Global Information Assurance Certification Paper

Security Policy

Assessment and Recommendations

Game-winners Issuance Administration Corporation (GIAC)

Prepared By: Ray Slepian
December 27, 2001
Version GISO 1.0 (October 30, 2001)

Security Policy - Assessment and Recommendations
Game-winners Issuance Administration Corporation (GIAC)

Executive Summary

This document presents a high-level security assessment of the computer systems environment supporting business operations for the Game-winners Issuance Administration Corporation (GIAC). As a result of this assessment, three core deliverables have been developed that provide, 1) identification of five key areas of security risk to the enterprise, 2) three high level and "high pay-off" security policy recommendations derived from these risks, and 3) one fully defined procedural document associated with a selected policies.

It is understood that these items will serve as reference material for future security policies and procedures to be developed in-house by GIAC. Accordingly, this assessment is composed of three main sections that reflect the deliverables:

- A description of GIAC's business and technical infrastructure environments
- Defined security risks and selected policy documents
- A selected security procedure document

Section I – GIAC's Business Environment and Technical Infrastructure

General Description

Game-winners Issuance Administration Corporation provides periodic payment benefits to winners of games of skill and chance played by millions of Americans annually. GIAC contracts with organizations, governments, and for-profit business entities to purchase their long-term prize pay-out obligations at a discount to the full payable amount. GIAC then provides annuitized "benefit" payments to the individual winners over a prescribed period of time. Winners are generated from any game source from state sponsored lotteries to high-stakes bingo games. At any point in time, GIAC's revenue flow is primarily derived from the difference between its total pay-out obligations and the market return on its investment fund (a.k.a. The Fund, or TF) from which the payments are made. In addition, GIAC receives a small service fee, collected monthly, through its original contracts with the game providers over the life of each contract.

GIAC's business success is highly dependent upon the development of deeply discounted contracts with game providers and on the length of the payout period to its winners. Longer-term winner obligations (annuities) are usually to the advantage of GIAC since this allows a greater period of time for TF return stability while reducing TF return risk.

In an effort to increase margins and to retain and attract business, GIAC embarked, in the mid 90's, on a program of improved servicing relationships with GP's and winners. Many of these improvements depend heavily upon technology upgrades that make possible a centralized customer service center, enhanced external commerce with GP's, and an internet account self-servicing capability for GP's and winners.

Business Operations

GIAC currently has nearly 500 employees. It is separated into multiple divisions responsible for the support of contracts, GP and winner accounts, marketing, technology, and employee services. In addition, it contracts with independent consultants for specialized services that are not readily available within the employee pool. A short description of the major divisions follows.

The Contracts Division maintains a marketing group to establish new GP accounts and service ongoing contracts, including a Contract Support Department that handles actuarial valuations, contract servicing, and the development and review of prospective contracts. The contracts group works very closely with the GIAC marketing group, which is responsible for acquiring new game provider customers. The Winners' Division provides winner support services through winner account managers that have the primary responsibility for interacting with winners. They respond to inquiries, maintain correct account and demographic information, handle requests for buy-outs (a growing profit center for GIAC), and any other winner's servicing needs. This group constitutes the primary workforce for the Customer Service Center. It should be noted

here that throughout this document, winners and game providers in the aggregate, are referenced as clientele.

Also important to key operations are the Benefits Payout and the Investments Divisions. Benefits Pay-out oversees winner financial accounting and affairs, while interfacing with their external financial intermediary organization (FIO) that maintains actual monetary accounts, makes payments to winners, and handles buy-out settlements. The Investments Division is composed of a small team of managers that have fiduciary duties to oversee TF accounting and performance, as well as, monitor the activities of the contracted external investment managers. The external managers report TF information to the FIO periodically. The FIO hosts reports and query capabilities for GIAC via an application service provider (ASP) function.

GIAC is also composed of the Administrative Division that manages internal budget and expense accounting, and a Human Resources Department to handle the organization's employee needs. The technology division is based upon a central model that supports nearly all of the organization's automated business functions. This division is the Winners Information Technology Services Division, or WITS.

All divisions report to an executive team leading Business Operations, Financial and Administrative Affairs, and Clientele Services. Independent Legal and Security Offices are composed of a large team of lawyers and a lone Information Security Officer (ISO). While the Legal Office reports directly to the CEO, the ISO reports to the Chief of Operations.

To sustain business operations, GIAC maintains five primary business relationships with, 1) game providers, 2) winners, 3) investment fund managers, 4) the financial intermediary and, 5) technical service providers such as internet and application service providers. Understandably, WITS plays a strategic and active role in building, acquiring, and supporting the information systems that are essential to meeting GIAC's objectives.

Information Technology Infrastructure

GIAC's technology infrastructure is defined by the internal and interface elements of the network and the attached devices that includes the mainframe, server computers, routers and firewalls, specialized storage devices and other elements. GIAC's network/device infrastructure is subdivided by firewalls into zones - logically and physically defined areas with similar protective needs or access characteristics. The IT infrastructure that supports GIAC's business activities is composed of the following major elements and technologies:

- Internal Network, Devices, and Applications – supports the office productivity functions (e.g., word processing, file storage and printing services, internal e-mail, etc.), the distributed business applications (custom or commercial-off-the-shelf), and servers and data storage facilities. In addition, a legacy mainframe environment has been a key element under heavy usage by the Winners, Benefits Payout, Contracts, Investments, and Administrative Divisions.

Business applications in the internal network are mostly transaction driven, registration or accounting oriented, and stored within the mainframe environment using a CICS environment to access VSAM files. Large scale MVS/JES batch processing is executed in the evenings and weekends to update key-entered paper transactions, propagate updates between the VSAM file systems and the key distributed data stores, or to create extract data files that periodically populate the interface zone repositories (i.e., Oracle DBMS). A strategic migration from the mainframe to distributed application and database hosting is under way.

Core distributed data (a.k.a., the corporate database) is accessed via a set of applications developed using a proprietary n-tier application environment, and is stored on Oracle databases. A migration to Java-based applications is underway that will standardize the application development environment and support internet-based technologies throughout the organization. The server operating system environment for distributed application is either UNIX or NT depending upon the type of application supported. NT is used primarily to host Microsoft based productivity applications such as Office, Outlook, and mail services, while UNIX is the system of choice for business applications. TCP/IP is implemented throughout the organization, supported on an Ethernet backbone. All client computers are, at least, Windows 95 or greater compliant.

Application access and fine-grained internal authentication/authorization services are controlled through RACF, NT, or Oracle security management systems; some are a combination of the above, or even completely "home-grown". To detect unplanned system usage, multiple sensors have been deployed strategically within the network. In addition, a large number of agents running on production servers provide an intrusion detection reporting capability. The vendor for these products is Real Secure. The internal network is connected to the external network in a restricted manner through the interface zone and through the use of the VPN technology (see the GIAC Network Diagram below).

