Global Information Assurance Certification Paper

INFORMATION CLASSIFICATION FACILITATES SECURITY AT A FINANCIAL INSTITUTION

GIAC ISO Certification Practical Assignment

Version 1.2 (February 9, 2002)

Prepared By:

Cynthia A. Bonnette
GIAC ISO Certification Candidate

Submission Date: April 29, 2002

TABLE OF CONTENTS

1.0 DESCRIPTION OF GIAC ENTERPRISES

GIAC Enterprises is a mid-sized financial institution based in the northeast United States. GIAC's corporate overview, information technology infrastructure, and business operations are described below.

1.1 Company Overview

Headquartered in Boston, Massachusetts, GIAC Enterprises is a $10 billion financial institution that serves retail and commercial customers in communities throughout Massachusetts and neighboring New England states. In addition to its corporate headquarters, GIAC operates 120 branch offices, five loan centers, and two data processing facilities. The company employs 3,200 people across all of its locations. GIAC's strategy is to offer convenient financial services at competitive prices. GIAC distinguishes itself from its competitors by offering full service in combination with a variety of automated delivery channels.

A nationally chartered bank, GIAC is regulated by the Office of the Comptroller of the Currency, a division of the U.S. Treasury Department that is responsible for supervising national banks. GIAC was established in 1980, through the merger of two local Boston banks. After surviving the challenging New England economic environment of the late 1980s and early 1990s, GIAC solidified its market position and began growing via acquisitions. Over the next decade, GIAC acquired five smaller financial institutions, and reached its present size in early 2000.

Management of GIAC is led by the President and CEO who joined GIAC at the time of the last acquisition in 2000. The management team is a mix of executives who have been with the organization for over ten years and four, including the CIO, who joined GIAC with the new CEO. The new CEO has generally maintained GIAC's traditional focus on basic banking products and community service. However, in light of increasing competition from other financial services firms, and various non-financial companies encroaching upon the marketplace, GIAC is starting to explore new strategic alternatives, including greater use of technology to increase operating efficiency and to expand its products, services, and delivery channels.

GIAC Enterprises Mission Statement: GIAC Enterprises is a diversified financial services company focused on creating value for its clients, employees, and shareholders. This value is created by:

- Partnering with clients to proactively understand and fulfill their financial needs through a diverse range of products, services, and delivery channels.
- Emphasizing dedication to local communities and excellence in customer service.
- Developing and rewarding employees for effectively managing their client relationships.
- Prudently investing capital to achieve profitable and sustainable growth for shareholders.

1.2 Information Technology Infrastructure

GIAC Enterprises' information technology infrastructure was designed to achieve two primary

objectives: to facilitate a secure environment for delivering financial services to its customers and to provide efficient and cost effective operations. Accordingly, GIAC's network facilitates access via the Internet for commercial customers and retail customers. Business partners can access GIAC via the Internet or, in certain cases, via the virtual private network. Employees primarily access the GIAC network from their desktop workstations, however, a small number of employees also have remote access via the dial-up remote access server.

The architecture diagram, which appears on the following page, outlines the information technology infrastructure for GIAC Enterprises. [This section references the GIAC Firewall and Perimeter Protection Assignment, v1.6, by Brad Sanford, entitled, "GIAC Enterprises Attempting to Achieve Defense in Depth," October 14, 2001. Internet Site Address(URL): http://www.giac.org/GCFW.php. The network diagram and infrastructure description have been modified to fit the situation described in this paper.]

Description of Specific Information Technology Components

In the current architecture, the network is divided into eight distinct segments:

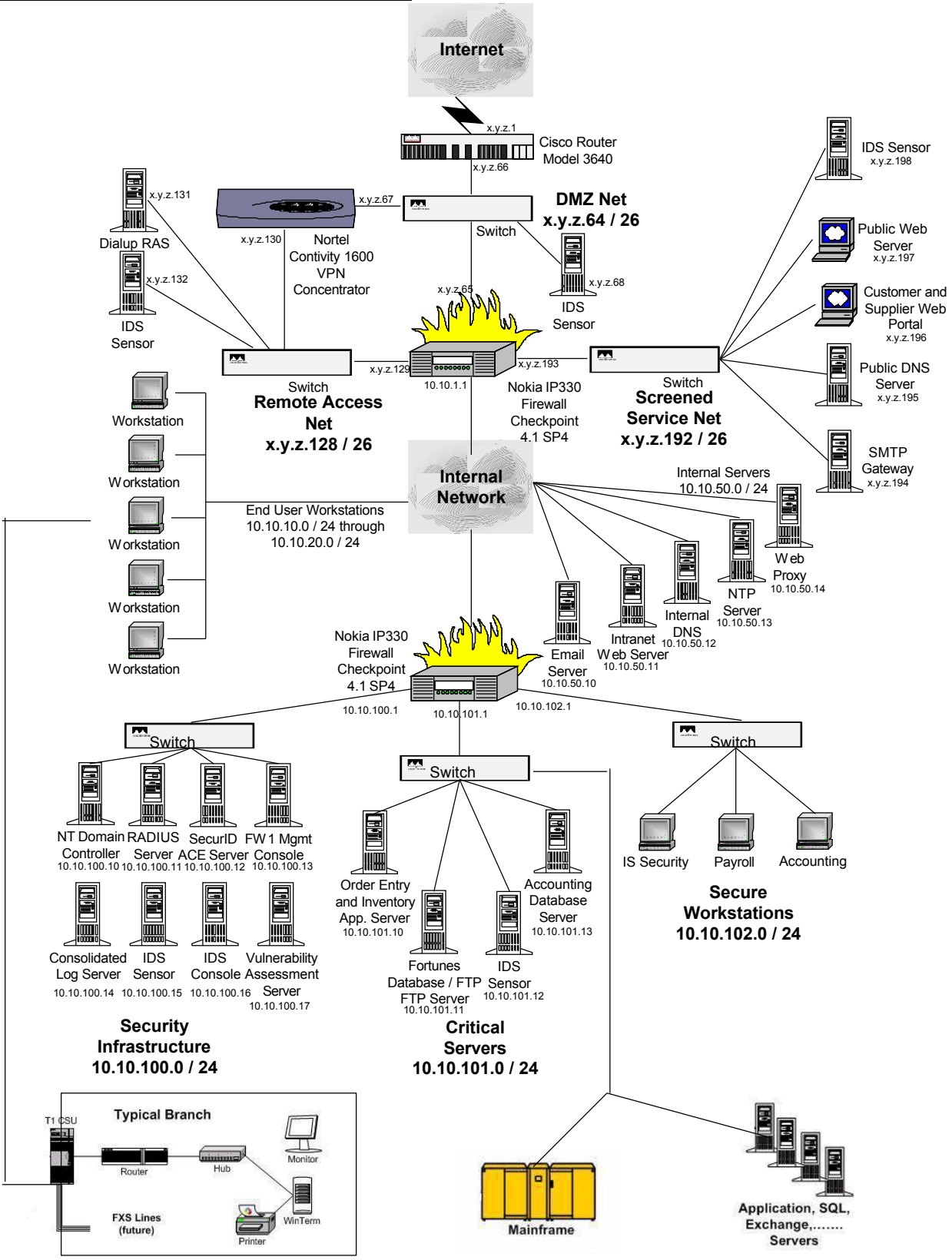
The Internet - GIAC is connected to the outside via its interface with the perimeter router. This is where GIAC Enterprises' retail and commercial customers can access their account information and communicate with GIAC via email and GIAC's public web site. It is recognized that this connection is also vulnerable to potentially malicious parties, as the Internet is a public network. Accordingly, requests originating from this segment are not be trusted unless independently authenticated.

