Global Information Assurance Certification Paper

GIAC Information Security Officer Practical

Security Policy for a Manufacturing Enterprise

Version 1.0
October 2001

By Jon M. Brage

December 15, 2001

GIAC Information Security Officer Practical
Assignment 1 – A Description of GIAC Enterprises

GIAC Enterprises – A Description

GIAC Enterprises is an ISO 9001/9002 certified business that repairs, refurbishes and re-manufactures critical electro-mechanical infrastructure components (e.g., large electrical generation components, manufacturing equipment, etc.) for governments and businesses. Physically, GIAC Enterprises is located on a 10 building wholly owned campus. This campus is a gated facility employing physical security through guards and closed circuit television monitoring of the perimeter. Personnel can only access the campus guarded gates or via turnstiles activated only by using GIAC Enterprises badges swiped through a badge reader. All employees must wear their GIAC Enterprises badges at all times when on campus or when working at off-site locations in an official work capacity.

Information Technology Description

The GIAC Enterprises Information Technology Infrastructure consists of workstations, laptops, printers, personal data assistants, servers, and other intelligent devices such as computer aided manufacturing equipment and inventory control devices. Most of these devices communicate across a TCP/IP based network infrastructure that consists of 100Base-T (within buildings) and 100Base-FI (primarily between buildings). The network infrastructure connects through a demilitarized zone (DMZ) to the Internet via two T1 lines. Additional external access to the network may be made through dial-in connections. A network operations center where the DMZ, primary switches and the server farms for the network are located is located in Building 6 as well as a testing network used to test proposed hardware, software and configurations. Figure 1 provides a schematic lay out of the infrastructure (Building 6 and the testing network are not specifically identified).

The primary operating system of the network is Windows NT® 4.0 (service pack 6a) supported with Simple Network Management Protocol (SNMP) for remote management of network devices. The network is protected by a DMZ from the internet where the company's public web server and File Transfer Protocol (FTP) server are located. A virtual private network (VPN) device is also located here and is used to establish secure links to critical business partners and clients via the second T1 line. GIAC Enterprises has a class C Internet address and performs TCP/IP address translation at the DMZ. Internally, GIAC Enterprises operates using class B TCP/IP addresses. Dial-in access to the network is also handled with a Windows NT® RAS server also located within the DMZ.

The network is divided internally into two Windows NT® domains. The first is called the GIAC Enterprises Open Network (GEONet). This portion of the network comprises those users that regularly interface with the public and/or the marketing of GIAC Enterprises. The second domain is called the GIAC Enterprises Closed Network (GECNET). This domain is where information that the GIAC Enterprises Management has designated as business sensitive, financial, operations, proprietary, etc., (collectively called sensitive information) is processed. Both networks share the same infrastructure, but user accounts and workstations are set up to access only domain

one at a time. GEONet trusts GECNet only.

The testing network does not connect to either the internal network or the Internet and is used to test new software and the security of new commercial off the shelf software and hardware. This network also serves as a repository of spare equipment for replacing failed critical components of the GEONet/GECNet infrastructure. Because GIAC Enterprises often performs repairs for the Department of Defense (DOD), GIAC Enterprise information systems are designed to meet the DOD Trusted Computer Systems Evaluation Criteria security level of C2. The information systems are also certified and accredited by the DOD per the DOD Information Technology Security Certification and Accreditation Process (DITSCAP).

GIAC Enterprises Campus Network Connectivity Schematic

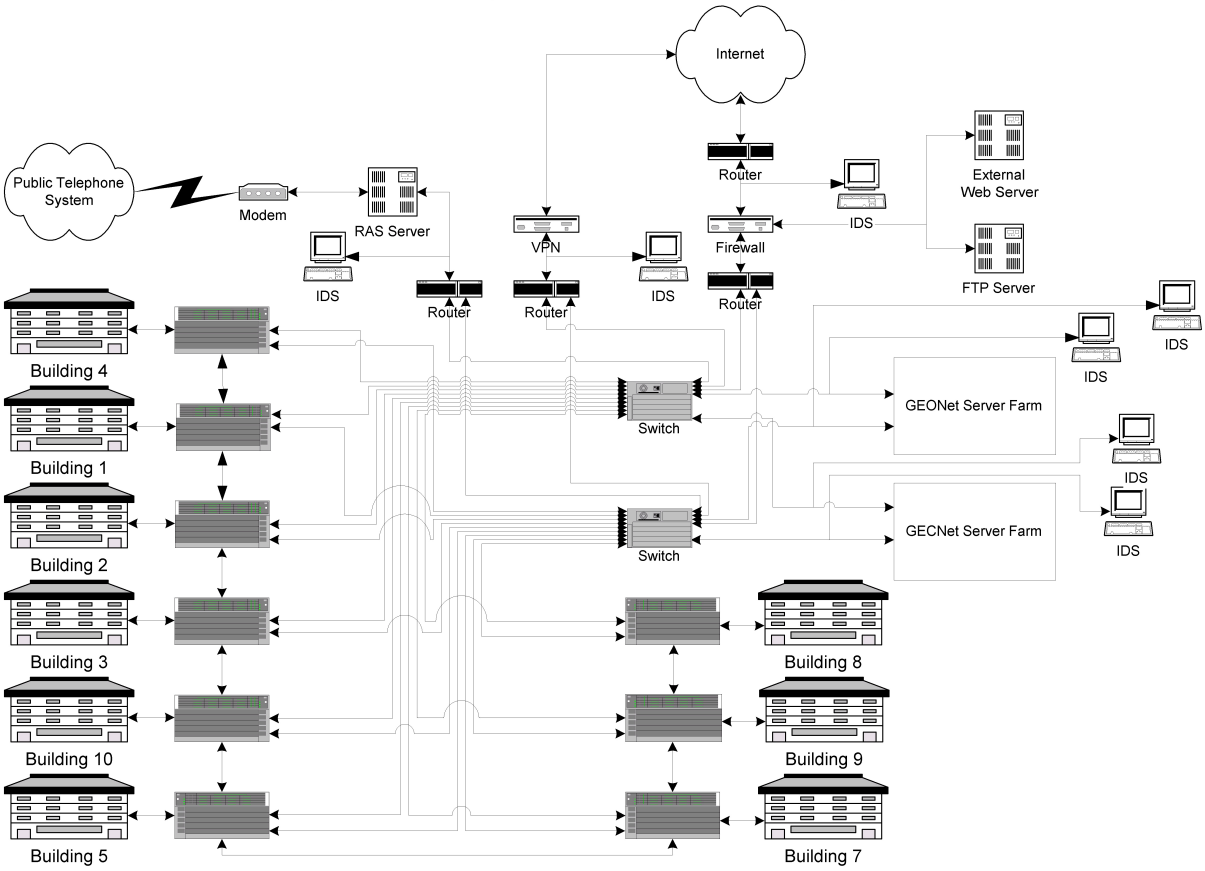

Figure 1

Business Operations

GIAC Enterprises repairs, overhauls and refurbishes complex critical electro-mechanical infrastructure components for governments and businesses either at the customer's site or within the GIAC Campus. All repair work is performed to written procedures and all deviations from original specifications are documented in writing. In order to conduct these repairs in a cost effective, high quality manner and create a

profit for the stock holders, GIAC Enterprises has invested heavily in automated management and engineering information systems.