Interface Zone – a networked area composed of devices, firewalls, and routers that provide a controlled transition zone for GIAC to the outside world (i.e., external network). This zone is sub-netted to handle transactions (and content) between external entities and GIAC using facilities such as e-mail, file transfers, a public web-site access, a protected (winners and game providers) web transaction-based zone, and a Virtual Private Network (VPN) facility for remote users and connections to the FIO. A "perimeter" (firewall) has been established to create an enterprise electronic gateway for most transactions. The perimeter is made up of special-function devices and software acting as an entry/exit-point consolidator so that all data can be inspected and sent to the appropriate transition zone for further processing - or rejected.

Applications and protective services in the interface zone are primarily hosted on NT systems. Today, web services are handled by Microsoft IIS. (This is under review.) All web applications that access confidential or sensitive clientele information are constructed using

an integrated web application development tool set that is Java 2E compliant. It also makes use of a proprietary user-interface design tool. Internet access to confidential information is protected through SSL sessions and password authenticated. GIAC's web identification and authentication facility is a custom-built application that stores credentials in an Oracle database. For all protected business transactions on the web, session states are managed by the web application server through the use of non-permanent cookies.

The public internet was built using Microsoft web tools. GIAC uses Cisco routers and firewall software running on NT servers. Firewall appliances are also placed within this zone. VPN technology has been implemented using Cisco products. Communications between the subnets is encrypted and authenticated via SSL. Data and transactions that pass between the interface and internal zones are filtered through another firewall.

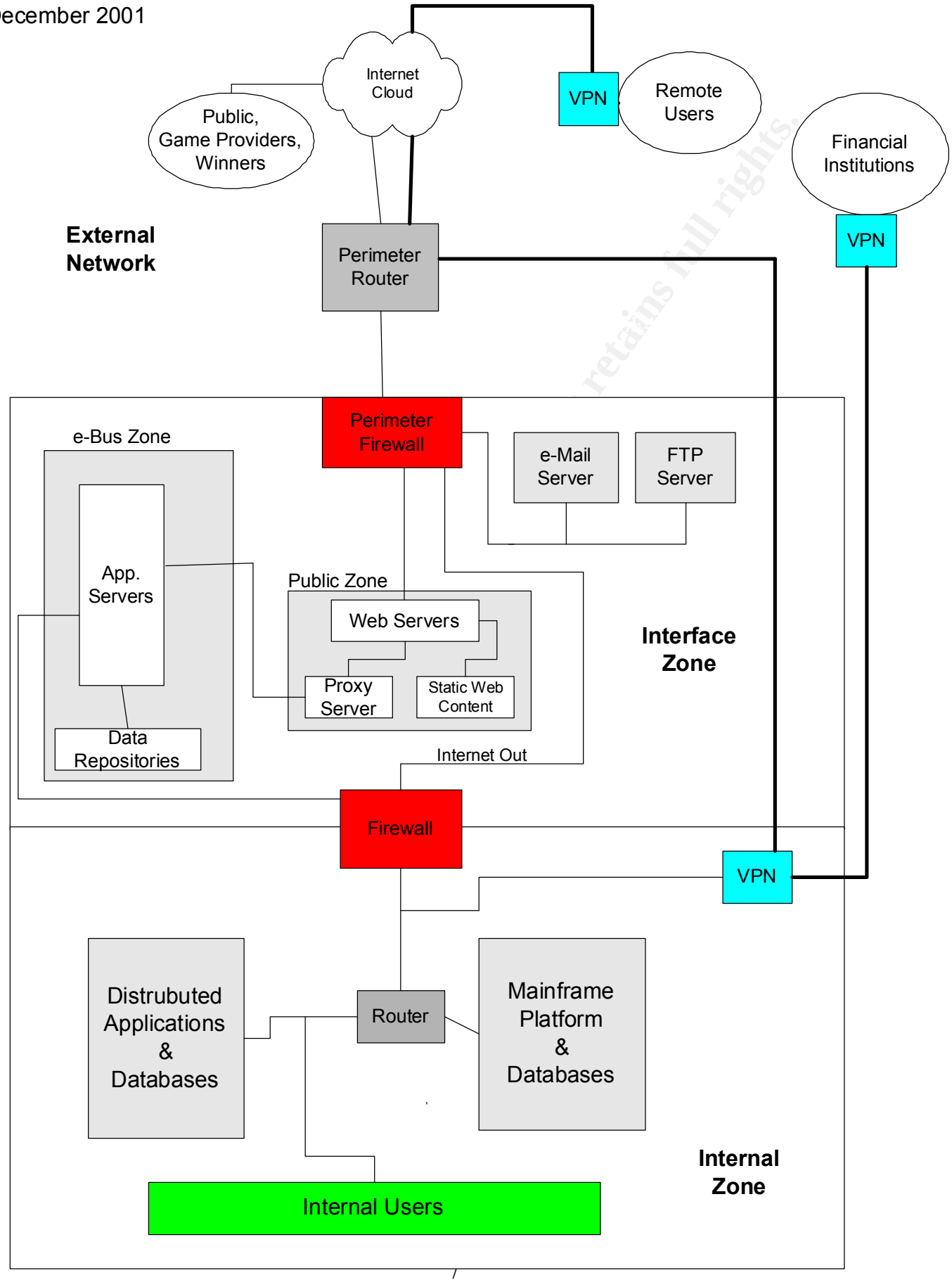
- External Network – includes the public internet, the network and devices, information storage, and applications that are not under the control of GIAC. This also includes ISPs for Internet connectivity and the ASP services provided by the financial intermediary.

  As previously indicated, business and winner transactions between GIAC and its ISP are protected by SSL sessions. Public access via the Internet is not encrypted. GIAC's financial intermediary organizations use the services of an ASP to provide financial data to all of the FIO's clients, including GIAC. Since application service providers are not under the direct control of GIAC, the organization relies on ASP policy compliance to assure that its data is handled properly. As of this time, external audits of the ASP and ISP are not performed. Contracted external investment managers also supply periodic data to the FIO's ASP for reporting purposes. A gateway router VPN with the FIO (the ASP is a subsidiary of the FIO) is used by GIAC to access the resultant investment reports and to run queries related to TF. The VPN also supports access to the FIO payment accounts reports and to remote users, who enter through a firewall gateway. Remote access is restricted to GIAC employees only. (See the logical Network Diagram below.)

GIAC Logical Network Diagram

This diagram is a logical depiction in that is indicates groupings of services, major functional areas, and high-level connections, but does not show details such as all firewalls and routers and their redundancies, or the detailed relationships between outside service entities. These entities include the financial institutions and ASP, and the contracted investment fund managers and the FIO. Information flow and specific application services are not shown. (Note: This diagram is original, but was constructed with assistance from staff.)

