Global Information Assurance Certification Paper

GIAC Healthcare Systems

GISO Certification Practical

January 11, 2003

GAIC ISO Certification

Practical Assignment

Version 1.2

Dennis Laughlin

1.0 ABSTRACT

This paper describes the operations of GIAC Healthcare Systems—a multi-entity regional tertiary healthcare operation. It includes the following items.

- A description of the clinical and business operations of the company.
- A description of the information technology infrastructure, including diagrams of the LAN, WAN, and Firewall/DMZ configurations.
- An analysis of 3 specific risks to the security of the company. The identified risks are lack of adequate application and systems access controls, poor control of remote access, and very limited disaster recovery/business continuity planning.
- The analysis and development of a specific policy and procedure to address one of the identified risks. The policy and procedure selected addresses “Access to Computer Systems”.

2.0 Description of GIAC HealthcareSystems

The GAIC Healthcare System was formed in 1980 with the merger of two competing healthcare facilities—Sisters Healthcare and Community Health Systems. Realizing the detrimental effects of direct competition, the local hospital boards of these competing entities met to identify and develop common, community-based goals. The resulting plan called for the formation of a not-for-profit community based tertiary healthcare system that would build on the strengths of both hospitals, would efficiently utilize community resources, and provide a common future that would be beneficial to the community and region.

Today, GAIC Health System is a multi-entity healthcare network comprised of one 450 bed regional medical center, four community based rural hospitals (120 beds total), six community based medical clinics, five senior care facilities, and a third party health plan administration organization (TPA). The primary location for GIAC Healthcare is located on a 10-acre campus, which contains the medical center, and three specialty hospitals—a cancer care institute, a rehabilitation hospital, and a cardiac institute. Across town is a wholly owned psychiatric treatment center.

Located in a predominantly rural area, GAIC Health serves as the only tertiary care facility in a 150-mile radius. The referral area includes the 4 owned hospitals, one military base hospital, 2 Veterans Administration hospitals, 3 Indian reservation hospitals, and 4 non-owned rural hospitals.

The primary business of GAIC Healthcare is the delivery of community based acute healthcare services, and regional tertiary specialty care. Community acute care is provided in each of the associated hospitals, with the tertiary care provided at the regional center, in addition, specialty outreach programs reach into the outlying communities.

The healthcare industry in general, and GIAC Healthcare specifically, has recently “discovered” the need for improved information security as a result of upcoming regulations from the federal government. These regulations are known as the Health Insurance Portability and Accountability Act of 1996 (HIPAA). These regulations are a small part of a comprehensive set of regulations put in place by the Centers for Medicare and Medicaid Services (CMS). These rules are intended to move the healthcare industry toward standardized electronic transactions, while establishing “industry standard “ information security and privacy. The most controversial aspect of the HIPAA regulations is the privacy rule. Privacy groups, healthcare and insurance associations, and individuals combined, submitted over 1500 pages of comments to the proposed privacy rule. This broad based concern illustrates very clearly that the “Crown Jewels” of any entity involved in healthcare is identifiable patient data. The privacy and security of this data is of paramount importance.

2.1 GIAC Healthcare IT/Technical Infrastructure

The technology environment in GIAC Healthcare is one of great complexity. Each of the clinical and corporate support areas has unique and specialized computing resource needs. The Individual clinical areas require a high degree of specialized technical support to provide advanced patient care. The corporate support areas require reliable, enterprise-wide applications. The required technology is seldom available from common vendors, which propels GIAC Healthcare toward a "best-of-breed" strategy for technology selection and procurement.

GIAC Healthcare operates the vast majority of their information system services from a centralized data operations center at the main healthcare campus. The data center is located in an environmentally controlled, UPS protected room. The entire main campus, and each remote hospital are protected with standby power. None of the remote clinics are protected in this manner. The single exception to the central data center approach is associated with each of the remote hospitals. To reduce overhead network traffic, each remote hospital has a Windows 2000 domain controller, and a Windows 2000 application server located on site. This server hosts the long-term care (LTC) administration software in addition to various minor applications, as needed for the particular hospital, surrounding clinics, and LTC facilities.

Network Configuration-Local Area Network (LAN)

Diagram 1 in Appendix B depicts the LAN residing on the main campus of GAIC Healthcare Systems. The LAN backbone consists of 5 FDDI 100 Mbps rings running on a Cabletron Smart Switch 9000. Each ring consists of Cabletron 2H252-25R and Matrix-E7 24 port FDDI uplink switches attached to individual 10 and 100 Mbps uplink hubs and switches.

Network Configuration-Wide Area Network (WAN)

The top half of diagram 2, located in Appendix C, illustrates the WAN between the main GIAC campus and each of the remote facilities. The WAN is comprised of a combination of dedicated T-1 connections between the central data center and the 4 remote hospitals; and 3 frame-relay clouds comprised of fractional T-1s from the data center to numerous local and regional physician's offices, LTCs, and select business associates.

The bottom half of diagram 2 is a conceptual representation of the GIAC Healthcare Internet connection; Checkpoint firewall; DMZ (with 2 servers); and private network. While the diagram shows 5 servers, the private network actually contains all of the remaining servers discussed in the following section. Also included in the configuration, although not shown in the diagram, are application servers and domain controllers (1 each) located at each remote hospital.

Internet connectivity is provided by the Cisco 4000 router. The GIAC LAN/WAN environment is protected with the Checkpoint firewall. As indicated in the diagram, all network traffic between GIAC facilities traverses dedicated/closed communication lines. The only regular Internet traffic is from the e-mail and FTP servers, which are located in the DMZ.

Systems & Application Servers

The server environment at GIAC Healthcare is comprised of 77 Intel based machines, and 3 IBM RS6000 machines. The Intel based servers include 69 Windows 2000 and NT servers and 8 Magic-Data General servers. The RS6000 servers run AIX UNIX. GIAC also maintains several spare servers that are typically configured in a non-production test environment. This test network includes two Windows 2000 servers, 1 AIX server and one Data General Server. A "snapshot" listing of the servers, their locations, and main function is found in Appendix D.

From a physical/networking standpoint, all of the servers listed reside behind the firewall except the email and FTP servers. These two reside in the DMZ.

Server Configurations

Servers are configured closely to the recommendations of the individual software application vendor. This is to ensure that the diverse applications hosted on the servers operate as designed. There is currently no written policy regarding minimum-security or hardening requirements for servers. System administrators patch their servers on a regular basis, but there is no policy stating this requirement. The Firewall administrator has attended SANS sponsored firewall training, and has used this training in conjunction with the vendor, to develop a procedure for configuring the firewall software.

Servers are grouped in the following categories

Servers That Support IT Infrastructure

This group includes servers configured as and hosting the following: DHCP/WINS, Domain Controllers, Print server, Backup software, Exchange Mail, Firewall, Interface Engine, Intranet, Antivirus, SMS. While many of these could be considered application servers, the primary objective of all of them is to provide a sound, reliable infrastructure for the network.

