GIAC Enterprises
Information Security Policies and Procedures for GIAC Medical Center

David Standish

GISO Basic Practical Assignment
Version 1.2

1. Description of GIAC Enterprises Medical Center

About the Medical Center

GIAC Enterprises Medical Center is a fully accredited, acute-care hospital with a 278-bed capacity located in the center of a small metropolitan city. The Medical Center is committed to providing quality, comprehensive, community-based health care services to more than 70,000 people annually, and as part of that commitment continually develops new and expanded services to meet the changing health needs of the communities it serves. The Medical Center employs a workforce of over 1,100 professional, technical, and support personnel. The majority of this workforce accesses the Medical Center's data network 24 hours a day, 7 days a week, 365 days a year.

The Medical Center offers a full continuum of health care services for people of all ages. Services include sophisticated diagnostic laboratory and radiology services, medical and radiation oncology services, renal services, cardiac services, and maternal and child health services. Comprehensive inpatient and same day surgical services, behavioral health services, and senior services including adult day care are also provided. Each one of these departments has various medical devices and data processing equipment requiring access to the Medical Center's internal data network.

The GIAC Enterprises Medical Center does not operate any branch offices but does maintain a WAN. This WAN provides connectivity to the Medical Center's internal data network for remote outpatient laboratories, private physician practices and telecommuting employees. This is facilitated via a combination of private leased line at 56kbps, Channelized T1, ISDN (PRI), and Internet access via a dedicated T1.

IT Infrastructure

The GIAC Enterprises Medical Center IT infrastructure is supported by fast routing / switching at the core. A fiber optic backbone carrying data at 100MB full duplex connects the core to switches and hubs installed in intermediate distribution frames strategically located throughout the main facility.

The internal network is physically segmented via fast routing/switching into six different networks for traffic separation purposes. Logically the network is divided into two major functional areas: 1.) The Clinical Network; 2.) The Corporate Office Network. In addition a demilitarized zone (DMZ) for untrusted access to an informational Web site and DNS is also in operation. (See diagram 1 in Appendix A.)

The core production systems at the Medical Center are its Clinical Systems. Two systems comprise this core: The Medical Data System and the Hospital Information System. The two systems are linked via an interface engine. Both systems are hosted on DEC (Compaq) Alpha 1000 hardware and talk to each other and their clients over the network via Ethernet and TCP/IP. The operating system environment of the “Medical Data System” is OpenVMS V7.2.The Hospital Information System operating environment is a proprietary OS called “MAGIC”. The client base of the clinical systems is mainly Intel Pentium based desktop PCs utilizing terminal emulation software to establish sessions with each host. Some dumb terminal console access is provided for in control areas.

The Corporate Office Network is comprised of over 500 Intel Pentium based desktop PC’s and 6 Compaq ML750-series servers. The servers are Microsoft NT and Windows 2000 advanced server based. They provide a full spectrum of back office services to the client base such as an Exchange email server, file and print services, database services, and an IIS Intranet Web site. The typical desktop client operating environment is Microsoft Windows 98 and 2000 pro.

Securely providing remote access to the Center's networks and sharing patient information with remote labs, clinics, and physician's offices is accomplished with a Cisco based network infrastructure. The main site (data center) provides three methods of access to the center's networks: 1.) Cisco 3030 VPN Concentrator 2) Internet access through a screening router (Cisco 2500 series) PIX 525 Firewall with 3DES VPN support and 3.) Back-up access via dial-up modem and ISDN through a Cisco AS 5300 providing AAA security via Cisco secure server & Tacacs+.

Business Operations

As a full-service acute care Medical Center, Giac provides health care services to its community and surrounding areas. Beyond collecting and processing its inpatient data, Giac Medical Center (GMC) supports over 50 remote sites including clinics, labs, wellness centers and physician practices.

Providing connectivity and sharing Protected Health Information (PHI) is more challenging in the 21st century for health care providers. New federal regulations mandate GMC to follow standards for privacy and security of all patient's health information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) includes security standards that must be implemented by GMC.

The occasional remote user such as management and support personnel, as well as the telecommuter, require secure and cost-effective access to the GMC data network and systems. Business associates connect to the Center's networks and systems on an as needed basis. The nature of this remote access and the sensitivity of the data require robust monitoring and audit capabilities on behalf GMC.