GIAC Network Diagram
December 2001



Section II – Security Risk Assessment and Policy Recommendations

Areas of Risk

Methodology

Data for the general risk assessment was developed from a series of workshops and interviews conducted with technical and business area leaders and staff, and with a representative of executive management. In addition, some of the external entities conducting business with GIAC were contacted to gain a more in-depth understanding of their business and technical relationship with GIAC. The reviews generated a comprehensive, yet high-level, view of the infrastructure, the types of systems in use or in the planning stages, strategic business objectives, and perspectives on the operational administration of services and technology. Data sensitivity was also evaluated where possible; unfortunately, no formal data ownership program within the organization exists today. Interviews were conducted over a four-week period. Summarized observations and more detailed security analysis follows.

General Observations

1. Like many organizations, GIAC must maintain a productive, yet secure relationship with its clientele and business partners.

2. In the future, GIAC will become even more dependent upon its technical assets and infrastructure to further it business initiatives.

3. The resultant environment will become even more inter-linked with outside entities, causing some blurring of the line between GIAC's organizational boundary and the outside world, thus making it more difficult to assure that assets are protected. This is seen in the growth of B2B and C2B service platforms.

4. Many of the risks to GIAC security may appear to be technology based when, in fact, they have a high degree of dependence upon the actions and activities of the people who support the business and technical infrastructure. To paraphrase Bruce Schneier in the introduction to Secrets and Lies - good security can be equated to the combined interactions of people, process, and technology.

5. A key and growing risk that is not yet on the "radar screen" is the use of external services, especially those hosted by the ASP. This also includes unknown interrelationships with other external entities. Not only does the ASP house data from GIAC's financial intermediary, but it also receives information from an ever-growing cadre of independent investment management organizations. So, while a VPN may provide a secure communication channel between GIAC and the ASP, the ASP also exchanges sensitive data with the FIO (its parent organization), and with the numerous investment managers employed by GIAC.

Data that are confidential and possibly strategic to GIAC is stored and communicated by several organizations in a sphere of operations that is out of the reach of GIAC's implementation of the defense in depth approach. (*Note this term equates to layered defenses, and is described in Charles VanMeter's article "Defense In Depth: A Primer".) Formalized recognition of these vulnerabilities has not yet occurred at GIAC.

The author recommends that GIAC adopt an "Offense-in-the Open" strategy. While external data protections are not fully addressed or within the scope of this document, suggested steps to implement this approach should be considered that protect information in transit or storage. "Offensive" steps include development of strong policies directed at external entities specifying operational and data protection standards. Other tactics include scheduled and "surprise" audits, the use of security self-audit checklists signed by top level management, and scanning these sites for vulnerabilities. Documentation related to non-disclosure and information release should also be maintained. Awareness and accountability are critical factors in this area.

6. Considering core GIAC business drivers (customer service, competitive posture among peers, full-service product delivery) and the technical infrastructure required to support these drivers, five main risk areas have been identified. These areas are selected because of the negative impact to the organization that they represent if not properly addressed. This includes loss or damage to critical systems or data, prolonged service interruptions, exposure of confidential data, damage to GIAC's reputation and the possibility of litigation, and the destruction of the trust relationship with clientele. After assessing GIAC's security posture, five key areas of concern have been defined below.

Areas of Specific Security Risks for GIAC

A detailed comprehensive risk assessment was not in the scope of this document. As a result some areas of equal import have not been addressed. A short list of these would include establishing an ongoing risk assessment program, a database protection program, implementation of encryption standards, external ASP practices (as noted above), and business resumption planning – a key element in any organization's strategic planning. While of equal value to those below, this document attempts to focus on key internal security strategies that provide a breadth of protection extending across the organization that is of significant value to GIAC if implemented. Each risk area provides an overview of the general vulnerabilities, the resulting consequences if they are not addressed, specific examples of deficiencies observed, plus high-level recommendations and their rationale.

1. Acceptable Use - Proper use of enterprise assets is essential for any organization's long-term survival. Use policy is a primary means to convey to employees, consultants, and business partners the limitations and obligations they have when accessing or using company assets. It clearly sets management expectations that data and assets are to be used only in a manner

consistent with reaching business goals. Key areas to clarify expectations are personal use of systems and assets, protection from misuse of business data, activities that may be illegal to the organization or society in general such as the use of business assets for harassment in the workplace, or the misuse of time. To be completely clear, specific examples of misuse must be included.

Data acquired from winners and partners that is confidential is done so with the trust or expectation that GIAC will apply the appropriate measures to protect it from accidental or intentional misuse. Without an Acceptable Use policy that is enforced, system users may not fully understand (or plead ignorance of) the consequences of their activities. They may not know where the line is drawn between true business use of assets and any other activities. Accidental or intentional unauthorized access to, or release of critical information can easily occur. (Misuse of company time and business resources can become a serious problem.) Without an acceptable use policy in place, corrective actions for abuses may not even be enforceable. Illegal activities that are not defined may not be prosecutable, and the integrity and privacy of intellectual property or confidential information can be compromised. In the most severe cases, these violations can be a real threat to GIAC's ability to remain a viable corporate entity.

GIAC now provides new employees a short statement regarding asset usage during initial orientation. This is not a comprehensive statement and in fact is on a faded copy containing some unreadable text. In addition, employees are not exposed to this material again in follow-up sessions. Formal security awareness training is not available at GIAC. Of equal concern, is that consultants and student assistants are not even exposed to these new employee sessions or the asset use expectations. Further, signatures are not solicited from this population on an independent basis, and may or may not exist with their consultant agency (from which most are actually deployed to GIAC). There is much room for improvement here; the benefits of which would be realized by both the organization and its paid resources.

Building and enforcing an Acceptable Use policy is a first step. Employees must be fully informed of its content and constraints. It may be necessary to have all employees and consultants sign a statement indicating that they have read and agree with the policy. Most important is to gain acceptance and compliance; enforcing this policy should only be necessary when employees choose to ignore its tenants. Ultimately, managers are key to reminding staff of its importance and monitoring compliance. Additionally, it may be necessary to develop several levels of expectation based upon an employee's role or level within the organization. The goal is to clarify before significant incidents occur in order to prevent them from occurring. Employees must realize the sincerity of the organization in this area to become fully committed to following this policy.

2. Access Control and Account Management – Strong and specific control over internal and external user access to the organization's systems and data are essential to protecting the confidentiality, integrity, and availability of those assets and establishing accountability.

This covers the access rights of all users and entities, including internal, external and system administrators. (This could also include automated processes as well - but to do so is not in the scope of this discussion.)

If GIAC fails to maintain access control through strong account management practice the results could be severe. They run the gamut of incorrect assignment of privilege to users, threats to data integrity, violations of confidentiality and privacy, information destruction or theft, and the introduction of malware (e.g., viruses). Access accountability does not exist in a poorly managed account environment.

