GIAC
CERTIFICATIONS

# Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering
"Security Leadership Essentials for Managers (Cybersecurity Leadership 512)"
at http://www.giac.org/registration/gslc

# Financial Security through Security Management

© SANS Institute

**Karen S. Urban**

Information Security Officer Training
GISO – Practical Assignment
Version 1.3 (February 7, 2003)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

## TABLE OF CONTENTS


Summary ..... 1

GIAC Enterprises ..... 1

- General Information ..... 1

- IT Infrastructure ..... 2
  - Network Perimeter ..... 3
  - Demilitarized Zone (DMZ) ..... 3
  - Firewall ..... 4
  - Secure Subnets ..... 4
  - Internal Network ..... 4

- Business Operations ..... 4
  - Customers ..... 5
  - Bank Staff ..... 6
  - Third Party Service Providers ..... 6

Risk Identification ..... 6
- Risk 1: Unauthorized Access or Use of Confidential Customer Information ..... 7
- Risk 2: Reduced Availability Due to Critical System Loss or Damage ..... 8
- Risk 3: Loss of Customer Information Integrity ..... 10

Evaluate and Develop Security Policy ..... 11

- Evaluate Security Policy ..... 11
  - Purpose ..... 11
  - Scope ..... 12
  - Policy Statement ..... 12
  - Responsibility ..... 12
  - Action ..... 12

- Revise Security Policy ..... 12

Develop Security Procedures ..... 15

- Password Assessment Procedure ..... 15
  - Purpose ..... 15
  - Responsibility ..... 15
  - Procedure ..... 15

Appendix A – GIAC Network Design ..... 17
Appendix B - GIAC Enterprise Password Policy (1/2001) ..... 18
References ..... 19


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

## Summary

GIAC Enterprises (GIAC) is a fictional bank that is experiencing many of the same challenges that face actual community banks today. In addition to dealing with ever-increasing bank regulations and a tight economy, GIAC is under constant pressure to implement new technologies in order to remain competitive with the products and services offered by much larger institutions.

For the bank to continue to grow and be successful, GIAC must strike a balance between these pressures and sound business practices. Growth cannot come at the expense of customer confidence.

This paper provides an overview of the bank, its network infrastructure, business flow and areas of potential risk. Also included are recommended steps for risk mitigation and improvements to certain policies and procedures.

## GIAC Enterprises

### General Information

Founded in 1917, GIAC Enterprises is a strong community bank headquartered in Austin, Texas. The bank serves a niche market of consumers and small business customers by providing competitive products and services with a level of high quality customer service not generally available from larger money center banks.

For the next seventy-five years, the bank's conservative ownership focused on slow, steady growth and capital retention. In the early 1990's, the bank began to establish branches. A new President and Chief Executive Officer joined the bank in 1997 and under his guidance, the bank moved into a period of modernization and expansion.

Over the next six years, systems continually changed. The bank moved away from manual processes and existing systems into newer technologies including wide area networks, browser based platforms and Internet access. In late 1999, the bank moved away from a twenty-year relationship with a data processing service bureau by converting the processing of core banking applications to an in-house system. During this period of system change came the passage of Section 501 of the Gramm-Leach-Bliley Act of 1999 (GLBA), which outlines requirements for financial institutions to protect consumers' personal financial information. As a nationally chartered bank, GIAC was required to develop and implement an information security program.

As of the end of June 2003, GIAC has grown into a $600 million dollar financial institution. With twelve full service branches, the bank's market now covers not only Austin, but also communities throughout Central Texas. Customers can access their accounts by telephone, voice response (VRU) units, the Internet or



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

any of the bank's fifteen automated teller machines (ATMs). The bank maintains a staff of just over 200 and experiences moderate to high job turnover. Earnings and asset growth continue to be strong, but rapid expansion and regulatory changes have placed pressures on the bank's IT infrastructure.

**IT Infrastructure**

As the IT infrastructure of GIAC Enterprises evolved, management's primary goal was security followed closely by integrity and availability. Three full time staff members perform GIAC's network administration. The network manager, although not new to the bank, is relatively new to his position. To supplement this staffing, the bank obtains certain services from consultants and other third party service providers. These services include, but are not limited to, certain firewall services, firewall configuration, and secure web hosting,

The IT infrastructure is centralized in the bank's three story corporate headquarters that was constructed in the early 1950's. The building was recently renovated to allow for possible tenant lease space in the upper floors. The branch locations connect to the network by either fiber optic or frame relay. These branch locations are either bank owned property or long-term lease space and vary from single purpose stand-alone bank buildings to space in strip shopping centers.

