect customer-facing systems to their own networks,

allowing them to restrict all access between these "production" systems and internal systems. It also allows maintenance to be performed on non-critical systems without affecting customer-facing systems. Developers have been segmented to their own network to allow them greater flexibility in experimenting with new products while minimizing the risk to other internal and customer-facing systems.

### *2- Confidentiality, Integrity, and Availability of customer-owned code and data*

As stated above, GIAC's developers perform much of their work for their clients on GIAC's internal systems. The program code or documentation that the consultants produce are generally the deliverable product for the client. Loss of a project's deliverables due to inadvertent or malicious corruption or deletion of files can be disastrous for the project, and may seriously damage relations with the client.

In addition, clients often provide test data that may contain proprietary information. Improper disclosure of this data may result in financial loss or embarrassment for the client, which would undoubtedly damage the relationship with GIAC. In extreme cases, the client may seek reparations for the damages from GIAC. Clients may also express concerns regarding the confidentiality of any information regarding their projects with GIAC, as GIAC often provides services for competing companies.

GIAC has taken the following steps to mitigate these risks:

a. *Utilize access controls for customer data.* Access to all files and data related to a client project is restricted to the consultants who are working directly on that project, plus their Team Lead and Practice Manager. These restrictions are applied by creating groups and applying the proper file permissions on file servers and within the CVS and database servers.

b. *Implement backup procedures.* GIAC purchased a server dedicated to tape backups. The cost of approximately $10,000 for the server, DLT library, DLT tapes, and software, in addition to the ongoing expense of replacement tapes and service contract with an off-site storage provider, was a considerable expense for GIAC. However, it was easily justifiable given the risks outlined above. A backup schedule and tape rotation was implemented to ensure that all appropriate data could be recovered to the point of the most recent backup. In addition, each day's backups are taken offsite through arrangements with their service provider, who also returns the appropriate tape from storage for re-use. GIAC chose to utilize the "standard" backup schedule of daily differential backups, with full backups being run each Sunday evening, as well as the last day of each month. Daily differential backups are retained in offsite storage for one week, weekly full backups are retained for one month, and monthly full backups are retained for one year. The December monthly backups are retained indefinitely. GIAC chose to implement ARCServe due to the availability of a client for backing up their Linux systems, as well as ARCServe's ability to manage the various media pools necessary for GIAC's backup scheme.

c. *Isolate each client's data.* The Product Development Practice is careful to isolate all data for each client. Any files stored on filesystems are stored in a separate directory structure for each client – files for two clients are never stored in the same directory. Each client has its own project within CVS, to ensure that source code generated for one client is not inadvertently made available to another client. Any content that is published to an HTTP server utilizes a separate virtual server or actual server instance for each client to ensure that users on one client's site cannot navigate to another client's site. Finally, any project that utilizes databases for storage must create their own database or server instance to isolate its data from all other projects.

In addition to the steps outlined above, GIAC's systems administrators have requested funding to implement the following improvements:

a. *Utilize separate backup system for Development.* Occasionally, client contracts may require GIAC to purge all customer data from their systems at the termination of the contract. While this has not yet been an issue, the current scheme of intermingling backups of "corporate" data with customer data would greatly complicate matters should this need arise. GIAC's administrators have attempted to address this by utilizing different media pools, but this turned out to be impractical with the current single-drive DLT library.

b. *Purchase more tapes to expand media pools.* Ideally, GIAC's administrators would like to utilize four sets of tapes for daily differential backups. This would allow a four-week worst-case scenario for recovering data, rather than the current one-week worst-case. (A file created on Monday and deleted on Saturday would have its backup overwritten the following Saturday.)