Primary Application Servers—These include the business and clinical applications that are most critical to the ongoing operation of GIAC Healthcare, They include the enterprise wide HIS system and individual applications that support the main revenue centers of surgery, radiology, and cardiac services. They include the Meditech health information system (HIS), Cerner Radiology system, the MSM Surgery system and the

Catalyst Cardiac system. These systems house the vast majority of the patient data at GIAC Healthcare, which, as in most healthcare operations is what comprises the "crown jewels" of the company.

Departmental Application Servers

These servers commonly host multiple smaller applications for several departments. The use of these applications is typically limited to a single department. These servers, and the applications that they host, while important of the operations of the department, would not be considered critical to the ongoing operations of GIAC Healthcare.

File Servers

The GIAC backup strategy includes nightly backups of all centrally located servers. It does not include any workstation backups. To ensure that users do not lose critical data, the use of local hard drives for file and data storage is discouraged. To that end, each user is assigned file-space on a networked drive. In addition, there is a file server dedicated to group file storage, and a server dedicated to the Information Systems department to facilitate downloading of software, drivers, etc.

Desktop Operating Systems

The primary desktop OS is Windows 2000. The Information Systems Department is in the final stages of a one year upgrade/replacement program in which they have replaced or upgraded approximately 800 desktop systems, upgrading software and hardware, as needed to move from Windows 95, and 98, to Windows NT4.0 & 2000. All Windows NT or 2000 desktops are locked down; users cannot modify, add, or delete configurations or software.

The main hospital Meditech HIS utilizes a combination of Windows based Terminal Servers and dedicated term servers.

2.2 Business Operations

As stated in the introduction, the primary business of GAIC Healthcare is the delivery of community based acute healthcare services, and regional tertiary specialty care. Healthcare in the hospital and clinic setting can be divided into two main functions—diagnostic services and treatment services. In addition, these functions require the full range of background business functions such as payroll, human resources, purchasing, regulatory compliance, IT, billing, etc.

The customer flow associated with the healthcare business is much like any other business. The customer (patient) comes in the front or back door, receives a service or product, and pays or is billed. Pertinent records of the transaction are maintained by the business.

The healthcare data flows however are unique when compared to most other businesses. There are several factors that contribute to this uniqueness.

Uniqueness factor #1: Healthcare data is traditionally more personal than other, non-healthcare customer information. The data gathered by the healthcare entity is considered the property of the patient, although the media it is stored on is considered the property of the business. This is one of the key concepts behind the propagation of the recent federal privacy and security regulation (HIPAA). These regulations require special protections regarding access to the patient's health record. Federal regulations commonly state explicitly who may, who must, or who cannot have access to these records.

Uniqueness factor #2: The customer, in many cases, does not pay for the service rendered. In addition, the customer's ability to pay for the service does not typically determine the service provided. There are many potential payers for the services provided to an individual patient. The patient may pay a portion of the bill, but an insurance company, HMO, Medicare, Medicaid, or some other third party payer commonly pays the major part of the bill. This requires the transmission of patient information to both the patient, and to other potential payers (sometimes several different payers). In many cases the third party payer will not pay the bill until they actually review the entire medical record.

Uniqueness factor #3: The individual responsible for bringing the customer to the business is usually not an employee of the hospital—a physician or an ambulance typically refers or delivers the patient to the hospital. These external entities require access to portions of the medical record for their billing efforts.

Uniqueness factor #4: In most cases, once the hospital delivers a service, the follow-up service does not occur at the hospital. It occurs at a clinic or physician's office. Sometimes they are affiliated with the hospital; many times they are not. This requires the sharing of information for the continued care and benefit of the patient, even with direct hospital competitors.

Uniqueness factor #5: In addition, the highly regulated healthcare environment requires numerous external entities to have access to medical and financial records, including federal agency auditors, insurance auditors, physician credentialing organizations, hospital and laboratory accrediting agencies, State Departments of Health, etc.

Each of these factors has a significant impact to the distribution of access to GIAC Healthcare data systems. The business impacts of ignoring or limiting the distribution of this data could severely impact the ongoing operations of GIAC Healthcare Systems. The information requests and needs of regulatory bodies, physicians, payers, and patients, must all be adequately addressed and balanced to ensure the business viability of

GIAC Healthcare, and the satisfaction of the regulators, business partners and customers.

Primary Applications

The main Health Information System (HIS) is provided by Meditech Inc. and includes separate modules for Admissions, Medical Records, Patient Care Information, Payroll, Billing/Accounts Receivable, Laboratory, Community Wide Scheduling, Executive Information Management, Materials Management, and Pharmacy. The Meditech system is written on a proprietary OS called Magic, and is installed on the 8 Data General, Intel Based, servers. Located in the main data center, this single application serves as the primary health information system for all of the affiliated hospitals. In addition, all affiliated clinics, and the majority of the local physician's offices access the Meditech system. All access to the Meditech system from these facilities is via the dedicated communications lines shown in the WAN diagram discussed earlier.

Other primary applications include the Cerner Radiology System, MSM Surgery system, and the GE Catalyst Cardiac system. These systems support the major revenue centers for the main hospital, and are critical to the success of the enterprise. While department based, access to these systems is spread throughout the hospital and to select specialty physician practices, again, via the WAN. The major applications, and many of the departmental applications as well, are interfaced with the Meditech HIS system via a Datagate interface engine.

Distribution of, and access to, the primary applications is currently very open. The current healthcare environment has historically been very open with access to patient information. The historical justification for this open access was that critical decisions are made on a daily basis, based on the information available in the patient's record. There is less risk to the patient and to the company to ensure that the information is distributed to anyone that may need it. Obviously, with the upcoming privacy and security regulations, this environment is changing, and will continue to change until the industry reaches something close to industry standard controls. The table below indicates the access provided to the primary applications.

Application	Employee Type	Facility	Type of Access
Meditech	Clinical-nurses, lab pharmacy, therapists	Every facility listed on the WAN diagram in Appendix C (29 facilities, including Main hospital)	Hospital clinician access to view and modify patient data is typically limited by role, and work area. Physician office personnel have full access to view all patients.

	Financial, Support, All Dept. Directors Physician office staff	All hospitals Physician offices	Financial Info is limited based on job role or business need. Access for billing information.
Cerner	Radiology Employees	Main hospital	Limited based on job role or business need.
	Radiologists (non-employed)	Have access from hospitals and from physician office	Currently can view all patient data. This is appropriate "all patient access" since Radiologists view all patents on their duty shift.
MSM Surgery	Surgery Department Employees	Main hospital	View and edit all scheduling and surgery materials information based on job role.
	Most Nurses	Main hospital	View surgery schedule for all patients.
Catalyst	Cardiac Services clinical staff	Main hospital	View and edit all patient clinical data.
	Cardiologist	Main hospital	View all patient data.

Additional application procurements scheduled within the next year include: human resources system, time & attendance, risk management, contract management, e-learning/education tracking, and a Radiology PACS system. The Radiology "Picture Archiving and Communications System" (PACS) will replace the physical storage of radiology films with electronic "films". This will be the first software system in place at GIAC Healthcare that will not have a manual process to replace the functionality if the system becomes unavailable for a time. This will push GIAC Healthcare management to address the business continuity/disaster recovery planning needs.