A disaster recovery contract is in place with SunGard Recovery Services to cover its core banking applications and related item processing operations. Short-term recovery services are provided from Scottsdale, Arizona and longer term from a trailer on or near the bank's headquarters. A recent external audit criticized the bank's business continuation plan because of outdated information and lack of testing.

GIAC is running a Windows 2000 operating system and employs the use of central group policies through Active Directory. Dell is the preferred provider for servers and other Intel based equipment. Microsoft has been standardized as the bank's office automation solution. Standard email services are provided using Microsoft Outlook 2000. Select staff members to send secure email use ZixMail. GIAC supports 205 user workstations. Approximately 150 desktops are located within the bank's headquarters and remaining eleven branch locations contain roughly five desktops each. Laptop use is extremely limited. Personal firewalls and anti-virus software from McAfee are installed on each laptop.

Updated anti-virus software is pushed down daily to all servers and workstations from McAfee ePolicy Orchestrator. The bank does not permit remote access to its network or utilize any wireless devices. Staff members are permitted to access the Internet for web and email traffic. Numerous third-party service providers require bank staff members to access customer service interfaces through the web.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Internet banking services are provided to both consumer and commercial customers and the bank accepts communication from GE's public website through the use of secure forms. The ebanking server is running Microsoft Internet Information Server (IIS).

GIAC's network, as shown in Appendix A, has limited external access points and the network design uses a multilayered architecture often referred to as "Defense in Depth." Multiple layers provide additional barriers between GIAC and an attacker and increase security by raising the cost of an attack. GIAC's layering is accomplished through the use of user authentication, access controls (permissions), routers, switches, firewalls, screened subnets, and a network based intrusion detection agent. These layers are supported by policies and procedures for acceptable use, information security, business continuation, Internet banking and physical security.

Utilizing the "Principle of Least Privilege" enhances security layering. GIAC's servers are hardened following generally accepted procedures for Windows 2000 systems. Some of the procedures used in server hardening are installing service packs, disabling all unnecessary services, enabling appropriate password settings and enabling appropriate logging. After the procedures are completed, the hardened server is tested to ensure that the process was performed correctly and that the system is secure.

*Network Perimeter*
The first layer of defense in the GIAC network design is the use of border routers. GIAC has two separate paths into its network from the Internet. The first path processes traffic originated through either Internet banking or secure forms found on the bank's website. This traffic routes through a third-party service provider firewall and is then sent by a dedicated 256K frame relay line to a Motorola Vanguard 6435 on the perimeter of the network. All other Internet connectivity is provided to the bank by a local Internet Service Provider (ISP) through a high-speed cable modem. The bank's ISP performs DNS services to shield the bank. Only the IP address of the cable modem can be seen from the Internet. Traffic received from the cable modem is directed to a Cisco 2651 router.

*Demilitarized Zone (DMZ)*
Although GIAC utilizes a third party service provider as the first line of defense for Internet banking traffic, the bank has placed the Internet banking Web server into a demilitarized zone or DMZ. A Cisco Pix 515e firewall provides the internal network with an additional layer of protection from the Internet. The only traffic permitted through the firewall is port 443 (HTTP protocol over TSL/SSL). The firewall also protects the web server from internal traffic. Network Address Translation (NAT) is used within the DMZ to forward traffic to the private address of the Web server.

To protect the bank's Exchange server and internal network, the mail relay server resides in a DMZ service network.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

*Firewall*
GIAC's second layer of defense is a Cisco Pix 515e firewall that performs stateful inspections. The firewall configurations are set by a Cisco certified technician engaged from a third party service provider. The firewall is set to deny by default, which allows only required services set in the bank's security policy. The firewall also runs NAT to an external IP address range. A network based Secure NetPro intrusion detection agent (NIDS) is installed behind this firewall. The agent monitors traffic from the firewall and is set to alert network admin staff by email and pager of any probable attacks.

*Secure Subnets*
Remote locations are connected to the network through secure subnets. Each subnet is linked to the primary internal network by either fiber optics or frame relay. Fiber optics is the preferred due to its enhanced security, but it is not cost effective for use in branches located outside of the immediate Austin area. Each branch subnet is composed of a Cisco 2651 router, a Cisco 2950 switch, a branch server and user workstations.