GIAC has an account management strategy but it is not focused on a single point of accountability. There are several methods to gain accounts depending upon what managers feel is required. Managers, or even staff, can contact administrators such as the e-mail administrator, or a UNIX administrator for application access, and the Oracle administrator or DBA for data access. Consultant accounts are established but are rarely revoked since they are not tracked through any central system as employees are via Human Resources. Aged accounts with no recent usage are not tracked unless an administrator is especially diligent or "has the time". The present Account Management policy is very narrowly focused towards administrators and not readily available to users. Account management is mostly dependent upon the knowledge and upkeep of seasoned employees. It is far from an institutional priority at GIAC.

Access to GIAC's systems and data should be closely controlled by establishing individualized accounts with restricted rights and privileges. Account management must be maintained through formalized administrative processes that clearly define roles and responsibilities for requestors, administrators, and users. GIAC's system users should be provided with account rights and privileges that allow access to only those assets and systems that are necessary to perform their job function. Users should also have defined behavioral expectations and responsibilities, for instance, not sharing their account or password with anyone, and to protect access by always using password protected screensavers. Awareness of positive activities related to access protection at an individual level is central to successful implementation of an effective account protection program. It is in this area that most employees are vulnerable. The practice of social-engineering is very effective and relatively easy for those with malicious intent to gain illicit account access. Improperly trained customer support and help desk employees can be just as likely to become victims of these schemes. Individual account protection strategies should be a core focus of security awareness and training programs at GIAC.
(See Access Control/Account Management Policy below.)

3. Infrastructure Security: Perimeter, Network, and Device protection – While this is a broad category that covers the network and all attached devices within the internal and interface zones, it is important to approach this at a high enough level so that crucial common principles can be applied consistently across the infrastructure. It is the author's view that once this perspective is clearly defined, more focused policies and practices can be defined

that drill down to the key elements that make up this infrastructure. GIAC must protect its infrastructure and the functionality it supports with a comprehensive defensive strategy. Ultimately, this is critical to realizing GIAC's core objectives.

Threats to GIAC are manifold. If GIAC does not adopt comprehensive protective strategies, the results could be lead to a very porous environment through the uneven application of security controls the enterprise. This is very much a "weakest link" dilemma. Risks include system-wide infections by viruses/Trojans/worms, disabling attacks on device operating systems or applications that can lead to stealth operations by intruders. Malicious attacks can result in system shut-downs, information theft or data manipulation. Internal attacks can result in data loss, manipulation, or loss of confidential information. Insiders with the right set of skills and motivation can sniff the network (i.e., intercept data packets with a hardware device), conduct password attacks to gain access to systems or data. In turn this could result in a host of problems such as, loss of intellectual secrets, revealing compromising information about individuals, identity theft, or destruction of data. For the organization these activities can be anything from a nuisance to the inability to carry on key business functions. In summary, losses can be severe.

GIAC has several major technical environments, plus a rather complex interface zone infrastructure. There are many environments to be protected. Observations indicate that while some of the infrastructure groups have developed structured procedures that are followed, others do not. While an IDS system is deployed, simple protective steps that span the infrastructure are not applied evenly such as patch deployments. One major exception is the area of malware protection. This program is in fact very well developed using a set of high-level principles that could provide great benefits to the other infrastructure areas if copied and implemented. Too much of the security practice for the infrastructure is fragmented and dependent upon the skills of individual administrators - and luck. Another area of concern for GIAC is the level of involvement and commitment of the various managers to a security strategy at all (not just to a comprehensive strategy). Since there are several infrastructure groups, each managed separately, and each with their own set of challenges, coordinated security has not been priority.

GIAC depends heavily on its data assets and information exchange and clientele access for its business success. Special attention should not only be focused in the areas designed to support public and business external data exchange transactions, but also on the possibility of internal compromise. Vulnerabilities are common for a variety of reasons – not the least of which is vendor inattention to security. But, a comprehensive set of practices across the infrastructure establishes the process and technical foundation on which the enterprise can build. This approach also supports a successful defense-in-depth strategy. A secure infrastructure policy is the glue that holds disparate environments together.
(See Infrastructure Security Policy below.)

4. Application Level Security – Devices and networks would serve no real purpose without the myriad applications (software) that "run" on them. Applications capture GIAC's key business data and provide critical information to its users and partners. This environment (systems and data) is in constant demand, while undergoing constant change. Applications also provide a direct link to one of the most crucial assets of the organizations – its data. A lack of sound security practices that integrate requirements and controls within the application development process can provide another gaping hole in the protective shield of the organization.

   Some of the key risks to GIAC of non-compliant applications are deficient user identity and authorization controls leading to unauthorized access and possible breaches of confidentiality and data integrity. Inappropriate exposure of production data to employees and consultants during the development/testing phases can result in privacy and confidentially exposure. Not following enterprise security standards leads to independent solution designs that may not conform to enterprise data protection standards. Such a standard could be an enterprise directory authentication platform with plug-in security routines for applications. Another serious concern is the potential for exploits based upon programmer-introduced illegal or malicious code in the system to be deployed. If GIAC does not apply structured security requirements and controls to application development and acquisition, security practices are practically left up to chance.

   Like many organizations, application security policy and practice are not formally recognized by most managers and project staff in GIAC. In this respect, GIAC is actually practicing a mangled interpretation of the principle of "due care" – a standard that is used to compare the activities of an organization with that of the average organization in its class. (Note: Due Care is discussed by Jack L. Strauss in his article "The Use of Intrusion Detection Technologies in Corporate Information Security Policy Implementation and Enforcement".) While some project leaders solicit security requirements, most do not. Even if they do, they are not comprehensive, nor are they organized in a manner that can be easily integrated into the systems development life cycle. Many are "controls" based, so that the requirements behind them are not necessarily clearly understood. Finally, when a project falls behind schedule, as most do, security implementation is one of the first areas to be jettisoned. Management and data owners do not seem to understand their full responsibility, or the trade-offs that results. The ISO is overburdened and cannot assure compliance with security practice in this area.

   Implementation of application level security requirements should not be neglected. It is important to assure each application development project meets at least minimum security requirements by production deployment. Residual risks that have not been addressed should be brought to the attention of management. They must be aware of and decide if the losses due to security risks are less than the potential gains of deployment for the business. Management must accept these risks to deploy the application. Applications developed without following enterprise security standards can unwittingly expose the entire organization to unnecessary risk and nullify the critical security measures already in place.

5. Security Awareness Training – Even the strongest fortress is not completely protected if its occupants are not well prepared for transgressions. This obviously applies to fortress soldiers whose job it is to protect the castle and its inhabitants. But even in that setting, proper knowledge of how to conduct oneself – from the leadership to common citizen – could make the difference between safety and dire consequences. A seemingly innocuous conversation with a stranger that reveals information such as the number of soldiers within the garrison, or that the protective walls are aging and not well maintained can be valuable information to the wrong person. Perhaps not so dramatic, but still applicable, GIAC must provide knowledge in the form of proactive security awareness and training to all resource users at each level of the organization. It cannot just depend upon its security specialists for full protection. An ongoing program of security awareness and training that is tailored to specific groups must become a cornerstone of enterprise security strategy.