The day-to-day support and administration responsibilities for most software applications are delegated to several Information Systems Applications Analysts. There are also 3-4 systems that cross departmental boundaries, but are not under the control of Information Systems. These are systems that were purchased or leased "around" the normal procurement process. The administration of these systems is typically not as controlled as those supported by the Information Systems.

3.1 Areas of Risk

As stated in the introduction, the crown jewels of any healthcare entity, GIAC Healthcare included, is the very personal, very private, patient data entrusted to them. To ensure the safety of this data, and to begin the compliance process regarding the HIPAA security rule, GIAC Healthcare completed a security self-assessment. Since this was the first information security assessment completed at GIAC Healthcare, it was not surprising that the findings from this security self-assessment included a wide range of issues. A preliminary risk assessment/ranking was completed to rank the findings in order of potential harm. Three or the top findings were:

- Lack of adequate application and systems access controls.
- Poor control of remote access.
- Inadequate business continuity/disaster recovery planning.

3.1.1 Application and Systems Access Controls

Overview of Threat

The implementation of user access controls across numerous systems and applications is inconsistent. The methods used for requesting and granting access are not uniform. Reporting of employee transfers and terminations is very lax, and does not encompass all applications and locations. There is no central repository to track an individual's access. Application administration is not centralized; it may be spread across several different departments or geographic locations.

Relevance to GIAC Health

High quality healthcare is predicated on the ability of the healthcare provider to gather, enter, access and evaluate critical information regarding the condition of patients. Historically, access to major systems was granted with the approval of the individual's immediate supervisor. Access to smaller non-IS administered systems was much less formal. In many cases, passwords were disabled or posted at the computer to allow full access for all area employees. The general approach in the healthcare industry, and at GIAC Health, was to provide relatively open access to patient information to facilitate patient care.

Potential Impact on GIAC Health

Access permissions based on individual need to know criteria is a key security principle, and is required by the proposed HIPAA security regulation. In addition, the HIPAA privacy regulation discusses the need for "minimum necessary" access. The existence of non-secured applications and non-maintained user accounts could be a very serious violation of security. These accounts typically enable read/write access to

a vast array of private patient information. The inappropriate release of this private information would be very detrimental to the public trust of the company, could be the basis for regulatory reviews, audits & potential Medicare exclusion, and would open GIAC Healthcare to possible litigation. The potential impact is high.

Likelihood of Exploit

GIAC Healthcare has approximately 4500 employees. Individuals change positions or leave the organization on a regular basis. The distribution of application administration responsibility to non-centralized personnel serves to dilute individual and departmental accountability, and makes it very difficult to ensure that access permissions are removed or modified in a timely manner. It is even more difficult in immediate termination situations. With distributed administration, open or disabled security on certain applications, and lax change reporting, the likelihood of exploit is high.

Mitigation Factors

Three primary issues must be resolved before this issue can be fully addressed. 1. Open/unsecured applications; 2. Distributed application administration; and 3. Lax reporting of personnel changes.

In the short term, GIAC Healthcare must develop an application security policy that sets standards of performance regarding application administration and minimum security measures. This policy will require timely administration, and unique user identification and passwords. In the very short term, the frequency of the "changes" notice from personnel will be increased from monthly, to weekly.

In addition, the GIAC Healthcare Information Systems Department will develop a "computer access rights" tracking system as an addition to their existing Help Desk software application. The current software already includes a method to e-mail and/or page individuals based on assigned duties, and could easily be used to alert both IS applications administrators, and remote, distributed administrators to required access changes. When the pending Human Resource software application is functional, data relating to transfers and terminations will be automatically uploaded into the Help Desk system, which will, in turn, notify the administrators of the required change. This will reduce much of the human-error involved in the current manual process, which creates delays in tracking and notification of terminations and transfers. Random audits of systems access databases as compared to the "access rights" database can serve as the audit mechanism. Physical walkthroughs, and periodic reviews of individual access rights could also be utilized.

3.1.2 Poor Control of Remote Access

Overview of Threat

The current policy of the hospital "Physician's Networking" Department is to grant free access to the main hospital HIS system to facilitate continued patient care and good hospital-physician relations. This access allows the physician's office staff the ability to access their patient's hospital records. This is a valid access need. The access granting process is not documented, thus it is very inconsistent. There are no written agreements between the hospital and the physician's offices that specify the duties and responsibilities of the parties involved. Past problems have included the addition of a non-secured wireless network to a physician office and significant password sharing. In addition, with the current configuration of the hospital HIS, it is not possible to limit the patients viewed at the physician office to patients belonging to a particular physician. They are able to view all patient treatment data in the system.

Relevance to GIAC Health

This situation exposes the "Crown Jewels", i.e. patient data, to entities/areas that are not in control of the hospital. In addition, this directly impacts the hospital-physician relationship, which is very politically charged.

Potential Impact on GIAC Health

The hospital has had previous complaints regarding inappropriate viewing of records. This situation has significant possibilities for inappropriate exposure of patient data, for which the hospital is liable. When the HIPAA regulations are in effect, continued incidents may be the basis for regulatory audits and reviews. This is a high impact issue.

Likelihood of Exploit

Incidents have already occurred, and will likely continue until the situation is controlled. Exploit probability is high.

Mitigation Factors

- Any actions taken to control or limit physician and physician staff access will potentially cause significant physician discontent, which is a major concern to the CEO of GIAC Healthcare. Changes to this process can legitimately be attributed to HIPAA regulatory requirements. This will assist with the political considerations, and will provide a defensible reason or justification to the CEO when he is faced with irate physicians.
- The main HIS system will require significant reconfiguration to provide appropriate access, and limit inappropriate access. Physician and staff work procedures regarding physician referrals must be consistently followed to allow the needed changes to work. In addition, the concept of data ownership is not understood or embraced in some departments. To facilitate better control of the access, the system must contain current and correct data regarding

the physician and any physician groups to which they belong. The physician data dictionary upkeep process must be formalized and be assigned to the Medical Staff Office. Currently, these duties are "farmed off" to the Information Systems Department resulting in delayed and inaccurate data entry. Once the data is correct, existing security features can be enabled to allow physicians to see only those patients for which they have a treatment or referral relationship. To allow for immediate referrals, (those that do not make it into the system before the need to see the patient,) each physician office will have individuals with the right to "self refer" patients to the physicians in the practice. This will be a highly audited feature, but will allow for critical overrides if needed. This emergency access is a requirement specified in the HIPAA security regulation.

3.1.3 Inadequate Business Continuity/Disaster Recovery Planning

Overview of Threat

The final threat identified, addresses the availability and integrity of the data center (equipment, software and environment). Industry standards, along with the HIPAA regulations and the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) guidelines all require business continuity/disaster preparedness. The current state of preparedness at GIAC is limited to a comprehensive backup process. There are no significant plans in existence to replace any or all of the components of the IT environment in case of accidental or intentional damage. This is even more critical due to GIAC Healthcare's reliance on a single data center, as opposed to a distributed approach. Other than the backup procedures, which are used on a regular basis, none of the written plans have been tested and verified as functional.

Relevance to GIAC Health

GIAC Healthcare depends on technology to provide quality healthcare. Without the existing systems in place and functioning, GIAC Healthcare could not treat the number of patients required, and still maintain the quality of care expected. Extended outages would also cause GIAC Healthcare to face significant financial losses.