## *3- Anti-Virus Protection*

Protection against malicious code of all sorts should be a major concern for every business. Financial losses due to lost productivity and employee overtime caused by a virus or worm can be substantial. However, companies such as GIAC Enterprises have an additional risk: they produce deliverables for their clients in electronic format. Including a virus with documents or programs delivered to a client could not only be harmful to that client, but would also gravely damage GIAC's reputation. To help guard against this, GIAC has implemented the following safeguards:

a. *Run anti-virus software on every Microsoft-based machine.* Every Microsoft-based desktop and server is required to have anti-virus software active at all times. Desktops are set to automatically update their virus signatures daily, and servers update twice per day. GIAC utilizes Linux servers except where an application that has been selected requires Windows, or when replicating a customer's environment that requires Windows. While Linux-based viruses do exist, GIAC feels that the threat is not sufficient to warrant anti-virus software on Linux systems other than mail gateways.

b. *Distribute all data on CD.* GIAC delivers all data to their clients on CD rather than floppy disks to ensure that it is not modified after it is recorded.

c. *Protect the "production" CD burner.* One PC has been designated as the machine that creates all CD's that are delivered to clients. No email clients or web browsers are permitted on this machine. All files are scanned for viruses prior to being burned to CD, and the CD is scanned on a different machine after being burned.

d. *Scan all customer-provided media on an isolated machine.* All customer-provided media must be scanned on a stand-alone machine before being used in a network-connected desktop or server. A PC has been designated for this task. The virus definitions must be manually updated prior to each use.

e. *Utilize Linux servers where possible.* GIAC utilizes a Linux server as their SMTP gateway, with TrendMicro's VirusWall anti-virus software to scan all incoming and outgoing email for malicious content. They also use Apache's HTTP server on Linux as their web server standard, and encourage their customers to do likewise. While this combination is not immune to security exploits, it has a much better track record than Microsoft's IIS of preventing vulnerabilities and quickly addressing vulnerabilities that are discovered. The importance of this criterion in selection of a web server platform is growing as malicious code such as viruses and worms increase their use of infecting web servers as a method of propagation. GIAC also utilizes Linux-based file and print servers, with Samba to make these resources available to Microsoft-based desktops.

## *4- Integration of Security With All Products and Service Offerings*

As previously mentioned, GIAC promotes the importance of security in all aspects of their services. While this is useful in marketing, GIAC also feels it is important to raise the standards of security in software development and systems administration roles, in addition to "classic" security functions such as firewalls, intrusion detection systems, and authentication systems. GIAC has taken the following steps to ensure the importance of security in all aspects of their business:

a. *Implement and follow coding standards.* GIAC has implemented standards for code development for the standard platforms they deal with – Java, JSP, PHP, VB/ASP, C++, and Perl. These standards include the use of bounds checking on all input and output, checking memory allocation and deallocation, and specific checking for divide-by-zero conditions. All database operations are also checked to ensure that query strings cannot be subverted by special characters. Any routines that deal with input from web browsers are checked to ensure that all input, including cookies, query strings, and hidden fields, has proper bounds checking and exception handling.

b. *Implement and follow database standards.* Security within databases is often neglected in favor of providing security strictly within applications. However, if the data can be accessed without the client application using "vanilla" query tools, security controls must be implemented within the database as well. GIAC's database consultants have established database design standards that include providing security at the database level. These include tracking individual users within the database (rather than an application-wide login), creation of roles or

groups for users based on their role within the application, and granting access only to the data that their role requires. Some of these items may introduce a level of complexity and maintenance that the client prefers not to assume, so the use of these controls is balanced with the security needs of the data in question.

c. *Implement and follow system configuration standards.* GIAC has also created standards documents for configuration of servers, desktops, and network devices, both for client and internal use. These standards follow the rule of creating a "trusted base" and adding only necessary functionality, rather than starting with a full configuration and removing unneeded software. If a consultant is installing a system at a client's site, that client's standards are utilized if any exist. (The consultants provide GIAC's standards to the client and generally encourage the client to upgrade their procedures should there be any discrepancies. The consultant may also recommend modifications to GIAC's standards based on suggestions from the client.)

d. *Educate all consultants.* All consultants are required to attend training in their field of specialty to keep their skills current with new products and technologies. This training must also include the security aspects of their specialty. Announcements regarding security issues of relevant technologies, including vulnerability alerts from mailing lists such as SANS, ISS, InfoWorld, or other such publications, are posted to internal discussion forums. Practice meetings include presentations from consultants within the practice regarding security issues that affect their areas of expertise. Consultants are also encouraged to be active in local and regional user groups to gain insight from a broader base of experience.

e. *Educate the client and community at large.* GIAC offers training to their clients on a wide range of subjects. These classes also emphasize the security aspects of the technology or product being studied. They also offer in-depth training on network security issues, Unix system security, and Oracle security. GIAC encourages their consultants to speak at user groups and conferences, and will reimburse expenses for these activities. GIAC also offers incentives to consultants who submit articles or white papers for publication.