The majority of remote users from labs, physician offices, clinics and elsewhere connect to the clinical systems via Client- to- Gateway connections. The business operations being performed are critical as this information is primarily patient health information. Blood test results, diagnoses, referrals, drug orders and claims information are just a few types of sessions being negotiated across the GMC network. Connectivity is provided to PC clients via VPN circuits using Cisco 3030 VPN Concentrator and VPN client software. Connections are made via 56kbps dial-up and Internet service provider broadband DSL and cable modem.

Other remote access is provided to management and support personnel via GMC owned laptop computers running Windows 2000 Professional and VPN connections with Cisco's VPN client software that supports 3DES IPSec. Connections are made via 56kbps dial-up and Internet service provider broadband DSL and cable modem.

A private business associate network also provides connectivity to a trusted business associate over a private 56kbps leased line and Cisco 2500 series routers.

An ISDN backup is provided through a Cisco AS 5300 with TACACS+ and AAA security.

Outbound web access as well as email is provided to a selected group of management and clinical staff.

Real-time Managed Intrusion detection devices are connected to the network at strategic locations throughout the GMC network and are monitored 24 by 7 remotely.

2. Risk Assessment

Major areas of Risk

Giac Medical Center is in the business of health care. The confidentiality, integrity, and availability of patient information are absolutely critical to the operation of the Medical Center and to the health and wellness of the community it serves. With the new federal HIPAA security standards it is now also a matter of law. There is a multitude of risks associated with the Medical Center's network infrastructure and one can only hope to minimize and mitigate those risks. Listed below are the three most critical areas of risk to Giac Medical Center:

1.) Business continuity disaster recovery
2.) Attack from Remote Access
3.) Attack from Viruses and Malicious Code

Business Continuity/Disaster Recovery

Threat

Patient health information is the "crown jewel" of Giac Medical Center. The systems and network infrastructure that stores, processes and provides access to patient information must be protected at all costs. Insuring the 24 by 7 operation of the clinical and business systems is top priority.

Concerns to the Medical Center

Although a disaster either natural or man-made is unlikely to occur, Giac Medical Center must be prepared to meet this threat. Natural disasters such as fire, flood, storms, and earthquakes along with man-made threats such as terrorism, construction accidents and even war happen every day. The terrible events of September 11, 2001 occurred in three different states proving that the unlikely is likely to occur. If a disaster were to strike the Giac Medical Center data center, which houses the core systems and network equipment, the Center's clinical and business operations would be most severely affected if not totally disabled.

Consequences to the Medical Center

The Centralized location of the core systems of the Medical Center increases the vulnerability to the risk of damage due to a disaster, as mentioned above. The core host systems provide a repository of clinical information on the patients who have been admitted to and are currently being cared for in the Medical Center. They also provided information on patients that have had tests and procedures at the Medical Center for as long as a month prior to discharge. The availability of the information is the main concern. Billing information is secondary concern, although extremely important for the continuance of operations. The funds from state and federal government programs require this information from the Medical Center on a scheduled basis. Loss of a small portion of this information could result in millions of dollars in lost revenue. Finally the GMC requires quick, accurate and current information to safely test its patients.

The loss of or damage to any of the core systems and the related data would negatively impact operations in the following ways:

1.) Loss of confidence in the patient population.
2.) Legal and regulatory consequences resulting in loss of licensing.
3.) Financial consequences resulting in loss of government funds and lost business revenue.
4.) Possibility of unsafe conditions for the Center's patients.

Mitigation

The following measures must be taken to protect GMC against the risk of a disaster:

- Develop a disaster recovery plan.
- Construct and equip a "HOT SITE" or "COLD SITE" for resumption of lost service.
- Procure or arrange for the availability of duplicate critical systems and applications.
- Contract for communications lines from the "HOT SITE" to the Medical Center's health care delivery location.
- Contract for off-site storage of critical data.
- Rotate backup media daily.

- Train IT staff and Medical Center key management on disaster recovery procedures.
- Test the plan bi-annually.