Potential Impact on GIAC Health

The ability to access patient records, and to conduct diagnostic tests, both in a timely manner, is critical to diagnosing and treating patients. While there are some manual backup procedures, losing the technology behind these services for a significant time, would cripple the hospital both functionally and from a business standpoint. The impact would be high.

Likelihood of Exploit

There have been several “close calls” on the main campus regarding loss of environmental control, localized flooding, and fire. In addition, the external environment has experienced tornados and other high winds, and floods. The potential exists to lose portions of the data center or critical components of the network infrastructure. The likelihood is ranked as a medium.

Mitigation Factors

There are several key factors that must be addressed before the development of a disaster plan would be possible.

- The importance must be stressed to upper management. While they understand that there are some risks involved with the loss of technology, they do not fully appreciate the full impacts for specific losses, nor do they understand the costs involved for the various solutions that may be proposed. The HIPAA regulations may help with this education effort. The regulations are specific in their requirements for business continuity/disaster planning. In addition, as GIAC Healthcare moves further toward fully electronic records, such as the upcoming Radiology PACS system, the vendors are including the redundant systems in their proposals, and are asking how we plan to provide the redundancy necessary.
- Second, GIAC Healthcare has neither the expertise, nor the time to conduct a full assessment. Consultants will be needed to develop a plan that includes a detailed risk/benefit/cost analysis.
- Finally, funding must be available to provide the necessary redundancy.

With the appropriate education and analysis, GIAC Healthcare management can make the appropriate, risk-based and cost effective decisions to provide the needed redundancy.

4.1 Evaluation of Current Computer Access Policy

This policy evaluation will review a current policy in use at the authors company. This policy, entitled *Access To Information Systems* is included in Appendix A.

Purpose

The purpose of this policy appears to be two or three fold.

- It states the policy of access based on "Need-To-Know",
- In the policy guidelines, it gives a list of acceptable uses for computers, and
- It provides a procedure for requesting, granting, modifying, and terminating computer access.

While it is not always wrong to combine policy and procedure in one document, you can easily lose focus regarding the main purpose of the document. In this document, the primary goal of the policy is not clear—it is hidden among the guidelines and procedures.

Background

There is very little offered regarding background. There is one policy included as a reference. In the case of a healthcare facility such as GIAC Healthcare, it may be appropriate to include a description of the regulatory environment, specifically, the HIPAA regulations.

Scope

This policy does not have a "Scope" reference line, but there is adequate evidence of the intended scope throughout the document. The ***APPLIES TO**: GIAC HEALTHCARE* and ***DISTRIBUTION:** All*, from the policy header indicate a corporate scope. In addition, the approval of both a Vice-President, and the CEO indicate a global corporate policy. A separate scope header would clarify policy coverage.

Policy Statement

The policy statement should identify the actual guiding principle of the document. In this case, the policy statement is mixed with a statement of importance, "*Confidentiality and security of information accessed when using information systems is essential",* followed by two policy items—*only authorized employees/agents of GIAC Healthcare shall have access to information systems* and *Entitlement to access shall be determined on an individual basis according to "need to know"*, followed by an enforcement statement—*and any unauthorized access will be subject to disciplinary action.*

The first statement limiting access to "*only authorized employees/agents"* is contradicted later in the policy guidelines when it states, *"Medical Staff and*

students may be granted access to information systems." There may be limited situations where members of the Medical Staff may be an agent or employee of GIAC. Students, in general would be neither employees or agents of GIAC.

Responsibility

The policy portion of this document indirectly implies responsibility when it identifies the department as Information Systems and the author and reviewers as Information Systems directors and team leaders. The procedures section does give guidance regarding who is responsible for the completion of certain actions. It spells out specific responsibilities for the new user, department directors, the Information Systems Help Desk, and the Personnel Department. The policy may not be specific enough regarding which directors are responsible for different groups requesting access.

Action

The policy portion of the document does not specify actions, but the procedure section lists specific actions for the new user, department directors, the Information Systems Help Desk, Personnel Department, and the Information Systems on-call staff member. It may be a better approach to include individual actions in a separate, but related procedure.

Enforcement

There is no section identified as enforcement, but there is an enforcement clause hidden in the policy guidelines. This would be much clearer if it were a separate, unambiguous item. Additionally, references to an audit policy, as a means to verify the stated actions would significantly strengthen the policy.

Additional Items

In evaluating this policy using the SMART test (Specific, Measurable, Achievable, Realistic, and Time Based,) several shortcomings are identified.

Specific—As stated earlier, the purpose is not clear. Several points are mentioned as goals in this policy.

Measurable—There are no metrics identified to measure, and no audit method or requirement identified.

Achievable—The procedures, as stated, seem to be achievable, but are not currently consistently followed. There have been numerous cases of individuals that are no longer employed at GIAC Healthcare, that have remained on the system roles for months if not years. This failure can probably be attributed to the lack of any measurement and enforcement criteria.

Realistic—as stated above, the process as defined, is not working. The current practice of filing the authorizations in the personnel file of the user is a one-way flow of data. On termination, the Help Desk notifies all systems and application administrators to verify that the individual must be removed from all the systems. Lack of communication and enforcement has severely limited the functionality of this policy.

Time Based—The policy does have an effective date, and a record of review dates. It does not specify the next review.

4.2 Revised Computer Access Policy

GIAC HEALTHCARE

POLICY NUMBER: IS—02

SUBJECT: ACCESS TO INFORMATION SYSTEMS

DEPARTMENT: INFORMATION SYSTEMS

APPLIES TO: GIAC HEALTHCARE PERSONNEL AND OTHER NON-GIAC PERSONNEL AND AFFILIATE PERSONNEL, AS SPECIFIED HEREIN

EFFECTIVE: June, 1990 **REVIEWED/REVISED:** September, 1996
August, 1999
August, 2002

DISTRIBUTION: All

AUTHORED BY: John Doe, Director, Information Systems

REVIEWED BY: Information Security Officer
Executive Director of Information Systems

APPROVED BY: Vice President of Networking Services
CEO/President

REFERENCE POLICIES

Confidentiality of Information: PRS-503
Progressive Discipline: PRS-502
Acceptable Computer Use Policy: IS-03

BACKGROUND

The Health Insurance Portability and Accountability Act (HIPAA) specifies minimum levels of information security for systems containing individually identifiable health information. GIAC Healthcare must establish appropriate administrative and technical controls regarding access to computer systems and data.

SCOPE

This policy covers ALL individuals requesting access to GIAC computer resources—ALL internal workforce members and ALL individuals external to GIAC Health.

POLICY STATEMENT

GIAC Healthcare workforce members will be granted access to GIAC computer systems following "need to know" criteria, and will be based on the individual's job or role requirements within the company as defined by their department director. Externally, access to GIAC systems will be granted based on the "continued-care" needs of our patients as determined by the Director of Networking.

All personnel requesting access to GIAC computer systems and networks are required to sign confidentiality statements prior to receiving access. For external access requests, the applicability of GIAC policies must be included as a requirement in a legally binding data-use agreement.