## *5- Prompt Creation and Deactivation of User Accounts*

Like many consulting firms, GIAC Enterprises experiences 15-20% staff turnover each year. New employees need to have their ID's created on GIAC's internal systems promptly so that they can be productive immediately. As with many consulting firms, GIAC often starts consultants on billable projects immediately after starting with the company, so a new consultant's inability to access tools and resources may very easily have an impact on billable work. If employees do not receive their own accounts promptly, GIAC has found that employees are more likely to share their own accounts and passwords. Conversely, when an employee leaves the company, steps must be taken to ensure that the employee no longer has access to internal or client systems or data. Fortunately, most employees leave on good terms, but GIAC's policies still require prompt revocation of a individual's access immediately upon termination to reduce the possibility of a former employee

accessing internal or client systems. GIAC has taken the following steps to ensure that user accounts are created and deactivated promptly:

a. *Document processes for account creation and deactivation.* All account administration processes have been documented. This assures that any systems administrator is capable of creating or deactivating accounts promptly.

b. *Automated notification to system administrators.* The HR system that GIAC utilizes is capable of sending emails when new employees are added and when they are terminated. These emails are sent to GIAC's system administrators so that accounts can be added and deactivated as soon as possible. The system administrators have investigated the use of automated account provisioning tools, but the workload is not yet sufficient to justify their expense. The emails that are sent when an employee is added include sufficient information to create the necessary accounts and assign the correct access permissions. While system administrators receive an email when employees are terminated, they are also notified immediately by HR to ensure that the employee's access is immediately revoked.

c. *Require approval for account requests.* GIAC's system administrators have implemented a simple web page for consultants to request new accounts or access privileges. The data collected on the page is sent to the user's practice manager, who then forwards it to the system administrators with their approval. No accounts are created without this approval process. The web page has recently been updated to record all requests to a database, facilitating a central location that stores all accounts and access rights for all users.

d. *Create only necessary accounts.* When a new employee joins GIAC Enterprises, all accounts and access permissions that they need are created. However, this is a very minimal set of accounts – email, NT/Samba domain, and a login for the time tracking system. Any account or access permission beyond this must be requested and approved by the practice manager as noted above.

e. *Automate account inventory.* GIAC's systems administrators have created scripts that extract the list of users for each computer system and application. These scripts were created to help support periodic audits of user accounts on all systems.

In addition to these measures already in place, GIAC is investigating the use of a centralized LDAP directory for use by all (or many) systems as a central source of authentication information. This will ease the prompt creation and revocation of user accounts.

## *Security Policies*

### *GIAC Enterprises Network Security Policy*

**Purpose:**

This Policy has been established to document baseline security requirements for data networks owned and operated by GIAC Enterprises. This includes local-area networks (LANs), campus networks, and wide-area networks (WANs). This Policy also defines terms to provide a common understanding of terms used in other network security documents, policies, and communications between employees.

**Scope:**

This Policy applies to all data networks owned and operated by GIAC Enterprises. This Policy also applies to any data network operated by GIAC Enterprises on behalf of a client inasmuch as it does not conflict with any policies the affected client may have in place; in such an instance, the client's policy will take precedence.