Attack from Remote Access

Threat

The need for secure remote access to the GMC network is vital to the business goals of GMC. The increasing number of connections to remote employees, physician offices, business associates, and consultants creates a higher level of vulnerability and increased risk of unauthorized access to the Center's sensitive data. In a health care environment the protection of confidentiality, data integrity, and availability is paramount.

Concern to Giac

Identification and authentication of remote users is a problem to say the least. The identity of network users is the basis for assignment of system access privileges that will be granted over a remote connection. It is essential that business operations not be disrupted by the malicious activities of an unauthorized remote cracker.

At the same time, it is essential to provide reliable encrypted data to physicians, business associates and remote employees who have a valid need to access the resources on the GMC network. The problem is compounded by the lack of control over security of a physician's or business associate's Internet connection and computer equipment. GMC is exposed to the vulnerabilities of remote users as they may be propagated by the inadequate security practices of the remote offices.

Consequences

GMC must protect the confidentiality of patient information. As mentioned previously, federal and state laws mandate this. Financial and sensitive business information must also be protected. A malicious attack by an unauthorized user can have far reaching consequences. If confidential patient information were to be obtained and exploited or sold for personal gain, the Medical Center's reputation would be ruined, not to mention possible civil and criminal penalties that might be brought against its officers or trustees. Ineffective authentication and authorization mechanisms as well as certain attacks on the network systems (“man in the middle”) could result in the above consequence.

Another consequence is the possibility of a virus or malicious code being propagated to the GMC network when a connection is established. The remote computer may have been compromised while offline or through its ISP by inadequate security policies and procedures of the remote office network. This has the potential to disrupt the network operations at GMC.

Mitigation

- Reliable authentication of users and systems. A secure remote access system employing a variety of strong authentication mechanisms for human users, and digital certificates to verify identities of machines and gateways for physician offices and business associates.
- Granular Access Control -- Providing administrators the control to grant access for all appropriate business purposes and those with a clinical “need to know”, while denying access for everything else.
- Strong encryption of data using VPNs that support 3DES and IPSec to protect confidentiality of data.
- Strong Passwords: Using at least six to eight alphanumeric characters, with no resemblance to any personal data. Properly educate users on password selection. Password aging measures that require periodic changes.
- Logging and Auditing of remote access.
- Deploy intrusion detection devices on each point of network entry and monitor 24 by 7.
- HIPAA regulations require business associate contracts and chain of trust agreements to have security standards language included to protect patient information received in the course of doing business with the Medical Center. These contracts must be implemented.
- Formal security policy on remote access for employees and physicians offices that includes a remote access agreement form to be signed before access is granted. Policy should also include a statement on certification by GMC’s IT department on remote equipment and software.

Attack from Viruses and Malicious Code

Threat

Several years ago most viruses spread primarily via floppy disk, but the Internet has introduced new virus distribution mechanisms. With email now used as an important business communication tool, viruses are spreading faster than ever. Viruses attached to email messages can infect an entire enterprise in a matter of minutes, costing companies millions of dollars annually in productivity loss and clean-up expenses.

Viruses won’t go away any time soon. More than 10,000 have been identified, and 200 new ones are created every month, according to the International Computer Security Association.

Concerns to the Medical Center

Viruses are common on the Windows platform due to the architecture of the processor and the operating system. Use of the Internet introduces additional threats via active code such as ActiveX and Java

GMC finds that there is an increase in the valid use of the Internet by its employees and for research purposes using Medical Center resources. The Medical Center PC resources are mainly Microsoft based. The Medical Center also realizes that email is increasingly becoming an important and widely used business tool within the organization. This increase in use of email and Internet Web sites directly increases the risk of damage and disruption to the GMC network.

Consequences

The Medical Center is first and foremost concerned with patient information. The loss of patient information is possible if a destructive worm were to infect the file systems of the servers that host clinical applications. There could also be data integrity issues raised as a result of a virus infection. Some systems may fail due to malicious code, thereby reducing the available resources to business operations.

Viruses introduced via email can bring down the Medical Center’s email server and significantly impact the business communications capabilities. Bandwidth could be denied via the flood of message produced by a self-propagating email virus. Finally the reputation of the Medical Center could be damaged as a result of a "Trojan Horse" virus that could use Medical Center resources to launch an attack elsewhere.