Company personnel must be able to use the GIAC Enterprises information systems efficiently to translate a set of repair specifications into working procedures that will pass through the contracting, procurement, engineering and production stages of a project. Critical information (i.e., information deemed to be proprietary or sensitive by the customer, original equipment manufacturer and or GIAC Enterprises management) must be maintained in a secure manner during this process. GIAC Enterprises uses a combination of commercial off-the-shelf (COTS) products as well as in-house developed solutions in order to automate some or all of those business functions.

Minimum Personnel Requirements for Accessing GIAC Enterprises Information Systems:
Employees are screened upon hire for criminal background and United States citizenship. Additionally, once employed, certain employees may also receive government clearances in support of potential and active government contracts.

Subcontractors, Business Partners and customers are granted access to GIAC Enterprises information and information systems based upon contractual need, Management's discretion and meeting the security provisions set forth in the applicable contracts. As a minimum, individuals from these organizations must be United States citizens in order to receive a GIAC Enterprises information system user account.

Standard User Computing Resources:
In general GIAC Enterprises provides all employees access to Office Automation software (Microsoft® Office 2000) that is expected to be used for general communications, correspondence and documentation of work progress. All employees have network accounts on the GEONet domain. The primary purpose of this access is to keep up to date on internal happening with in the organization (primarily via the GEONet Intranet web pages). Electronic Mail is part of each user's account using Microsoft® Exchange/Outlook 2000.

Personnel that the GIAC Enterprises Management has authorized to access GIAC Enterprises sensitive information are provided accounts on the GECNet domain. These accounts also are supported with Microsoft® Exchange/Outlook 2000 using a separate mail server that is located on the GECNet Domain.

Workstation and Servers on GEONet and GECNet:
All workstations are members of both domains and the user selects which domain they login to. All workstations and servers are protected with anti-virus software. The GEONet and GECNet exchange servers do pass e-mail between each other, however, the GECNet exchange servers perform a rigorous key word search of all mail sent to GEONet and the Internet. Data on file and internal web servers are protected by access control lists based upon management defined access policy. Databases are

developed to manage data based upon roles that meet the management defined access policies. All data within databases, file and web servers are audited for unauthorized access and activity. All servers are located in one of two computer centers, called server farms. Physical access to the server farms is strictly controlled and monitored by the Security Department. Electronic access to the GIAC Enterprises information systems is limited to only "authenticated" users. Intrusion detection monitoring is performed within the DMZ and at the entrance to the GEONet and GECNet server farms in order to monitor for unauthorized access.

Specialized Data Processing Requirements:
Remote site users and each GIAC Enterprises department require some specialized data/data processing capability. In general these requirements are as follows:

1. The Accounting Department uses an in house developed Oracle database used for financial management, budgeting and time keeping. This database is linked to the Industrial Management System databases.

2. The Human Resources Department uses commercial software to maintain personnel records. An in-house developed Oracle database, the Qualifications Tracking System (QTS), is used to track personnel qualifications (to industry and customer standards). This database is linked to the Industrial Management System databases.

3. Management uses the Industrial Management System (IMS), an in-house developed Oracle database that provides for project management, resource projection (personnel and financial).

4. The Quality Assurance Department uses an in-house developed Document Management System (DMS) based upon web technology and an Oracle database. A COTS Statistical Analysis software package is also used for in depth trend analysis.

5. The Engineering Department uses the IMS to plan for the accomplishment of proposed and contracted projects. The DMS is used to track and manage procedures issued to accomplish contracted projects. To support the writing of these procedures, COTS computer aided design (CAD) and Computer Aided Engineering (CAE) software (depending upon the customer requirements) is also. The Engineering Department uses a variety of proprietary software that original equipment manufacturer's (OEM's) developed to supports many of the components repaired by GIAC Enterprises. Additionally, materials and supplies are specified for ordering using the Supply Department's Requisition Management System (RMS).

6. The Production department uses the various CAD and CAE software and computer aided manufacturing software that supports their numerically

controlled manufacturing equipment. Production also uses the Supply Department's RMS.

7. The Supply Department uses in-house developed document control and inventory management software that uses web-based technology and an Oracle database. This software/hardware system is called the Requisition Management System (RMS) and tracks technical specifications for materials and services from the identification of need by the Engineering and Production Departments through the contracting cycle, receipt inspection, storage and eventually till it is used.

8. The Environmental Monitoring Department uses several automated data collection instruments to monitor GIAC Enterprises compliance with environmental quality, health and safety regulations. Additionally, they access the RMS to track Material Safety Data Sheets for hazardous materials ordered and used by GIAC Enterprises.

9. The Software Development and Information Technology Department utilizes a large number of software development and monitoring tools.

10. The Security Department utilizes the QTS to track areas and systems personnel are authorized to access.

11. Remote Users - management, marketing, engineering, production personnel using GIAC Enterprises owned Laptops. These individuals require access to GEONet and/or GECNet when off-campus. Access is through dial-in to the RAS server using intelligent secure tokens (SmartCards) for short term situations. For longer term (or where contractually provided for) a dedicated VPN connection may be established.

GIAC Enterprise Security Policy

GIAC Enterprises handles information that by contract, policy or government regulation or law must be protected from unauthorized access. GIAC Enterprises has built information systems used to access that information. The design of these information systems (networks, databases, etc.) is such that that access is controlled. Information that is inaccessible to authorized users prevents the function of the business. Also, perfect control of information access is currently not economically possible. Therefore, system design is limited to cost-effective controls and an acceptance of risk for that which can not be controlled or foreseen. GIAC Enterprises philosophy for protecting information is to employ a policy of least privilege and to design for defense in depth. There are five major areas of concern that this policy must handle:

1. Data Availability, Integrity and Confidentiality
2. Security Awareness Training
3. Acceptable Use
4. Remote Users
5. Intrusion Detection

Data Availability, Integrity and Confidentiality

Data Availability, Integrity and Confidentiality are first in importance to GIAC Enterprises. If data is not available to those who need it, then business can not function. If the data is not correct, therefore un-reliable, mistakes are made causing re-work and lost customer satisfaction, both of which affect the bottom line. If data is not kept confidential, GIAC Enterprises' business reputation is lost and possible legal action, both civil and criminal, could be incurred. Again, loss of data confidentiality ultimately affects the bottom line. If GIAC Enterprises can not design information systems that allows for the detection and notification of unauthorized access to GIAC Enterprises information, customer confidence in our ability to protect their information is affected and contracts can be lost or cancelled. If GIAC Enterprises can not control the configuration of the deployed information systems, then it is not be possible to ensure the designed controls of the systems can and are properly working. Should uncontrolled elements be introduced into GIAC Enterprises information systems, it can no longer be assumed those systems are part of a controlled environment and the risk to the information stored and processed there will no longer be known or manageable.

