Global Information Assurance Certification Paper

GIAC Design Firm
Design for a Better Future
Mr. Curt Sizemore
Information Security Officer Training – GISO Basic Practical
Version 1.2

Abstract

GIAC Design Firm is a small business providing assistance to companies redesigning the exterior of existing buildings or structures. GDF maintains a main office in Spokane Washington, where 35 office employees work. This document details the GDF IT infrastructure, business operations, and some of the areas of risk. The document also outlines the steps necessary to mitigate some of those risks, as well as outlining the necessary steps to creating Microsoft Active directory accounts for GDF.

Assignment I – Describe GIAC Design Firm

General Description

GIAC Design Firm (GDF) is the largest consulting design company in the state of Washington. GDF was incorporated in 1990. The company's first contract was with the city of Spokane. The company was founded by two brothers and has grown to more than 35 employees spanning seven states. GDF customer base includes government agencies, corporations, and schools. They provide design assistance for redesigning the exterior of existing buildings or structures. GDF overseas the modifications to existing buildings and provides design ideas for current as well as future projects. They are focused on providing strong customer service insuring that each customer is satisfied. Each contract awarded by GDF includes an on-site GDF representative to oversee the work for the duration of the project.

GDF Management: 4 Employees

This group is composed of GDF's President/Owner, Vice President/Owner, General Manager, and Chief Information Systems Security Officer (CISSO). The General Manager must hold at least a MBA and have specialized training in computer systems administration. The CISSO must hold at least a four year college degree. The CISSO must also maintain a General Information Security Officer certification (GISO).

GDF Designers: 6 Employees

Provides architectural plans in support of contracts awarded. The designer meets perspective clients and, with the assistance of the writer/editors, creates contract proposals. All designers are required to have at least a four year college degree, with a specialty in computer aided design.

GDF Writer/Editors: 6 Employees

This team works with the designers to create contract proposals. The team is also responsible for cataloging all documents for archival storage. The members

of this team are required to have at least a four year college degree with experience in writing contract proposals. In addition they must maintain product certification in current Microsoft products such as Word, Excel, PowerPoint, and Publisher.

GDF Information Technology (IT) Department: 3 Employees

This group maintains all IT infrastructure devices, including desktop support, server maintenance and support, and field employee connectivity. In addition this group implements new technology as it becomes available. IT must also maintain an inventory of all IT devices. This inventory includes software and hardware of all devices owned by GDF. Each member is required to have the minimum of a four year degree in Computer Science. In addition all members are required to maintain industry standard certifications such as, Microsoft System Engineer (MSCE), Certified Cisco Network Associate (CCNA), or A+ certification.

GDF Office Staff: 4 Employees

This group provides clerical office support to all employees. This includes maintaining the employee leave calendar, answering phones, and managing the company contact list. Each employee is required to have a two year degree with a focus on Office Automation. In addition each member is required to attend training courses in the use of Microsoft Office in business.

GDF Field Staff: 10 Employees currently (new staff added with each contract)

This group provides on-site contract support for each awarded contract. The employees are required to be on-site at each location through the duration of the contract. The field staff employee will coordinate all work being performed at the site. If changes are required, the field staff will incorporate the change and transmit the necessary information back to the main office. Each field staff employee is required to have a bachelor's degree, with a specialization in architectural design. Each employee must employ the use of a computer aided design program provided by GDF.

GDF Human Resources: 2 Employees

These employees are responsible maintaining all benefit and salary for the company in accordance with local, state and federal law. Each member is required to have a four year college degree, with a background in human resources management. Employees in the human resource department will use an electronic human resource management system such as PeopleSoft.

GDF Legal Department: Not on staff

GDF contracts the Law Office of Levy, Smith and Barnes LLC for all legal issues.

IT Infrastructure

GDF's network consists of routers, switches, firewalls, workstations, and various types of servers. All networking equipment at GDF is made by Cisco. All servers and workstations are manufactured by Dell Computer Corporation. See Table 1 for a listing of model numbers of the networking equipment. The network is divided into three segments behind the boarder router. The first segment is directly connected to the boarder router creating the companies Demilitarized zone (DMZ). The DMZ houses the external Web server, SMTP gateway, and external DNS server. The main switch provides two separate virtual LAN segments (VLANs) for servers and workstations. The border router also serves as the company's virtual private network (VPN) provider. The final entry point into the GDF network is the dial-up router. The dial-up router is firewalled to only allow certain type of traffic from the dial up employee.

The border router is GDF's primary entry point for the GDF network via a T-1 provided by the local internet service provider. This router also provides client VPN support for field employees and the network segment for the DMZ. All servers in the DMZ are Dell 2550 Enterprise servers running Microsoft Windows 2000 Standard server with all current service packs and security hot fixes. The web server in the DMZ runs Apache web services. Microsoft services are used for both DNS and SMTP services. All unnecessary services have been uninstalled or disabled for security purposes. The SMTP server uses Sybari Antigen to scan for both viruses and SPAM email. Each message is scanned with five different virus definition providers. Every server in the DMZ has a documented baseline configuration that is maintained by the IT staff and certified by the CISSO. All data destine for the internal network passes through firewall-1 from the external internet connection. Firewall-1 is running Cisco's PIX based operating system. This firewall is configured to block all unsolicited network traffic. The enterprise router sits between firewall-1 and the main switch. This router also provides the necessary router connection for the dial-up router. The dial-up router is firewalled by firewall-2. The dial-up router employs the use of RSA secure ID and dial back technology. The dial-up router connects to the local telephone company via a T-1 providing 24 dial-in lines. The main switch provides the two VLANs for the main office. The two VLANs are used for end user workstations and the server farm. All workstations are Dell GX400s running Microsoft Windows 2000, with all the latest service packs and hot fixes. All workstation use Dell's on board network interface card. All workstations are configured from tested software images that include Microsoft Office XP Professional (including Publisher) and Norton Antivirus Corporate Edition 8.0 client installed. In addition to the standard workstation configuration the design workstations have AutoCAD installed. All servers are Dell 2550 Enterprise servers running Microsoft Windows 2000 with all the latest service packs and hot fixes. The email server used by GDF is Microsoft Exchange 2000. The email

server uses Sybari Antigen for virus protection. All messages are scanned with five separate virus definition providers. The development web server runs Microsoft IIS 5.0. The RSA Ace server is version 6.2. This Ace server is used to authenticate the VPN or dial-up users. All servers use gigabit network interface cards. All servers have a baseline configuration documented. The baseline information is maintained by the IT staff and certified by the CISO. All field employees use Dell Inspiron 8100 laptops. Each laptop is configured with an internal Ethernet adaptor and US Robotics V.34 PCMCIA modem. The laptops run Microsoft Windows 2000 profession with all the latest service packs and hot fixes. Each laptop uses Black ICE defender personal firewall. The file system is also encrypted with PGP version 8.0. All laptops are loaded from a central image server that includes, Microsoft Office XP Professional (including Publisher), Norton Antivirus Corporate Edition 8.0 client, and AutoCAD. PGP 8.0 is loaded on the laptops for secure communication and transmission of files. Each laptop uses the RSA secure ID client. Secure ID key fobs are used to gain access to the laptop. Contract files are encrypted using PGP 8.0. All Designer, Writer/Editor, Management, IT staff, and Field employees are given a PGP private key. This key is used to digitally sign and send encrypted documents. All keys are housed on a central server. Copies of those keys are stored in a bank safety deposit box. Files are encrypted using PGP version 8.0 desktop. Upon termination of an employee the private encryption key is returned to GDF. The key is then revoked and archived. If the laptop is lost or stolen, the PGP key is revoked immediately upon discovery of the loss. See Figure 1 in Appendix A for a graphic version of this description.

Physical Security

GDF data center is a key part of GDF conducting business. The data center is protected by a magnetic key card system provided by KeyTronics. Access to the data center is limited to Management, CISSO, and IT staff. Unauthorized staff must be accompanied by an authorized staff member at all times. For fire protection GDF uses the following:

- Fire door to the server room
- Fire suppression system
- Fire detectors
- Fire alarm system which automatically notifies authorities
- Fire system tested and certified annually

In the event of a fire emergency, GDF has a well documented emergency evacuation plan. The climate in the room is controlled and maintained to strict guidelines. The room environment is monitored by an IMS 4000 by Sensaphone. This system is configured to notify the IT Staff if the temperature in the room changes two degrees or more. The entire room is powered by an APC Symmetra Power array. The batteries in the power array are tested monthly

automatically by the UPS. The batteries are on a preventive maintenance plan with the manufacture.

Business Operations

GDF is a fast growing small company that relies heavily on the GDF IT infrastructure. GDF provides customers with state of the art design to update and improve the appearance of existing buildings. Potential customers contact GDF when they have buildings that need to be redesigned. GDF visits the potential customer and photographs the existing structure. In addition a GDF employee meets with the company representative to establish a business relationship. Information and data collected at the job site is transported back to the main office. The Designer and Writer/Editor begin the process of creating a contract proposal. The Designer will use the photographs to create a three dimensional model of the potential redesign. Using the 3-D model, the designer will develop a preliminary list of materials needed. In addition, the Designer will estimate the time and total cost of the proposed job. The 3-D graphic design will be performed with AutoCAD. The cost and time estimations will be calculated using an in-house Estimate database, created in Microsoft Access. This database includes data collection of all contract projects previously performed by GDF. The Designer will provide the Writer/Editor with a graphical design and list of materials. The Writer/Editor will take this information and put it into contract form. The contract will be created using Microsoft Word XP. The Writer/Editor and Designer will meet with the General Manager of GDF and the General Manager must approve the proposal prior to the contract being finalized. The Designer will then meet with the customer to present the proposal and answer any questions. If modifications are necessary, the Designer will send the modifications to the Writer/Editor. The Writer/Editor will make the necessary changes to the contract. The Designer will then meet with the General Manager for approval of the modified contract. The document will then be transmitted through the GDF email system using PGP encryption to the customer. The public encryption key will be provided to the potential customer prior to the document being transmitted. If electronic transmission is not available the document will be couriered to the customer. After the contract proposal is accepted GDF will begin making arrangements for the on-site field employee. The IT staff will determine what type of connection should be used. If the new company already has high speed internet access then VPN access will be used, provided this is acceptable to the new customer. Dial-up lines are ordered in the event that VPN is not an option. This dial-up line will be used only for the purpose of connecting to GDF. Since this extends the network perimeter of GDF, the plan for connection must be pre-approved by the CISSO. Once on-site the field worker will begin the process of contracting the work. The on-site field worker will be the new company's primary point of contact at GDF. The field worker will hold a certified copy of the contract. If contract changes are requested, the field worker must submit the change to the main office for approval. This will be accomplished using PGP encryption through the GDF

email system. Change proposals will only be accepted through the GDF mail system. After the change has been approved by the General Manager at GDF, the amendment to the contract will be transmitted back the field worker using PGP encryption. Upon completion of the con tract the external connection to the GDF network will be terminated. The contract will be archived and final cost data will be collected and added to the GDF estimation Microsoft Access database.

Table 1

Device	Manufacture	Model	IOS version
Border Router	Cisco	2621	12.2 (T)
Enterprise Router	Cisco	2621	12.2 (T)
Main Switch	Cisco	4000	6.3
Border Firewall	Cisco	Pix525	6.2
Dial-up Firewall	Cisco	Pix525	6.2
Dial-up Router	Cisco	AS5300	12.2 (T)

Assignment 2 – Identify Risk

Areas of Risk

GDF has been in business for more than ten years. During this time GDF has accumulated customer data that is used to estimate future projects. This data is vital for GDF to conduct business. GDF uses an in-house database to manage this data. This database is only access by GDF employees with the proper security. The GDF Estimate database is the crown jewel of GDF. The individual contract files are equally vital to GDF business. The contract files hold the raw data that is used to create the estimate database. Theft of these files, by outsiders or internal employees would be detrimental to GDF business. If acquired by a competitor, these files could be used to under bid contracts being pursued by GDF. If the files were deliberately altered or deleted by GDF employees the result would be over or under bidding of projects resulting in loss of revenue. By providing internet access for the GDF employees, GDF risks are similar to those of other companies. Malicious software or viruses could enter the GDF network. GDF also relies heavily on the companies file and email servers. While it is not practical to address all susceptibilities, this document focuses on four possible targets that would have the greatest impact on GDF business. The four primary areas of risks are:

1. Firewall-1 comprise will cause entire network collapse.
2. Introduction of virus or malicious software to attack the GDF network.
3. GDF estimate database corruption
4. Access to GDF contract files

Risk 1: Firewall-1 comprise will cause entire network collapse

IT resources can be significantly damaged or comprised by unauthorized individuals. By providing field workers connectivity to the internal network GDF has dramatically increased the threat of a possible attack from sources outside GDF. Firewall-1 is the only means of protection for the GDF internal network when connections are made from the internet. If the main firewall is breached the entire network is wide open to the internet. If a hacker gained access through Firewall-1 they could access every system in the GDF network. The GDF Estimate database would be at risk which is the company's crown jewels. The database is used to estimate new contract proposals. GDF also maintains architectural drawings of customers. These drawings could show access points into a secure physicality, as GDF has many government agency customers. This could cost GDF many dollars in lost revenue if GDF files are compromised.

Prevention

In order to reduce the risk, the operating system on Firewall-1 is running the latest version. The firewall also has a well documented configuration. This configuration is certified by the CISO. When firewall changes are required, prior approval must be obtained by the firewall administrator prior to implementing the changes. Each router in the network uses Network Address Translation (NAT), providing an extra layer of protection against attacks if the firewall is breached. The management port on the firewall is only accessible from inside the GDF network or through a secure VPN connection. The VPN connection requires the use of the RSA secure ID. The management port requires SSH telnet services be used to manage the device. Being located in the data center also provides physical security to the device.

Mitigation

While it is impossible to fully eliminate all risks, the following suggestions would help to reduce some of the vulnerabilities.

- GDF could purchase a second firewall. In the event of a breach, the stand-by firewall could be put into place. This would allow the breached firewall to be removed, and the GDF network repaired. The purchase of a stand-by firewall would also be useful in the event of hardware failure.
- GDF could purchase another firewall to place in series with the current firewall. This provides a "speed bump" in the event the outer firewall is breached. This may give GDF time to notice that a change has occurred and shut down the external internet connection.

Risk 2: Introduction of a virus or malicious software to attack the GDF network

Viruses, worms and malicious software represent a major concern for the IT industry. Since the attack of the well known "Melissa" email virus, many companies have realized that viruses can cause significant down time,

translating to lost revenue during remediation. When attempting to reduce the possibility of infection by a virus it is important to look at all the possible entry points and attempt to reduce each of these points into your network. Also a key element to discuss is selection of an anti-virus software vendor. GDF uses the following steps to evaluate potential anti-virus vendors:

- How often are the virus definition files updated? These files should at least be updated weekly. Many viruses are created daily.
- In the event of a major virus out break, does the vendor provide "quick" virus definition updates? If you find one vendor that provides the virus definition files quickly, this could reduce your possible infection window. This can quickly translate into money saved.
- Does the software provide an option to scan files with multiple virus definition files? You will find that by putting all your eggs in one basket is not always the best choice. Scanning files with different vendors may result in finding a potential virus that one vendor might have missed or can't detect.

Prevention

GDF has a multi-step anti-virus approach. To the best extend possible GDF scans all data at every entry point into the GDF network. All email that is processed by GDF is scanned for viruses. The SMTP gateways use an anti-virus program made by Sybari, called Antigen. Antigen scans every message real-time with five different virus definition manufactures. These vendors include: Computer Associates, Symantec, Sophos, Norman, and Network Associates. This provides good protection, since no one vendor may be able to detect newly created viruses. Antigen also provides for "file stripping"; this helps to reduce possible threats from files that may be undetected by the anti-virus vendors. By stripping all files that can execute automatically, this dramatically reduces the risk of infection. Antigen also checks daily for virus pattern file updates. In the event of an out break the IT staff can force the software to apply the update; this helps to reduce the window of exposure. The internal email server is also configured in the same way. This also helps reduce the possibility that an attack can be launched from inside GDF. The software will quickly catch any files that may be launched by GDF employees. Finally the workstations and laptops have local virus scanning installed. The product installed locally is Norton Anti-virus Corporate Edition (CE) 8.0 client. All workstations and laptops on the GDF are required to have Norton anti-virus CE installed. All workstations and laptops get virus pattern file updates from a central CE server. All settings inside the CE client are locked and the users are unable to change any setting. Both real-time and email scanning is enabled. Any input media (floppy and CD-ROM) placed in the workstation or laptop is scanned for viruses immediately upon access. All GDF servers also have Norton CE installed, with real-time virus protection enabled. To further reduce the risk of viruses on the file servers and email servers, no email clients are installed on the servers.

GDF has a scan schedule for all devices. This will help to identify viruses that may have been delivered before the virus was known by the industry. All file servers, email servers, workstations, and laptops are manually scanned weekly. In the event of an out break all systems are scanned immediately after the virus definition files have been updated.

Mitigation

While GDF has taken steps to reduce the potential against virus attacks here are some areas that can be improved.

- Currently GDF only has one server providing virus definition updates in the enterprise network. By setting up multiple servers this would provide GDF with redundancy in the event the primary server is unavailable.
- Currently GDF laptop users connect to the enterprise network for virus pattern updates. Since many of these systems use private network connections on site, they should be configured to pull the updates from Symantec directly, in the event the GDF network is unavailable.
- While GDF uses SPAM filtering on the SMTP email servers, this may be improved by a subscription based content filtering service. The current system is labor intensive for the IT staff to manage. While SPAM doesn't always contain viruses, it could lead users to internet sites that may be created for the purpose of spreading viruses.

Risk 3: GDF Estimate database corruption

For ten years GDF has collected data on all projects completed by GDF. This data is vital to providing the Designers with information on creating cost estimates for new contracts. Since many potential customers don't have unlimited budgets, it is very important that the designer give the best possible estimate for the proposed work. In addition to providing estimate information, this database also is the company's archival record system. This database was developed by the company's owner when the company started ten years ago. The database is access by all Designers in "read" only mode. The database is updated by the database administrator, with guidance from the owner of GDF.

Prevention

GDF limits the "write" access to this database to reduce the possibility of corruption. Values placed in the database have validation rules, such that the information entered must meet certain criteria. This helps to reduce the possibility of placing data in the database that is not accurate. Regular consistency checks are ran of the database, this helps to reduce records that may be corrupted. The database is housed on a server that uses RAID level 5 technology. This helps to reduce the risk of actual hardware failure. The full

database is backed up nightly to backup tape. The backup tapes are stored off-site in a secure location. One year of backup tape is retained for this database.

Mitigation

GDF relies on the use of this database in the daily business of the company. Here are some ways that GDF may reduce the threat of corruption of this asset.

- Currently this database uses Microsoft Access XP. While Access XP is sufficient GDF may find greater reliability with a more robust database engine, such as Microsoft SQL 2000. SQL would provide GDF with greater security and integrating checking. Also SQL would increase the performance of the database. Currently when records are updated in the database the entire Access XP database is re-written. SQL on the other hand only updates/adds the individual record that is being accessed. Microsoft SQL may be cost prohibitive to GDF as the server software is expensive. Also you would need to hire additional staff to manage the SQL server.
- While GDF backs up the data nightly, GDF could consider performing disk to disk backups through out the day. This would reduce the number of records lost since you could use the last disk backup, instead of pulling the data from the previous night's backup tape.
- Installing this database on a mirrored/clustered server would help reduce down time. This would provide GDF with a stand by server that could be used in the event of a server hardware failure. This could prove to be cost prohibitive at GDF.

Risk 4: Access to GDF contract files

Over the course of conducting business for the past ten years GDF has accumulated a large number of contract files. These contract files are used as templates to create new potential contracts. The Designers and Writer/Editors use these files on a daily basis. These files are storage in a central location so all Designers and Writer/Editors can access the files. These files are critical for GDF to conduct business.

Prevention

The GDF contract files are stored on the main File serbver on the GDF network. As stated previously GDF uses all Microsoft Windows 2000 Standard servers. The file system used for storage is NTFS. NTFS provides GDF with individual file level security. The disk used to house this data is configured for RAID level 5 technology, this helps to reduce the possibility of hardware failure. The security model followed at GDF uses the "Principles of Least Access". Only users who

need access to the contract files receive this access. Below is a listing of what staff members have access to these files and what type of access level rights:

Staff	Type of access
Management	Full control
IT Staff	Full control
Designers	Limited access, read only
Writer/Editors	Limited access, read only
Field workers	Limited access, read only to current contract
All other staff	No access

All access levels are controlled by security groups. The above users are added to the security groups based on the needs of the employees which are determined by the general manager. GDF also uses PGP signatures for authenticity. All workers with access to the contract files are required to have a PGP signature. Using the PGP signatures and time/date stamps, GDF has developed a procedure for version control. This procedure is not included in this document. The IT staff is required to add the new contract files to the filing system, under the guidance of the management staff. These files are backed up nightly. The tape backups are stored at an off-site environmental controlled locked room.

Mitigation

GDF has taken many steps to ensure that this data is protected against loss. Here are some additional steps that can be taken to help further reduce the risk of loss.

- While files are backed up nightly, this only provides GDF with a restore of files backed up from the night before. This in fact still could cause GDF loss of data as files could potentially be damage before the backups occur. One way to reduce this risk would be to setup a server that is replicating this data real-time. As files are changed or added to the system, they could be added to a separate server automatically using Microsoft's RoboCopy. Since RoboCopy doesn't require any special hardware this could be any server that has free drive space.
- GDF could deploy a document management system. This document management system would monitor the changes and updates preformed. Many document management systems provide companies with features that reduce the problem of document version control. Currently at GDF document version control is a problem.

Assignment –3 Evaluate and Develop Security Policy

The following policy is based upon a policy in use at my company. The policy has been sanitized to protect the company. See appendix B for the policy evaluated.

The purpose statement is adequate. The statement states the general purpose for the policy, as well as, defines my company's resources. It establishes a risk management program and a company-wide security awareness program. The policy requires the creation of procedures for detection by some intrusion detection system. Lastly the purpose begins to define the responsibilities of IT resources.

The Scope of this procedure is needs work. The scope doesn't clearly define who the policy applies to and needs to be expanded upon.

The Policy statement should contain additional information. While the policy statement begins to discuss the computer accounts, known as User ID, it leaves out important information about how passwords are managed. In addition, it doesn't address how access rights are removed once an employee has separated from the company. There is no information regarding virus protection requirements for all company computers. Nor does it address the policy prohibiting employees from bringing personal computers into the work place.

Responsibilities

The Responsibilities section does a fair job of addressing the issues. It first deals with general employees. There is no mention of the requirement of each employee to attend a mandatory security awareness program. The system administrators section needs work. The section doesn't address backups, server virus protections, or disaster recovery plans. In addition, no formal review process was established. On a positive note, the roles are defined adequately. Each role is clearly stated and well defined.

The Action section is missing from the policy. This will need to be addressed. The action section should include information about who is required to transmit the policy. This should detail how the policy arrives to each employee. It should also include information on when this transmission should occur.

Here is the revised/rewrite of the policy adapted for GDF.

GDF Manual: Information Security Manual
Section Name: Protection of Companies IT Resources
Issued Date: 1/1/2003
Revision date: Due 12/1/2003
Approval: _____ John Doe, President

I. PURPOSE

This issuance establishes policy for the protection of the physical, financial, and information resources, as well as the reputation, image, legal position, and other tangible and intangible assets of GDF.

This policy will:

- establish a risk management program commensurate with the criticality and sensitivity of information resources to GDF
- increase company-wide awareness of and compliance with applicable laws, regulations, policies, standards and procedures
- establish security requirements for design, development, implementation, and operation of information technologies (IT) and systems
- outline procedures for detecting, evaluating, reporting, and addressing threats to or disruptions of, normal operations
- delineates responsibilities for the stewardship of GDF's information resources

II. SCOPE

This policy applies to all employees at GDF. This policy applies to all equipment owned by GDF.

POLICY

GDF information resources shall be managed to ensure the appropriate degree of security, confidentiality, integrity, accessibility, authenticity, reliability, and accuracy based on the criticality and sensitivity of the information.

Education

All new GDF employees must attend a mandatory security awareness course. This course will cover both IT security policies along with physical building security. The course must be completed by the end of the second month of employment. All employees are required to attend a mandatory annual security awareness program.

User ID creation

GDF individuals shall be formally authorized for access to information resources, and shall exercise all authorized access to computer-based information and systems through an electronic identity (commonly called a "User ID" or a "computer account") that maps uniquely to her/him. The computer-controlled limits on what can be done by the "User ID" will be expanded – from the standard default of no access – only enough to assure that the individual's assigned duties can be performed, a so-called "least privilege" configuration. In special circumstances, an individual may have more than one "User ID" assigned; but

each “User ID” must map uniquely to him/her and may only be used by him/her. The level of trust vested in the employee shall be determined on an individual basis based on the individual job function and the results of the background checks.

Password procedure

Each unique User ID provided will be assigned a password. Each password will contain a minimum of eight characters. This password will be changed every 60 days. The password must meet complexity requirements. The complexity requirements state that the password may not include any part of the User ID. Three of the four complex characters chosen must be special in nature, example: uppercase, symbol, numeric, or lowercase. Please see the GDF Password Policy V1.3 for full details. When the administrator initially creates the account, he/she will set up the account such that the default password will change the next time login is attempted. At this point the end user is the only person with knowledge of the password. If however the password is forgotten, the Administrator will reset to a standard password thus, restarting the process. Passwords should never be written down where they may be seen by others. The system also keeps a record of the last ten passwords used; this is to prevent the user from choosing the same password each time. After the password has been successfully changed, the user will be unable to modify the password for six days, unless authorization is obtained by a management official. In addition to the above password procedure, the field employees have an additional security step. GDF mandates that all remote dial-up or VPN connections use RSA security tokens®. This token is comprised of two parts. The first part consist of a user selected 4 digit PIN number, in addition to the four digit PIN number, the token contains a six digit random number sequence that changes every sixty seconds. GDF mandates that all dial-up connections are performed with dial back technology; this is a requirement of the GDF Dial-up policy V1.2.

Access rights

All access rights are determined by a management official, in accordance with the GDF Access Rights Policy V1.4. The management official will then instruct the administrator to carry out the rights assignments. Rights assignments work off the “principle of least privilege”. Upon separation from the company the management official will need to notify the administrator for access changes. The management official will also need to make any adjustments access rights based on job duty changes.

File encryption

All files not accessed in 30 days must be encrypted, with the exception of files located on the Field user laptops. All data on the Field user laptops must be encrypted at all times.

General Disaster Recovery

All data will be backed up each night. The most current backup will be stored at an off site location in an environmentally controlled space. Backups will be tested weekly to ensure that they are usable. Each server will have a documented disaster recovery plan. This plan will be tested every 6 months and updated as necessary. All Administrators are required to be accessible 24 hours a day either by phone or on site. A rotational schedule will be established to fulfill this need. In the event of a Field laptop failure, the IT department will have spare laptops that can be mailed to the remote user.

IV. RESPONSIBILITIES

A. GDF general employees

All GDF general employees are responsible for:

- being knowledgeable of and adhering to this policy and other GDF policies, federal laws, federal regulations, standards, and procedures pertaining to information protection and system security
- taking no action to compromise the security, integrity, reliability, or authenticity of data, information or systems
- reporting immediately any known or suspected compromise or threat to sensitive or critical information or to an IT system administrator or a management officials
- protecting and securing sensitive information from unauthorized disclosure. This includes, but is not limited to, practices such as leaving your computer unlocked while away from your desk and leaving your computer powered on at the end of the work day.
- protecting and securing software and hardware assigned to or used by them, this includes, but is not limited to encrypting all files that are transmitted via email
- using the assigned unique personal identifier, User-ID, digital certificate, RSA identity token. It is imperative that employees safeguard both personal identifier(s) and associated pass-code(s). This includes, but is not limited to the sharing of passwords among co-workers or recording the password to be used by any other employee
- abiding by equipment, software, or access controls and configurations assigned to them unless specifically authorized by the system administrator to make a modification. This includes accessing only the computer equipment specifically assigned to you by a management official. No sharing or borrowing of computer hardware is permitted by GDF employees. At no time will non-GDF computer hardware be permitted within the boundaries of GDF company property
- reading and agreeing to the terms outlined in the " GDF Confidentiality Agreement"

- complying with legal requirements governing use of software licenses, copyrights, and trademarks. No un-authorized software will be loaded on GDF computers. The IT staff will make weekly random inspections to identify the use of unauthorized software. If upon inspection, it is discovered that non-authorized software has been loaded, privileges will be immediately revoked. Such violation is grounds for the immediate termination of all parties involved

B. Management Officials

Management Officials are responsible for adhering to all general employee policies as well as:

- ensuring employees are informed of and comply with all applicable federal laws, regulations and policies related to this policy as well as complying with all GDF policies, standards and procedures
- authorizing access privileges for individual employees and conveying such authorization and any restrictions to the systems administrator
- ensuring the immediate termination of relevant access privileges by promptly notifying the systems administrator when the authorized association or a specific information resource has been terminated
- consulting with both the Human Resources Management Office (HR) and the Chief Information Systems Security Officer (CISSO) prior to assigning the level of position sensitivity for all supervised employees
- ensuring all IT staff that are responsible for critical systems either rotate out of their normal job responsibilities or take leave during each leave year. During this time all job responsibilities should be performed by another member of the IT staff, ensuring critical operations are not person-dependent

C. System Administrators

System administrators are responsible for:

- complying with GDF IT standards and procedures
- documenting authorizations from manager(s) for the granting of unique or non-standard access to information resources for GDF employees
- conducting duties with the least authority necessary to perform a given function. This includes using two accounts to perform job functions. Each system administrator will have two User IDs, one with standard user access and the other with administrative privileges. The Administrator must perform administrative functions with the administrative account as described in the previous statement
- providing access to information resources according to the principle of allowing the least privilege access necessary for each user, organization,

or process, operating within their span of control in compliance with the management official

- planning, designing, recommending to managers and operating such physical, technical, and procedural actions necessary to preserve the integrity, authenticity, reliability, accuracy, confidentiality, and accessibility of information resources and systems. This would include: nightly backups, virus definition updates, software patches applied and tested disaster recovery plans
- rotating out of the normal job responsibilities or taking a scheduled leave during the course of the leave year. During this leave, all job functions should be performed by another employee to ensure system integrity and proper operation are not person-dependent

D. Business Stewards

Business Steward is the management official to whom responsibility for the company's mission objective is assigned. In addition, this person directs or controls the budget, personnel, and information resources necessary to accomplish that mission.

The Business Steward is responsible for:

- determining the sensitivity level of data
- determining the level of system criticality
- assessing risk to, and vulnerabilities of, GDF information resources periodically, and responding in a coordinated manner to resolve vulnerabilities and address risk either by control measures or by acknowledging it as a "residual risk"
- establishing and maintaining a security plan, contingency plan, disaster recovery plan, and continuity of operations plan (COOP) as well as accrediting and authorizing the plans
- establishment, operation, change, and retirement of resources
- assigning the technical steward(s) for the information resource
- determining the access rights/restrictions for system users in consultation with CISSO
- conducting risk and vulnerability assessments periodically, including tests of security and contingency plans
- establishing and enforcing procedures needed to create an appropriate trust environment necessary when work must proceed before required background checks are available

E. Technical Stewards

Technical Steward are persons, other than the Business Steward, who function in the role of either a principal investigator or principal user of an information system or as the principal information technology professional responsible for

the system. The primary role of the technical steward is to ensure that the specified functional characteristics of the system are produced as authorized by the Business Steward.

The Technical Steward is responsible for ensuring that systems and applications function in compliance with all appropriate IT laws, policies, and standards and in accordance with her or his organization's protocols and procedures, as established in the applicable security plan.

This responsibility includes:

- planning, designing, testing, and implementation of operating systems and technologies – whether new or recently revised. This should be done carefully and in collaboration with fellow technical stewards and other technical staff to ensure the overall security and integrity of all GDF information resources
- managing and overseeing all security requirements
- applying access restrictions directed by the Business Steward
- taking the necessary corrective actions immediately in the event a critical or sensitive system or information resource is suspected to have a serious vulnerability
- identifying and taking necessary corrective actions to reduce risks, nonstandard conditions, and unauthorized activities
- maintaining inventories of information resource assets, e.g., hardware, software, and data. Reports of these activities should be provided to GDF officials on a regular basis
- determining, according to the established standard, when it is necessary for an employee to sign a Confidentiality Agreement; therefore, assuring that the agreement reflects currently assigned accesses and authorities and that it is signed and on file before the individual is provided with the intended accesses

F. GDF Chief Information Systems Security Officer (CISSO)

The GDF Chief Information Systems Security Officer is responsible for:

- providing technical leadership and coordination of GDF's overall information security program
- coordinating the development, updating, and implementation of technical standards and control techniques necessary to ensure compliance with federal information processing standards and GDF policies and procedures
- identifying and maintaining a current inventory of GDF's critical assets. This list should be reviewed with Business Steward on a routine basis
- evaluating the relative importance of each asset in the inventory (criticality), assessing risks to the most important (vulnerability), and

identifying interdependencies among internal systems and between internal and external systems
- coordinating the development of, as well as archiving and updating security plans for all critical assets
- designing, planning and conducting intrusion tests. Evaluating testing results and identifying risks based on these results. The results of the intrusion testing should be routinely reported to designated agency officials

G. Human Resources Management Office

The Human Resources Management Office (HR) is responsible for:

- ensuring that positions are designated with the appropriate sensitivity level
- conducting necessary background checks on GDF employees as required
- creating, maintaining, and promoting a role-based security training curricula
- identifying, advertising and presenting appropriate training aimed specifically at maintaining technical skills and knowledge across the variety of staff assigned to the various information resource roles

Action

Mr. John Doe will be presented this policy no later than 1/1/2003. Once approved, Mr. John Doe will transmit this policy to all management officials. The Management officials will then transmit to the employees. Employees will be required to have completed all mandatory security training by 2/28/2003.

Assignment 4 – Develop Security Procedures

Background
This procedure will detail the steps necessary to provide a user with access permissions, based on the security policy modified above. This procedure will detail the steps needed for office staff. This procedure will document the steps that Management officials and Administrators need to perform. With out this procedure GDF would be at risk of providing users with rights that could cause data loss to GDF. This procedure will be revised quarterly until 1 year has passed. At that point the procedure will be reviewed yearly. All updates and changes to this procedure must be fully documented and approved by the Chief Information Systems Security Officer.

New Employee Access permissions

GDF Procedure: Granting new employee Access permissions
Issued Date: 1/10/2003
Revision date: Due 4/10/2003
Approval: _____ Joe Security, CISSO
Approval: _____ John Doe, President GDF

Human Resources

1. HR performs the necessary police check
2. HR assigns User ID (lastnamefirstintial@gdf.com)
3. HR gives User ID to Management Official

Management Official

1. Based on the job hired for Management Official decides what user level access is needed, in accordance with the GDF Access Permission Policy V.14.
2. Management Official goes over the Information Security Manual for GDF. The new employee acknowledges that he/she agree with the policy by signing the policy.
3. Management Official then instructs the Administrator to create the User ID and apply the appropriate permissions

Administrator

1. The administrator uses Microsoft's® "Active Directory Users and Computers" to create the User ID in active directory.
    a. Right click on the "Users" OU and click "new"
    b. Type in the user information requested, example :last name, First name, etc
    c. Enter the User ID supplied by HR

d. Place check on “User must change password at next logon”
e. Enter the following for password: secret01@ (note 01 is for January, substitute the current two digit month designation)
f. Click “finish”
g. Right click on the new account and choose “properties”
h. On the Account tab click the “logon to” button.
i. Type in the machine name of the computer that this user has been assigned
j. On the Member Of tab click “add” Add the user to the groups supplied by the Management Official
k. On the Profile tab enter a home folder drive letter and path. The standard drive letter for GDF is “U”. The standard path is \\gdfhomeserver\user\%username%

2. Helping the user to login the first time
   a. Discuss with user the current password policy and instruct new user to think of a new password that should be used that will meet the complexity requirement of the system.
   b. Click “OK” and accept the computer use policy that is displayed on the screen.
   c. While at the new users computer supply the User ID and one-time password to the user.
   d. The security of the network will then instruct the user to change his/her password.
   e. Click “ok” and the system will respond in success or failure of the password change.
   f. After successfully logged in show user the necessary drive letters that are used at GDF. GDF uses drive G for group data and drive U for user data.
3. Final procedure
   a. Give user a copy of the Acceptable Computer use policy, having them sign after they have read the policy.
   b. Have user sign the acknowledgement of this policy on the form presented by the Administrator.
   c. The Administrator will then return this form to HR.
   d. HR will then schedule the mandatory Security Awareness Program

References

Krychiw, Steven, “SecurID: A Secure Two-Factor Authentication”, February 28, 2001, http://rr.sans.org/authentic/securid.php.

SANS password policy, http://www.sans.org/newlook/resources/policies/Password_P olicy.pdf

Sherrod, David H, “Securing Access: Making Passwords a Legitimate Corporate Defense”, January 15, 2002, http://rr.sans.org/authentic/sec_access.php.

“Cisco Systems”, http://www.cisco.com/

“Enabling Strong Password Functionality in Windows 2000”, Microsoft.com. http://support.microsoft.com/default.aspx?scid=kb;en-us;225230

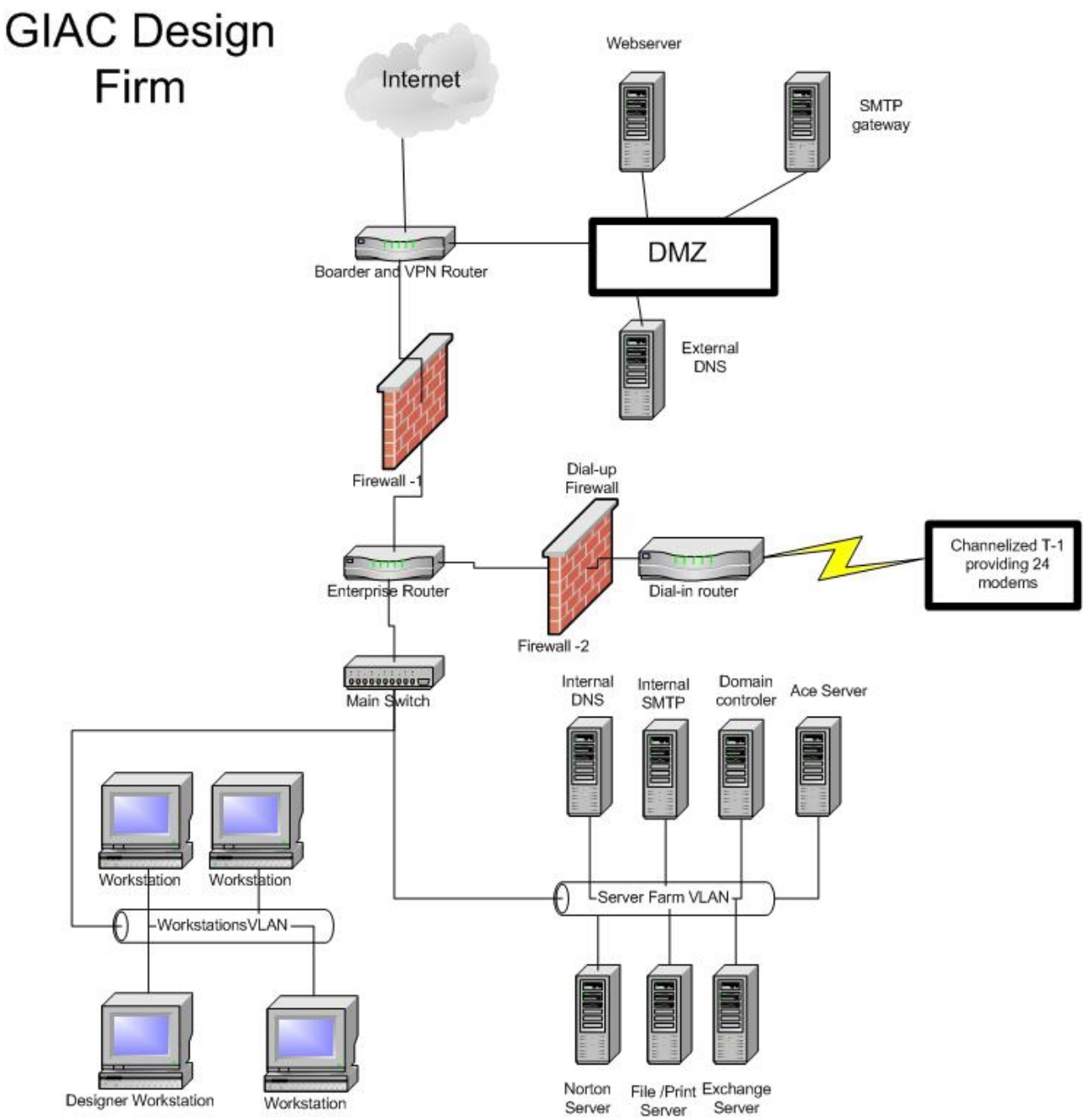
“Compaq Systems”, http://www.compaq.com

“Dell Computer Corporation”, http://www.dell.com

“Antigen for Exchange”, http://www.syabri.com

Appendix A

Figure 1



Appendix B

This is the part of my company's security plan referenced in this assignment. This document has been sanitized to protect my company.

PROTECTION OF {MY COMPANY} INFORMATION RESOURCES

I. PURPOSE

This issuance establishes policy for the protection of the physical, financial, and information resources, as well as the reputation, image, legal position, and other tangible and intangible assets of {MY COMPANY}.

This policy:
• Establishes a risk management program commensurate with the criticality and sensitivity of information resources to {MY COMPANY}.

• Increases company-wide awareness of and compliance with applicable laws, regulations, policies, standards and procedures;

• Establishes security requirements for design, development, implementation, and operation of information technologies (IT) and systems;

• Requires procedures for detecting, evaluating, reporting, and addressing threats to or disruptions of normal operations;

• Delineates responsibilities for the stewardship of {MY COMPANY}'s information resources.

II. SCOPE

All {MY COMPANY} associated individuals who are granted access privileges to information systems.

III. POLICY

{MY COMPANY} information resources shall be managed to ensure the appropriate degree of security, confidentiality, integrity, accessibility, authenticity, reliability, and accuracy based on the criticality and sensitivity of the information.

{MY COMPANY} individuals shall be formally authorized for access to information resources, and shall exercise all authorized access to computer-based information and systems through an electronic identity (commonly called a "User ID" or a "computer account") that maps uniquely to her/him. The computer-controlled limits on what can be done by the "User ID" will be

expanded – from the standard default of no access – only enough to assure that the individual's assigned duties can be performed, a so-called "least privilege" configuration. In special circumstances, an individual may have more than one "User ID" assigned; but each such "User ID" must map uniquely to him/her and may only be used by him/her.

The level of trust vested in the individual shall be determined for each individual and appropriate background checks and/or clearances shall be completed prior to actual access to the asset or assumption of special trust duties. Where delay in obtaining required checks will significantly impede urgent program activity, an individual may perform work where sufficient procedures are in place to create an appropriate trust environment.

IV. RESPONSIBILITIES

A. {MY COMPANY}-Associated Individuals

All {MY COMPANY}-associated individuals are responsible for:

• Being knowledgeable of and adhering to this policy and other federal policies, laws, regulations, standards, and procedures pertaining to information protection and system security;

• Taking no action knowingly to compromise the security, integrity, reliability, or authenticity of data, information or systems.