**Policy:**

1. A name and coloring scheme will be used to classify each network within GIAC Enterprises. The classification scheme is based upon the security requirements of the network, based on the services offered on that network and the connectivity between that network and other networks. The classifications are:
    a. *Trusted (Green):* A network is considered trusted if it is owned and managed by GIAC Enterprises. Generally the "core" enterprise or corporate network.
    b. *Untrusted (Red):* A network that is not owned or managed by GIAC Enterprises, or containing unknown or untrusted security controls. Untrusted networks should be assumed to be hostile. The Internet and client's networks are both examples of untrusted networks.
    c. *Atrium (Amber):* An atrium is generally used to provide services to untrusted networks, or as a transition between untrusted and trusted networks. An atrium used to house web servers, serving connections to the untrusted Internet and initiating connections to the trusted internal network, is an example of an atrium. Lab networks are also considered to be amber networks.
2. Traffic passing between two networks must meet the following requirements. If network traffic must pass through an intermediary network (such as from a trusted network to an untrusted network and finally to an atrium network), the connection is bound to the requirements of the network with the lowest level of trust.
    a. A packet-filtering firewall will serve as the demarcation point between two networks of differing security classification. If one of the networks is not Ethernet, the traffic will be bridged to Ethernet on the network with the lowest level of trust. For example, the bridge connecting an untrusted token-ring

network to a trusted Ethernet will be placed on the token-ring side of the firewall.

b. Firewall policies will restrict traffic to ports, protocols, and services to meet specific business requirements. These requirements must be approved by the practice manager of the Networking Practice.

c. Connections originating in an untrusted (red) network and terminating in a trusted (green) network must utilize strong encryption and strong authentication.

3. No device other than a firewall may have physical connections to two networks of different security classifications. In cases where this does occur, all connections on that device will assume the lowest level of trust of any of the connections. There are two important implications of this:

   a. VLAN's (Virtual Local Area Networks) serving networks of different security classifications may not reside on the same switch.

   b. If a server in an atrium has a second network connection used for backups, the backup network connection must be considered an amber connection and *cannot* be considered trusted.

4. Network-based intrusion detection systems must be deployed in each amber and green network. The systems must be tuned specifically to allow for expected traffic but to alert the appropriate individuals or groups immediately when there is evidence that the security perimeter has been compromised.

5. At this time, no business justification has been provided for the use of wireless (such as 802.11b) devices on the GIAC Enterprises network. Use of such devices must be restricted to lab networks. As noted above, lab networks are considered amber networks and must therefore be separated from trusted networks by a firewall.

**Ownership:**

This Policy is owned by the Practice Manager of the Networking Practice. It must be reviewed annually. Modifications to this policy must be approved by the President and CEO of GIAC Enterprises.

The Security Team of the Networking Practice is responsible for conducting an annual audit of GIAC Enterprise's networks to ensure compliance with this policy.

**Compliance:**

All employees of GIAC Enterprises share the responsibility for compliance with this Policy. Intentional violations of this policy may result in disciplinary action up to and including termination of employment. Any deviations from this policy must be documented and approved by the Practice Manager of the Networking Practice and by the President and CEO of GIAC Enterprises. All deviations must be kept on file and reviewed annually as part of the compliance audit.

All networks owned and operated by GIAC Enterprises must be in compliance with this policy within 30 days of its approval.

**Glossary;**

- Strong Authentication: Authentication methods are considered to be "strong" if they require more than one factor to verify a user's identity. There are three factors to be considered in authentication – they are generally referred to as "something you know, something you have, and something you are." The use of a user ID and password is considered to be single-factor, as it is comprised solely of "something you know." The combination of a user ID with a one-time-use password, such as a SecurID token, is an example of two-factor authentication. Three-factor authentication generally combines a user ID with biometric controls such as a fingerprint or retinal scan. GIAC Enterprise's standard for strong authentication is RSA's SecurID product.
- Strong Encryption: GIAC Enterprises requires the use of industry-standard, publicly available encryption algorithms. An algorithm is considered "strong" if it has not yet been broken or requires a prohibitively long period of time to crack. As of the time of this writing, the 3DES, Blowfish, and AES algorithms are considered "strong" if keys of sufficient length are used. However, due to constant advances in both computing power and encryption techniques and policies, GIAC's Security Team should be consulted before implementing any system that includes encryption.