The DMZ (De-Militarized Zone) Network – This area resides outside GIAC's perimeter firewall and virtual private network (VPN) concentrator. This network is protected from the Internet only by the perimeter router. This network is where the internal interface of the perimeter router and the external interfaces of the firewall and VPN concentrator are connected. GIAC Enterprises hosts no network services in the DMZ.

The Remote Access Network – This area is connected to the inside interface of the VPN concentrator and an "internal" interface of the perimeter firewall. This network is essentially a screened subnet that has been dedicated to remote access. The dial-up remote access server (RAS) is also connected to this network. This network is considered a "semi trusted" network. In order to gain access to this network, a user must authenticate to either the dial-up RAS or the VPN Concentrator.

The Screened Service Network - This is the network where all of the servers that provide network services to the Internet reside. The public web server and customer web servers reside here, as does the public Domain Name Service (DNS) server and the public email gateway. All servers residing in this segment are considered critical, with hardened operating systems patches kept current at all times. This area is recognized as highly vulnerable to attack and therefore appropriate controls and settings at the firewall are critical.

Diagram of GIAC Enterprises IT Architecture



The Internal Network - This area resides inside the firewall and is connected to the internal interface of the perimeter firewall. The internal network is where most of the employees' workstations are located. In addition, this is where branch offices are connected. Servers that provide services to the entire company such as email, internal DNS, and intranet web servers are located here, as well. This network is designed to be maintained completely separate from any external network other than connections that pass through the perimeter firewall.

The Security Infrastructure Network – This area is a secured internal network that resides behind one interface of the internal firewall. Servers that compromise the security infrastructure of GIAC Enterprises reside on this highly restricted segment. Only the information technology security team has general access to the systems located on this segment, which contains many of the most sensitive security devices and servers on the GIAC Enterprises network.

The Critical Servers Network – This area is a secured internal network that resides behind one interface of the internal firewall. There are several mission critical company servers and databases that reside on this segment. In addition, there is a connection to GIAC's mainframe and application servers that host a number of essential banking services and process sensitive account information.

The Secure Workstations Segment – This area is a secured internal network that resides behind a third interface on the internal firewall. This network segment is reserved for individuals with special security needs. The IS Security department, as well as several individuals from the accounting and payroll departments have workstations residing on this segment.

Other key elements of the information technology architecture include:

Switches - GIAC Enterprises has enhanced the security of its networks through the use of switches as a means by which edge connectivity to the network is provided to the end users and servers. This helps to limit the ability of any system on the network to monitor the network traffic of others on the network without first modifying the configuration of one of the switches.

The Perimeter Router - This router represents the first layer of defense in GIAC Enterprises' network security architecture. However, the primary purpose of this router is to provide connectivity to the Internet, with security its secondary function. The perimeter router helps GIAC Enterprises protect its network by screening inbound traffic and blocking packets based on their origin, destination, behavior patterns, and other signals of undesirable or anomalous activity. In addition, the perimeter router helps GIAC Enterprises block certain outbound traffic that demonstrates suspicious behavior (e.g., potentially spoofed source addresses).

The Perimeter Firewall – This firewall represents the primary network control point within the network. Its placement segregates the GIAC Enterprises network into four main segments: the DMZ network, the screened service network, the remote access network, and the internal network. Except for the special case of traffic going between the remote access network and the DMZ network, all traffic that needs to go from one GIAC Enterprises segment to another must

pass through the perimeter firewall. The security policy enforced by the firewall is the primary network access control protecting GIAC Enterprises from network based attacks.

The VPN Concentrator - This is the only device other than the perimeter firewall that controls the flow of network traffic between the four GIAC Enterprises segments. It provides a means for network traffic the get from the DMZ (and therefore the Internet) to the remote access network and the reverse. The VPN concentrator enforces a security policy that requires authentication and strong encryption before allowing such communication to take place.

The Dialup Remote Access Server - This server exists solely to provide access to certain GIAC Enterprises employees who do not have a personal Internet Service Provider and therefore do not have the ability to access the VPN concentrator from the Internet. The RAS requires authentication before allowing the dial-up user to the remote access network.

Intrusion Detection Sensors - The intrusion detection sensors exist to monitor the network for signs of suspicious activity and to generate alerts upon the discovery of such activity. The sensors are deployed at various key points within the network where suspicious activity is likely to be seen. The sensors are deployed on all three external legs of the perimeter firewall, as well as on the security infrastructure and critical servers networks. All intrusion detection sensors are configured to report any "detects" back to a centralized console that provides a unified view of alert activity across all sensors. The console resides on the protected security infrastructure network and is monitored in information technology security staff.

SMTP Gateway - A virus scanning SMTP gateway has been deployed on the screened service net to facilitate the delivery of email to and from the Internet. The email is scanned for viruses and then passed on to the internal email system. Email sent from the internal email system to Internet email addresses is forwarded from the internal mail system to the virus scanning gateway which acts as an SMTP relay for the internal email system.

Web Proxy - A virus scanning web proxy is deployed on the internal network to facilitate more secure browsing of the web as well as to conserve bandwidth through the caching of frequently viewed web pages on the local server.

The Internal Firewall - This firewall has its external interface connected to the internal network and has three additional interfaces which support secured internal network segments, the security infrastructure network, the critical servers network, and the secure workstations network. The primary purpose of the internal firewall is to create secure internal network segments for internal systems that need to have a heightened security posture.

All servers on the DMZ, screened service network, and remote access network are running Slackware Linux 8.0 with Kernel 2.4.9. These servers have been appropriately hardened for service as bastion hosts. The DNS server is running Bind 8.2.5, the web servers are running Apache 1.3.22, and the SMTP gateway is running Sendmail 8.12.1 and Interscan Viruswall 3.6 with updated scan engines and virus signatures.

The security infrastructure network contains the RADIUS, SecurID ACE, and NT Domain authentication servers, as well as the firewall and intrusion detection management consoles, and other servers that provide sensitive security related functions (e.g., the consolidated remote logging server and the vulnerability assessment server). The critical servers network contains the mission critical business servers that house the applications and sensitive customer data that are essential to GIAC's business operations. The end-user workstations network contains workstations comprised of Dell PCs operating on Windows NT. The workstations are assigned static IP addresses due to their need for heightened security, either because of the information stored on the workstation or because of the sensitive nature of the applications that must be accessed by the user of those workstations.

1.3 Business Operations

Overview of GIAC Enterprises' Business

As a financial services company, GIAC's primary operations are concerned with maintaining account information for its customers and processing financial transactions. GIAC's customers conduct business with the company through a number of delivery channels, including physical branch offices, automated teller machines (ATM), and Internet banking. Whereas the history of banking has centered on the physical exchange of cash, checks, and other valuable property, banking has rapidly evolved into an information-based business. Accordingly, GIAC's ability to maintain the trust of its customers and meet their financial needs depends on its ability to provide consistently accurate, readily available, and convenient access to account data and facilitate transactions.