Mitigation

The Following Steps can prevent and eradicate viruses:

- Training users on the proper procedures to prevent computer virus infection and recognition of email attachments that may be malicious.
- Installation of anti-virus software on all Medical Center PCs.
- Installation of anti-virus software on all Medical Center servers.
- Automatic update of signatures weekly.
- Filter email content and prohibit certain email attachments.
- Filter Web downloads.
- Keep all clients and servers patched with the latest bug-free patches.
- Prohibit “Sneaker Net” to a practical degree.
- Insure all remote offices are protected with AV software.
- Insure all remote offices update AV signatures regularly.
- Install AV software on all GMC laptops and insure that the user updates signatures regularly.
- All PCs and servers, both remote and local, should be scanned regularly.

3. Evaluate and Develop Security Policy

Please refer to the Policy in appendix A.

The Policy being evaluated here -- “Remote Access Policy” -- was taken from the following Web page:

http://www.hhic.org/hipaa/pdf/remote.pdf

Evaluation

Purpose and Scope Statement

This policy has both favorable and unfavorable aspects. Overall, the policy is very easy to read and understand. The sections on definitions and reference to other related policy are good additions. The precise language clearly states the general intent of the policy. It is immediately clear that the policy addresses remote access to the company's data by employees, physicians, and business associates (partners). This information is stated in the **PURPOSE** establishing the issue immediately. It would be better to include a **SCOPE** statement to establish the intended audience for the policy, as well as the chain of oversight and authority for enforcement if not included in the responsibility section.

Background Statement

Considering the importance of the issue of remote access at Giac Medical Center, the policy can be improved by adding a **BACKGROUND** statement. It is important to include information on why remote access is offered to the employees, physicians, and business associates. Cultural, technical, and economic motivators could also be included here.

Policy Statement

The main usage expectations are mentioned in this statement, but it is incomplete as written. There could be a few more expectations listed, and the VPN requirements must be present in the policy and not referred to in HFCA policy. This being a health care provider’s policy on remote access, the HIPAA requirements and standards must also be included. The expectation and responsibility for logs is a good piece of this policy as written. However, this statement might be better placed in the **Action** section. A remote access agreement statement needs to be added to complete the expectations.

Responsibility

This policy is lacking a statement on responsibility. There is no information in this policy regarding the author or the administrative authority that supports it. The policy would be enhanced by the addition of a statement identifying those responsible for policy implementation. A statement regarding enforcement of policy violations would also be a good addition to this section.

Action

This policy is also missing a section describing specific actions and time frames. As mentioned above, issues such as the signing of agreements by employees and physicians should be detailed in this section. If disciplinary action is not included in the responsibility section it should be added and expounded on in this section.

Policy Revision

Below is a revised Remote Access policy[i] that would better serve Giac Medical Center:

APPROVED BY: CIO/CFO/CISO	**PREPARED BY: Information Security Officer**
EFFECTIVE DATE: April 1, 2002	**SUPERSEDES:** NA
DISTRIBUTION: Organization wide	**JCAHO STANDARD(S): Management of Information**
	NJDHSS REG(S): NA **HIPAA REG(S): 45 CFR PART 142**

Purpose of Policy

The purpose of this policy is to establish the security requirements for eligible employees, physicians, and business associates that require remote access to Giac Medical Center information assets. To define expectations for use of the Medical Center's remote access services including modem, access server, Virtual Private Network (VPN) and Internet access to terminal services; to establish accounting and auditing policy for remote access use; to determine the chain of responsibility for misuse of the remote access privilege.

Scope

The policy is intended to serve as a guideline to all employees, physician offices and business associates requesting or currently accessing Giac Medical Center's data network and computer systems from non-medical center locations.

Background

Giac Medical Center provides remote access to its data network and computer resources for telecommuting and traveling employees. By providing this remote connectivity it becomes very convenient and economical for employees to access the business network and resources to conduct long-distance work. The same access is provided to physicians so their offices may receive test results on their patients as quickly as possible. Certain business associates have the same privileges so they may conduct business efficiently with the Medical Center. This access however introduces risk to GMC's systems; risk of inappropriate access, unauthorized data modification, compromised confidentiality of patient health information and possible disruption of services. The following standards are provided by GMC for the above reasons.