*Internal Network*
The central component of the network is the desktops, file servers, daily file backup systems and core bank processing system which are all maintained at GIAC's headquarters. Generally, these servers attach to a Cisco 2950 switch that is behind the firewall and NIDS. The exception is that the mainframe server also attaches to a Cisco 2820 switch to allow a third party service provider to access the server for debit card transaction authorizations. A dedicated 256K-telephone line links the bank to the third party provider.

Other servers maintained in this area are the DNS server (runs active directory and DHCP), the file print server, Win server (tracks all internal computer names for communication), Telebank (VRU) server, Anti-virus server (McAfee ePolicy Orchestrator), Exchange server, Image server (cold storage and certain other components of the core banking application), Teller server (supports teller systems) and the New Account server (supports account opening platforms).

**Business Operations**
GIAC's business flow involves receiving and processing financial transactions to generate a profit for its shareholders. It begins with the acquisition of customers through the sale of products and services to both consumers and businesses. The bank earns revenues when customers acquire and use bank products, such as deposit or loan accounts. This business flow will continue as long as the bank is able to attract and maintain more customers and related financial transactions than it loses through customer terminations. To accomplish this, GIAC must supply products and services that meet or exceed customer financial needs and that are accurate, available and secure.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Each customer and financial transaction results in the creation of a customer record, which is ultimately processed through and stored in a combination of the core banking application and other network applications. These records generally contain a customer's name, date of birth, tax payer identification number, account number, balances as well as other information that federal law considers to be nonpublic personal information (NPI). Federal law and banking regulations established under Section 501 of the Gramm Leach Bliley Act (GLBA) require the bank to:

> "insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer"[1].

These customer records are essentially GIAC's "crown jewels" and they are key to the continuation of the business flow.

*Customers*

As a community bank, GIAC strives to provide competitive products and services with exemplary customer service. Customers are able to choose how and when they interact with the bank. For those who prefer to deal one-on-one with a bank staff member, GIAC provides twelve branch locations with generous business hours to fit most customers' needs. Customers may stop by in person or simply pick up the phone. Branch staff identify the customer by photo identification or by the use of a series of security questions and answers provided by the customer at account opening.

To meet the needs of customers who prefer the self-service approach, the bank offers a telephone voice response unit (VRU), automated teller machines (ATMs), Internet banking and other access devices such as debit or credit cards. These services are available 24/7. Each of these systems must access the bank's core processing system in order to assist the customer in completing a transaction. A balance inquiry through the VRU, a withdrawal from an ATM and a bill payment through Internet banking all use components of the IT infrastructure to gain access to the core processing system.

The customer must first authenticate into a self-service system prior to be given access. The required authentication method varies based upon the information and transactions requested by the customer. Each authentication method is multilayered and based upon something that the customer possesses and something that the customer knows. For example, to withdraw funds from an ATM the customer must possess an active debit card and know the personal identification number (PIN).

[1] Comptroller of the Currency, Administrator of National Banks



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

*Bank Staff*
In order to sell a product, process a transaction or provide customer service, bank staff members must access one or more applications on the network. The core banking application, Microsoft Office applications (Word, Excel and Outlook), and Internet Explorer are utilized daily by almost all staff members.

In continuing with the "Principle of Least Privilege," user access to the network and core banking application is assigned using security templates that are based upon job function. The security templates not only grant access, but also provide further restrictions to user rights within each application. For example, a teller may have read-only rights to a policy folder while the Senior Operations officer has full rights to the folder. A loan officer can inquire into a customer's account but cannot make any changes.

Once a staff member has been authorized for network access by his or her department manager, the bank security officer and the network administrator, the staff member is assigned a user ID and initial password.

GIAC utilizes physical security restrictions to further protect its systems and confidential customer information. The bank has implemented a basic master-key system for each building and limited those staff members possessing the top level key or access code for the perimeter security system. There are numerous restricted areas within each location, including network administration and data processing.

*Third Party Service Providers*
Internet bill payment, debit card processing and ATM driving are outsourced to third party service providers to gain systems expertise and cost efficiencies. Communication with these providers is facilitated primarily through secure web interfaces provided by the third party.

**Risk Identification**
GIAC's "crown jewels" are the customer records and corresponding customer information systems. The value of these records to the bank and the customer has long been recognized and is now protected by federal law (Section 501, GLBA). Bank customer information and customer information systems are attractive targets for attack. Perceived ease of generating quick money through fraudulent transactions and the growing market for customer information are just two of the many reasons why. By performing a quick search, any Internet user can find news sites that report on banks that have been attacked and other sites that claim how easy it is to hack into a bank.