Banking transactions generally involve activity in new or existing deposit and loan accounts, or payment related services. Transactions may be initiated by customers directly, by GIAC employees in branches or corporate offices, or by service providers who have partnered with GIAC to offer specific services or operations. The general flow of GIAC's business involves requests for information, transactions, or services by customers, which may be presented via any of the delivery channels referenced above. In the case of a branch office, customers will physically present a deposit or withdrawal request to a GIAC employee for processing. In the case of remote transactions, customers will enter their request for payments, etc., directly into an information system (e.g., ATM, bank web site, or telephone).

With reference to GIAC's information technology architecture (and the diagram on page 3), transactions will enter the system via the employee workstations, branch offices, self-service banking channels (Internet, ATMs), and bank partners (service providers). From these entrance points, the information will pass to the Internal network, where it then moves through a firewall and then travels to various application servers, the mainframe, or other database servers for storage or processing.

One of the many challenges faced by GIAC in terms of its information flow is the need for consistency in the accuracy and security around sensitive information in both physical and electronic form. For example, GIAC will receive sensitive information from customers in the

form of paper documents at branch offices. Other confidential paper documents will be created by GIAC employees and partners. In some cases, this information will also exist in electronic form (e.g., scanned copies) and in other cases, only a paper or electronic record will exist. As a result, GIAC's policies, procedures, and practices require consistency in terms of how information (physical and electronic) is gathered or created, processed, stored, and ultimately disposed.

Information Technology Needs and Activities

Business operations at GIAC involve three primary groups: customers, employees, and business partners (including service providers and vendors). Each of these groups has some form of access to GIAC's information systems and each group has specific needs and control requirements that pertain to the nature of their activities.

Employees – GIAC employees include customer contact personnel (e.g., branch employees, call center staff, loan and investment officers, operations staff, information technology staff, and corporate employees such as executives, auditors, accountants, etc.). Nearly all employees require access to basic information systems resources such as internal email, the GIAC intranet, and standard Microsoft Office Suite applications. Beyond this basic level, employees require access to additional information, applications, and resources depending on their job function. For example, customer service employees require various levels of access to customer account information. Operations staff requires access to the bank's general ledger system. Executives require access to various management information reporting systems.

To facilitate these requirements and also to implement structured controls, GIAC's information system has been designed as follows. All information processing systems, databases, and applications are accessed through the internal network. Each employee is assigned a user code and password with which they can log in to the GIAC internal network and access the basic level of applications (email, intranet, MS Office, etc.). Access to other applications (including Internet access) depends on the employee's profile, which is set based on their job description. All workstations are configured uniformly and most have had the floppy disk drive and CD-ROM drives disabled. Some employees (primarily executives and travelling loan officers) are assigned laptop computers, which can access the GIAC network via dial-up to the remote access server. Another group of employees (primarily manager and corporate employees) can access GIAC Web-based email remotely through their personal Internet connections; however, they cannot access any applications on the GIAC internal network in this manner.

Customers - GIAC's customers include both retail (individual consumers) and commercial (businesses) segments. Customers can access GIAC's financial products and services with the assistance of a GIAC employee by visiting a branch office or using the call center. Customers can also use several self-service channels, such as ATMs and Internet banking. With respect to requirements and controls, GIAC customers demand convenient, reliable, accurate, and efficient service from all delivery channels. GIAC's information systems can provide real-time transaction processing and account balance reporting. All customer delivery channels require some form of authentication; however, the methods vary (branches require photo identification, ATMs require

cards and PIN codes, Internet banking requires a user code and password).

Business Partners- GIAC has established relationships with a number of business partners to offer specialized products and services to its customers. An example is GIAC's partnership with Riskless Insurance Company, which allows GIAC to offer a variety of insurance products that are underwritten by Riskless. Based on their agreement, GIAC collects insurance applications and forwards the information to Riskless for processing. The accounts are jointly serviced. Accordingly, certain employees at Riskless have access to GIAC's virtual private network and certain GIAC employees have access to a similar network at Riskless to exchange relevant information.

GIAC also has a number of relationships with service providers and vendors for specific information technology needs. Examples include software development and support for critical applications such as deposit and loan account processing. GIAC contracts with SuperData to run their core processing program and maintain the application. A similar arrangement is in place with SuperWebSoft to support the Internet banking application, which GIAC has licensed and runs in-house. GIAC's technology partners exchange data files via controlled access to the virtual private network.

2.0 RISK IDENTIFICATION

As a financial institution, the foundation for GIAC Enterprises' business is the trust and confidence that customers place in GIAC's ability to safeguard and manage their accounts. Accordingly, the three most significant risk issues for GIAC are: (1) unauthorized access to sensitive customer information, (2) corruption or loss of critical data, and (3) critical system failure or lack of availability. All three of these risks relate directly to GIAC's "crown jewels" which is customer data—specifically, customer data that is confidential or otherwise not publicly available. While GIAC also holds other sensitive information, including competitive strategy and certain "corporate secrets", customer data is particularly important due to the essential requirement for trust in banking. Furthermore, banks are required by Federal regulation to safeguard customer information, and GIAC's failure to comply could result in serious consequences. Each of the three risk areas are discussed in detail below including the nature of the risk, its significance, relevant vulnerabilities and threats, and potential mitigating controls.

2.1 Risk Area 1 - Unauthorized Access to Sensitive Customer Information

Customer information, specifically non-public sensitive information about customers' financial transactions and account balances, represents the "crown jewels" of GIAC Enterprises. The entire relationship between GIAC and its customers is based on trust and confidence that GIAC will safeguard customer information and manage it reliably.

Nature of the Risk

Unauthorized access to customer information, by an intruder from the outside or an insider exceeding their authority, violates the trust that GIAC customers have placed in their financial

institution. Depending on the results of the breach, the damage to GIAC and its customers can vary. For example, if the unauthorized access results in identity theft, fraud, or a misappropriation of funds, GIAC's customers could suffer material harm. Accordingly, GIAC could face a combination of financial losses and reputation damage, in addition to possible legal and regulatory complications. If unauthorized access involves multiple customers' accounts, the extent of the damage can be further magnified.

Significance of the Risk

As a financial institution, GIAC Enterprises is subject to the requirements of the Gramm-Leach-Bliley Act and implementing regulations for safeguarding customer information. Accordingly, GIAC is required by law to "… insure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer." [Federal Register: February 1, 2001 (Volume 66, Number 22) 12 CFR Part 30, et al., Interagency Guidelines Establishing Standards for Safeguarding Customer Information.] The regulatory requirements effectively raise the significance factor for this risk area due to the added concern for penalties and enforcement actions for non-compliance. In addition, financial losses and reputation damage resulting from unauthorized access to customer information could be substantial.

Relevant Vulnerabilities and Threats

The extensive amount of customer information processed and stored by GIAC's information systems, the number of employees and business partners with access rights, and the multiple connections between internal and external networks, gives rise to a number of potential vulnerabilities that could ultimately result in unauthorized access. Furthermore, due to the inherent value of customer information, this data is also a primary target for internal and external threat sources. The combination of numerous potential vulnerabilities (e.g., poor access controls, weak encryption, inadequate perimeter defense) with highly motivated threat sources results in a significantly high level of risk.