   Many types of threats are present to the external and internal environments of all organizations. However, not all or even the most effective defensives are implemented via the complex technical solutions. Much vulnerability occurs at points within the organization that represent targets of least resistance. They are the "low hanging fruit" most easily accessible with the least amount of effort. And, they are not obvious to most users. An example is an employee who steps away from their desk for lunch but forgets to activate their desktop password-protected screensaver. The employee's business files, e-mails, systems and network access can be fully exploited by anyone with malicious intent. This could have serious consequences to GIAC. A short list of easy targets includes lax desktop protection practices (e.g., deactivated screen savers, poor password selection and protection, and logon Id sharing), lack of client virus updates, and easy physical access to areas storing sensitive information.

   GIAC does not have a formalized security awareness and training program (SAT). While many employees are motivated to protecting information from disclosure or misuse, they lack a formal understanding of the effective practices to do so. Most interviewed or observed did maintain password confidentiality, but were frustrated with the need to maintain several passwords for disparate systems and the periodic change requirements. They were sincere in trying to maintain clientele confidentiality, but did not link password updates with providing good protection to privacy of information. Instead they see it as something that is imposed upon them by restrictive technical management. A reasonable conclusion is that they do not fully appreciate some of the ways their activities play an integral role in protecting their clients. Also of concern, few have been properly prepared to recognize or respond to social engineering practices that take advantage of the conflicting goals of providing good customer service while preventing release of confidential information.

   While staff has a hazy picture of their role in security, management seemed even more detached, though theirs is a higher level of responsibility. Attitudes generally seemed to reflect a kind of unconscious delegation of security to the experts. While espousing strong commitment to protection of assets, few seemed to understand their role and responsibilities,

either as data owners or through the actions of their staff. Confusion also exists in the differentiation of business management's role vs. the data custodial role of the WITS Division. The result is that accountability has not been clearly established. This can become a serious issue in the event of a major security incident (or even become the cause of such an incident). Indicative of this confusion, formal incident response has been left up to the technical staff. As in the case of infrastructure security, incident response is understood and interpreted according to technical group membership. With the exception of the virus protection group, where it does exist, response planning does not usually include business management.

Technical support groups such as the Help Desk, with a more focused role in protecting assets (yet a strong mandate to assist users in maintaining system access) follow protocols for password resets and reestablishing client sessions. Interviews indicated, that new staff are not formally trained but rely on more experienced staff for their information. They would be well served if they received in-depth training, especially regarding social engineering practices typically targeting these employees. System administration has been discussed in the infrastructure risks section of this document, however, it is worth mentioning here that the need for ongoing in-depth training in proper device and system software administration is crucial to maintaining a strong security profile at GIAC. Training provided by organizations such as the SANS Institute would be beneficial.

The benefits of even a minimal SAT program at GIAC are many. An example: By gaining an understanding of the importance of each employee's role in asset protection through good password practices, an employee is much less likely to (knowingly or unknowingly) defeat security through the use of weak passwords or attempt to make multiple password changes to return to a favorite one. Easy exploitation of vulnerabilities can be dramatically reduced. Management practices should result in the oversight and reinforcement of positive security practices with established accountability. Focused training for the 'soldiers' (e.g., Help Desk and system administrators) should shore up weakened 'walls' and the practices that provide protective and detective layered defenses for GIAC. The security profile measurement bar for the enterprise should be raised by several notches. Beyond this, though, SAT provides staff and management with an improved sense of competence in reducing vulnerabilities and in reacting to suspicious activities.
(See Security Awareness Training Policy below.)

Security Policies

The three policies selected for this document are Access Control/Account Management, Infrastructure Security (Perimeter, Host, and Network Protection), and Security Awareness Training. The selected policies are broad in scope; this is intentional so that the most information possible can be conveyed in these important areas. The policy format used is a combination of the risk assessment requirements and additional resources with which the author has become familiar. Policies include a column on the left side to identify key focus areas and

embedded links in the text that reference current or future policies or procedures. These are denoted by the use of brackets – []. For clarity, responsibilities may be identified within the text of the policy "bullets"; otherwise a separate section describes responsible participants and activities. Finally, each policy contains a Link section for further expansion. Direct references or citations are not included in the policy as a matter of form. Where critical, references are shown in the Link section.

GIAC Enterprises Security Policy
Access Control/Account Management
Version: P001, December 27th, 2001
*See Links at end of policy for citations

Purpose	To describe GIAC's electronic resource access control and account management practices To build a foundation from which management procedures and standards can be developed
Background	GIAC's computer systems and the data used by them are fully owned by the GIAC Enterprises. GIAC's information resources are protected intellectual and physical property, clientele and business partner data, and employee information and productivity resources. Access to, and use of, these resources must be restricted to those with an explicit need to a specific resource, and only for the beneficial purposes of the organization. Access to these assets will be granted based on the principle of "least access" and will be consistent with system and data confidentiality, integrity, and availability. All access rights will be controlled through the issuance of usage accounts. Account administration assures that appropriate access rights are established, provides user accountability, and usage auditability. The Access Control/Account Management Policy defines account principles, usage controls, administrative structure, and high-level roles and responsibilities.
Scope	This policy applies to all employees, consultants, contractors, and external entities with a need to use, interface with, or administer GIAC's computer systems and data. Access is only granted through the GIAC sanctioned Account Management (AM) Procedure. Access to any person or entity that is not controlled by the AM process is prohibited. This policy **does not** cover access control functions such as those associated with granular field and data access that is usually controlled within specific business applications. It **does not** cover specific access control lists for operating systems or firewall rules normally used to discriminate between appropriate device and software interfaces within the enterprise.
Policy Statements	

Account Management	• The Account Management (AM) function shall be created to administer all electronic asset access, including user and system administrator accounts. • AM shall be a separate function that reports to the WITS Division. • Procedures defining Account Management functions, account issuance, account rights and responsibilities, and account administration life cycle events will be created. [Link – New Account Request Procedures] • The AM group shall create a user account document that defines system user responsibilities (e.g., password creation and protection, screen saver protection, client workstation configuration changes, etc.). This document will be distributed to all new system users at the time of new account set-up. • All AM procedures and documents shall be created and maintained by the AM group manager and approved by the Chief of WITS and the ISO.
User Accounts	• Access to GIAC's systems and data by individuals and entities will be controlled through the creation of individual accounts that are linked to specific devices, systems, or applications (or a combination of these). • All system users will obtain access to GIAC's electronic assets via the formal AM process prior to accessing any system or data owned by GIAC or its business partners. • Stored individual account information will be protected from unauthorized access by security procedures representing the strongest level of security in use at GIAC. [Links: Data Ownership and Classification, Infrastructure Security] • Access to data will only be granted to individuals with the (auditable) request of the data owner or from their designated Account Requestor (AR). • Accounts will only be granted to users with completed signed non-disclosure and Acceptable Use documents. It is the responsibility of the Account Requestor to confirm and store these documents. • Accounts will only be provided to users upon auditable request from an approved Account Requestor. • All account changes will be processed through the AM process • Generic or group accounts are not permitted without receiving a variance from the ISO. • Any changes in status of Account Requestors will be reported to the Account Management function by the data owner. • Account access information will be stored and backed-up in such a manner as to be available to the Disaster Recovery team if needed.