Security Awareness Training

Security Awareness Training is of prime importance because people build and use information systems and ultimately, compromise those systems, The strongest policy, the best safes, the highest level of encryption are all worthless of people do not properly use and safeguard them. Therefore, making authorized users, system administrators, and management aware of their role in the protection of GIAC Enterprises information is critical to the success of protecting this information.

Acceptable Use

Acceptable Use refers to what uses GIAC Enterprises information systems may be

used for that the GIAC Enterprises Management considers acceptable. The GIAC Enterprises information systems are provided for the purpose of conducting profitable business. The well being and morale of GIAC Enterprises employees directly affects the ability of GIAC Enterprises to be competitive, therefore GIAC Enterprises management recognizes the value in allowing some non-business related usage of GIAC Enterprises information systems. However, the information systems are not provided solely for the personal use of employees. Misuse of company assets will affect the cost of doing business, the reputation of the company and possibly criminal and civil liability.

Remote Users

Remote users are a fact of how GIAC Enterprises does business. Protection of information systems remote users carry with them and the secure transmission of that information such that it can not be intercepted is of prime importance. Transmission of company data or the security of that data on those remote information systems directly impacts the company's ability to maintain data Confidentiality.

Intrusion Detection

Intrusion Detection is the last major area of concern. It does not directly relate to the bottom line of the company. It however is the primary tool that is used to determine if the information systems are protected as well as designed and to determine if anyone has accessed company information systems (therefore had access to the data). Unless the company knows there has been no unauthorized access with a measurable resource, the company has no way to protect itself from attack, loss of competitive edge, or civil and criminal liabilities.

Security Policy

I. Data Availability, Integrity and Confidentiality

A. *Purpose*

The purpose of protecting of GIAC Enterprises information falls into three categories:

1. To ensure that GIAC Enterprises information is available to company employees and business partners as defined by management policy, government regulation and contractual obligation.
2. To ensure that the integrity of GIAC Enterprises information ensuring it is reliable and with out question.
3. To ensure that the confidentiality of GIAC Enterprises information is maintained ensuring that only those individuals that GIAC Enterprises Management has authorized to access that information can do so and those who are not authorized can not.

B. *Background*

Information is only useful when it is available and the integrity of the information is without question. To be financially useful requires that it be kept confidential from our competitors. In order to meet these needs successfully, information systems must be

able to provide the information with these three attributes: availability, integrity and confidentiality.
The information stored and used on the GIAC Enterprises information systems comprises personnel data, proprietary business data, strategic planning information, financial and accounting information in addition to the general information needed to run an enterprise from day to day. Loss, compromise, corruption or denial of access to any information that resides on the company's information systems will be negatively impact the success and reputation of the company. The purpose of protecting GIAC Enterprises information is to retain the company's maximum competitive edge while conforming to governmental regulations and contractual obligations that stipulate the protection of certain information.

C. *Scope*

All information processed, stored, transmitted and otherwise manipulated on GIAC Enterprises owned information systems is the property of GIAC Enterprises unless otherwise noted in contractual agreements and governmental regulation. All such information processed, stored, transmitted and otherwise manipulated on GIAC Enterprises information systems must be protected in accordance with this policy.

D. *Policy Statement*

All GIAC Information shall be protected from loss of availability, integrity and confidentiality by all employees, business partners and subcontractors. The management of GIAC Enterprises is the final authority on who may access GIAC Enterprises information. GIAC Enterprises management determines the minimum acceptable level of protection for GIAC Enterprise information and what risks are acceptable with regard to the integrity, availability and confidentiality of that information. The protection system for GIAC Enterprises information is based on the principles of "least privilege" and "defense in depth".

E. *Responsibility*

GIAC Enterprises Management is responsible for:

1. Determining who shall be granted access to GIAC Enterprises information. Management responsible for authorizing and funding improvements for the protection of GIAC Enterprises information or formally accepting the risk of not authorizing recommended improvements.
2. Accepting the risk to GIAC Enterprises information.
3. Setting categories of GIAC Enterprises information such that access controls to that information can be developed.
4. For setting the minimum trust criteria (i.e., no criminal record, U. S. citizen, final government clearance, etc.) required for employees to receive access to the defined categories of company information.

The Software Development and Information Technology Department (SD/IT) is responsible for:

1. Providing information systems that provide a minimum acceptable level of

availability as determined by management. These information systems shall ensure the integrity and confidentiality of GIAC Enterprises data as defined by management.
2. Informing management of the threats facing those information systems and the vulnerabilities of use those information systems and evaluating risks of those threats and vulnerabilities.
3. Recommending methods of mitigation of threats and vulnerabilities based on a cost/risk analysis methodology.
4. Validating the security of information systems work as designed and the designs incorporate the ability to be monitored and/or audited.

The Security Department is responsible for:
1. Providing physical security for the information systems provided by SD/IT and is responsible for ensuring all users of those systems meet the minimum trust criterion set by management to access the various categories of GIAC Enterprises information.
2. Identifying threats to GIAC Enterprises and informing Management and SD/IT of those threats.

The Human Resources Department is responsible for:
1. Incorporating into position descriptions and maintaining up to date the management approved minimum trust criteria that are required for each position description.
2. Incorporating into position descriptions and maintaining up to date the management approved minimum information categories required for incumbents of those positions.

All users of GIAC Enterprises information systems are responsible for:
1. Assisting in the maintenance of the integrity and confidentiality of the GIAC Enterprises information to which they are authorized to access.
2. Not conducting any activity that contributes to the denial of availability, loss of confidentiality or integrity in that information either through the misuse of information system resources or the introduction of malicious code.

F. *Action*

Management shall:
1. Define what GIAC Enterprises Information shall be accessed by employees, and what information can be released to the public, business partners and subcontractors.
2. Define and review annually the information categories used to determine how GIAC Enterprises information shall be compartmented on GIAC Enterprises information systems and determine their continued acceptability based upon the current operational environment and contractual requirements.
3. Define and review annually the trust criteria required for individuals to be granted access to a specific category of GIAC Enterprises information and to

determine their continued acceptability based upon the current operational environment and contractual requirements.

4. Review annually (or more often if circumstances dictate) the current threats and vulnerabilities facing GIAC Enterprises Information and determine if the current level of protection is adequate.
5. Approve which information categories can be accessed for each user of GIAC Enterprises Information Systems. This approval shall be based on Security's determination of what are trust criteria level the user meets and the user's need for access.
6. Ensure that subcontractors and business partners are contractually obligated to protect GIAC Enterprises information.
7. Review SD/IT recommendations for security upgrades and either authorize and fund their recommendations or formally accept the risk.
8. Review the annual Security recommendations for employees and subcontractors and take action as recommended or formally accept the risk(s).
9. Determine the impact of unauthorized access to the GIAC Enterprises campus and information when so notified by Security and/or SD/IT. Management shall determine if business partners and customers shall be notified based upon this evaluation.