Potential Risk Mitigation Controls

To address this risk, GIAC can implement a number of technical, administrative, and physical controls. Specific examples include strong access controls (e.g., authentication and authorization processes) for systems that contain sensitive customer data. Strong encryption should be used whenever customer data is transmitted over an insecure network or is otherwise not protected by strong access controls. In addition, employees, customers, and business partners must all be educated on GIAC's information security policy which should outline baseline controls that protect access to customer data. The policy should identify classes of information that require extra safeguards (e.g., sensitive customer data) and restrict access to only authorized users.

2.2 Risk Area 2 - Corruption or Loss of Critical Data

In addition to the risk of unauthorized access to customer information, GIAC also faces the significant risk that critical data may be corrupted or lost. Critical data may include customer information, in addition to other proprietary information of an essential nature (e.g., strategic business documents, corporate financial data, etc.) This risk area is heightened for many of the same reasons as the first risk area. Specifically, GIAC's customers and business partners place great trust in a financial institution to protect information assets and ensure their accuracy and reliability.

Nature of the Risk

The information assets of GIAC Enterprises, its customers, its employees, and its business partners must not only be protected from unauthorized access, but also safeguarded from damage, corruption, or outright loss. Such damage or loss could be caused by system faults, failures, natural disasters, intentional acts by humans, or inadvertent errors. If the "crown jewels" (i.e., sensitive customer information) were to be materially damaged or lost, GIAC could face a number of serious consequences including financial loss, reputation harm, and possible legal or regulatory penalties.

Significance of the Risk

GIAC's reputation as a financial institution is based on the trust that it will protect information assets from loss or damage. In addition the provisions of the Gramm-Leach-Bliley Act, referenced above, also stipulate that financial institutions must protect customer information from threats and hazards to security and integrity. Therefore, the obligation faced by financial institutions to guard customer information from loss and damage is significantly greater than that for a non-financial company. The corruption or loss of mission critical corporate data could result in the inability to complete plans, submit required regulatory reports, and meet contractual obligations to business partners.

Relevant Vulnerabilities and Threats

Vulnerabilities that could contribute to a situation where data is damaged, corrupted, or lost include reliance on a single system, database, or application for a sensitive or mission-critical function. Other vulnerabilities may include the failure to provide for protective physical controls around sensitive systems (e.g., protection from environmental hazards including water and fire damage. Inadequate access controls could also present vulnerabilities to malicious human acts such as sabotage, and innocent mistakes. Threat sources that may act upon these areas of weakness include natural disasters, corporate insiders, and external parties such as terrorists or hackers who seek to cause harm. Financial institutions represent a particularly inviting target for terrorists and hackers due to their high visibility and significance to the critical infrastructure of the United States.

Potential Risk Mitigation Controls

To address the risk associated with damage, corruption, or loss of critical data, GIAC should

implement a number of controls. Most importantly, GIAC needs to institute a process for the regular back-up and off-site storage of relevant data. A comprehensive incident response plan, in addition to a disaster recovery strategy and business continuity plan should be in place, so that in the event of a problem GIAC is well-prepared to respond. Access controls, including authentication and authorization procedures, should be in place to limit exposure from insiders and outsiders that might inflict intentional or unintentional damage on GIAC systems. Furthermore, GIAC should institute procedures to regularly test applications and databases for integrity, particularly after any system changes or modifications.

2.3 Risk Area 3 – Critical System Failure or Lack of Availability

The next most significant risk to GIAC Enterprises involves critical system failure or lack of availability. Specifically, GIAC's role as a payments processor requires that systems be reliable and available to send and receive transactions and accurately report account balances. Customers depend on immediate access to their account information and the ability to immediately transfer or receive funds. GIAC's inability to meet those expectations could result in loss of business, reputation damage, and possibly legal consequences if the customer's inability to access account information maintained by GIAC results in significant harm.

Nature of the Risk

System failure or unavailability could result from a single or combined failure among GIAC's interconnected critical processing systems. For example, a failure in the delivery channel (e.g., ATM network) could prevent a customer's payment request from being received and processed. A failure in the processing application could prevent a transaction request from being completed. Any of these, or similar events, would result in serious problems for GIAC customers, who would be unable to access their account information or conduct financial transactions. Accordingly, GIAC would find itself in the position where it is unable to provide its core business service.

Significance of the Risk

The risk of system failure or unavailability is particularly serious for a financial institution. Recent news reports from Japan have highlighted serious computer problems at the Mizuho Banking Company. Due to system failures, Mizuho has been unable to process ATM transactions and numerous prescheduled electronic payments for several weeks. As of April 22, 2002, the amount of unsettled payments at seven major utilities in Japan amounted to 25.9 billion yen due to Mizuho's computer problems. Complications resulting from the computer system disruption have also caused the share price of Mizuho Holdings to decrease by 6.6% to Y285,000 between 29 March 2002 and 22 April 2002. ["Mizuho Computer Woes Point to Slow Pace at Japan's Banks," Phred Dvorak, Australasian Business Intelligence, Apr 24, 2002.]

Relevant Vulnerabilities and Threats

System failures and loss of availability could result from operational problems, malfunctions,

programming errors, natural disasters, and intentional acts of sabotage. Potential vulnerabilities that could lead to such situations include poor system designs that permit single points of failure and inadequate capacity. Other vulnerabilities can include weak access controls and perimeter defenses that may allow the introduction of malicious code or a worm that absorbs system resources. Threat sources that could exploit these vulnerabilities include denial of service attacks launched by hackers, insiders or outsiders plotting sabotage, natural disasters or adverse environmental conditions, and inadvertent human error. As evidenced by the extensive media attention to the Mizuho situation, an attack that cripples a financial institution is high profile and therefore attractive to hackers and terrorists.

Potential Risk Mitigation Controls

To mitigate the risk of system failure and lack of availability, GIAC should institute a number of controls. Specifically, system design should be reviewed periodically for traffic patterns and to avoid any single points of failure or congestion. Delivery channels should be monitored for availability and capacity. GIAC should also ensure that controls are in place to protect against threats from internal or external attackers seeking to disrupt the system. Such controls include access protections (e.g., authentication and authorization) and perimeter defenses (e.g., firewalls and screening routers to prevent disallowed traffic and malicious code). Disruptions from environmental hazards and natural disasters can be mitigated by physical security protections. Furthermore, plans and policies for incident response, disaster recovery, and business resumption should be in place to facilitate timely recovery.

3.0 SECURITY POLICY EVALUATION AND DEVELOPMENT

The greatest risk faced by GIAC Enterprises is Risk Area 1 discussed above, the potential for unauthorized access to sensitive customer information. To address this risk, GIAC should implement an Information Classification Policy that will accomplish the following objectives: (1) define specific categories of information so that all system users are aware of *what* needs to be protected, (2) establish rules for *how* information in the respective categories should be treated, and (3) clarify roles and responsibilities for implementing the policy, including interpretations and exceptions. A comprehensive Information Classification Policy will help GIAC to ensure that safeguards and controls are appropriately targeted at the most valuable information assets.