Policy

An appropriate GMC executive must approve access to GMC electronic assets from remote locations. An employee, physician or business associate requesting remote access must complete the Remote Access Agreement, available from the Information Services Department at the Medical Center.

Remote access via modem should be through an approved security device such as a dial-back system or hardware token technology. Access to GMC internal network from outside its defined network perimeter must be controlled by privileged access controls.

If VPN technology is utilized for remote access, then the VPN system must conform at least minimally to a level of encryption protection equivalent to that provided by an algorithm such as; Triple 56 bit DES (defined as 112 bit equivalent) for symmetric encryption; 1024 bit algorithms for asymmetric systems; and 160 bits for the emerging Elliptical Curve systems. GMC reserves the right to increase these minimum levels when deemed necessary by advances in techniques and capabilities associated with the processes used by attackers to break encryption.

All computing devices accessing the GMC network are subject to equipment and software certification by GMC's Information Services Department.

Employees, physician offices and business associates accessing and/or transmitting patient's health care information via remote access methods must comply with state and federal privacy and security regulations including the ***Health Insurance Portability and Accountability Act of 1996, (HIPAA) requirements for individual's rights with respect to protected health information.***

Responsibility

Access Control Responsibility

Access to confidential clinical and financial information will be granted on a need-to-know basis. Thus owners of information, with the assistance of the Information Services (IS) Department, must review employees' information needs by receiving certification of such information needs from the employee's department director. To ensure appropriate levels of access, a variety of security measures will be instituted as approved by the Management of Information Committee.

Monitoring Responsibility

The IS management team or department managers will determine which remote activities or remote data access must be monitored. The network administrator will configure the system to log these activities/accesses and to produce reports. Network administrators will monitor remote user activity (including system and data access) in accordance with GMC organizational and IS policies. Inappropriate activities will be reported to user management.

The Human Resources department will review ongoing remote access for employees and verify that a person is still employed by GMC and that they are still qualified for remote access. Human Resources is also responsible for notifying the IS department within one working day of effective termination or disqualification of the employee from remote access. The IS department is responsible for revocation of access rights for physicians and business associates.

Action

Remote Access users are ultimately responsible for the use of their system accounts. The user must protect the confidentiality, integrity, and availability of GMC's information assets by protecting phone numbers, login processes, and maintaining strong authentication tokens in their possession at all times. The remote user must not connect their remote computers to other private networks while their GMC connection is active.

Use of another employee's authentication token is strictly prohibited. Any unspecified actions that may compromise the security of the GMC network, computer resources, or patient information are also forbidden.

Any employee, physician office, or businesses associate who suspects that the remote access system is being misused is required to report the misuse to the GMC help desk immediately.

Violation of this policy will result in disciplinary action, up to and including termination of employment, and is subject to civil and/or criminal prosecution.

4. Develop Security Procedures

This section contains a procedure documenting the steps necessary for the saving and printing of remote access logs. This is only one procedure among many that are required to implement the Giac Medical Center's organizational policy on remote access to the GMC network

Background

Remote system access to Giac Medical Center's computer network is available to authorized employees, physician offices and business associates. There are three options for remote access to the Giac Medical Center network:

1) Connecting via a user's existing Internet connection to the IS Terminal Services server.
2) Connecting via dial-up to the IS Access server.
3) Connecting via the VPN Concentrator

The Computer Operator of the day shift is responsible for printing the remote access log on a daily basis. The technical support manager is responsible to ensure that all access is warranted to identify unsuccessful attempts to access the system, and to review the printout. If the technical support manager detects questionable access, the IS Director is immediately notified. The Information Security Officer will be immediately informed if a breach in security is identified. The activity log is printed, initialed and approved by the reviewer, placed in the binder labeled "REMOTE ACCESS LOGS", and retained for 6 months. The Information Security Officer will randomly audit network access logs, both online and in printed archives.

Procedures

Access server

Use the following procedure for printing *Access* server logs. The logs are saved on a daily basis at **GMC1\\ntsecure\passed authentications**. The files are all saved with the following name: Passed Authentications 2001-11-01, where the year-month-date is listed for each respective day.