System Administrator Accounts	[Link: Business Recovery and Disaster Recovery] • Access should only be provided to the systems required to conduct the specific business functions assigned to the individual using the principle of least access. • Technical staff, responsible for mainframe and server software configurations and security administrative functions, will obtain User accounts as described in the User Accounts section of this policy. • Specialized accounts to provide network, device, and software administration support will follow more restricted procedures. • Administrators of the network and devices will receive their accounts via by the WITS chief or designee. • System administrators shall not act as Account Fulfillers (by setting up account access rights on servers) in the AM process for their own accounts. • Administrators functioning as Account Fulfillers will only provide access to systems and data as a result of receiving a proper request notification from the AM process. • See the following Policies and Procedures for detailed System Administrator account maintenance. [Links: Identification and Authentication Policy, System Administration Policy and Procedures]
Responsibility & Limits	• The WITS Account Management group is only responsible for centralized administration (facilitation) of the account request process. [Link: New Account Request Procedure] • Data owners will be established by the senior management level of the organization. For purposes of this policy, data owners will directly, or through their designee, classify and authorize access to the data. (Full responsibilities are defined in a separate policy.) [Link: Data Ownership] • Account Management will maintain an updated copy or list of all approved Account Requestors and Fulfillers. • Data owners will report any change in Account Requestors immediately to the AM group or chief of WITS • It is the responsibility of all GIAC managers to follow the AM process to grant accounts to employees and consultants. • It is the responsibility of all GIAC managers to report any changes in the status of their employees and consultants that may impact access to systems and data and to request the appropriate changes to user accounts in a timely manner.

Compliance	Employees, contractors, consultants, and any system users of GIAC found to be out of compliance with this policy will be subject to disciplinary action up to and including termination. And, depending upon the severity of the action, could be subject to legal prosecution.
Authority	All policies have been reviewed and approved by GIAC executive management. Any activities deemed to be illegal will be handled by the proper authorities in accordance with state and federal laws.
Links & References	Embedded in policy text New Account Request Procedures – See Section 3 Additional references are documented within SANS Seminar texts and other sources cited at the end of this document.

GIAC Enterprises Security Policy
Infrastructure Security – Perimeter, Network, Devices,
Version: P001, December 27th, 2001
*See Links at end of policy for citations

Purpose	To identify GIAC's technical infrastructure security needs as an integrated whole that is dependent upon the sum (and protection) of its component parts To build a foundation from which management procedures and standards can be developed
Background	GIAC's computer systems environment is a key component of its business success in delivering critical services to its employees, clientele and partners. The foundation of the technology infrastructure is the network and the devices attached to it. This infrastructure is complex; supporting many component functions that require specialists at many levels to properly support its total functionality. GIAC has a strong interest in the sanctity of this environment from at least two levels. First, from the enterprise perspective, the infrastructure must be designed and architected in a highly coordinated manner to provide an effective, reliable, and safe environment to internal and external users and applications. Second, each major element of the architecture, down to the device level, represents a link that must be equally well protected so that exploitation of any one component does not put the entire infrastructure at risk. This policy is directed at the first view of the infrastructure. It is directed at common practices to be followed throughout the technical infrastructure that act as a unifying objective for all infrastructure support groups. An additional set of policies and procedures will address the more fine-grained needs of the infrastructure sub-environments. [Link: Various policies/procedures]
Scope	This policy is focused on the enterprise view of the technical infrastructure, its component parts and their interrelationships. While it applies to the support of all of the major elements of the technical infrastructure including computers, firewalls, routers, storage devices, and the network that connects them, its goal is to treat infrastructure management as a coordinated whole. This policy **does not** cover the more granular specifics of operating systems, firewall settings, database security, or NT vs. UNIX. These are discussed in detail in complimentary policy and procedure documents.

Policy Statement	
Centralized Planning and Change Management	• An oversight body known as the Enterprise Infrastructure (EI) Group will be created to address GIAC's technical infrastructure at its highest levels. • EI will be responsible for enterprise architecture strategy development and to provide enterprise impact analysis and approval of new, or changing, business application needs. • EI will be composed of enterprise level managers and specialists from groups such as DBA, ISO, architecture, infrastructure and applications management, desktop support management, (and others as required), and will report to the chief of WITS. • The Infrastructure Manager will chair the EI committee. • Enterprise change-management procedures will be developed by EI and made available to technical project managers during the planning stage of any projects that may impact EI. • Project managers will work closely with the EI at all stages of project development, but especially during the general and detailed design cycles. • Cleansed architectural documents should be made available to all qualified project managers or change agents to enable them to incorporate enterprise standards in their design. • Only EI approved deployments will be allowed in the production environment. • Security of GIAC's systems and data will be a prime driver in granting design and deployment approval.
Infrastructure Managers	• Infrastructure managers will form a working-group to establish a set of common administrative practices between their areas, regardless of the platform supported. This group will meet periodically to create and upgrade these common practices (CP). Examples include change management, configuration control, device security profile maintenance, deployment practices, etc. • Common Practices will be documented and stored in a location available to staff on a needs basis. Infrastructure managers will determine individual access rights. • Infrastructure managers will develop an assurance program based upon common practices. They are also responsible to see that staff are properly trained, resourced, and implement the CPs. • Infrastructure managers are responsible to resolve or correct deficiencies indicated by scans or other sources of input that result from the implementation of CP.

	• The Infrastructure Section Chief has the ultimate responsibility to see that all infrastructure managers implement CPs.

Common Practices	• Structured procedures, defined as Common Practices will be defined in (at least) the following areas that apply to all infrastructure groups.
	  • Device OS configurations will be maintained on a "mastered" medium, such as CD ROM, and updated regularly. Servers will only be configured from the most recent master.
	  • A change management process will be developed to serve as a model to implement common infrastructure changes such as patch and upgrade management.
	  • Patch installation will be proceduralized.
	  • On all new or reconfigured devices, systems security elements, such as IDS agents and sensors, must be installed according to practice. [Link: Security Maintenance]
	  • Deployment procedures will include testing and vulnerability scans and include zones and servers that interact with the entity being deployed.
	  • Configuration and vulnerability scans will be completed on installed devices on a frequent basis in all environments. Management will review resultant reports periodically.
	  • Key production system monitoring will occur regularly. [Link: System Monitoring and Reviews]
	  • Incident Response procedures that define the steps from detection to completion must be in place for all groups.
	  • Network topology maps will be developed and maintained for each area. A high-level roll-up map will summarize the topology and infrastructure interrelationships in a single diagram.