3.1 Sample Policy

The following Sample Information Sensitivity Policy was obtained from the SANS Security Policy Project, SANS Institute Web site.
[URL: www.sans.org/newlook//resources/policies/policies.htm.
Policy URL: www.sans.org/newlook//resources/policies/Information_Sensitivity_Policy.doc].

Sample Information Sensitivity Policy

1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of <Company Name> without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect <Company Name> Confidential information (e.g., <Company Name> Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Infosec.

2.0 Scope

All <Company Name> information is categorized into two main classifications: Public and Confidential.

Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to <Company Name> Systems, Inc.

Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in <Company Name> Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of <Company Name> Confidential information is "<Company Name> Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to <Company Name> by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into <Company Name>'s network to support our operations.

<Company Name> personnel are encouraged to use common sense judgment in securing <Company Name> Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

3.0 Policy

The Sensitivity Guidelines below provide details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as <Company Name> Confidential information in each category may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the <Company Name> Confidential information in question.

3.1 Minimal Sensitivity: General corporate information; some personnel and technical information

- Marking guidelines for information in hardcopy or electronic form: [Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".] Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "<Company Name> Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "<Company Name> Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, <Company Name> information is presumed to be "<Company Name> Confidential" unless expressly determined to be <Company Name> Public information by a <Company Name> employee with authority to do so.

- Access: <Company Name> employees, contractors, and people with a business need to know.

- Distribution within <Company Name>: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

- Distribution outside of <Company Name> internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

- Electronic distribution: No restrictions except that it be sent to only approved recipients.

- Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

- Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

- Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.2 More Sensitive: Business, financial, technical, and most personnel information

- Marking guidelines for information in hardcopy or electronic form: [Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".] As the sensitivity level of the information increases, you may, in addition or instead of marking the information "<Company Name> Confidential" or "<Company Name> Proprietary", wish to label the information "<Company Name> Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

- Access: <Company Name> employees and non-employees with signed non-disclosure agreements who have a business need to know.

- Distribution within <Company Name>: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

- Distribution outside of <Company Name> internal mail: Sent via U.S. mail or approved private carriers.

- Electronic distribution: No restrictions to approved recipients within <Company Name>, but should be encrypted or sent via a private link to approved recipients outside of <Company Name> premises.

- Storage: Individual access controls are highly recommended for electronic information.

- Disposal/Destruction: In specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

- Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.3 Most Sensitive: Trade secrets and marketing, operational, personnel, financial, source code, and technical information integral to the success of our company

- Marking guidelines for information in hardcopy or electronic form: [Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".] To indicate that <Company Name> Confidential information is very sensitive, you may should label the information "<Company Name> Internal: Registered and Restricted", "<Company Name>

Eyes Only", "<Company Name> Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of <Company Name> Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

- Access: Only those individuals (<Company Name> employees and non-employees) designated with approved access and signed non-disclosure agreements.

- Distribution within <Company Name>: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

- Distribution outside of <Company Name> internal mail: Delivered direct; signature required; approved private carriers.

- Electronic distribution: No restrictions to approved recipients within <Company Name>, but it is highly recommended that all information be strongly encrypted.

- Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

- Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

- Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.0 Enforcement

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

5.0 Terms and Definitions

Appropriate measures - To minimize risk to <Company Name> from an outside business connection. <Company Name> computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access <Company Name> corporate information, the amount of information at risk is minimized.

Configuration of <Company Name>-to-other business connections - Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required - Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods - Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential - You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail - Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here…]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files - Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within <Company Name> is done via a license. Please contact the appropriate support organization if you require a license.

Company Information System Resources - Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge - To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls - These are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use man chmod to find out more about it). On Macs and PCs, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links - These are all network links that originate from a locale or travel over lines that are not totally under the control of <Company Name>.

Encryption - Secure <Company Name> Sensitive information in accordance with the Acceptable Encryption Policy. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication – This method is accomplished by using a one time password token to connect to <Company Name>'s internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security - Physical security means either having actual possession of a computer at all

times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link - This is an electronic communications path that <Company Name> has control over it's entire distance. For example, all <Company Name> networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes represent a private link. <Company Name> also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which <Company Name> has established private links include all announced acquisitions and some short-term temporary links.

6.0 Revision History

Approval Date: Anydate
Approved By: <Company Name> Board of Directors

3.2 Evaluation of Sample Policy

The sample policy has a number of significant weaknesses that limit its effectiveness. Its purpose statement should be strengthened to emphasize how the policy relates to the company's overall information security objectives. The scope statement is flawed in that it fails to express what is covered by the policy and in what situations it applies. Instead of defining the extent of the policy, the scope statement contains information that more appropriately belongs in the policy statement section. Other weaknesses include the lack of designated responsibility for the policy itself and the absence of guidelines for granting exceptions. Aside from the identified weaknesses, the sample policy is reasonably effective in providing specific guidelines and instructions for protecting information at varying sensitivity levels.

Specific elements of the sample policy are evaluated in further detail below:

Purpose – The sample policy provides a reasonably good statement of purpose; however, it fails to reference the company's overall information security objectives. The purpose statement indicates that the intent of the policy is to provide instructions to employees regarding what information can be disclosed to non-employees and what information cannot be shared outside the company. The purpose statement also provides clarification that the policy pertains to information that is stored or shared by any means, including electronic and physical records; however, this comment would more appropriately belong in the scope statement.

Background – The sample policy does not have a background statement. While not a material deficiency, a background statement would be helpful, given the noted weaknesses in the purpose

and scope statements.

Scope – The scope of the sample policy is unclear. Rather than describing the nature of information covered by the policy and the types of situations that are addressed, the scope statement begins with the definition of two main classifications for company information. The statement then proceeds to offer examples of what types of information fall into the respective classifications. The scope statement fails to define the extent and coverage of the policy, and instead outlines information that more appropriately belongs in the policy statement section.

Policy Statement - While the sample policy does a reasonably good job of providing specific guiding principles, the statement is weakened by the introduction which states, "Use these guidelines as a reference only, as <Company Name> Confidential information in each column may necessitate more of less stringent measures of protection…" An effective policy statement outlines guidelines and rules that are expected to be followed, not just used as a reference. The policy statement is clear and specific in the way that it outlines guidelines for document marking, access, internal distribution, external distribution, electronic distribution, storage, and disposal. However, the policy is also confusing in that it does not explain how the two categories of information identified in the scope section (public and confidential) correspond to the three sensitivity levels outlined in the policy section (minimal sensitivity, more sensitive, and most sensitive).

Responsibility – The sample policy does not have a section on responsibility. Furthermore, the policy is weak in defining roles and responsibilities. While it is stated that all company employees are responsible for following the policy, there is no indication of who is responsible for overseeing and maintaining the policy itself. The policy does not address how exceptions will be handled and directs employees to "Infosec" for questions about the guidelines and "your manager" for questions about information classification.

Action – The sample policy implies that the three levels of sensitivity guidelines are to be immediately followed by all employees; however, this message should be stated more clearly. The policy includes an enforcement section, which notes that employees who violate the policy may be subject to disciplinary action. However, there are no provisions for audits or reviews to evaluate compliance with the policy. While the guidelines for accessing, distributing, storing, and disposing of information define the actions that are expected, further clarity could be added by providing dates and frequencies (e.g., electronic data should be erased after 90 days).