Not all threats originate externally with hackers or other computer criminals. GIAC's rapid IT expansion, moderate to high staff turnover and regulatory changes have created an environment that could encourage internal abuse.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

According to a recent survey conducted jointly by the Computer Crime Institute and the San Francisco Federal Bureau of Investigations Computer Intrusion Squad, 80% of all network abuse originates internally. The internal threat sources often stem from a staff member's carelessness, a disgruntled staff member, or a staff member who joined the bank specifically with criminal intent.

**Risk 1: Unauthorized Access or Use of Confidential Customer Information**
GIAC's use of a user ID and password (single factor) to authenticate into network and core banking applications coupled with its frequent staff turnover heighten the risk of unauthorized access to or use of confidential customer information.

Although single factor authentication is commercially acceptable, it could make the bank susceptible to network monitoring (sniffing), password cracking and other common attacks. Frequent staff turnover could cause new hires to be placed into a job without receiving proper training. In order to cope with staffing shortages, existing staff members may resort to password sharing and eventual disregard for information security policies.

Unauthorized access to or use of confidential customer information could have many detrimental results. The bank could incur financial loss due to fraudulent transactions. GIAC's reputation may be damaged, potentially creating an environment where customers may be lost to competitors. If perceived damage from unauthorized access or improper disclosure is caused to customers, the bank may be found liable in court. Additionally, the bank would be subject to added regulatory scrutiny and possible sanctions.

Numerous steps should be taken to mitigate this risk:

- Implement an effective information security training and awareness program that includes customer information security, acceptable use and password guidance. Training should be provided to all new hires and to existing staff on an annual basis. This training should include a brief test to document the users understanding and knowledge of required policies and procedures;

- Implement a "warning banner" on the network login screen to reinforce the user's awareness and acceptance of bank IT policies. Encourage staff awareness through positive reinforcement tools, that is reward staff for doing things right;

- Strengthen password controls. As a part of the strengthening process, the bank must update its bank's password policy to encourage appropriate password selections and to reduce the threat of password sharing. The network administrator should implement controls available in Windows 2000 (passflt.dll) to eliminate the worst choices of password. GIAC should change its methodology of using the staff member's first


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

initial and last name for assigning user IDs as these are easily guessed. The bank should evaluate its systems to determine its ability to convert to the use of either two-factor authentication or single use authentication. If all systems are not able to function with these stronger authentication methods, management should consider the feasibility of partial implementation on high risk systems;

- Perform periodic password assessments using filtering software such as @stake's LC4. Filtering will not only identify weak passwords, but it can be used to reinforce password policies and further employee awareness;

- Perform regular network vulnerability scans and verify the configurations of the firewalls and routers. The results of these reviews should be used to correct any vulnerabilities found. These scans also serve to audit the bank's procedures for hardening its systems;

- Strengthen the bank's intrusion detection systems by adding a host based intrusion detection system;

- Using sample policies and procedures available from The SANS Institute as a template, GIAC should implement strong incident handling procedures. All impacted staff members should be trained and the procedures tested periodically;

- Perform background checks on all new hires, not just IT staff. Even lower paid staff members have some access to confidential customer information that could be sold to information brokers or used to commit fraudulent transactions and identity theft;

- Centralize GIAC's incoming telephone, fiber and other communications points of entry at each of its locations. Segregation from other tenants should be implemented where branches are located in buildings shared with others; and

- Require the use of secured email, using Zixmail or similar application, for any outbound email that contains confidential customer information.

**Risk 2: Reduced Availability Due to Critical System Loss or Damage**

Bank expansion, technology advances and the reduction of manual processes has made GIAC highly dependent upon its IT systems. In today's world, bank customers expect their services to be available and system downtime is not acceptable.

Directly related to this risk are threats that originate from both natural and environmental sources. These include power outages, storm related damage, data communications failures, hardware failure and misuse of resources. Other


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

threats include the shutdown of systems due to malicious acts from external sources such as a denial of service attack, malicious code or viruses.

A recent audit criticized certain portions of bank's Business Continuation Plan and indicated that it had not been adequately tested. Additionally, GIAC's IT infrastructure is multilayered, however it does not contain adequate redundancies. No fail over plan is in place for border routers, firewalls or communications links such as fiber optics, frame relay and Internet access. A failure in any one of these areas could cause all or part of the bank's network to become unavailable.