1. Open Windows Explorer and locate **GMC1\\ntsecure\passed authentications** folder.
2. Double click the file that represents the date you need to print. The file will automatically open in Excel.
3. Place the report in the technical support manager's mail bin.

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address
11/30/2001	10:37:13	Authen OK	REMOTE99	Default Group	9095551212/5555555	Async91	198.097.24.22
11/30/2001	13:18:45	Authen OK	REMOTE99	Default Group	9095551212/5555555	Async92	198.097.24.22
11/30/2001	13:43:56	Authen OK	REMOTE99	Default Group	9095551212/5555555	Async93	198.097.24.22
11/30/2001	18:06:51	Authen OK	REMOTE98	Default Group	9095551212/5555555	Async94	198.097.24.22
11/30/2001	20:25:32	Authen OK	REMOTE98	Default Group	9095551212/5555555	Async95	198.097.24.22

Remote Terminal Server

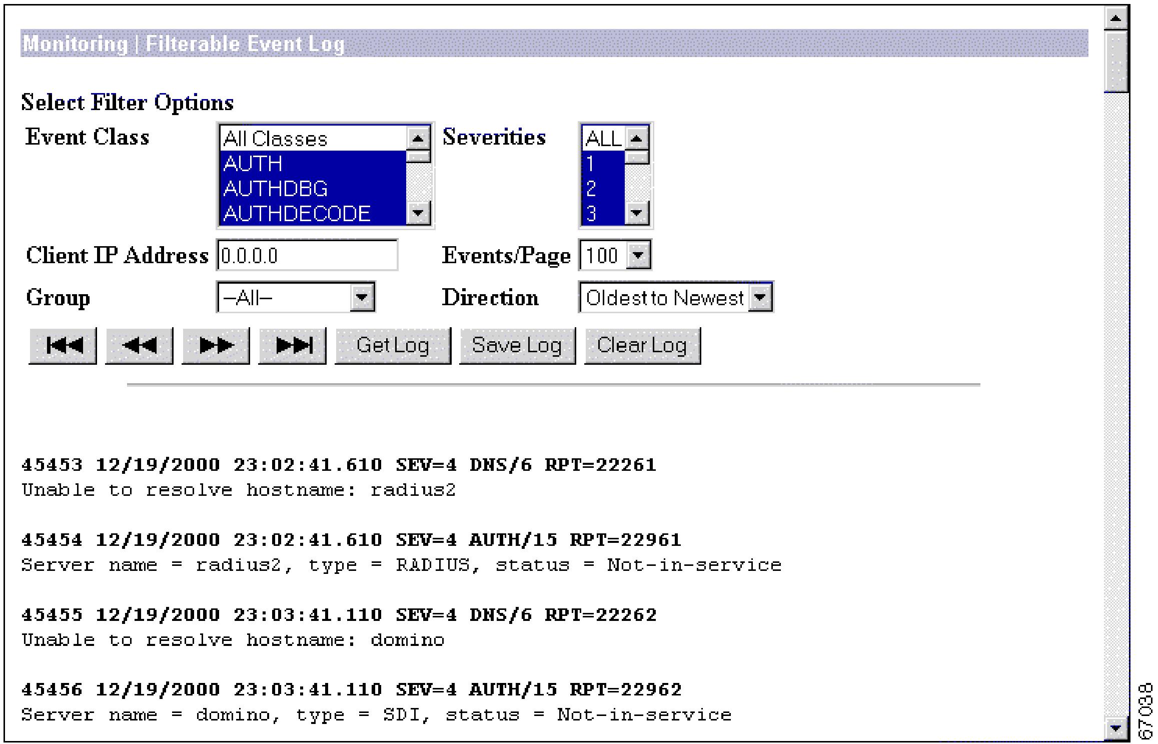
Use the following procedure for printing *Remote Terminal Server* Event Viewer logs. The logs are generated at usage intervals on Windows NT and Windows 2000 Servers and display successful and failed access to the remote terminal server.

1. Open **Event Viewer** from the local PC.
2. Right click on **Event Viewer (local)**. When given the option, choose **Connect to another computer**.