Infrastructure Administrators	• Administrators will become knowledgeable of, contribute to, and follow the CPs as defined. • Administrators will work with Infrastructure managers to further define more granular procedures that are specific to their area of expertise, but are based upon, and linked to the CP models and practices. • Administrators will report all security incidents immediately. [Link: Security Incident Response Policy] • Administrators will play a key role in preventing, detecting, and responding to potential security incidents and will act as the first line of human defense under the Defense-in-Depth paradigm.

Responsibility & Limits	• Common practices are meant to provide models or templates for activities that are similar across the infrastructure. It is everyone's responsibility to be sure this is adhered to, especially Infrastructure management and top leadership. • It is the responsibility of the infrastructure chief to be sure that the Infrastructure Enterprise Group activities and decisions are communicated to and coordinated with the infrastructure managers especially if there is an impact on the common practices.
Compliance	Employees, contractors, consultants and any system users of GIAC found to be out of compliance with this policy will be subject to disciplinary actions.
Authority	All policies have been reviewed and approved by GIAC executive management.
Links and References	Embedded in policy text Additional references are documented within SANS Seminar texts and Chris Brenton's, Mastering Network Security, Bruce Schneier's Secrets and Lies and other sources at the end of this document

GIAC Enterprises Security Policy
Security Awareness and Training
Version: P001, December 27th, 2001
*See Links at end of policy for citations

Purpose	To describe GIAC's security awareness and training policy and to underline its importance to the organization To build a foundation from which management procedures and standards can be developed
Background	GIAC's supports awareness and training in every area of competence necessary for employees to be successful in fulfilling their mission and adding to the success of the organization. Security awareness and training are a critical element in building employee competence. Awareness is the bottom line of good security practice. It is necessary for all employees and system users to reach a basic level of awareness to make them much less susceptible to internal and external security threats. Security training takes this a step further. It is directed to those employees in more sensitive positions, frequently handling confidential data, or working closely with technical systems. The Security Awareness and Training Policy (SAT) defines the need for a formal program, who should receive this education, role-based education, and basic employee responsibilities.
Scope	This policy applies to all employees, consultants, contractors, and external entities with a need to use, interface with, or administer GIAC's computer systems and data. This policy defines the program and high level contents. It **does not** cover detailed content for the many specific duties performed by employees within the organization. It is also not inclusive of the technical knowledge or procedures used by Help Desk staff or by system administrators in the practice of infrastructure support. This type of training will be provided through more focused educational exposure.
Policy Statements Security Awareness Program	• GIAC will develop an ongoing Security Awareness and Training (SAT) program that is structured to meet specified goals of security education. • These goals should be commensurate with those of similar organizations following best practices in security awareness. The

	program will also require customization to meet the specific requirements of GIAC. • Development and execution of the SAT program will be the responsibility of the organization's Information Security Office. The ISO is responsible for its administration. • The primary goals of the program are to protect electronic system data and assets through knowledgeable activities and safe practices of system users. • An intranet page supporting security awareness and updates will also be established and maintained by the ISO.
Program Focus	• The SAT must be developed in a manner that it clearly targets distinctive groups within GIAC. • Groups include GIAC employees, GIAC consultants and contractors, GIAC general management and technical management, and top-level management. • The ISO may contract with an external security service agency for general awareness training. The HR Division must be party to this training plan and the delivery of the training. • The ISO may not contract with external partners for security awareness and training beyond the general staff level. This training, which reveals more about the enterprise and its data, will be developed and conducted from within the organization and under the direct control of the ISO. • Training for top-level management and general management must include Legal Office briefings and issues consideration, plus consequences of non-compliance with security policy. • Specialized training may be required for individuals handling the most sensitive information and may be coordinated with the management of the specific employee's division to provide the correct focus. • General SAT should be held annually at a minimum, and be part of new employee orientation. A comprehensive, but high-level security manual, should accompany this training. The manual should be reviewed and updated yearly. • Distribution of the manual and a brief orientation should be held for all contractor and consultants within the first two weeks of formal activities for GIAC. • SAT for managers should be held throughout the year with enough sessions to assure that all managers receive training at least two times in any annual period.
SAT Program Content	• Awareness programs for general employees is focused upon building

	security awareness in areas such as password protection, physical access to work areas, social engineering, identifying confidential data, and malware. It will also be directed toward understanding the consequences of poor security practice. • Awareness training for managers will emphasize the importance of their role and responsibility in promoting good security practices among their staff. Where managers are responsible for the integrity of data stored in enterprise databases, data ownership is required. [Link: Data Ownership and Classification Policy] • High-level management must understand their responsibility to their subordinates, as well as, the consequences of security breaches to the organization. This includes legal implications, concepts of confidentiality and ownership, and the concept of due care. Awareness at this level is an educational and information exchange process.
Responsibility & Limits	• Key responsibilities have been identified in the text of the policy.
Compliance	Employees, contractors, consultants and any system users of GIAC found to be out of compliance with this policy will be subject to disciplinary action.
Authority	All policies have been reviewed and approved by GIAC executive management.
Links & References	Embedded in policy text Additional references are documented within SANS Seminar texts and USC's Security Awareness internet site: www.usc.edu/org/infosec/sate.htm.

Section III – Security Procedure

GIAC Enterprises Security Procedure
New-Account Request Procedures
Version: Pr001, December 27th, 2001
*See note at end of procedure for citations

Background
Restricting system and data access to only those users with a specified need is a key means of protecting the confidentiality and integrity of GIAC's data assets. Restricting authority, or access to specific services and systems also enables GIAC to assure that information is available only to users with a business need for this information. Protecting system and data assets helps GIAC maintain its trust relationship with its business partners and clientele. To accomplish the goal of user access control, GIAC will assign an individual account to each user that will grant the user with specific rights and privileges. These rights and privileges are assigned depending upon the role the user plays within the organization. This procedure defines the process of requesting a new account for general system access, the key roles responsible for completing the request, and key documents to support the process. Remote access accounts are not described in this procedure. (See the Remote Account Request Process.)

Procedure Owner
Account Management Unit (AMU), Winners Information Technology Services Division
For more information, contact the AMU manager.

Key Definitions

Term	Definition and Primary Responsibility
User	GIAC employee, consultant, contractor, business partner, or person with formal permission to access the organization's electronic systems or data.
Account	Method used to provide restricted access through rights and permissions to individuals using system assets.
Logon Id	Means used to identify authorized user of system assets and to associate rights and privileges with that user.
Data Owner	Usually a division chief, is the individual responsible for the protection of the data under their control, any changes to the data, and access rights. The data owner will, in most cases, delegate the user access request process to a designee or requestor.
Requesting Manager	The manager or authorized individual who retained the services of the new employee or consultant and is responsible for completing the New Account Request Form to be processed by the Requestor.
Requestor/Designee	Designated by a data owner, requestors are the only GIAC staff besides data owners authorized to approve and request system access for users of systems accessing their data.