Reduced availability due to critical system loss or damage could have many detrimental results. The bank may incur financial loss due to damage of computer equipment and programs, fees for restoration, and lost opportunity due to down time. An unavailable or unreliable system may damage the reputation of the bank, potentially creating an environment where customers may be lost to competitors. An environment where IT systems are mismanaged could lead the bank to be subject to added regulatory scrutiny and possible sanctions.

Numerous steps should be taken to mitigate this risk:

- Implement redundancy by installing an additional border router, firewall and second Internet connection. The firewall should be configured to support stateful failover using an Ethernet link. The second Internet connection should be from a different ISP to continue GIAC's Internet availability in the event the first provider's service or link fails;

- Increase UPS capability. Install a auxiliary power generator to provide emergency power to the bank's network and core bank processing systems housed at the bank's Austin headquarters;

- Implement a fail-over strategy to compensate for an extended outage of the bank's fiber optic or frame relay connectivity to branch locations;

- Update the bank's Business Continuation Plan (BCP) and implement a program to ensure the periodic maintenance of the plan. This should include quarterly review and update of all dated material and an annual review of all critical asset inventory lists, operations and recovery procedures. The BCP should be tested semi-annually. All staff members must be trained and participate in plan testing; and

- Perform periodic testing of back up tapes to ensure backups are performed according to schedule and that the tapes actually restore accurately.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**Risk 3: Loss of Customer Information Integrity**

Key to the bank's continued business flow is the integrity of its customer information and information systems. Accuracy of account balances is just one part of customer information integrity. The customer's identifying information (name, address, tax identification number, etc.) must be correct, the account product must function as it was disclosed to the customer, account access must be as agreed, and the list goes on from there.

As with unauthorized access to customer information, integrity can be compromised from both internal and external sources. Corruption and even deletion of customer information can originate with hacking, malicious codes (malware) and viruses. Most recently, email has been used successfully to launch the Bugbear.b virus that targeted many financial institutions.

Internally, customer information integrity can be compromised through unintentional acts such as errors in data entry. Unfortunately, other internal sources are disgruntled employees and staff members who have become aware of a system vulnerability.

Once again, GIAC's staff turnover and rapid IT growth amplifies these threats. GIAC has implemented numerous systems and software applications in a relatively short period of time. This environment of constant change could distract network administration staff from the important work of system monitoring and logging of information. Errors made in network configurations may go unnoticed as network staff move on to the next project. These errors could open up a vulnerability that could be used to damage customer information records or critical systems. The error rate in data entry and customer file maintenance on customer records could elevate in those departments with frequent turnover. Inadequate training and staff member monitoring contribute to these errors and to the bank's ability to find and correct these issues.

If the integrity of customer information became questionable, the bank would suffer damage to its reputation. This would potentially create an environment where customers may be lost to competitors. If perceived damage is caused to customers and other third parties that rely on the accuracy of bank information, GIAC may be found liable in court. GIAC would be subject to added regulatory scrutiny and possible sanctions.

Numerous steps should be taken to mitigate this risk:

- Utilize separation of duties. All changes must be authorized with a source document. All changes to customer information must be logged and monitored. Any changes made to customer account records by one staff member should be reviewed by a second staff member to ensure authenticity and accuracy.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Monitor the reports produced by the bank's anti-virus software to determine that all desktops, laptops and servers are receiving the anti-virus updates daily. Use a layered approach to anti-virus software by running products from two vendors on different segments of the network;

- Implement a proxy server or content filtering system, such as SurfControl, to screen all incoming emails and attachments as well as outgoing web traffic. Filtering will also mitigate the risk of lawsuits and negative publicity stemming from inappropriate content of email and Internet use;

- Enable floppy drives and CD-ROMs on user workstations on an exception basis only. Any exception must receive authorization from the bank's security officer and network administrator;

- Develop a communications channel to educate staff members on the dangers of viruses, worms and other malicious codes. This must include procedures for notifying network admin if a virus, etc. is suspected in their workstation. GIAC should readily supply anti-virus software to staff members for use on home computers.

- Review and enhance procedures for monitoring audit and system logs from all network devices. Implement a log consolidation tool such as NetIQ's VigilEnt Security Manager;

- Additionally, the bank should install a network integrity system such as Tripwire on all servers and network devices; and

- Enhance change control procedures for firewalls, routers and switches. Require documentation for each change including appropriate signatures for authorization.

## Evaluate and Develop Security Policy

### Evaluate Security Policy

The Password Policy shown as Appendix B is based upon a policy in use at the author's company. The existing policy indicates it was last revised in January 2001 and it may not correlate with the bank's current network environment. It appears to be missing many of the basic components of a good security policy.

*Purpose*
No purpose is stated for the policy and it is not clear what risk, if any, the policy is intended to address. No background information is available. The policy does not indicate if this is a "stand-alone" policy or if it is part of a higher-level policy.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

*Scope*
The policy requires all microcomputers owned or leased by GIAC to be password protected and further requires each employee to establish a password. The policy needs to clarify if it applies to all employees or just a certain area or department. It needs to state whether or not it also applies to temporary employees, consultants or third party service providers.

It is not clear exactly what systems or specific applications on the microcomputer must be password protected. It appears that it may apply only to the network and not specific applications within the network, such as the bank core processing application.

*Policy Statement*
The policy statement is comprised of seven components each of which sets out a specific requirement for the staff member's password. These include password length, general composition, timeframe for change, confidentiality, screensavers and consequences for entering an invalid password.

This section does not provide sufficient guidance for proper password selection. The length and character composition are not enough information to assist the employee in selecting a password that would not be susceptible to password cracking.

*Responsibility*
The policy does not clearly assign responsibility. It does not clearly define where the binding authority for the policy originates or any consequences for noncompliance.

*Action*
The only action required by the policy is to change the password no less frequently than every 45 days.

**Revise Security Policy**
The following policy was obtained from The Sans Security Policy Project (http://www.sans.org/resources/policies/Password_Policy.doc). The policy was revised to fit the needs of GIAC Enterprises.

**Overview**
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of GIAC Enterprises' entire corporate network. As such, all GIAC employees (including contractors and vendors with access to GIAC Enterprises systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

**Purpose**
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

**Scope**
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any GIAC facility, has access to the GIAC network, or stores any non-public GIAC information.

**Related Documents**
GIAC Information Security Policy

**General Policy**
All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis. All production system-level passwords must be part of the information security (InfoSec) administered global password management database.

All user-level passwords (e.g., email, web, desktop computer, core banking application, etc.) must be changed at least every thirty days.

Passwords must not be inserted into email messages or other forms of electronic communication. Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

All user-level and system-level passwords must conform to the guidelines described below.

**Guidelines**
**A. General Password Construction Guidelines**
Passwords are used for various purposes at GIAC. Some of the more common uses include: user level accounts (including core banking application), web accounts, email accounts, screen saver protection, voicemail password, and local router logins.

Strong password construction is essential to the overall security of the GIAC IT infrastructure. All system users must be aware of how to select strong passwords.

*Poor, weak passwords have the following characteristics:*

- The password contains less than eight characters;
- The password is a word found in a dictionary (English or foreign);


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- The password is a common usage word such as: names of family, pets, friends, co-workers, fantasy characters, etc.;
- Computer terms and names, commands, sites, companies, hardware, software;
- Birthdays and other personal information such as addresses and phone numbers;
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.;
- Any of the above spelled backwards; and
- Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

*Strong passwords have the following characteristics:*

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: *Do not use either of these examples as passwords!*

**B. Password Protection Standards**

Do not use the same password for GIAC accounts as for other non-GIAC access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various GIAC access needs. For example, select one password for the core banking system and a separate password for IT systems.

Do not share GIAC passwords with anyone. All passwords are to be treated as sensitive, Confidential GIAC information.

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- Do not use the "Remember Password" feature of applications (e.g., Outlook, Internet Explorer, etc.).


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Do not use another staff member's password, not for any reason.

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every 30 days (except system-level passwords which must be changed quarterly).

If an account or password is suspected to have been compromised, report the incident to the Security Officer and change all passwords immediately.

**Enforcement**
Password cracking or guessing may be performed on a periodic or random basis by Network Administration or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**Revision History**
Version: 1.0
Approved by: GIAC Board of Directors
Date: August 15, 2003

**Develop Security Procedures**

**Password Assessment Procedure**

*Purpose*
To enforce password policy and to verify strong password use or discover weak password use by using one of several 'password cracking' tools. Weak or poorly chosen passwords may result in the compromise of the GIAC network that could result in unauthorized access to or damage to confidential customer information.

*Responsibility*
The Network Administrator is responsible for performing quarterly password assessments under the direction of the Security Officer.

*Procedure*

1. Obtain Password Assessment Authorization form from the shared network admin forms directory. The completed form must indicate which network


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

domains, servers and desktops will be scanned. The form must be approved by the Senior Operations Officer. *In no event should the password filter be run without this authorization.*

2. Verify that systems to be scanned have a recent backup. Test backup tape before beginning the assessment.

3. Run password filter according to directions supplied by software vendor.

4. Print reports to document any passwords that failed the requirements of the password policy.

5. If a password is guessed or cracked during one of these scans, the user must be notified and be required to change it immediately.

6. All first occurrences of failed passwords will be reported to the user's manager and the Human Resource Officer. The user will be required to attend a security awareness training session.

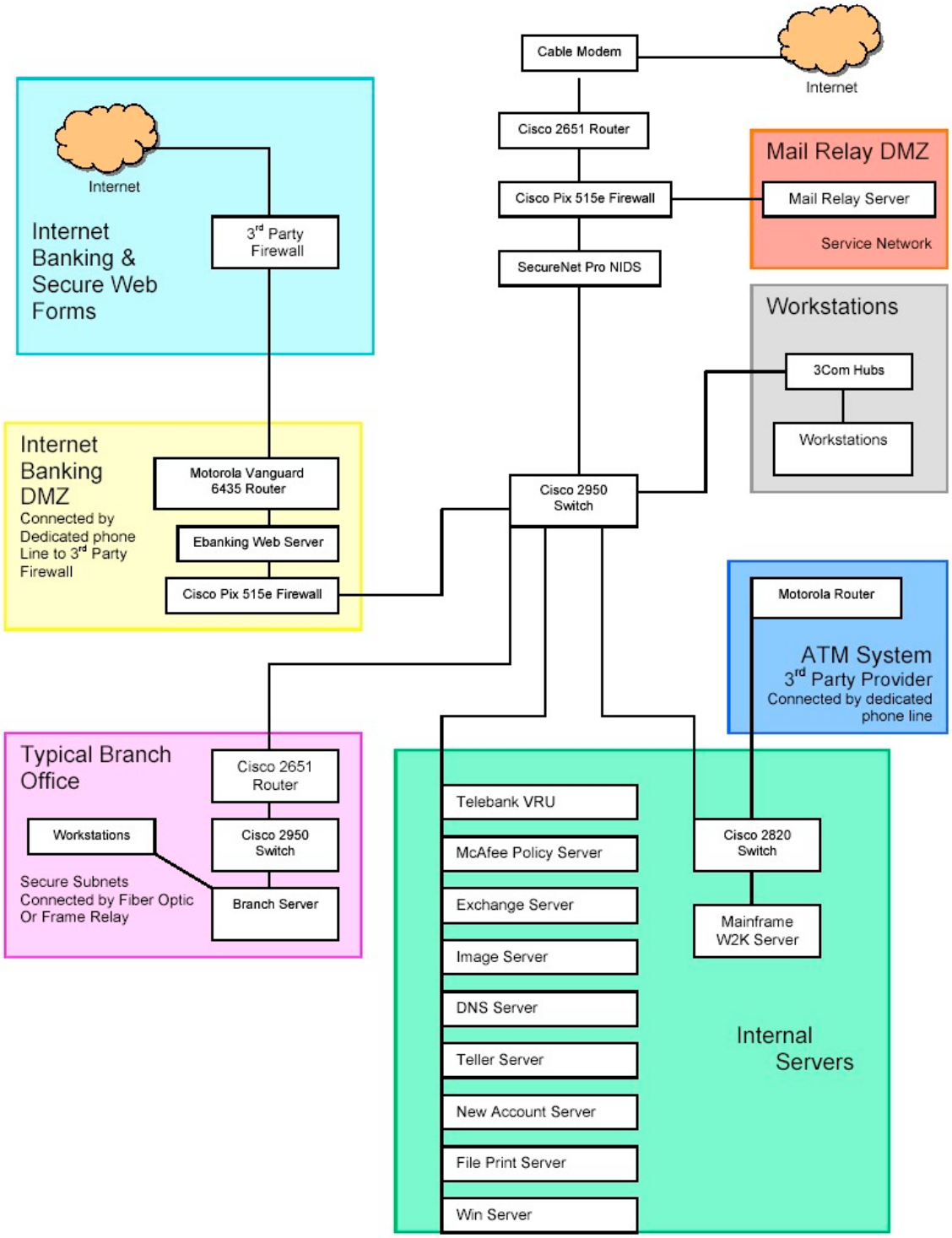
7. If the user experiences subsequent occurrences of password failure, the user account will be disabled.

© SANS Institute 2003, Author retains full rights.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

## Appendix A – GIAC Network Design






© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

## Appendix B - GIAC Enterprise Password Policy (1/2001)

The following policy is based upon a policy in use at the author's company.

All microcomputers belonging to or leased by the Bank, or any computer attached to or that utilizes the Bank's networking system must be password protected, excluding DOS based computers.

A. At no time shall anyone not employed by the Bank be allowed access to any of the Bank's computers. The only exception to this will be vendors and contractors who are working under the direct supervision of the Information Systems group.

B. Each employee shall establish for himself or herself a unique identifying password, 6 to 8 alphanumeric characters in length, with no embedded networks or special characters.

C. Each employee shall change his or her password no less frequently than every 45 days.

D. Each employee shall maintain the confidentiality of his or her password and should not disclose it to any other person. No employee shall request or require any other employee to disclose his or her password. Executive management will reserve the right to require members of the Technology Divisions to disclose their passwords upon termination from the Bank, as needed, to protect the best interests of the Bank and its operating systems.

E. Each employee shall establish a screen-saver password for the Bank computer assigned to him or her, which shall be set to three (3) minutes or less and utilized by the employee if the computer is to be left unattended for more than three (3) minutes, in order to safeguard the computer from unauthorized use. (Win95 Screen saver password)

F. Screen saver passwords are also subject to the confidentiality requirements of section C., above and shall be changed by the employee not less frequently than every 45 days.

G. If you enter your user ID or password incorrectly three or more times, your user account will be disabled.


© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

## References


Network Associates, Inc. “ePolicy Orchestrator™” URL:http://www.networkassociates.com/us/products/mcafee/antivirus/fileserver/epo.htm (31 July 2003).

Brooke, Paul. “Building an In-Depth Defense.” Network Computing. 9 July 2001. URL: http://www.networkcomputing.com/1214/1214ws1.html (1 August 2003).

Microsoft Corporation. “Windows 2000 Security Hardening Guide, Version 1.2.” URL: http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=15e83186-a2c8-4c8f-a9d0-a0201f639a56 (14 August 2003).

Comptroller of the Currency, Administrator of National Banks. “Guidelines Establishing Standards for Safeguarding Customer Information.” OCC Bulletin 2001-8. 15 February 2001. URL: http://www.occ.treas.gov/ftp/bulletin/2001%2D8.doc (2 August 3003).

Richardson, Robert. “2003 CSI/FBI Computer Crime and Security Survey.” Computer Security Institute. URL: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf (12 August 2003).

Guard, Mary Beth and Guard, Michael L. “Physical and Digital Threats to Financial Institutions in the Wake of the Terrorist Attacks” 12 October 2001. URL: http://www.bankersonline.com/security/cyberthreats.html (2 August 2003).

“Password Protection Policy.” SANS Institute – Security Policy Project. URL: http://www.sans.org/resources/policies/Password_Policy.doc (16 August 2003).

Comptroller of the Currency, Administrator of National Banks. “Threat Posed by New Internet Virus (Bugbear.B).” OCC Alert 2003-09 12 June 2003. http://www.occ.treas.gov/ftp/alert/2003-9.doc (16 August 2003)

Rainbow Technologies, Inc. “Two-Factor Authentication – Making Sense of all the Options.” 2 February 2002. URL: http://www.itsecurity.com/papers/rainbow2.htm (15 August 2003).

@stake. “LC4 - The Password Auditing and Recovery Application.” URL: http://www.@stake.com/research/lc/ (15 August 2003).

Cisco Systems. “Using Pix Firewall Failover.” URL: http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_chapter09186a008017278a.html - 1002067 (17 August 2003).

Tripwire, Inc. “Legislation Affecting Bank Security - Ensuring Integrity and Trustworthiness of Electronic Data in Compliance with GLB/OCC Requirements.” Tripwire White Paper. 2002.




© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

URL:http://www.tripwire.com/files/literature/white_papers/GLB_OCC_White_Paper.pdf (31 July 2003).

NetIQ. “Enterprise Security: Moving from Chaos to Control with Integrated Security Management from NetIQ.” 9 December 2002.
URL: http://download.netiq.com/Library/White_Papers/NetIQ_wp_Security.pdf (1 August 2003)

© SANS Institute 2003, Author retains full rights.



© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.