3. A list will appear. Select the name of the Terminal Server.
4. Right click on **Security** and select **Save Log file as**. Save the file as a **text** (.txt) file. Remember the location that you saved the file to.
5. Print out the log file and place in the technical support manager's mail bin.

VPN Concentrator

Use the following procedure for saving and printing *VPN Concentrator* Event logs. The VPN Concentrator records events in nonvolatile memory, thus the event log persists even if the system is powered off. The VPN Concentrator event log holds 2048 events and it wraps when it is full; that is, entry 2049 overwrites entry 1, etc. Use the scroll controls (if present) to display more events in the log.



Event Class: All Classes, AUTH, AUTHDBG, AUTHDECODE
Severities: ALL, 1, 2, 3
Client IP Address: 0.0.0.0
Events/Page: 100
Group: –All–
Direction: Oldest to Newest

```
45453 12/19/2000 23:02:41.610 SEV=4 DNS/6 RPT=22261
Unable to resolve hostname: radius2

45454 12/19/2000 23:02:41.610 SEV=4 AUTH/15 RPT=22961
Server name = radius2, type = RADIUS, status = Not-in-service

45455 12/19/2000 23:03:41.110 SEV=4 DNS/6 RPT=22262
Unable to resolve hostname: domino

45456 12/19/2000 23:03:41.110 SEV=4 AUTH/15 RPT=22962
Server name = domino, type = SDI, status = Not-in-service
```

Fig 2 "

1. Navigate to the Monitoring | Filterable Event Log screen on the VPN3030.
2. Make the following option selections: Event Class=All Classes, Severities=All, Client IP Address= 0.0.0.0, Group All, Events/Page=100, Direction=Oldest to newest.

3. Click **Get Log**. The Manager opens a new browser window to display the file. The browser address bar shows the VPN Concentrator address and log file default filename; for example, 198.128.127.7/LOG/vpn3030log.txt.
4. Click the **File** menu on the *new* browser window and choose **Save As....** The browser opens a dialog box that lets you save the file. The default filename is vpn3030log.txt. Change the name to match the date in mm/dd/yy format i.e. vpn120100. Remember the location that you saved the file to.
5. Print out the log file and place in the technical support manager’s mail bin.

Appendix A

Network Diagram Figure 1 (on next page)

Sample Policy

Remote Access Policy

I. Purpose

The purpose of this policy is to establish the security requirements for eligible employees, physicians, and business partners that require electronic access to [Company Name s] information assets.

II. Policy

Access to [Company Name s] electronic assets from remote locations must be approved by an appropriate [Company Name] executive. If a remote access system utilizes dial-up modems, they must be expressly configured to provide secure network access. Access to [Company Name s] internal network from outside of its defined network perimeter must be controlled by privileged access controls. If Virtual Private Network (VPN) technology is utilized for remote access, then the VPN system must conform at least minimally to the Health Care Financing Administration s (HCFA) Internet usage security policy, which outlines specific requirements for VPN security. Logs of all inbound access into [Company Name s] internal network by systems outside of its defined network perimeter must be maintained. Systems administrators must regularly review these logs, or use automated intrusion detection systems to inform them of suspicious activity.