SD/IT shall:

1. Provide information systems, within the level of risk that management deems acceptable, that make GIAC Enterprises Information available to those individuals that management has authorized, in a secure manner where ever management has determined those individuals require access to that information.
2. Provide information systems to all GIAC Enterprises employees, customers, business partners, and subcontractors as directed by management. SD/IT shall provide access to these users to the GIAC Enterprises information based upon their meeting the management specified trust criteria and information categories approved by management.
3. Prepare an annual risk assessment of the threats and vulnerabilities to GIAC Enterprises information and present it to management. SD/IT shall provide recommendations on methods for mitigating those risks and their estimated costs to implement.
4. Assess the use of Information Systems by business partners in protecting GIAC Enterprises information and inform management if these practices are meet the contractual requirements set by management and determine if those practices are sufficient to meet the level of acceptable risk set by management.
5. Recommend contractual requirements to management for inclusion into contracts with business partners and subcontractors. SD/IT shall review Information Systems requirements being required of GIAC Enterprises by customers for GIAC Enterprises ability to meet those requirements and shall recommend to management their acceptability, additional cost to the company and/or alternatives and their cost.

6. Continuously monitor the GIAC Enterprises information systems for unauthorized access or activity. SD/IT shall protect the information system in the event of discovery unauthorized access and inform management of all such events. SD/IT shall inform management of unauthorized access within one (1) hour of discovery.
7. Validate the security design of information systems meets the minimum security specified by Management. SD/IT shall use intrusion detection and incorporate auditing into applications that stores or processes and the designs incorporate the ability to be monitored and/or audited.
8. Implement a system of configuration control for GIAC Enterprises information systems (hardware and software) that enables the controlled deployment and secure operation of GIAC Enterprises information systems.

Security shall:

1. Provide Management with a report stating if an employee meets the trust criteria stated in the position description for which they were hired or promoted to.
2. Provide to Management a report stating if subcontractors, business partner and customer personnel that require access to the GIAC Enterprises campus and/or information systems meets the minimum trust criteria required by Management.
3. Provide management annual recommendations on whether employees and subcontractor personnel meet or continue to meet the minimum trust criterion set by management to access the various categories of GIAC Enterprises information.
4. Provide physical security from unauthorized access to SD/IT information systems that reside within the GIAC Enterprises campus and ensure that unauthorized personnel do not gain access the campus.
5. Continuously monitor the GIAC Enterprises campus for unauthorized access. Security shall protect campus in the event of discovery unauthorized access and inform police immediately and management within 1 hour of discovery of all such events.
6. Provide an annual threat assessment to management and SD/IT of the threats facing GIAC Enterprises. Security shall provide such information to management and SD/IT should significant change in threats be realized between annual assessments.

Human Resources shall:

1. Annually review all position descriptions and incorporate the latest Management approved minimum trust criteria level required for all positions.
2. Annually review all position descriptions and incorporate the latest Management approved minimum information categories to which the positions are authorized access.

Users shall:

1. Physically secure any GIAC Enterprises information or information system assets (including personal data assistants, laptops, bar code scanners, etc.) in

their personal possession to prevent loss of GIAC Enterprises information stored on those systems.
2. Protect their access to GIAC Enterprises information systems such that no one else can gain access to GIAC Enterprises information or information systems through their user account.
3. Not place GIAC Enterprises information on personally owned or contractor owned information systems without the express written permission of management.
4. Conform to all information policies as part of their responsibility to protect GIAC Enterprises information and information systems.
5. Not engage in any activity that contributes to the denial of availability, loss of confidentiality or integrity in GIAC Enterprises information either through the misuse of information system resources or the introduction of malicious code.

II. Security Awareness Training

A. *Purpose*

To inform authorized users, system administrators, programmers, management, etc., of their roles in providing protection to GIAC Enterprises information and information systems.

B. *Background*

The weakest link in protecting information is the uninformed personnel that builds and/or uses and information system. Unless individuals know how to design and use an information system securely, the information will not be secure and will be released to unauthorized individuals. This will result in loss of confidence in GIAC Enterprises by our customers and potential customers and lead to loss of business and profitability.

C. *Scope*

All individuals that design, maintain, or use GIAC Enterprises information systems shall receive training in the use and protection of those systems. Individuals responsible for the design and operation of those systems shall also receive training in the design and operation of those systems.

D. *Policy Statement*

All authorized users shall receive information security awareness training on a continuing basis for the GIAC Enterprises information system as a whole and for any specialized program or software they may be authorized to use. All system administrators and programmers shall receive training in the systems and software used to design and operate GIAC Enterprises information systems. All database and system administrators shall provide initial user and continuing training on the secure user of the systems they are responsible for to all users of those systems. Management will budget for and fund such training.

E. *Responsibility*

Management is responsible for:

1. Budgeting for the training of all authorized users, system and database administrators, and programmers of GIAC Enterprises information systems.
2. Budgeting for the training of all personnel responsible for the development, operations and maintenance of GIAC Enterprises information systems.

All system and database administrators and programmers are responsible for:

1. Taking the minimum level of training necessary to securely maintain and/or use the hardware and software they support.
2. Developing and maintaining initial and continuing user training that will be used to train all authorized users of those systems in the proper use and security of those systems.
3. Developing and disseminating refresher security awareness training to all authorized users of their systems.

Security is responsible for developing and maintaining personnel and physical security training for all GIAC Enterprises employees as well as sub-contractors, business partners, customers and all other visitors to the GIAC Enterprises campus.

Human Resources responsible for:

1. Ensuring that all GIAC Enterprises personnel receive training for in the use of GIAC Enterprises information systems they are authorized to access as well as the personnel and security training developed by Security.
2. Ensuring that all system and database administrators and programmers receive the minimum level of training necessary to securely maintain and/or use the hardware and software they support as stated in their position descriptions.
3. Ensuring that all GIAC Enterprises personnel successfully complete the commercially developed training to be taken by authorized users, system and database administrators and programmers for which GIAC Enterprises pays for.
4. Providing knowledgeable instructors with good presentation skills to present GIAC Enterprises developed information systems and security training.
5. Obtaining feedback from instructors and students who present and attend locally developed information systems and security training and incorporating the feedback into said training.

All users are responsible for taking the initial and refresher training developed for the systems they are authorized to access.

F. *Action*

Management shall:

1. Budget for the training of all authorized users, system and database administrators, and programmers of GIAC Enterprises Information systems.
2. Budget for the training of all personnel responsible for the development, operations and maintenance of GIAC Enterprises information systems.

All system and database administrators and programmers shall:

1. Are responsible for taking the minimum level of training necessary to securely maintain and/or use the hardware and software they support.
2. Develop and maintain initial user training that will be used to train all authorized users of those systems in the proper use and security of those systems.
3. Develop and disseminate refresher security awareness training to all authorized users of their systems.

Security shall develop and maintain personnel and physical security training.