RESPONSIBILITIES

1. EVERY person granted access to GIAC computer resources must have a Department Director or Administrative Staff Sponsor who will sign the access request form, verifying that the requested computer access is required based on "Need-To-Know" or continuity-of-care criteria.
   - Internal workforce members assigned to individual departments—Department Directors
   - All external individual access (physician office personnel, clinic personnel, etc.—Networking Vice President or Department Director
   - Medical practitioners (physicians, nurse practitioners, physician assistants, medical students, etc)—Medical Staff Director
   - All clinical and non-clinical students, interns, etc.—Directors of affiliated schools, in conjunction with the sponsoring Department Director or Administrative sponsor
2. Data Owner, where identified, is responsible for verifying job or role-based access needs.
3. Individual requesting access—The individual will be responsible for completing an access request form and a confidentiality statement, and will comply with all policies relating to confidentiality and information security.
4. Information Systems Help Desk, and individual applications administrators—grant and remove access, as required.
5. Human Resources and Individual Department Directors—responsible for notifying the Information Systems Help Desk when an individual no longer requires previously assigned computer access.
6. Compliance/Internal Audit will conduct periodic audits of user access.

ENFORCEMENT

Periodic audits will be conducted to verify compliance with this policy.

Failure to follow this policy may result in loss of computer access rights and may subject GIAC employees to additional disciplinary action, up to and including termination, according to policy PRS-502: Progressive Discipline.

4.3 Computer Access Procedure

GIAC HEALTHCARE

PROCEDURE NUMBER: IS—02-A

SUBJECT: PROCEDURE TO REQUEST, GRANT, CHANGE, AND TERMINATE ACCESS TO GIAC INFORMATION SYSTEMS

DEPARTMENT: INFORMATION SYSTEMS

APPLIES TO: GIAC HEALTHCARE PERSONNEL AND OTHER NON-GIAC PERSONNEL AND AFFILIATE PERSONNEL, AS SPECIFIED HEREIN

EFFECTIVE: January, 2003 **REVIEWED/REVISED:** Annually

DISTRIBUTION: All

AUTHORED BY: John Doe, Director, Information Systems

REVIEWED BY: Information Security Officer
Executive Director of Information Systems

APPROVED BY: Vice President of Networking Services
CEO/President

REFERENCE POLICIES

IS-02 Access To Information Systems

PROCEDURE

New Access Account Request/Creation

New Employee or Internal Workforce Member

1. Personnel Department will collect and place the employees signed confidentiality agreement in their employee file.
2. The Department Director responsible for the employee's computer access will generate a completed (all applicable signatures) "Computer Access Request Form". The Access Request Form is maintained on-line and is available to all Directors. These forms are updated periodically. This form is to be delivered to the Information Systems Help Desk for account creation. This may be completed before the employees first day of work.

3. Help Desk personnel will verify the presence of the appropriate signatures for the requested access, and will document the need for account creation in an IS work order. This work order will be assigned to each system administrator responsible for creating the required accounts. The access granted will be documented in a Computer Access Tracking System (CATS). When the work order is closed (completed), the signed forms are routed to personnel, and are placed in the individual's personnel file.
4. The appropriate system and application administrators will create the appropriate accounts.
5. The Help Desk will notify the Department Director of the completion of the accounts.
6. The Department Director shall ensure that the new employee receives the appropriate training regarding the appropriate use of GIAC computer systems.

Medical Staff, Medical Students, and other medical practitioners (Nurse Practitioner, Physician Assistant, etc.)

Medical Staff may be granted access to information systems. The same procedural guidelines as listed above, will apply for granting, changing and terminating access. The Medical Staff Office Director shall be responsible for physician access. The Medical Staff Office will collect a completed confidentiality agreement and access request form. The access request form will be routed to the Help Desk. The Medical Staff Office will maintain the completed forms.

Students—Nursing, Lab Tech, Radiology Tech, Pharmacy Tech, PT/OT, etc

Students and interns may be granted access to information systems as required for educational purposes. The same procedural guidelines for granting, changing and terminating access shall apply. The Directors of the Schools, in conjunction with the Nursing Service Director and the individual Department Directors, shall define and be responsible for all student access, including maintaining signed forms.

Physician Office Staff and Business Associate Staff

1. Before access can be granted, a signed and dated contract (Business Associate or Chain-Of-Trust) will be executed between GIAC and the external entity.
2. Each individual requesting access shall sign and return a confidentiality agreement, and a completed access request form.
3. Physician office staff will route requests for access through the Networking Department or the physician networking support analyst. The Networking Department Director will authorize the access. The Networking Department will maintain the completed forms.
4. Business Associate personnel will route the request through the Department Director responsible for the business associate agreement. Completed forms will be kept with the contract.

5. The same procedural guidelines for granting, changing and terminating access shall apply.

Account Updates/Changes

When a revision in a user's access is required, the responsible Department Director will complete the same steps outlined under "New Access Account Request/Creation". The new access request form should reflect the total required access and the effective dates, not just additions or changes.

Help Desk personnel will verify that the final access granted to an employee is limited to that specified in the new authorization form. After completing the requested revisions, the Information Systems Help Desk will notify the user of the access change. The Help Desk then forwards the signed form to the appropriate department for filing.

Termination

Employee or Internal Workforce Member

1. When an employee or internal workforce member terminates, Personnel will notify the Help Desk. The notification must include the employee's name and termination date.
2. In the event of involuntary termination of an employee or internal workforce member:
    a. During normal business hours, the responsible Department Director or acting supervisor is responsible for the immediate notification of the termination to Personnel. Personnel will notify the Information Systems Help Desk immediately. The Help Desk will immediately remove the terminated employee's access.
    b. If an employee or internal workforce member is suspended pending termination outside of normal business hours, the responsible Department Director or acting supervisor will notify the Information Systems department "on-call" staff member immediately. The on-call staff member will immediately remove the terminated employee's access.
3. Once a week, the Personnel Department will provide the Help Desk with a list of terminations and department transfers. The Help Desk will verify that the access changes have occurred.

All Other Individual Access

Termination notification requirements will be included in all agreements and contracts with outside entities. The Department Director responsible for authorizing the individual's access shall immediately notify the Information Systems Help Desk of all terminations.

5.0 Appendix A—Original Policy, Access to Information Systems

GIAC HEALTHCARE

POLICY NUMBER: IS—02

SUBJECT: ACCESS TO INFORMATION SYSTEMS

DEPARTMENT: INFORMATION SYSTEMS

APPLIES TO: GIAC HEALTHCARE

EFFECTIVE: June, 1990 **REVIEWED/REVISED:** September, 1996
August, 1999
August, 2002

SUPERCEDES:

DISTRIBUTION: All

AUTHORED BY: John Doe, Director, Information Systems

REVIEWED BY: IS Team Leader

APPROVED BY: Executive Director of Systems Development
Vice President of Networking Services
President

REFERENCE POLICY

Confidentiality of Information PRS-503

POLICY STATEMENT

Confidentiality and security of information accessed when using information systems is essential. Therefore, only authorized employees/agents of GIAC Healthcare shall have access to information systems. Entitlement to access shall be determined on an individual basis according to "need to know" and any unauthorized access will be subject to disciplinary action.