**Revision History:**

| *Date* | *Version* | *Author* | *Comments* |
|---|---|---|---|
| 1/25/02 | 1.0 | Terry Miesse | |
| | | | |

**Approval:**

_____ _____

President and CEO, GIAC Enterprises Date

_____ _____

Practice Manager, Networking Practice Date

## *GIAC Enterprises Information Classification Policy*

**Purpose:**

Information is a vital asset in any corporation, and it must be properly protected as any other asset would be. This Policy describes the classification scheme used for all information within GIAC Enterprises. The levels of classification within this scheme are based on the value of the data, and the potential damage to the company – criminal, financial, competitive, or public relations - should the information be improperly disclosed.

**Scope:**

This Policy applies to all information stored or transmitted within GIAC Enterprises, regardless of form, format, or medium. As such, it applies to both paper and electronic media. These policies should be applied to the verbal distribution of information (including telephonic and teleconferencing) as appropriate.

**Policy:**

1. All company information must be classified by one of the following levels:
    a. *Public* – Information whose disclosure would have no negative impact of any sort on the company. Public information may be disseminated freely to individuals and organizations both inside and outside the company. One example of Public information is press releases.
    b. *Internal* – Information whose disclosure to individuals or organizations outside of the company could possibly damage the company. This damage may be in the form of criminal liability, financial or competitive damage, or a loss of public "good will." Internal information may be disseminated freely to individuals within the company. Dissemination of Internal information to individuals or organizations outside the company requires the completion of a non-disclosure agreement and approval of a divisional executive. Examples of Internal information include company financial results and organizational announcements.
    c. *Customer Confidential* – Information related to a specific client whose disclosure to individuals or organizations outside of GIAC Enterprises and the involved client could possibly damage either company. Customer Confidential information may be disseminated to individuals dealing directly with the customer and to management within GIAC Enterprises. Dissemination of Customer Confidential information to the customer organization may or may not be appropriate depending upon the information and the role of the individual within the customer's organization. Examples of Customer Confidential information include contract proposals and customer's strategic business plans.
    d. *Restricted* – Information whose disclosure to certain individuals within the company could potentially damage the overall operations of the company.

Dissemination of Restricted information to individuals within the company must be confined to those with a defined business need to know the information. Dissemination of Restricted information to individuals or organizations outside the company requires the completion of a non-disclosure agreement and approval of the Company President. If the information is in hardcopy or electronic format, a list of all individuals with access to the information must be maintained. Examples of Restricted information include employee payroll data and any information regarding to a pending company merger or acquisition.

2. All information in printed or electronic format must be clearly labeled with its classification level. Any information not labeled should be assumed to be Internal.
3. The value of all information changes over time. The classification level of all stored information should be reviewed periodically to ensure that its classification is correct given the current value of the information.

**Ownership:**

This Policy is owned by the Chief Financial Officer of GIAC Enterprises. Modifications to this policy must be approved by the CFO and the President of GIAC Enterprises.

The Chief Financial Officer is responsible for ensuring that an annual audit of all stored information is conducted to ensure compliance with this policy.

**Compliance:**

All employees of GIAC Enterprises share the responsibility for compliance with this Policy. Intentional violations of this policy may result in disciplinary action up to and including termination of employment. Any deviations from this policy must be documented and approved by the Chief Financial Officer and by the President and CEO of GIAC Enterprises. All deviations must be kept on file and reviewed annually as part of the compliance audit.

All stored information under the management of GIAC Enterprises must be in compliance with this policy within 90 days of its approval. This policy must be communicated to all employees within 5 days of its approval.

**Revision History:**

| *Date* | *Version* | *Author* | *Comments* |
|---|---|---|---|
| 3/11/02 | 1.0 | Terry Miesse | |
| | | | |

**Approval:**

_____ _____

President and CEO, GIAC Enterprises Date

_____ _____

Practice Manager, Networking Practice Date

## *GIAC Enterprises Account Administration Policy*

**Purpose:**

The purpose of this policy is to ensure that user accounts and access permissions are created and revoked in a timely fashion. Failure to create accounts promptly may result in lost productivity and delays impacting customer deliverables. This also fosters an environment where users share ID's and passwords. Failure to revoke accounts and/or access permissions promptly results in users having access to applications or resources that is no longer appropriate. Failure to deactivate and remove old accounts also provides an avenue for systems to be compromised by former employees, or others who learn of idle but active accounts.