III. Definitions

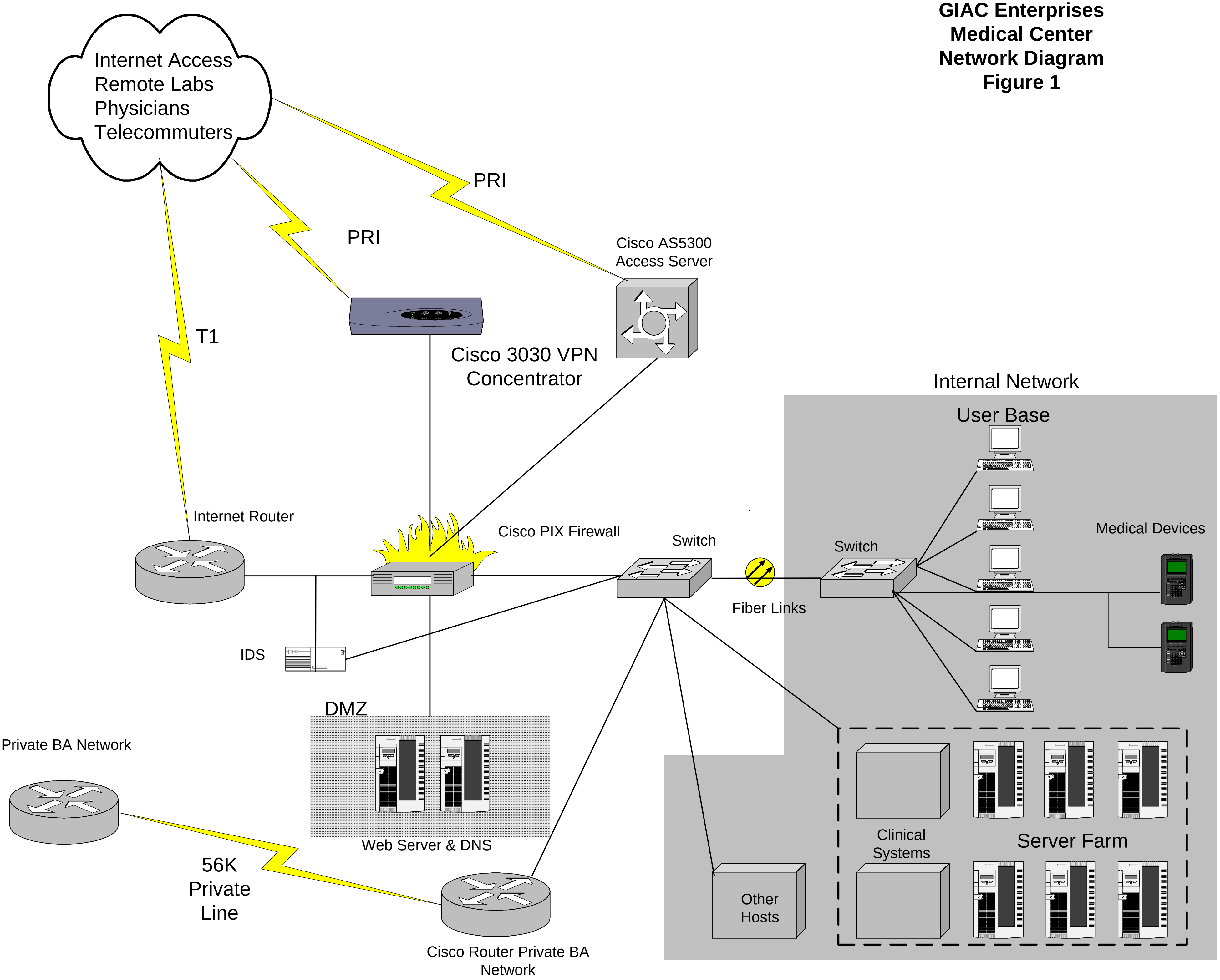
Defined network perimeter — refers to the total internal computer network, which may include secure wide-area connectivity to other external branch site local area networks. Privileged access controls — include unique user IDs and user privilege restriction mechanisms such as directory and file access permissions, and access control mechanisms based on either context-based or role-based criteria.

Context-based access criteria — are access control mechanisms based on the context of a transaction (e.g. time-of-day, location of user, strength of user authentication).

Role-based access criteria — are access control mechanisms based on pre--defined roles, each of which has been assigned the various privileges needed to perform that role. Each user is assigned to one or more pre-defined roles.

IV. References/Related Policies

- Information Systems Access Policy
- Password Policy



GIAC Enterprises
Medical Center
Network Diagram
Figure 1

References

Further information is available through the following:

Information Security Management Handbook Harold F. Tipton; Micki Krause volumes 1, 2,and 3, 4th edition published by Auerback

Cisco Products Web Site http://www.cisco.com

Microsoft TechNet Security Web Site
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp

Sans Institute Web Site Information Security Reading Room
http://rr.sans.org/index.php

[i] Portions of this policy comes from the sample remote access policy (pg.114) in Information Security Management Handbook Harold F. Tipton; Micki Krause 4th edition published by Auerbach

[ii] Fig 2 Taken from Cisco product documentation at http://www.cisco.com/univercd/cc/td/doc/product/vpn/vpn3000/rel3_5_1/admin/filevlog.htm