Human Resources shall:

1. Ensure all GIAC Enterprises personnel receive initial and continuing training in the information systems they are authorized to access as well as the personnel and security training developed by Security.
2. Ensure that all system and database administrators and programmers receive the minimum level of training necessary to securely maintain and/or use the hardware and software they support as stated in their position descriptions.
3. Ensure all GIAC Enterprises personnel take the training received by authorized users, system and database administrators and programmers.
4. Provide knowledgeable instructors with good presentation skills to present GIAC Enterprises developed information systems and security training.
5. Institute a method of obtaining feedback from instructors and students who present and attend information systems and security training and incorporating that feedback into GIAC Enterprises developed training.

All users shall take the initial and refresher training developed for the systems they are authorized to access prior to accessing those systems.

III. Acceptable Use

A. *Purpose*

This policy outlines what GIAC Enterprises deems is the acceptable manner in which GIAC Enterprises Information Systems are to be used.

B. *Background*

Information Systems are provided for people to use. GIAC Enterprises information systems are designed to operate in a certain manner in order to perform required business functions. If people do not use the systems as designed, the information systems may or will not operate as designed. If they do not operate as designed, the risk to the information and the processes carried out on those information systems can not be predicted with accuracy and the level of acceptable risk that Management has set will most probably be exceeded. To prevent this from occurring, users of the information systems must use the systems in a manner consistent with their design. Basic assumption that are the foundation of the design of GIAC Enterprises Information systems are:

1. Internet usage will be for business purposes and not for general personal use.
2. Only reviewed and authorized software will be used in order to prevent the introduction of malignant software (viruses, Trojans and worms).
3. Only reviewed and authorized hardware will be used in order to prevent the introduction of unplanned for design elements (such as alternate pathways to the information systems).
4. Access to the network(s) shall be controlled through certain designed pathways. No other pathways are allowed such as modems on workstations, etc.
5. Access to the network and Management defined repositories of information (databases, data warehouses, etc.) shall be accessed by authorized individuals and this access will be controlled by have unique user accounts for all users on the network.
6. GIAC Enterprises Information Systems and the information residing and processed on those information systems are the property of GIAC Enterprises.
7. All users are informed of their responsibilities including this policy and that they should have no expectation of privacy for any information they place on or process over GIAC Enterprises owned information systems.
8. GIAC Enterprises Information Systems will not be used as the basis of criminal activity.
9. GIAC Enterprises makes every effort to provide a non-hostile work environment, free of information that could be construed by users as harassment or offensive to their personal beliefs or ethics.

C. *Scope*

This policy applies to all users of GIAC Enterprises Information Systems.

D. *Policy Statement*

All users of GIAC Enterprises shall use GIAC Information Systems in a manner that does not place the Information Systems or GIAC Enterprises in a position of liability: either financial, civil or criminal. This shall include but is not limited to the following:

1. All users are subject to this policy and consent to its provisions by accessing any GIAC Enterprises Information Systems.
2. Usage of GIAC Enterprises Information Systems is provided for business purposes and not for general personal use. Personnel that obtain prior written permission from Management may use the GIAC Enterprises Information Systems for personal use provided it does not affect systems operations or put the company into a position of liability. Personal usage of GIAC Information Systems may be withdrawn at any time at the discretion of the Management.
3. Internet access from GIAC Information Systems shall be done by authorized users that have received prior written permission to use the Internet from Management. Unauthorized access is considered a violation of this policy.
4. All software used on GIAC Enterprises Information Systems shall be reviewed in a controlled manner in a controlled environment by SD/IT prior to installation on

to any production GIAC Enterprises Information System. Upon a satisfactory written recommendation which shall include installation and usage parameters to Management, Management will formally approve the use of the software that can then be placed on GIAC Enterprises Information Systems (purchased if required) consistent with the recommended controls listed by SD/IT.

5. All hardware used on GIAC Enterprises Information Systems shall be reviewed in a controlled manner in a controlled environment by SD/IT prior to installation on to any production GIAC Enterprises Information System. Upon a satisfactory written recommendation which shall include installation and usage parameters to Management, Management will formally approve the use of the hardware that can then be placed on GIAC Enterprises Information Systems (purchased if required) consistent with the recommended controls listed by SD/IT.
6. No personal hardware, freeware, or shareware shall be allowed on GIAC Enterprises Information Systems.
7. All personnel requiring access to the any GIAC Enterprises Information System shall submit the appropriate access request to SD/IT and receive Management approval prior to receiving access to those systems.
8. All personnel shall have unique user accounts to all GIAC Enterprise information systems except where Management deems it is in the best interest of the company or is required by specific software. All such instances of exception shall be documented and receive prior written Management approval.
9. Users shall not share passwords or allow other GIAC Enterprises personnel to use their access the GIAC Enterprises Information Systems with out being personally present. Users shall not allow any non-GIAC Enterprises personnel to use their account, even when in their presence without prior written approval of Management.
10. GIAC Enterprises Information Systems and the information residing and processed on those information systems are the property of GIAC Enterprises.
11. All users are to be informed of their responsibilities when using GIAC Enterprises Information Systems including this policy. Users shall be informed that they have no expectation of privacy for any information they place on or process over GIAC Enterprises owned information systems.
12. GIAC Enterprises Information Systems will not be used as the basis of criminal activity.
13. GIAC Enterprises Information Systems shall not be used to access, process, store information such as political ideology, pornographic material, religious material or any other none business related information as defined by Management that can reasonable be expected to create a hostile work environment or that could be construed by users as harassment or offensive to their personal beliefs or ethics.

E. *Responsibility*

Management is responsible for:

1. Providing written approval and funding or disapproval of any software recommendation submitted by SD/IT for the use of proposed software prior

placement onto any production GIAC Enterprises Information Systems.
2. Providing written approval and funding or disapproval of any hardware recommendation submitted by SD/IT prior to the use of the proposed hardware to store, process or otherwise handle GIAC Enterprises information.
3. Reviewing and accepting the risk for allowing personnel to share user accounts and for providing prior written documentation of approval for all instances presented in writing by SD/IT to Management.
4. Determining what information is to be considered political ideology, pornographic material, religious material or any other none business related information that can reasonably be expected to create a hostile work environment or that could be construed by users as harassment or offensive to their personal beliefs or ethics.

SD/IT is responsible for:
1. Reviewing software proposed for use on GIAC Enterprises Information Systems.
2. Reviewing in a controlled manner in a controlled environment proposed software and shall develop configuration guides and usage standards for all software that shall be recommended to Management for approval.
3. Submitting recommendations to Management that include configuration guides and standards and shall outline the cost and risk in using the proposed software.
4. Reviewing all hardware proposed for use in processing, storing or otherwise handle GIAC Enterprises Information.
5. Informing all personnel that GIAC Enterprises information systems and the information residing and processed on those information systems are the property of GIAC Enterprises.
6. Reviewing in a controlled manner in a controlled environment proposed hardware and shall develop configuration guides and usage standards for all hardware that shall be recommended to Management for approval.
7. Submitting a recommendation to Management that includes these guides and standards and shall outline the cost and risk in using the proposed hardware.
8. Ensuring all authorized personnel have unique user accounts to all GIAC Enterprise information systems except where Management has deemed it is in the best interest of the company or is required by specific software and shall
9. Informing all users that they have no expectation of privacy for any information they place on or process over GIAC Enterprises owned information systems.
10. Presenting all instances of discovery to Management of all information they considered to be political ideology, pornographic material, religious material or any other none business related information that they feel creates a hostile work environment or that could be construed by users as harassment

or offensive to their personal beliefs or ethics.

All personnel are responsible for:

1. Reading and understanding this policy.
2. Consenting to the provisions of this policy is prior to being granted access to any GIAC Enterprises Information Systems.
3. Submitting the appropriate access request to SD/IT and receiving Management approval prior to receiving access to GIAC Enterprises information systems.
4. Obtaining prior written permission from Management in order to use any GIAC Enterprises information systems for personal use.
5. Understanding they shall not have an expectation of privacy to personal information they may place onto GIAC Information Systems and any such information may be used in any manner at Management's discretion without the approval of the individual and without any compensation.
6. Understanding that personal usage of GIAC Enterprises information systems may be withdrawn at any time at the discretion of the Management.
7. Obtaining Management's prior written permission to use the Internet via GIAC Enterprises information systems and the access responsibly and shall not go to inappropriate Internet sites (sites that could be construed by Management to incur liability or creating a hostile work environment).
8. Not downloading unauthorized software and copyrighted information via the Internet except for SD/IT personnel who shall do so onto specific GIAC Enterprises information systems set up for this purpose that are isolated from the GIAC Enterprises networked systems.
9. Not placing personal hardware, freeware, or shareware onto GIAC Enterprises Information Systems without prior written approval of Management.
10. Protecting and not sharing their passwords or allow other GIAC Enterprises personnel to use their access the GIAC Enterprises Information Systems with out being personally present.
11. Not allowing any non-GIAC Enterprises personnel to use their account, even when in their presence without prior written approval of Management.
12. Understanding this policy and understanding their responsibilities when using GIAC Enterprises Information Systems.
13. Not using the GIAC Enterprises Information Systems for criminal activity.
14. Not using the GIAC Enterprises Information Systems to access, process, store information such as political ideology, pornographic material, religious material or any other none business related information as defined by Management that can reasonable be expected to create a hostile work environment or that could be construed by users as harassment or offensive to their personal beliefs or ethics
15. Reporting to Management information they discover and considered to be political ideology, pornographic material, religious material or any other none business related information that they feel creates a hostile work

environment or that could be construed by users as harassment or offensive to their personal beliefs or ethics.

F. *Action*

Management shall:

1. Provide written notice of the withdrawal of the privilege of approved individuals to use the GIAC Information Systems for personal usage.
2. Forward to SD/IT all approved requests for personnel usage or for access to the Internet.
3. Grant approval to for personal use of GIAC Enterprises information systems if the request is justified and they have received the written confirmation from the individual that requested to use GIAC Enterprises information systems for personal use that the individual understands they shall not have an expectation of privacy to personal information they place onto GIAC Enterprises information systems and that Management may use any and all such information with out additional compensation or the approval of the individual and the privilege of using the GAIC Information Systems may be withdrawn at any time at the discretion of the Management.
4. Provide written approval and fund or disapproval of any software recommendation submitted by SD/IT for the use of proposed software prior placement onto any production GIAC Enterprises information systems.
5. Provide written approval and funding or disapproval of any hardware recommendation submitted by SD/IT prior using the proposed hardware for storing, processing or otherwise handling GIAC Enterprises information.
6. Review and accept or reject the risk for each instance where it is proposed that personnel should be allowed to share user accounts. Management shall provide prior written approval for all instances where the risk is deemed acceptable and present it to SD/IT.
7. Determine what information is to be considered political ideology, pornographic material, religious material or any other none business related information that can reasonable be expected to create a hostile work environment or that could be construed by users as harassment or offensive to their personal beliefs or ethics and shall make available guidelines on this subject to all personnel.

SD/IT shall:

1. Process Management approved requests by individuals for personal use of GIAC Enterprises information systems or access to the Internet from GIAC Enterprises information systems to allow such access and/or begin monitoring of such usage as is deemed appropriate.
2. Provide isolated information systems for the purpose of reviewing in a controlled manner in a controlled environment any proposed software and/or hardware.
3. Review software and/or hardware proposed for use on GIAC Enterprises Information Systems.

4. Develop configuration guides and usage standards for all software and/or hardware to be recommended to Management for approval for use on GIAC Enterprises information systems.
5. Submit in writing a recommendation to Management that includes configuration guides and standards for proposed software and/or hardware and shall outline the cost and risk in using the proposed software to GIAC Enterprises information systems.
6. Ensure all authorized personnel have unique user accounts to all GIAC Enterprise information systems except where Management has deemed it is in the best interest of the company or is required by specific software and shall document all such instances of exception and obtain the required prior written Management approval.
7. Provide mechanisms for informing all personnel that:
    - GIAC Enterprises Information Systems and the information residing and processed on those information systems are the property of GIAC Enterprises each time an individual accesses a GIAC Enterprises Information system. Where possible, such mechanism shall require positive action by the user to proceed with activity on the information system they are attempting to access.
    - Users of GIAC Enterprises Information Systems have no expectation of privacy for any information they place on or process over GIAC Enterprises owned information systems.
    - All personnel are responsible for not using the GIAC Enterprises Information Systems for criminal activity.
    - All personnel are responsible for not using the GIAC Enterprises Information Systems to access, process, store information such as political ideology, pornographic material, religious material or any other none business related information as defined by Management that can reasonable be expected to create a hostile work environment or that could be construed by users as harassment or offensive to their personal beliefs or ethics.
8. Present all instances of discovery to Management of all information they considered to be political ideology, pornographic material, religious material or any other none business related information that they feel creates a hostile work environment or that could be construed by users as harassment or offensive to their personal beliefs or ethics.

<u>All Personnel shall</u>:

1. Read and understand this policy and consent to its provisions prior to being granted accessing to any GIAC Enterprises information systems.
2. Submit a written request for permission to use GIAC Enterprises Information Systems for personal use to Management prior to making such personnel use.
3. Obtain Management's prior written permission to use the Internet via GIAC Information Systems shall be and shall acknowledge in writing that they

shall:

- use the access responsibly and shall not go to inappropriate Internet sites (sites that could be construed by Management to incur liability or creating a hostile work environment).
- not downloading unauthorized software and copyrighted information via the Internet (except for SD/IT personnel who shall do so onto specific GIAC Enterprises information systems set up for this purpose that are isolated from the GIAC Enterprises networked systems).

4. Acknowledge in writing prior to being granted access to GIAC Enterprises information systems that they are responsible for not placing personal hardware, freeware, or shareware onto GIAC Enterprises information systems without prior written approval of Management.
5. submit in writing the appropriate access request form to SD/IT and receiving Management approval prior to receiving access to any GIAC Enterprises information system.
6. Acknowledge in writing that they are responsible for protecting and not sharing their passwords or for allowing other GIAC Enterprises personnel to use their access the GIAC Enterprises Information Systems with out being personally present.
7. Acknowledge in writing that they are responsible for not allowing any non-GIAC Enterprises personnel to use their account, even when in their presence without prior written approval of Management.
8. Acknowledge in writing that they understand and are responsible for what is contained within this policy and understand their responsibilities when using GIAC Enterprises information systems.
9. Report to Management information they discover and considered to be political ideology, pornographic material, religious material or any other none business related information that they feel creates a hostile work environment or that could be construed by users as harassment or offensive to their personal beliefs or ethics.

GIAC Enterprises Security Procedures – Procedure for the Implementation of Configuration Management for New or Newly Discovered Information Systems – Hardware

In order to assure that new hardware will not degrade the current level of security all hardware must be evaluated for impact to the security of the information systems it will be attached to. New hardware is defined to be any item that has not previously been evaluated and there is no current GIAC Enterprises developed/approved configuration guide that can be used to configure the new equipment without deviating from an existing approved configuration guide. SD/IT shall employ this procedure for all hardware proposed for connection to any GIAC Enterprises information systems will be analyzed in accordance with the following procedure:

1. Research the hardware in order to determine the type of information system characteristics are part of the hardware, such as:
    a. Is the hardware equipped with volatile memory (i.e., if power is removed from memory, all stored data is lost)?
    b. Is the hardware equipped with non-volatile memory (i.e., if power is removed from memory, all data remains)?
    c. If non-volatile memory is used, is there an operating system to manage the memory device (i.e., is there a Disk Operating System (DOS))?
    d. Does the hardware have the capability of receiving data (i.e., does is it scan documents, can it down load data from communications ports, can electronic data files be received through floppy disks, etc.,)?
    e. Does the hardware have the capability of sending or downloading data (i.e., does it beam or transmit data to another device, record data onto separate media, etc.,)?
    f. Does the hardware have the capability of processing data (i.e., does it manipulate the data and change it is in some manner)?
    g. Determine the methods of usage for which the hardware can be expected to be employed for (e.g., scanning, copying, printing, photographing, recording, Internet access, playing music or videos, etc.).

2. Determine if an existing GIAC Enterprises approved configuration procedure can be used to configure the new hardware.
    a. If an existing GIAC Enterprises approved configuration procedure can be used, obtain the hardware, configure a stand-alone environment that will fully test the hardware and then configure the hardware with the approved configuration guide.
        i. Note any deviations from the configuration guide and prepare an evaluation report noting the risks involved in using the hardware that are different from the current hardware to which the configuration guide applies.
        ii. Forward the report of the analysis with a recommendation of acceptance or rejection to Managing Director of SD/IT (a Management position).

iii. If the recommendation is for acceptance also include in the report any additional mitigation procedures that should be employed and the acceptable ways the hardware is intended to be used (i.e., develop a usage standard). Also list the ways in which the hardware can be expected to be misused (if any).
iv. If approved for use by the Managing Director of SD/IT, the hardware may be placed on GIAC Enterprises information systems as recommended in the report. The approved configuration guide shall then be updated to include the new hardware along with the recommended new mitigation procedures, changes to current configuration checklists and validation testing procedures, as well as list the acceptable and unacceptable manners in which the hardware is to be used.

b. If an existing GIAC Enterprises approved configuration procedure is not available, continue to research the hardware.
    i. Determine if there exists industry or manufacturer's recommended practices for the hardware, such as the National Security Agency Configuration Guide for Windows NT (reference 5), the SANS Institute List of Top 20 Security Vulnerabilities, or Microsoft's Guide to Securing Windows NT. Use the guidelines discovered to develop a configuration guide, otherwise develop a guide based upon current GIAC Enterprises best practices.
    ii. Determine based upon GIAC Enterprises policies, current operations procedures and the proposed configuration guide if the hardware is capable of being configured to meeting the GIAC Enterprises level of security. If the hardware is not capable of meeting the required level of security, prepare a report outlining the risks and submit it to the Managing Director of SD/IT with the recommendation that the hardware is not acceptable for use in GIAC Enterprises information systems.
    iii. If the hardware is capable of meeting the GIAC Enterprises level of security (or if directed in writing by the Managing Director of SD/IT to continue) obtain the hardware, configure a stand-alone environment that will fully test the hardware and then configure the hardware with the proposed configuration guide. Develop and test mitigation strategies until an acceptable configuration can or can not be established.
    iv. Prepare the configuration guide for the new hardware, including configuration checklists, mitigation strategies, and validation testing procedures.
    v. Forward the report of the analysis with a recommendation of acceptance or rejection to Managing Director of SD/IT.
    vi. If the recommendation is for acceptance also include in the report the proposed configuration guide that should be employed. The configuration guide shall include any additional mitigation

procedures that should be employed and the acceptable ways (usage standard) the hardware is intended to be used. The configuration guide shall also list the ways in which the hardware can be expected to be misused (if any).

vii. If approved for use by the Managing Director of SD/IT, the hardware may be placed on GIAC Enterprises information systems as recommended in the report and the configuration guide shall be finalized with a list of the acceptable and unacceptable manners in which the hardware is to be used.

3. Prepare user manuals and user training (if determined to be necessary based upon the potential for users to use the hardware in ways that will render the operation unsafe based upon the assumptions of acceptable use listed in hardware's configuration guide and usage standards. SD/IT shall issue a copy of all manuals and initial training to all known users expected to be using the new hardware.

4. SD/IT shall also provide the user manuals and training information to Human Resources. Human Resources will integrate the information on the new hardware into the personnel training program.

5. SD/IT shall also provide the user manuals and training information to Security. Security will integrate the information into the Physical Security Operations plan as necessary.

6. The following is an example of the above procedure. It will out line an example of discovery of new hardware and the steps taken to account for and place new hardware onto a GIAC Enterprises information system.

    a. The Audio Visual Production Center has a digital copier that they have leased. They discovered that it could be connected to a network allowing print jobs to be sent directly to the copier (brand name of the copier has been excluded as the functional portion of the copier that is of concern is provided to most copier manufacturers by Electronics For Imaging™, (www.efi.com)). They put in a request to SD/IT to hook it up to GECNet.
    b. The SD/IT Help Desk personnel who received the request directed it to a supervisor as they have not previously had a request to add copiers to the network and it is not a piece of hardware procured via the normal channels for information systems.
    c. The SD/IT supervisor sends out SD/IT personnel to look at the copier. They discover the copier has a "computer" attached and there is capability to attach it to networks and telephone lines. The copier can be used as a copier, scanner, printer, and fax machine. They immediately advise the supervisor.
    d. The supervisor presents the findings to the Managing Director of SD/IT and recommends the discontinued use of what is obviously an information system until the hardware can be researched, evaluated and a proper

configuration developed and implemented. The Managing Director agrees and issues an order (in writing) to discontinue use to the Audio Visual Production Center via their Managing Director (Human Resources).