3.3 Revised Policy

Based on the foregoing evaluation, the Sample Information Sensitivity Policy has been substantially modified to address the specific needs of GIAC Enterprises. The resulting (and re-titled) Information Classification Policy is provided below:

Information Classification Policy

1.0 Purpose

The Information Classification Policy is an integral component of GIAC Enterprises' Information Security Program. Information classification is intended to ensure that information entrusted to GIAC Enterprises by its customers and partners, in addition to GIAC's proprietary corporate data, is protected by appropriate safeguards. Recognizing that sensitivity and criticality will vary based on the source, purpose, and use of the information, this policy outlines criteria for determining classifications and related treatment.

2.0 Objectives

The objectives of information classification are to:

- Ensure that information and data that warrants a particular level of treatment is handled accordingly.
- Ensure consistency of information/data treatment across the organization.
- Provide a basis for measuring and benchmarking controls relative to the information and data they protect.

3.0 Scope

The information covered in this policy includes, but is not limited to, information that is either stored or shared via any means. This includes electronic information, information on paper, and information shared orally or visually (e.g., telephone and video conferencing). Also included is any information in storage or in electronic or physical transmission outside of GIAC's facilities (e.g., service providers).

When determining the appropriate classification, consideration will be given to the nature of information (its source, use, and purpose) and the need for protective measures (confidentiality, integrity, and availability). Classification categories are defined in Section 6.0.

Nothing in this document, including the rules for information storage and destruction, are intended to contradict any existing legal or regulatory recordkeeping requirements that apply to the retention of certain documents and data. In all instances, laws and regulations must be met; however, to the extent that they do not conflict, the guidelines outlined in this document should also be followed.

4.0 Policy

GIAC's policy is based on the premise that our customers are entitled to have their financial affairs managed with due care. Safeguarding information about GIAC's transactions and the transactions of customers and prospective customers, as well as shareholders and suppliers, is required of all employees. Accordingly, no information regarding a prospective or current

customer, shareholder, supplier, or a particular business transaction at GIAC may be released to anyone without the consent of the particular individual or corporation to whom the information applies. In no event should a bank employee respond to a subpoena or a court order without direction from the Legal Department.

Confidential information obtained as a result of employment with GIAC shall not be used for the purpose of furthering or attempting to further anyone's private interests, financial benefit, or personal gain. Use or disclosure of this type of knowledge or information can, in certain circumstances, result in civil or criminal liability against the employee and/or GIAC. Unless there is a legitimate business need for employees in another department or affiliate, or another employee in your department, to know about the transaction or the confidential information, the information should not be communicated.

All GIAC information will be accorded certain treatment based on its classification. The respective class is determined based on the characteristics outlined in Section 6.0. The classes and related treatment are considered effective as of the date of this policy statement and do not require any specific labeling or distinguishing features.

The information protection requirements outlined in Section 7.0 provide rules for the treatment and protection of respective classes of information, which by their definition have varying degrees of sensitivity. GIAC employees are advised to consult with the Information Security Officer when guidance is needed in applying this policy.

5.0 Responsibility

Responsibility for overseeing the implementation of this policy is assigned to GIAC's Information Security Officer.

All employees are expected to familiarize themselves with the guidelines that follow. It should be noted that the classification definitions were created as guidelines and are intended to emphasize common sense steps that can be taken to protect GIAC, its customers, and its partners.

6.0 Classification Categories

6.1 Confidential

Definition: Confidential information consists of highly sensitive customer information, mission critical corporate information (e.g., proprietary, trade secrets, payroll, information subject to attorney/client privileges), or proprietary/critical data of GIAC partners. Compromise of confidential information could result in serious harm to GIAC in terms of financial, legal, and reputation consequences.

Examples:

All customer non-public information, as defined by federal regulations addressing privacy

protection and data sharing (Regulation P). This includes account information, social security numbers, etc. A good rule of thumb for GIAC employees is that customer information that would not otherwise be found in the public telephone directory should be treated as confidential.

GIAC's proprietary or critical corporate information (e.g., trade secrets or other sensitive competitive information). This includes information about possible strategic activities, such as mergers, asset sales, re-organizations, audit reports, business plans, etc. A good rule of thumb for GIAC employees is that information about GIAC's internal financial information, future strategies, new products or services, market campaigns, threatened or pending litigation, etc., should be treated as confidential.

GIAC business partners' and affiliates' proprietary or critical information (e.g., trade secrets or other sensitive competitive information). This includes information similar to that described above for GIAC. A good rule of thumb for GIAC employees is that information about GIAC partners' and affiliates' financial condition, future strategies, audit reports, new products or services, market campaigns, etc. should be treated as confidential.

6.2 Sensitive

Definition: Sensitive information consists of valued data (e.g., customer lists, non-confidential customer information) that requires a medium level of protection. Compromise of sensitive information could result in moderate financial loss or reputation harm.

Examples:

Customer data that is not designated "confidential". This includes customer data that might be found in public sources like public telephone directories or the Internet (e.g., phone numbers, addresses, etc.). This also includes customer lists or databases that include customer names in combination with one or several other data elements.

GIAC's non-public information that does not meet the criteria for "confidential." Certain corporate information requires significant protection, but to a lesser extent than trade secrets or critical data. Examples include employee handbooks, procedures manuals, non-published or not-yet-published rates and terms for loan and deposit products, and other information that may be known to GIAC employees about the organization, but is not generally announced to the public.

GIAC business partners' and affiliates' non-public information that does not meet the criteria for "confidential." Similar to the examples provided above for GIAC's sensitive data, information about GIAC business partners or affiliates that is not general public knowledge, but falls short of the definition for "confidential" should be treated as sensitive. Examples include procedures manuals and information about existing products and services.

6.3 Public

Definition: Public information is information that is obtained from, or otherwise generally exists

in, public sources (e.g., newspapers or telephone directories) and can freely be given to anyone without any possible damage to GIAC.

Examples:

Customer data that is not sensitive or confidential. Generally, this category will be rare, as GIAC's policy is to treat customer data as sensitive, if not confidential. It includes information that was not gathered specifically by GIAC (e.g., provided by an independent source) and does not contain any non-public elements. Examples include a list of names that was provided to GIAC from an external marketing company. Data that represents aggregate information about a group of customers, but does not include their names or other identifying characteristics, may be treated as public information.

GIAC's public information. This includes information that GIAC's public affairs office has previously disclosed through print or other media. Examples include information on GIAC's public web site, information in press releases, advertisements, investor materials, SEC filings and other published financial statements (e.g., annual report, quarterly reports, etc.).

GIAC partners' and affiliates' public information. This includes information that GIAC business partners and affiliates have previously disclosed through print or other media. Examples are similar to those listed above for GIAC's public information. As a rule of thumb, GIAC employees should consult with management or a representative of the partner or affiliate organization to confirm whether the information should be treated as public data.

6.4 Default Classification

In the event that there is any uncertainty about the appropriate classification for certain information, GIAC's policy is to treat the information according to the higher category's requirements. For example, if there is doubt regarding whether information should be treated as sensitive or public, the default is to treat it as sensitive. When information systems or physical storage facilities contain a combination of data from more than one category, the entire system or facility should be treated according to the rules for the most sensitive data involved. In such situations, employees should consult with GIAC's Information Security Officer for guidance.