Fulfiller	Usually a technical administrator who will, upon authorized request, grant specific privileges (by setting up a local account) to access network services, a server, an application, or a database. Services and applications can include e-mail, internet access, and workstation productivity suites, such as Microsoft Office.
Password	A secret string of characters known only to a user that is used after a user identifies him/herself to the computer system with a logon ID. The password is used to authenticate that the user is really who they say they are since no one else should know it. Password characteristics are based upon enforced standards to be sure they are not easy for unauthorized users to guess.
Account Manager	Also known as facilitators, account managers (the Account Management Unit or AMU) are a group of designated account specialists within the Winners Information Technology Services Division who interface with account requestors and facilitators. AMU assures proper processing of accounts in the agreed upon timeframes and audits current and old accounts for proper usage.

Enabling Documents (electronic and paper)

Data Owner Reference	Identifies the complete list of owners organized by system and identifying the data that they are responsible for. This document also identifies the authorized designee of the data owner and is maintained by Account Management Unit.
List of Accounts	An electronic database that is maintained by AMU, but manually updated whenever an account status is changed through the request process.
Non-Disclosure	Legal document maintained by the ISO and signed by all system users and employees verifying that they understand their role in the protection of confidential information. An account requestor may not make a request for a new account without verifying that this document has been signed by the user.
New Account Request	Paper document completed by account requestors that identifies new users by name, ssn, requesting division, access required, and requestor signature among other pieces of information. This document is processed and stored by AMU. A copy with pertinent comments (if any) is sent back to the original requestor.

New Account Request Procedure Steps

Procedure Begin

- This process begins when a manager or authorized person employed by GIAC receives final approval from HR (for new employees), or gains final approval via contract (for consultants) to complete the recruitment process

- The requesting manager will complete a New Account Request form including the key elements listed below. Items in parentheses indicate the responsible individual. It is important that this form is submitted to the AMU at least one week prior to the start date of the new employee/consultant
  - SSN of employee/consultant (Manager)
  - Name of employee/consultant (Manager)
  - Unit hiring/contracting (Manager)
  - Start date (with GIAC) (Manager)
  - Requested account set-up date (Manager)
  - Requesting Manager Signature and phone extension (Manager)
  - Authorized Requestor signature and phone extension (Requestor)
  - Date of Request (Manager)
  - Check boxes of system access and services needed (Manager/Requestor)
  - Comments – to include systems or services not included above (Manager, Requestor)
  - Check boxes to verify receipt of signed Non-Disclosure and Acceptable Use documents (Manager)
- The New Account Request form will be submitted to AMU via office mail or hand delivered. It is confidential information and should be in an appropriate enclosure and marked for receipt by AMU.
- An AMU Account Manager will review the form, validate the Requestor and that the form is complete. If necessary, the Account Manager will contact the Requestor for clarifications if necessary. It is the role of the Requestor to resolve any discrepancies with the Manager related to content and access rights.
- The AMU Account Manager will also add the appropriate demographic information regarding the request to the List of Accounts database. Specific account information will be added by AMU as the Fulfiller verifies their creation.
- Once verified, AMU will then create an e-mail notification (using an existing template) from the Request form and send via a distribution list to the appropriate Fulfillers such as the Exchange administrator, Novell, CICS (RACF), and administrators of requested distributed systems where access will be required.
- Fulfillers will set up appropriate accounts on the devices or systems that enable access to only those specifically noted on the e-mail request, and only in those areas of their specific responsibility. If there is a need, the Fulfiller will contact the AMU Account Manager for clarification – not the Manager or Requestor.
- When a Fulfiller has completed a new account set-up in their respective area, they will reply to the e-mail from the Account Manager with an affirmative message. (Unless there are specific difficulties, which must be handled in a timely manner.)
- The AMU Account Manager will collect the returned e-mail confirmations, validate these with the original Request form, and record those accounts that have been established in the List of Account's database.
- When all accounts and access have been established and the List of Accounts database has been updated, the Account Manager will sign and date the Request form and return it to the Requestor. Any accounts that cannot be fulfilled will be recorded on the New Account

Request form and returned to the Requestor, the List of Accounts will not be updated in this case for these specific accounts. Follow-up activities are the responsibility of the Account Manager and the Requestor or Fulfiller, depending upon the nature of the problem.

- If all accounts and services have been established successfully, the returned Request form to the Requestor terminates the new-account requests process. The Requestor will store the form for future audit purposes.

Procedure End

Comments

*Note: A variant of this procedure is currently in use at an organization with which the author is familiar. It is, however, more automated (using Outlook forms) than the above. The author chose to describe this as a manual procedure to add more description. In addition, the format is not the same as the original procedure. The text description has been developed by the author from knowledge of the procedure - it is not copied. The Non-Disclosure and Acceptable Use documents are not in the original process.

Works Cited

"Awareness, Training and Education", University of Southern California, www.usc.edu/org/infosec/sate.htm

Brenton, Chris, Mastering Network Security, SYBEX, Network Press, 1999

Briney, Andy, "Security Focused: Overview, Security Breaches, Risks of E-Commerce, Security Policies", Information Security Magazine, Vol 3, Number 9, September 2000, pp 40-68.

DoD Information 'Technology Security Certification and Accreditation Process, Department of Defense Instruction, Number 5200.40, Dec 30, 1997

"From ATM to VPN: Create a letter perfect, high-speed architecture", Auerbach Analysis, September 11, 2001, www.trechrepublic.com/article.jhtm…11aue01.htm&fromtm=e036&_requestid=26310

Prince, Frank, "Translating Security for Managers", Information Security Magazine, Vol 4, Number 1, January 2001, pp 30-31.

SANS Institute, Information Security Officer Training, San Diego, October 2001

"The SANS Security Policy Project", SANS Institute resources, www.sans.org/newlook/resources/policies/policies.htm

Schneier Bruce, Secrets and Lies, Digital Security in a Networked World, Wiley Computer Publishing, 2000

Strauss, Jack L., "The Use of Intrusion Detection Technologies in Corporate Information Security Policy Implementation and Enforcement", May 18, 2001, SANS Information Security Reading Room, www.sans.org/infosecFAQ/intrusion/corp_infosec.htm

Tippett, Peter, "Sweat the Easy Stuff", Information Security Magazine, Vol. 4, Number 5, May 2001, pp 44-46.

Various Authors, GIAC Basic Security Policy, Version 1.35, September 5, 2000, Edited by Carol Kramer, Stephen Northcutt, Fred Kerby

"VPN security and placement", November 14, 2001,Research Note - Gartner, www.trechrepublic.com/article.jhtm…14ern01.htm&fromtm=e036&_requestid=26405

VanMeter, Charles "Defense In Depth: A Primer", February 19, 2001, SANS Information Security Reading Room, www.sans.org/infosecFAQ/start/primer.htm

Woods, Charles Cresson, "Information Security Roles and Responsibilities" (Special State of CA Presentation), Department of Information Technology Seminar, April 24, 2001