• Reporting immediately any known or suspected compromise or threat to sensitive or critical information or IT system to the system administrator, other appropriate IT staff;

• Protecting and securing sensitive information from unauthorized disclosure;

• Protecting and securing software and hardware assigned to or used by them;

• Using the assigned unique personal identifier, e.g., User-ID, digital certificate, identity token, etc., and associated pass-code, (e.g., password, one-time password generator, PIN, etc.), for access to all password-protected systems and for safeguarding both personal identifier(s) and associated pass-code(s);

• Abiding by equipment, software, or access controls and configurations assigned to them unless specifically authorized to change them;

• Completing a "Confidentiality Agreement" for access to certain types of information acknowledging authorized accesses and the obligations and restraints associated therewith;

• Complying with legal requirements governing use of software licenses, copyrights, and trademarks.

B. Supervisors and Managers

Supervisors and managers are responsible for:

• Ensuring employees are informed of and comply with this policy, applicable Federal laws, regulations and policies, as well as related {MY COMPANY} policies, standards and procedures;

• Authorizing access privileges for individuals and conveying such authorization and any restrictions;

• Ensuring immediate termination of relevant access privileges when the authorized association with {MY COMPANY} or a specific information resource is ended;

• Determining, in consultation with the Human Resources Management Office (HR) and the organization's Information Systems Security Officer (ISSO), and assigning the level of position sensitivity for all supervised employees;

• Ensuring all IT staff who are responsible for critical systems either rotate out of their normal job responsibilities or take leave during the leave year to help ensure that critical operations are not person-dependent.

C. System Administrators

System administrators are responsible for:

• Complying with {MY COMPANY} IT standards and procedures;

• Documenting authorizations from supervisor(s) or manager(s) for the granting of unique or non-standard access to information resources for {MY COMPANY}-associated individuals or organizations;

• Conducting duties with the least authority necessary to perform a given function;

• Providing access to information resources according to the principle of allowing the least privilege access necessary, for each user, organization, or process operating within their span of control;

• Planning, designing, recommending to managers and operating such physical, technical, and procedural actions necessary to preserve the integrity,

authenticity, reliability, accuracy, confidentiality, and accessibility of information resources and systems;

• Rotating out of the normal job responsibilities or taking at least some scheduled leave during the course of the leave year to help ensure that systems integrity and proper operation are not person-dependent.

D. Business Stewards

A Business Steward is a management official to whom responsibility for the company's mission objective is assigned. This person also directs or controls the budget, personnel, and information resources to accomplish that mission. The Business Steward is responsible for the following activities under his or her area of responsibility:

• Determining the level of data or information sensitivity;

• Determining the level of system criticality;

• Assessing risk to, and vulnerabilities of, agency information resources periodically, and responding in a coordinated agency-wide manner to resolve vulnerabilities and address risk either by control measures or by acknowledging it as a "residual risk;"

• Establishing and maintaining a security plan, contingency plan, disaster recovery plan, and continuity of operations plan (COOP) and personally accrediting and authorizing the plans and the establishment, operation, change, and retirement of the resource;

• Assigning the technical steward(s) for the information resource;

• Determining the access rights/restrictions for system users;

• Conducting risk and vulnerability assessments periodically, including tests of security and contingency plans.

• Establishing and enforcing procedures needed to create an appropriate trust environment, when work must proceed before required background checks are available.

E. Technical Stewards

A Technical Steward is someone, other than the Business Steward, who performs as either a principal investigator or principal user of an information system or as the principal information technology professional responsible for

the system, ensuring that the specified functional characteristics of the system are produced as authorized by the Business Steward.

The Technical Steward is responsible for ensuring that systems and applications function in compliance with all appropriate IT laws, policies, and standards and in accordance with her or his organization's protocols and procedures, as established in the applicable security plan. This responsibility includes:

• Planning, designing, testing, implementing, and operating systems and technologies – whether new or updated, carefully and in collaboration with peers and agency-level technical staff, to ensure the overall security and integrity of {MY COMPANY} information resources;

• Managing security requirements;

• Applying access restrictions directed by the Business Steward;

• Taking necessary corrective actions immediately when a critical or sensitive system or information resource is discovered to have a serious vulnerability.

• Identifying and taking necessary corrective actions to reduce risks, nonstandard conditions, and unauthorized activities;

• Maintaining inventories of information resource assets, e.g., hardware, software, and data and providing those to agency officials as needed;

• Determining, according to the established standard, when an individual is required to sign a Confidentiality Agreement, assuring that the Agreement reflects currently assigned accesses and authorities and that it is signed and on file before the individual is provided with the intended accesses.

F. Security Stewards

A Security Steward is someone, other than the Business Steward and normally not a Technical Steward, who is formally designated as the ombudsman for information protection and systems security (IPASS) for the system. Each general support system and each major application shall have a designated Security Steward.

The Security Steward is responsible for:

• Advising both the Business and Technical Stewards on IPASS matters throughout the development life-cycle.

• Advising the Technical Steward on evaluation of requests for exceptions to standard procedures and conditions.

• Evaluating the completeness and appropriateness of IPASS control measures, and collaborating with appropriate parties on the security, COOP, training and other plans.

• Monitoring operations informally and assuring that both electronic logs are kept and reviewed and formal audits are conducted periodically.

F. {MY COMPANY} Chief Information Security Officer (CISO)

The {MY COMPANY} Chief Information Security Officer is responsible for:

• Providing technical leadership and coordination of {MY COMPANY}'s overall information security program;

• Coordinating the development, updating, and implementation of technical standards and control techniques necessary to ensure compliance with federal information processing standards and {MY COMPANY} policies and procedures;
• Coordinating a {MY COMPANY}-wide identification of {MY COMPANY}'s critical assets and developing and routinely updating an inventory of {MY COMPANY}'s critical assets;

• Determining the relative importance of each asset in the inventory (criticality), assessing risks to the most important (vulnerability), and identifying interdependencies among internal systems and between internal and external systems;

• Coordinating the development of, archiving, and updating Security Plans for the most important critical assets;

• Designing, planning and conducting intrusion tests, evaluating results and identifying risks, and routinely reporting results of intrusion testing to designated agency officials;

G. Human Resources Management Office

The Human Resources Management Office (HR) is responsible for:

• Ensuring that positions are designated with the appropriate sensitivity level;

• Conducting necessary background checks on {MY COMPANY}-associated individuals as required;

• Creating, maintaining, and promoting a role-based security training curricula and courses;

• Identifying, advertising and, as needed, presenting appropriate training aimed specifically at maintaining technical skills and knowledge across the variety of staff assigned to the various information resource roles.