**Scope:**

This Policy applies to all accounts created on computer systems, network devices, and applications owned and operated by GIAC Enterprises. This Policy also applies to any computer systems, network devices, and applications managed by GIAC Enterprises on behalf of a client inasmuch as it does not conflict with any policies the affected client may have in place; in such an instance, the client's policy will take precedence.

**Policy:**

1. The following accounts will be automatically created when a new employee joins the company:
   - Email
   - Time tracking system
   - NT/Samba (for desktop and file/print authentication)
2. Requests for the creation of any accounts other than those automatically created must be approved by the employee's Practice Manager or divisional executive (i.e. CFO for administrative employees). No account changes should be executed until the request has been approved.
3. All requests for account creation or additional access permissions must be entered via the User Tracking System. If a request cannot be accommodated by UTS, it must be submitted via email to the GIAC system administrators email alias. Any requests that are received via email that are within the capabilities of UTS must be rejected and entered via UTS.
4. All account requests must include a lifespan for the account. If an employee requires access to a database for the duration of a project, and the project has been sized for 60 days, the lifespan indicated on the request should be 60 days. If an account is needed for longer than the originally requested lifespan, an extension must be entered via UTS and follow the same approval process as a new account request.
5. All accounts whose lifespan has been exceeded should be deactivated.

6. All accounts associated with an employee who leaves the company must be deactivated immediately upon the termination of their employment.
7. If an employee leaves the company while assigned to a customer project, the administrative contact at that customer must be notified that the employee is no longer an employee of GIAC. Any procedures that the customer has in place regarding terminated consultants, including (but not limited to) the return of identification badges or the deactivation of any accounts on the customer's systems, must be followed and/or facilitated.
8. When an employee leaves a project, all accounts associated with that employee specific to that project, such as application logins, must be deactivated immediately upon their reassignment away from the project.
9. All deactivated accounts should be purged after an appropriate period of inactivity, not to exceed 6 months. This period may vary between various computer systems, network devices, and applications.
10. An audit of all GIAC systems will be conducted periodically, no less frequently than once per calendar year, to ensure that only appropriate accounts and access permissions are active. During these audits, all accounts and access permissions will be reviewed. Any accounts that cannot be justified will be deactivated.

**Ownership:**

This Policy is owned by the Practice Manager of the Networking Practice. It must be reviewed annually. Modifications to this policy must be approved by the President and CEO of GIAC Enterprises.

The Security Team of the Networking Practice is responsible for conducting an annual audit of GIAC Enterprise's computer systems, network devices, and applications to ensure compliance with this policy.

**Compliance:**

All employees of GIAC Enterprises share the responsibility for compliance with this Policy. Intentional violations of this policy may result in disciplinary action up to and including termination of employment. Any deviations from this policy must be documented and approved by the Practice Manager of the Networking Practice and by the President and CEO of GIAC Enterprises. All deviations must be kept on file and reviewed annually as part of the compliance audit.

All computer systems, network devices, and applications owned and operated by GIAC Enterprises must be in compliance with this policy within 30 days of its approval.

**Revision History:**

| *Date* | *Version* | *Author* | *Comments* |
|---|---|---|---|
| 3/11/02 | 1.0 | Terry Miesse | |
| | | | |

**Approval:**

_____ _____

President and CEO, GIAC Enterprises Date

_____ _____

Practice Manager, Networking Practice Date

# Section 3 – Security Procedure

## *Employee Termination Procedure*

**Purpose:**

This Procedure details the steps that should be followed when an employee leaves the company. This Procedure is should be used by GIAC's system administrators to ensure that a terminated employee's accounts are properly deactivated on all systems. Failure to follow this Procedure may result in a terminated employee being able to gain access to computer systems, networks, or applications owned or managed by GIAC Enterprises. Inactive but enabled accounts also provide a point of entry for other unauthorized users to gain access to these systems. Exploitation of this access may result in damage to the systems or compromise of information. It may also result in liability to the company, if compromised systems are used as a "jumping-off point" to further compromise computer systems or applications belonging to other companies, particularly to customers of GIAC Enterprises.

**Scope:**

The steps included in this Procedure relate *only* to any access that the employee may have to computer systems or networks owned or managed by GIAC Enterprises. This Procedure does *not* include any HR-related tasks, such as benefits- or payroll-related activities.

**Procedure:**

1. The on-call system administrator should be notified via email by the workflow system within the HR application when an employee has been terminated. In cases where the employee is being asked to leave the company, or any other time where the parties involved are concerned about any actions the departing employee may take, the Human Resources representative involved in the employee termination process should notify the system administrator immediately, either in person or by phone, that the employee is being terminated and that their access to all computer and network systems should be immediately revoked. While it may place the system administrator in an uncomfortable position, it is most effective to notify the system administrator prior to the actual termination of the employee so that any necessary research may be done ahead of time. This will allow the system administrator time to remove the employee's access to any critical systems while the employee is being notified of their termination.
2. Disable the user's email account by locking their account on the mailhost. (Utilize the *passwd –l* command.)
3. Lock the user's NT/Samba account by disabling their account in the NT User Manager applet.

4. Disable the user's timesheet login by updating their status to "term". (This currently requires an SQL query. A modification to the user administration form has been requested. This procedure will be updated when it is complete.)
5. Utilize the User Reporting function in the User Tracking System to find all systems where the user has an account. Disable these accounts using the appropriate procedure for each account. In the case of database applications, disabling the user's login for the database instance will disable their login to all applications in that database instance.
6. Run the find_user script from the sysadmin account on the mailhost. This script will query all systems and applications for a given user ID. This can be used to double-check that there were no ID's created that may have been missed by the UTS report in the previous step.
7. Change any administrative passwords the employee may have had access to. If the employee was a member of the Networking Practice, the administrative passwords on all internal machines and network equipment must be changed. Update the hardcopy password list that is maintained by the Network Practice Manager, and update the encrypted file that contains the appropriate passwords. (If unsure of this file's location, contact a member of the Security Team.) Notify all members of the Networking Practice and any other system administrators that the administrative passwords have been changed via email.
8. Check with the employee's most recent project manager to determine if any other non-human ID's (ID's used by applications to connect to other systems) may need to have their passwords updated. If any ID's are identified, notify the project manager of those systems.
9. Send an email to the employee's divisional executive (Practice Manager or CFO) with a list of all accounts that were deactivated. Copy the Security Team's email alias on this email. This will flag these accounts to be double-checked at the next security audit.
10. If the employee is a consultant who is leaving the company while assigned to a customer project, the Project Manager is responsible for ensuring that the administrative contact at the customer is notified that the consultant is no longer an employee of GIAC Enterprises. The Project Manager is also responsible for providing any further information needed to facilitate any procedures the customer may have for removing the consultant's access from their systems. Finally, it is the Project Manager's responsibility to ensure that all necessary items are returned to the customer, including identification badges or any other equipment or accessories that the customer may have provided to the consultant.

**Owner:**

This Procedure is owned by the Security Team of the Networking Practice. The owner is responsible for updating the Procedure as new systems, processes, and tools are introduced into the GIAC Enterprises corporate environment. Changes to this

Procedure must be approved by the GIAC lead system administrator and the Security Team's lead consultant.

**Revision History:**

| *Date* | *Version* | *Author* | *Comments* |
|---|---|---|---|
| 3/11/02 | 1.0 | Terry Miesse | |
| | | | |

# References

Building an in-Depth Defense, Brooke Paul, 7/9/2001 issue of Network Computing (http://www.networkcomputing.com/1214/1214ws1.html)

Centralized Backups, Michael J. Gallagher, 8/11/2001, published on SANS "Information Security Reading Room" (http://rr.sans.org/recovery/central.php)

The Hows and Whens of Tape Backups, Howard Marks, 3/5/2001 issue of Network Computing (http://www.networkcomputing.com/1205/1205ws1.html)

Acceptable Encryption Policy, SANS Security Policy Project (http://www.sans.org/newlook/resources/policies/Acceptable_Encryption_Policy.pdf)

Information Sensitivity Policy, SANS Security Policy Project (http://www.sans.org/newlook/resources/policies/Information_Sensitivity_Policy.pdf)