7.0 Information Protection Requirements

The following table outlines GIAC's requirements for protecting the respective classes of information.

	Public	**Sensitive**	**Confidential**

Access Restrictions – Internal	Restricted to GIAC employees with a business need to know.	Restricted to GIAC employees with a business need to know, as designated by management.	Restricted to GIAC employees with a business need to know, as designated by management.
Access Restrictions – External	Restricted to contractors, partners, and members of the public with a business need to know.	Restricted to non-employees (e.g., contractors, partners), designated by management, with approved access and signed non-disclosure agreements.	Restricted to non-employees (e.g., contractors, partners), designated by management, with approved access and signed non-disclosure agreements.
Physical Transmission – Internal	Standard interoffice mail and file distribution methods are permitted.	Standard interoffice mail and file distribution methods are permitted.	Direct delivery is required; Envelopes must be marked confidential.
Physical Transmission – External	U.S. mail and other public or private carriers are permitted.	U.S. mail or approved private carriers are permitted.	Direct delivery with signature requirement is required. U.S. mail or approved private carriers are required.
Electronic transmission – Internal	Internal electronic mail and electronic file transmission methods are permitted. No restrictions except that information be sent to only recipients with a business need.	Internal electronic mail and electronic file transmission methods are permitted to those persons who have a business need to know.	Internal electronic mail and electronic file transmission methods are permitted to those persons who have a business need to know. Messages must be marked, “confidential-do not forward.”

Electronic Transmission – External	Approved electronic mail and electronic file transmission methods are permitted. No restrictions except that information be sent to only recipients with a business need.	Electronic mail or electronic files may only be sent via controlled transmission (e.g., private link, password-protected, or encrypted). Recipients must have a business need to know, as designated by management, with signed non-disclosure agreements. Recipients of sensitive information via fax should be notified in advance and instructed to retrieve the fax promptly.	Electronic mail or electronic files may only be sent via controlled transmission (e.g., private link, password-protected, or encrypted). Recipients must have a business need to know, as designated by management, with signed non-disclosure agreements. Recipients of confidential information via fax must be notified in advance and instructed to retrieve the fax promptly.
Physical Storage	Information should be protected from loss and unnecessary viewing by those who do not have a business need to know.	Information should be safely stored (e.g., placed in a desk or file cabinet) when not in use. Information should be protected from loss and viewing by those who do not meet the above noted access requirements.	Information must be secured (e.g., locked in a desk, cabinet, storage bin, or warehouse) when not in use. Information must be protected from loss and viewing by those who do not meet the above noted access requirements.

Electronic Storage	Electronic information should have standard access controls (e.g., password protected network or computer terminal). Standard back-up procedures should be followed.	Electronic information should have standard access controls (e.g., password protected network or computer terminal). Sensitive information should not be stored on shared network directories if any of the individuals who have access to the shared directories do not have a business need to know. Sensitive information should not be stored on removable media or devices (e.g., floppies, laptops, PDAs) without standard access controls.	Electronic information must have standard access controls (e.g., password protected network or computer terminal). Confidential information must not be stored on shared network directories if any individuals who have access to the directories do not have a business need to know. Confidential information must not be stored on removable media or devices (e.g., floppies, laptops, PDAs) without standard access controls.
Disposal/Destruction – Physical Media	Discarded paper, files, and printed material should be destroyed according to GIAC's standard policies and procedures.	Discarded paper, files, and printed material should be destroyed in a manner that ensures that "sensitive" discarded paper, files, and printed material are controlled according to the Physical Storage Guidelines described above, until they are ultimately destroyed (e.g., during collection and transportation). Destruction may be achieved by shredding or de-inking.	Discarded paper, files, and printed material should be destroyed in a manner that ensures that "confidential" discarded paper, files, and printed material are controlled according to the Physical Storage Guidelines described above, until they are ultimately destroyed (e.g., during collection and transportation). Destruction may be achieved by shredding or de-inking.

Disposal/Destruction – Electronic Media	Electronic data should be periodically deleted/ removed, according to GIAC's standard procedures for PC and network maintenance.	Electronic data should be deleted/removed reasonably soon after it is no longer needed. Electronic files should be erased periodically according to GIAC's standard procedures for PC and network maintenance.	Electronic data must be deleted/removed immediately after it is no longer needed. Electronic files must be erased promptly according to GIAC's standard procedures for PC and network maintenance.

8.0 Enforcement

All GIAC employees are responsible for complying with this policy. Reference is made to GIAC's Code of Conduct for enforcement guidelines, including the consequences to GIAC employees for violating the provisions of this policy.

9.0 Exceptions

Exceptions to the policies and guidelines outlined in this document may be approved by GIAC's Information Security Officer based upon extenuating circumstances. It is expected that any such exceptions will pertain to the means and methods used to protect information in unusual circumstances, but not the need to protect such information**.** Employees seeking an exception should consult with their managers for guidance regarding submission of a formal request to GIAC's Information Security Officer.

10.0 Revision History

Approved By: GIAC Board of Directors, Corporate Governance Committee

Date: April 20, 2002 (Initial approval)

3.4 Overview of Key Policy Modifications

A number of significant changes were made to the sample policy, which resulted in the foregoing GIAC Information Classification Policy. A summary of material enhancements and modifications is provided below:

Purpose – The purpose statement of the sample policy was revised and tailored to GIAC's situation. A specific reference to GIAC's information security objectives has been added.

Objectives – A statement of objectives was added to expand on the purpose statement.

Scope – The scope statement was revised significantly to address a number of weaknesses noted

in the sample policy. Specifically, the scope statement outlines the extent of the policy and the nature of situations that it addresses.

Policy – The policy statement outlines GIAC's high level expectations for the treatment of sensitive and mission critical information. The policy statement references specific classifications for information, and corresponding rules for treatment, which are respectively outlined in separate sections.

Responsibility – The revised policy statement includes a new section on responsibility. GIAC's Information Security Officer is charged with responsibility for overseeing the Information Classification Policy and all employees are responsible for complying with the policy.

Classification Categories – The revised policy includes a new section that describes the classification categories. For GIAC, three classification categories are established (confidential, sensitive, and public) as opposed to the sample policy's two categories (confidential and public). Specific examples are provided in the revised policy along with a "default" classification that provides guidance for employees when it is not clear what classification applies to certain information.

Information Protection Requirements – The revised policy includes a new section that outlines rules for protecting the three classes of information in various situations. To simplify the presentation of these rules, a table was created that displays the rules that apply to each of the three classes of information with respect to access restrictions, internal and external transmission, storage, and disposal practices.

Enforcement – The section on enforcement has been modified to reference GIAC's employee code of conduct, which addresses disciplinary actions for violating corporate policy.

Exceptions – A section has been added to the revised policy to address the possible need for exceptions. GIAC's Information Security Officer is given responsibility for addressing requests for exceptions to the Information Classification Policy.

Revision History – A section has been added to the revised policy for tracking revisions and approvals to the policy. Since this policy is new, the information provided reflects the date that the policy was initially adopted by the Corporate Governance Committee of GIAC's Board of Directors.

Definitions – The definitions section in the sample policy was not incorporated into the revised policy as many of the terms in the sample policy were not used.