e. The Managing Director also issues a request to managing Director of the Supply Department to provide a list of all instances where such hardware has been leased and that the Supply Department should now send all requests for such equipment to the SD/IT department for technical approval prior to purchase from this point onward.
f. SD/IT personnel immediately begin researching the capabilities of the copier per the above procedure. They determine from the manufacturer that the copier has a large amount of volatile memory chips used to operate the basic copier. For enhanced features and network support, the manufacturer uses an Electronics For Imaging™ (EFI) "Fiery" platform. Researching with EFI, it is determined that several versions are available and that EFI provides their systems to most copier manufacturers. The platforms come in several operating system varieties: Windows NT® 4.0, Linux, and VXworks®. All are equipped with hard drives. The hard drives are partitioned so that images from the copier (platen) are sent to one partition and data from the network to the other. The copier was also equipped with a CD-ROM drive and a Zip drive.
g. SD/IT personnel visited the local copier supplier for a demonstration of the system and through questioning and observation determined they should be able to take the GIAC Enterprises Windows NT® 4.0 Configuration Guide and configure it to GIAC Enterprises requirements. They were uncertain what copier features would be disabled.
h. SD/IT arranged (through the Supply Department) for the EFI platform used on copier in the Audio Visual Production Center to be replaced with an EFI Fiery Z4 which operates on Windows NT® 4.0.
i. Using a GIAC Enterprises provided keyboard, monitor and mouse, the SD/IT personnel attempted to research the current configure of the Fiery Z4. This effort failed because the Z4 is configured by default to not accept input from a keyboard and mouse. Contacting the company leasing the copier to GIAC Enterprises, it was determined that to be able to interface with the operating system required a change in the Fiery BIOS. The required BIOS was available as an additional line item that can be leased or purchased.
j. The replacement BIOS feature was requested and added. SD/IT personnel were then able to investigate the current set up and found:
    i. The version of Windows NT 4.0 was up dated to only service pack 5.
    ii. There was no anti-virus software installed.
    iii. The administrators password and guest account were set at the default settings.
    iv. The autoexec.bat file was set up to error check upon booting the system and if errors were found, the system would be re-installed from an image of the system. This capability was based upon the Symantec Ghost™ software.
    v. The CD-ROM drive could not be prevented from being booted from

by disabling the BIOS setting as the command sequence for accessing the BIOS was not found and was not available from the copier manufacturer or EFI.

k. Based upon the above findings, SD/IT personnel installed a GIAC Enterprises owned SCSI hard drive (of equal size to the Fiery Z4 hard drive) in place of the Z4 hard drive and proceeded to install the software provided with the copier. The resulting installation was identical to the one found on the EFI provided hard drive. From this installation, they proceeded to configure the Windows NT® 4.0 to GIAC Enterprises standards. The installation was updated to service pack 6a and all the latest patches approved by GIAC Enterprises. Accounts were disabled/re-set to GIAC Enterprises standards (such as disabling the guest account, assigning new password to the administrator's account, etc.). Except for the placement of a password on the system's BIOS and using the EFI modified version of Windows NT® 4.0 software, all standard settings could be made and tested satisfactory. Because the BIOS could not be entered to disable the CD-ROM and Zip drives, they were disabled by physically disconnecting them. Since the Autoexec.bat file provided for the automatic reinstallation of the whole hard drive image, the Symantec® Ghost software and all backup image files were deleted to prevent the execution of this feature and tested to insure it no longer worked.

l. The SD/IT personnel then tested the local features of the copier. These tests showed that there was no relation to the EFI Fiery (even when totally disconnected) when using the copier platen except for the size of copy jobs. Copy jobs that exceeded the volatile memory size prevented the full use of some of the fancier copier features because these larger jobs would normally be placed onto the EFI Fiery hard drive partition set up for this purpose. User accounts at the platen were not controlled by the EFI Fiery and were limited to numeric user id's and pass codes.

m. SD/IT personnel then tested the copier by establishing it as a device on the SD/IT Windows NT Testing Network and performed testing to see if printing capability was impaired. All test showed the copier worked correctly from the test network.

n. SD/IT personnel then wrote a report of their findings and recommended the use of the copier provided the copier was physically secured from non-authorized personnel, the EFI Fiery was configured to GIAC Enterprises Windows NT configuration policy where the CD-ROM drive, Zip drive, and Ghost software and restoration image were disabled and the exception for allowing the use of the EFI Fiery version of Windows NT® 4.0 was allowed. It was recommended (consistent with existing GIAC Enterprises policy on these features) the fax capability and the off-site support by the copier provider would not be connected or used. It was also recommended that since this was leased equipment that the lease be modified to state that any hard drive placed into the EFI Fiery Z4 was to become GIAC Enterprises owned equipment and that the provider of the copier be reimbursed for replacement hard drives.

o. The Managing Director of SD/IT accepted this recommendation. The copier was then placed back in original condition, configured and tested to the new configuration standard and placed into service. Special GIAC Enterprises Training guides were not prepared as the special use and operation requirements applied only to SD/IT personnel and existing operations training was deemed sufficient to cover these devices. However, special training was prepared for all GIAC Enterprises personnel that handled U.S. Government classified information. The training emphasized the using only copiers authorized and posted for classified copying when making copies of classified information. The special training included information on the new copiers and noted that these copiers when replacing older (analog) copiers may not be authorized to copy classified information where previous copiers were. This information was included because previous copiers were not located in areas approved for the open storage of U. S. Government classified information where the new copiers would now have to meet these requirements since they are equipped with hard drives. Security was notified of these new physical protection requirements so they could update their procedures as needed.

p. The Supply department updated the lease to show ownership of the copier hard drive and updated their procedure for noting that these devices required SD/IT concurrence for purchase/lease by GIAC Enterprises.

GIAC Information Security Officer Practical
References

1. International Organization for Standards (ISO) 9001:2000, Quality Management Systems – Requirements; available on-line for purchase at http://www.iso.org/iso/en/CatalogueListPage.CatalogueList
2. International Organization for Standards (ISO) 9002:1994, Model for Quality Assurance in Production, Installation and Servicing; available on-line for purchase at http://www.iso.org/iso/en/CatalogueListPage.CatalogueList
3. Department Of Defense Standard 5200.28, Department Of Defense Trusted Computer System Evaluation Criteria, December 1985; available at http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html
4. Department Of Defense Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP), December 30, 1997; available at http://mattche.iiie.disa.mil/ditscap/DitscapFrame.html
5. National Security Agency Windows NT Security Guidelines: Considerations & Guidelines for Securely Configuring Windows NT in Multiple Environments, 3 June 1999; Trusted Systems Services, 1998; available at http://www.trustedsystems.com/downloads.htm
6. The SANS/FBI Twenty Most Critical Internet Security Vulnerabilities (Updated) The Experts' Consensus Version 2.501 November 15, 2001 ©; available on their Web site: http://www.sans.org/top20.htm
7. Microsoft Corporation *Installing and Securing Windows NT® 4.0 Installatio*n, 2001; available on their Web site: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/nt4new.asp
8. Electronics For Imaging, Fiery Z4 Product literature, 2001; available on their Web site: http://www.efi.com/products/fiery_z4_overview.fhtml
9. Symantec Corporation Ghost™ Product literature, 2001; available at their web site: http://enterprisesecurity.symantec.com/content/displaypdf.cfm?pdfid=34&PID=na&EID=0