POLICY GUIDELINES

It is the policy of GIAC Healthcare to promote appropriate use of information at all times through the implementation of policies and procedures regarding access, hardware, software, data, users, and other aspects. Everyone who uses computing resources has

the responsibility to use them in an ethical, professional and legal manner. This means the users agree to abide by the following conditions.

7. Each user must present a signed Information Systems Access Request Form prior to gaining access to information systems. Signed forms are placed in the individual's personnel file. The Information Systems Access Request Form is maintained on-line and is available to all managers. These forms are updated periodically.
8. Passwords are confidential. An employee to whom a password is issued will be held responsible for the data that is accessed under their password. Therefore, the employee is also responsible for "logging off" when they leave a terminal or personal computer unattended.
9. If an employee suspects that someone has accessed an account using a password other than his or her own, the employee should contact his or her supervisor immediately. The supervisor should, in-turn, notify the Information Systems Help Desk. Any employee making or attempting access to unauthorized information will be subject to disciplinary action up to and including immediate termination.
10. Medical Staff and students may be granted access to information systems. The same procedural guidelines for granting, changing and terminating access shall apply. However, Administration and the Chief of the Medical Staff shall be responsible for physician access, including maintaining signed forms. The Directors of the Schools, in conjunction with the Nursing Service Director and department managers, shall define and be responsible for all student access, including maintaining signed forms.
11. The Information Systems department has the responsibility to gather information to diagnose problems and investigate security violations. Information Systems will maintain the privacy of individual activities and information viewed fulfilling these duties, unless the user has violated hospital policy, or any Federal, State or Local laws.
12. The department director or appropriate Administrative Staff may have access to their employees' passwords and knowledge of any on-line activities of the employees.

PROCEDURES

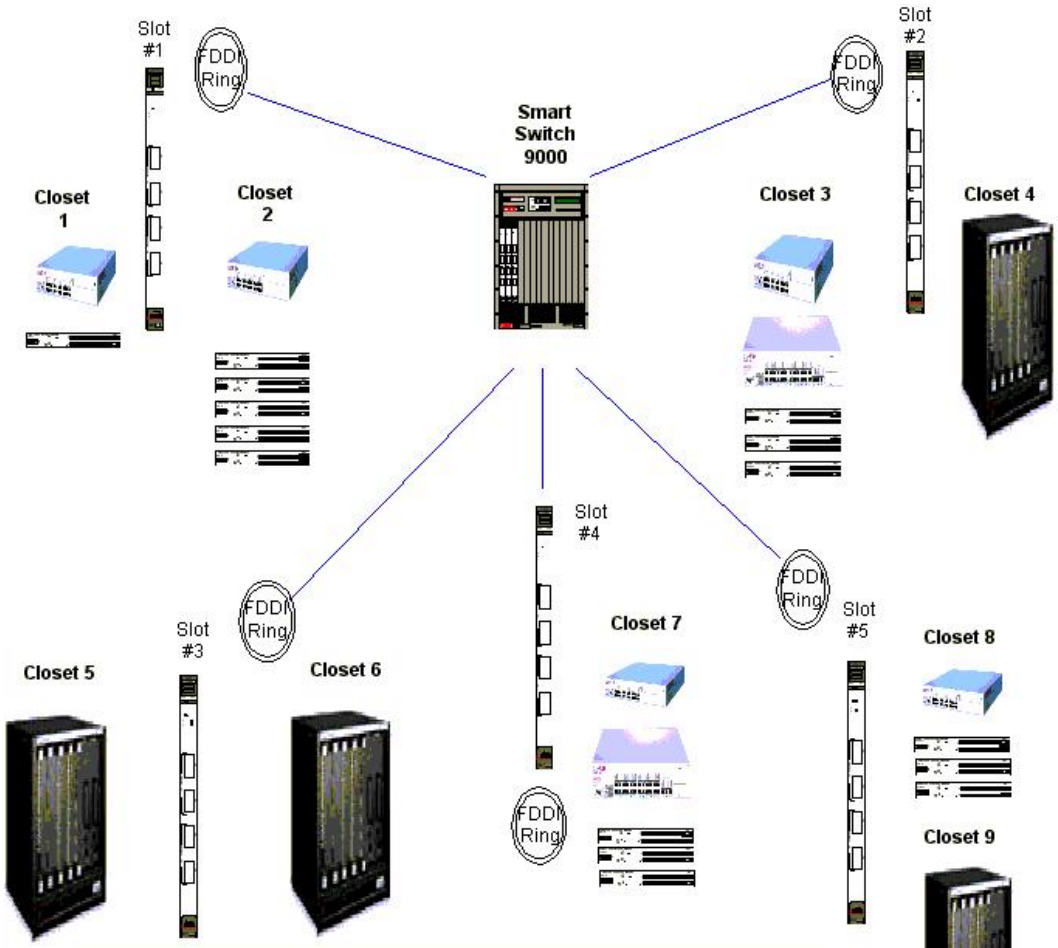
4. New Users
    a. Personnel requires that all new employees sign a Confidentiality Agreement when hired.
    b. The department director or supervisor submits a signed Information Systems Access Request Form indicating the access required.
    c. After assigning the new user with appropriate access, the Information Systems Help Desk notifies the user regarding his or her password. The Help Desk will forward the signed form to Personnel for filing.
5. Updates/Changes

a. When a revision in a user's access is required, the department director will complete and submit a new-signed Information Systems Access Request Form. The form should reflect the revisions needed.
b. After completing the requested revisions, the Information Systems Help Desk notifies the user. The Help Desk then forwards the signed form to Personnel for filing.

6. Termination
    a. When a user terminates employment, Personnel notifies the Information Systems Help Desk of the employee's name and termination date via electronic mail.
    b. In the event of involuntary termination of an employee:
        i. During normal business hours, the department director or acting supervisor is responsible for the immediate notification of the termination to Personnel. Personnel notifies the Information Systems Help Desk immediately of this termination. The Help Desk promptly removes the terminated employee's access.
        ii. If an employee is suspended pending termination outside of normal business hours, the Information Systems department "on-call" staff member is notified immediately by the department director or acting supervisor. They promptly remove the terminated employee's access.
7. At the end of each month, Personnel provides the Information Systems Help Desk with a list of terminations and department transfers. The Help Desk verifies the terminated employees' access has been removed. Updates required due to department transfers require a newly signed Information Systems Access Request Form presented to the Help Desk by the employee's new department director.

6.0 Appendix B—GIAC FDDI LAN Backbone

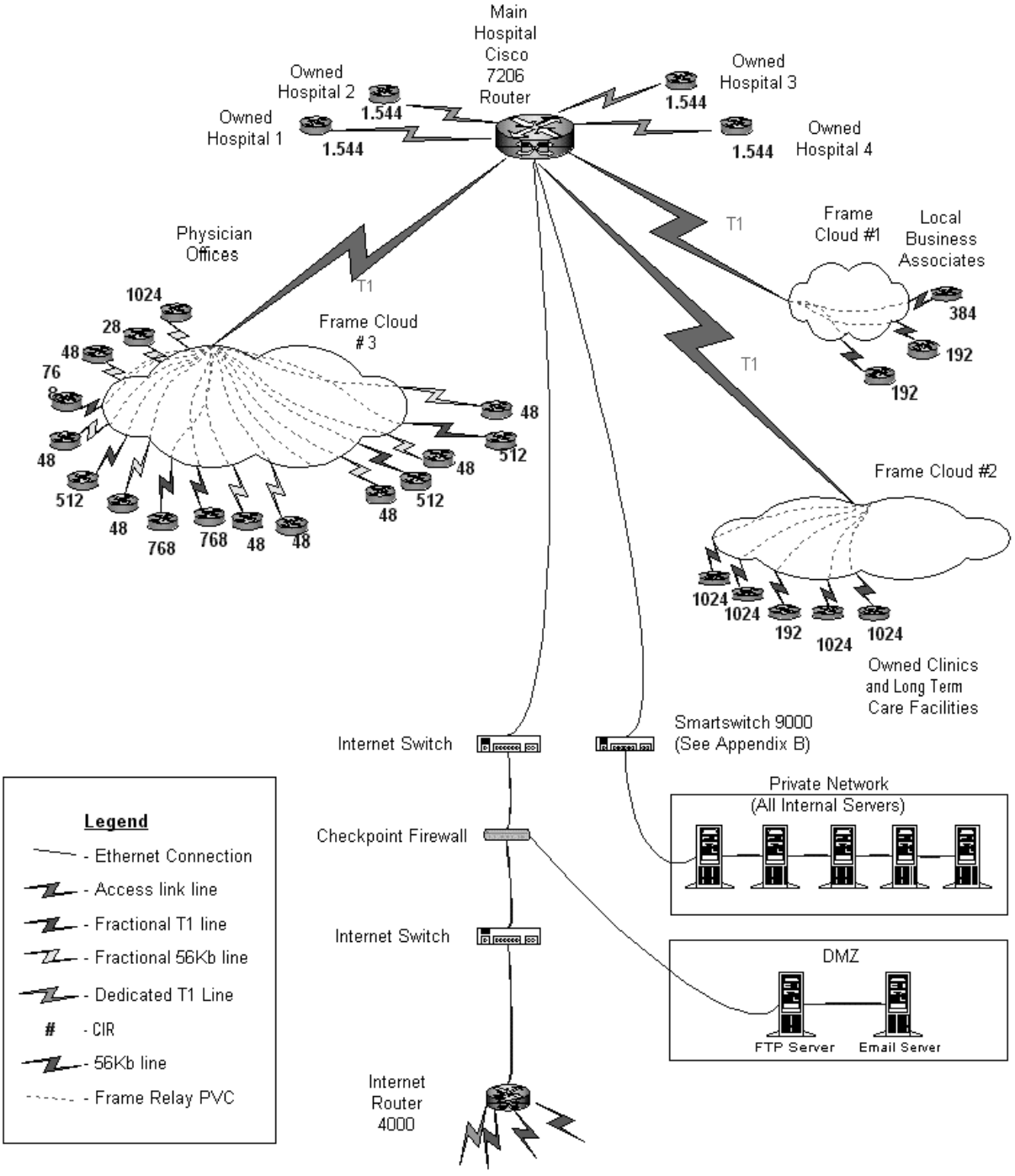
Diagram 1—GIAC Local Area Network



Closet 1	Cabletron 2H252-25R Switch 10/100 24 port FDDI uplink
	1 individual SEH hub with a 10 mgb uplink
Closet 2	Cabletron 2H252-25R Switch 10/100 24 port FDDI uplink
	5 individual SEH hubs-each has a 10 mgb uplink
Closet 3	Cabletron 2H252-25R Switch 10/100 24 port FDDI uplink
	1 ELS10-27TX with a 100 mg uplink
	3 individual SEH hubs-each has a 10 mgb uplink
Closet 4	Cabletron Matrix E7, Switch 10/100 48port,
	Cabletron Matrix E7 6H303-48 (3) FDDI uplink
	Cabletron Matrix E7 6E233-49(1)
Closet 5	Cabletron Matrix E7, Switch 10/100 48port,
	Cabletron Matrix E7 6H303-48 (3) FDDI uplink
	Cabletron Matrix E7 6E233-49(1)
Closet 6	Cabletron Matrix E7, Switch 10/100 48port,
	Cabletron Matrix E7 6H303-48 (3) FDDI uplink
	Cabletron Matrix E7 6E233-49(1)
Closet 7	Cabletron 2H252-25R Switch 10/100 24 port FDDI uplink
	3 individual SEH hubs-each has a 10 mgb uplink
Closet 8	Cabletron 2H252-25R Switch 10/100 24 port FDDI uplink
	3 individual SEH hubs-each has a 10 mgb uplink
Closet 9	Cabletron Matrix E7, Switch 10/100 48port,
	Cabletron Matrix E7 6H303-48 (3) FDDI uplink

7.0 Appendix C—GIAC WAN Configuration

Diagram 2—GIAC WAN Configuration



8.0 Appendix D – Server Listing and Locations

SERVER	LOCATION	OS	FUNCTION	Applications	Category
ABBOTT	GIAC Main	2000	ARCSERVE	Backup Software	Infrastructure
CLIFF	GIAC Main	NT	OUTLOOK WEB ACCESS	Mail - Web Server	Infrastructure
DRYSDALE	GIAC Main	2000	FIREWALL	Firewall Server	Infrastructure
ELVERNA	GIAC Main	NT	SMS	Network Management Applications	Infrastructure
EXTERMINATOR	GIAC Main	2000	NORTON ANTIVIRUS SERVER	Network Management Applications	Infrastructure
GILLIGAN	GIAC Main	2000	WIN2000 PRINT SERVER	WIN2000 Domain print server	Infrastructure
GRANNY	GIAC Main	2000	EXCHANGE MAIL SERVER (SECOND)	Backup Server	Infrastructure
JANE	GIAC Main	NT	EXCHANGE SERVER	Mail server	Infrastructure
JETHRENE	GIAC Main	NT	WGDATA DFS ROOT/ BDC	Domain Controller	Infrastructure
JETHRO	GIAC Main	NT	INTRANET WEB SERVER	Intranet Web Server	Infrastructure
LESTER	GIAC Main	2000	RADIUS SERVER	RAS Software	Infrastructure
LOVEY	GIAC Main	2000	DHCP/WINS PRIMARY		Infrastructure
MARGARET	GIAC Main	2000	WIN2000 DOMAIN CONT/DFS ROOT	Win2000 Domain Controller	Infrastructure
MARIE	GIAC Main	NT	NT 4. 0 BDC	Backup Domain Controller	Infrastructure
MAX	GIAC Main	AIX UNIX	INTERFACE ENGINE	DATAGATE	Infrastructure
PEARL	GIAC Main	2000	ARCSERVE	Backup Software	Infrastructure
RAVENSWOOD	GIAC Main	2000	WIN2000 DOMAIN CONT/DNS	WIN2000 DOMAIN CONTROLLER & DNS	Infrastructure
SAM	GIAC Main	NT	NT 4. 0 PDC/DFS ROOT	Domain Controller	Infrastructure
SKIPPER	GIAC Main	2000	PRINT SERVER/WINS 2NDRY	PRINT SERVER / SECONDARY WINS SERVER	Infrastructure
WOODY	GIAC Main	2000	WEBTRENDS/WEBSENSE	Internet Tracking	Infrastructure
BO	GIAC Main	NT	APPLICATION SERVER	Cerner RRD Server (Remote Report Distribution)	Primary Application
BOSSHOGG	GIAC Main	NT	APPLICATION SERVER	Cerner Certification Server	Primary Application
BROKER	GIAC Main	NT	APPLICATION SERVER	Radiology	Primary Application
CHER	GIAC Main	2000	APPLICATION SERVER	ORACLE INTRANET PORTALS	Primary Application
DG-1	GIAC Main	MAGIC	Main HIS	MEDITECH	Primary Application
DG-2	GIAC Main	MAGIC	Main HIS	MEDITECH	Primary Application
DG-3	GIAC Main	MAGIC	Main HIS	MEDITECH	Primary Application

DG-4	GIAC Main	MAGIC	Main HIS	MEDITECH	Primary Application
DG-5	GIAC Main	MAGIC	Main HIS	MEDITECH	Primary Application
DG-6	GIAC Main	MAGIC	Main HIS	MEDITECH	Primary Application
DG-7	GIAC Main	MAGIC	Main HIS	MEDITECH	Primary Application
DG-8	GIAC Main	MAGIC	Main HIS	MEDITECH	Primary Application
ELLY_MAE	GIAC Main	NT	APPLICATION SERVER	Cardiac Services applications	Primary Application
FESTER	GIAC Main	AIX UNIX	ORACLE DB	ORACLE	Primary Application
FRANK	GIAC Main	2000	APPLICATION SERVER	Surgery Application Server	Primary Application
HOTLIPS	GIAC Main	2000	APPLICATION SERVER	Surgery Application Server	Primary Application
JASPER	GIAC Main	NT	APPLICATION SERVER	CARDIAC APPS (HOLTER)	Primary Application
KLINGER	GIAC Main	2000	APPLICATION SERVER	Surgery Application Server	Primary Application
LILLITH	GIAC Main	2000	USER HOME DIRECTORIES	Onsite and Offsite user home directories	File Server
LUKE	GIAC Main	NT	APPLICATION SERVER	IIS Cluster	Primary Application
LURCH	GIAC Main	AIX UNIX	APPLICATION SERVER	PRACTICE MANAGEMENT SOFTWARE	Primary Application
MEDIBUY	GIAC Main	2000	IS DEPT STORAGE	IS Dept Storage	File Server
MSI	GIAC Main	2000	IS DEPT STORAGE	IS Dept Storage	File Server
NORM	GIAC Main	2000	GROUP STORAGE	WGDATA	File Server
POTTER	GIAC Main	2000	APPLICATION SERVER	Surgery Application Server	Primary Application
RADAR	GIAC Main	2000	APPLICATION SERVER	Surgery Application Server	Primary Application
ROSCOE	GIAC Main	2000	APPLICATION SERVER	CERNER CHARTING SERVER	Primary Application
SONNY	GIAC Main	2000	APPLICATION SERVER	ORACLE INTERNET PORTALS	Primary Application
TRACEMASTER	GIAC Main	NT	APPLICATION SERVER	Cardiac Services ECG	Primary Application
ALF	GIAC Main	2000	APPLICATION SERVER	Medical Record's Coding software.	Departmental Application
ARNOLD	GIAC Main	2000	APPLICATION SERVER	Interqual server	Departmental Application
BESSIE	GIAC Main	NT	APPLICATION SERVER	Applications Server	Departmental Application
CATALYST001	GIAC Main	NT	APPLICATION SERVER	Catalyst server	Departmental Application
CCHECKER	GIAC Main	NT	APPLICATION SERVER	IIS Cluster	Departmental Application
CLINK_2	GIAC Main	NT	APPLICATION SERVER	MAC LAB SERVER	Departmental Application
COACH	GIAC Main	2000	APPLICATION SERVER	HCIS HOME HEALTH SERVER	Departmental Application
EARL	GIAC Main	2000	APPLICATION SERVER	IMPAC AND ERS SERVER	Departmental Application
EDDY	GIAC Main	NT	APPLICATION SERVER	Dictaphone Cluster	Departmental Application

GINGER	GIAC Main	NT	APPLICATION SERVER	BED TRACKING	Departmental Application
HERMAN	GIAC Main	NT	APPLICATION SERVER	Dictaphone Cluster	Departmental Application
IMAGEGEPOOL	GIAC Main	NT	APPLICATION SERVER	GEMNet Server	Departmental Application
JED	GIAC Main	NT	APPLICATION SERVER	PAT. SRV. APPS (MIDAS)	Departmental Application
LILY	GIAC Main	NT	APPLICATION SERVER	Dictaphone Cluster	Departmental Application
REBECCA	GIAC Main	2000	APPLICATION SERVER	MISC. DEPARTMENTAL	Departmental Application
STARSKY	GIAC Main	2000	APPLICATION SERVER	CCI INTERFACE WORKSTATION	Departmental Application
LTC 1 Apps	LTC 1	2000	DOMAIN CONTROLLER		Infrastructure
LTC 1 DC	LTC 1	2000	APPLICATION SERVER	AccMed's AccuMax and AccuAdd-On	Primary Application
Owned 1 DC	Owned 1	2000	DOMAIN CONTROLLER		Infrastructure
Owned 1 Apps	Owned 1	2000	APPLICATION SERVER	AccMed's AccuMax and AccuAdd-On	Primary Application
Owned 2 DC	Owned 2	2000	DOMAIN CONTROLLER		Infrastructure
Owned 2 Apps	Owned 2	2000	APPLICATION SERVER	AccMed's AccuMax and AccuAdd-On	Primary Application
Owned 3 DC	Owned 3	2000	DOMAIN CONTROLLER		Infrastructure
Owned 3 Apps	Owned 3	2000	APPLICATION SERVER	AccMed's AccuMax and AccuAdd-On	Primary Application
Owned 4 DC	Owned 4	2000	DOMAIN CONTROLLER		Infrastructure
Owned 4 Apps	Owned 4	2000	APPLICATION SERVER	AccMed's AccuMax and AccuAdd-On	Primary Application
Spare	GIAC main	AIX Unix	NON-PRODUCTION	test	
Spare	GIAC Main	2000	NON-PRODUCTION	test	
Spare	GIAC Main	2000	NON-PRODUCTION	test	
Spare	GIAC Main	2000	NON-PRODUCTION	test	

9.0 References

The following references were used before and during the completion of this assignment.

SANS Track 9 – Information Security Officer Training, 9.1 SANS Security Leadership, Part 1, 9.2 SANS Security Leadership, Part 2, 9.4 SANS Information Security Policy: A Roadmap for Security Officers, 9.5 Defense In Depth, The SANS Institute, 2002

Kovacich, Gerald, Information Systems Security Officer's Guide, Boston: Butterworth-Heinmann, 1998

Peltier, Thomas, Information Security Policies, Procedures, and Standards: guidelines for effective information security management, New York, Auerbach Publications, 2002

Peltier, Thomas, Information Security Risk Analysis, New York, Auerbach Publications, 2001

Schneier, Bruce, Secrets & Lies: digital security in a networked world, New York, John Wiley & Sons, 2000