4.0 SECURITY PROCEDURES DEVELOPMENT

GIAC's Information Classification Policy outlines requirements for protecting information based on its classification as confidential, sensitive, or public. One of the most important requirements involves access restrictions. In order to ensure that access restrictions are implemented

appropriately and consistently, procedures are needed that address how GIAC employees are granted system access rights and how these rights are administered. The procedures need to provide for initial verification of the employee's job function and related access needs. The procedures also need to address how access privileges will be reviewed (e.g., for inactivity or unusual patterns), and revoked upon termination. The following procedure outlines the actions to be taken by system administrators to ensure that the systems under their care are only accessed by authorized GIAC users.

4.1 Information Security Procedure

GIAC System Administration Procedure

1.0 Objective

All systems within GIAC Enterprises represent tools used for gathering, storing, and maintaining internal and external information. In many cases, these systems contain information that is Confidential or Sensitive, as defined by GIAC's Information Classification Policy. These systems require controls to ensure that access privileges are only granted to authorized users. Therefore, designated individuals will be assigned system administrator duties in order to maintain proper control over these systems to ensure the confidentiality and integrity of the information within the systems. The actions outlined below define the duties and responsibilities of system administrators and should be followed for all systems within GIAC Enterprises.

2.0 Responsibility

The system administrator is responsible for establishing users of the system. This role includes, but is not limited to:

a. Determining who is authorized to approve users of the system (e.g., department managers, branch managers, etc.).
b. Defining written documentation to be maintained supporting the approval.
c. Evaluating the access being approved, so that only access that is absolutely necessary for the user is granted.
d. Discouraging anything other than inquiry only access for managers to ensure proper segregation of duties.

3.0 Periodic Review of System Users

The system administrator is responsible for reviewing the system users on an ongoing basis to ensure that only current employees have access to the system. This review is to be performed at least quarterly using system-generated reports. Any terminated or transferred employees no longer needing access should be removed.

4.0 Documented Review of System Reports

The system administrator or designee shall be responsible for performing a documented quarterly

review of all system-generated reports including but not limited to parameter maintenance, and security reports. Documentation may be maintained directly on the reports or through the use of a log and should contain the date and initials of the reviewer.

5.0 System Administrator Independence

The system administrator shall be independent of all daily activities for the system in which they have been assigned system administrator duties.

6.0 System Administrator Knowledge

The system administrator shall be responsible for maintaining a proficient knowledge of the system and the access levels available.

7.0 Periodic Management Reviews

The system administrator shall be responsible for providing management with a system generated listing of individuals under their authority and the current access assigned to those individuals. This shall be done at a minimum of once every six months and management will be asked to review the listing, approve it, and return it to the system administrator. The system administrator shall maintain this documentation for a minimum of 1 1/2 years.

8.0 Verification Before and After System Changes

The system administrator shall be responsible for verifying the access levels of users before and after any conversions and/or enhancements to the system for which they have been given system administrator duties, to ensure that access levels remain appropriate. It is emphasized that only access that is absolutely necessary should be allowed.

4.2 Evaluation of the Procedure

The foregoing procedure for system administrators facilitates the implementation of GIAC's Information Classification Policy by ensuring that access rights are assigned to employees based on their job requirements. Accordingly, access to Confidential and Sensitive information can be effectively restricted to only those with a "business need to know."

The System Administration Procedure address each of the following areas:

What actions should be carried out – Specific actions to be carried out include: (1) Determining who is authorized to approve system users and establishing related documentation; (2) Reviewing current system users for appropriateness; (3) Reviewing system security and maintenance reports; and (4) Providing management with lists of approved users, and (5) Verifying user access levels before and after any system conversions or enhancements.

Why those actions are important – In the Objective section, it is noted that the actions outlined

in the procedure are important due to the essential nature of GIAC's information systems and the need to ensure their confidentiality and integrity.

Who is responsible for carrying out the actions – All of the actions outlined in the procedure are the responsibility of system administrators. These individuals are assigned responsibility for overseeing certain GIAC information systems, and may or may not be part of the information technology department. For example, the system administrator for the General Ledger system, will likely be an employee in the Finance Department due to their familiarity with the application and system users.

When and where the actions should be taken – The procedure specifically states that certain actions (e.g., system reviews for current users and documented review of system reports) must occur quarterly. Other actions (e.g., verifying access levels before and after system modifications) occur on a case-by-case basis.

How the actions can be verified – The actions required by the procedure can generally be verified based on reports and other documented output. For example, at least every six months, the system administrator must provide to management a list of individuals under their authority and these individuals' corresponding access rights. The process of reviewing and approving this list will confirm that appropriate access privileges are being maintained. This, in turn, confirms that the objectives of GIAC's Information Classification Policy are being met.

SECTION 5.0 - APPENDIX

5.1 References

"501(b) Examination Guidance: *Examination Procedures to Evaluate Customer Information Safeguards*," FDIC Financial Institution Letter FIL-68-2001, August 24, 2001, URL: http://www.fdic.gov/news/news/financial/2001/fil0168.html.

Dvorak, Phred, "Mizuho Computer Woes Point to Slow Pace at Japan's Banks," Australasian Business Intelligence, April 24, 2002.

Hutt, Arthur E., Bosworth, Deymour, and Hoyt, Douglas B., (Editors), Computer Security Handbook, Third Edition, NY, NY, John Wiley & Sons, Inc., 1995.

Information Security Officer Training Program (Track 9) Course Material, the SANS Institute, Course conducted at Tysons Corner, VA, March 2002, Reference materials are available at URL: http://giactc.giac.org/cgi-bin/momaudio/s=9.4.1/a=XgudlNq9y1I/ISO_41_policy_risk.

Peltier, Thomas R., CISSP, "Information Protection Fundamentals," CSI Editorial Archive Copyright 1998, Computer Security Institute Web Site, URL: http://www.gocsi.com/archive/policy.html.

Power, Richard, "CSI Roundtable: Experts Discuss the Role of Data Classification Now and in

the Future," Computer Security Journal, Spring 1998 (Vol. XIV, No. 2), Computer Security Institute Web Site, URL: http://www.gocsi.com/round.htm.

"Sample Information Sensitivity Policy," Source: SANS Security Policy Project, SANS Institute Resources, URL: http://www.sans.org/newlook//resources/policies/policies.htm, URL for Policy: http://www.sans.org/newlook//resources/policies/Information_Sensitivity_Policy.doc.

Sanford, Brad, "GIAC Enterprises Attempting to Achieve Defense in Depth," Practical Assignment For GIAC Firewall and Perimeter Protection, Version 1.6, October 14, 2001, URL: http://www.giac.org/GCFW.php.

"Security Standards for Customer Information: Guidelines Establishing Standards for Safeguarding Customer Information," FDIC Financial Institution Letter FIL-22-2001, March 14, 2001, URL: http://www.fdic.gov/news/news/financial/2001/fil0122.html.

Stoneburner, Gary, Goguen, Alice, and Feringa, Alexis, Risk Management for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, NIST, U.S. Department of Commerce, Special Publication 800-30, October 2001, URL: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Swanson, Marianne, Security Self-Assessment Guide for Information Technology Systems, NIST, U.S. Department of Commerce, Special Publication 800-26, November 2001, URL: http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf.