Managing Risk in a Manufacturing Environment

GIAC Information Security Officer
Certification Practical Assignment
Version 1.2

Prepared by: Randy Olson
November 6, 2002

Abstract

This document describes the risks associated with GIAC Enterprises, which is a manufacturing organization. It outlines the business operations and describes the Information Technology infrastructure. Major risks are identified; a sample Information Security policy is reviewed and revised for use within GIAC Enterprises. This policy identifies the risk process and preventative and detection controls required to mitigate the risks within GIAC Enterprises. An Information security procedure is documented that pertains to the policy.

Table of Contents

1. GIAC Enterprises

1.1. Description of GIAC Enterprises

GIAC Enterprises is a manufacturing organization in a single location. GIAC Enterprises is a high quality manufacturer of widgets. GIAC enterprises is a 24 hour per day operation and operates for 11 months at full production and takes a major maintenance shutdown once per year lasting one month.

GIAC Enterprises employs approximately 1500 employees. All raw materials for the manufacturing of the widgets is located within the 100 square miles of company property. Chemicals and other critical supplies are required to be trucked onsite to maintain the manufacturing process. GIAC Enterprises currently has secured long-term contracts with three companies for supply of high quality widgets. GIAC Enterprises does not sell widgets to consumers.

1.2. Business Operations

Business Flow

The main manufacturing process consists of three major steps. The first step is the preparation of the raw materials located on the company property. The next step is the complex mixing process to develop the unique material used in the manufacturing process. The last step in the manufacturing process is the robotic manufacture of the high quality widgets.

Significant supporting business processes include the provision of utilities, providing maintenance services, inventory control, research and development, and distribution of the widgets. Other administrative processes include financial systems, human resource systems, engineering, and Information systems.

Critical Information Technology resources required to support key business functions include the Process Control network, servers, and operator consoles. Real-time production status is collected into the production warehouse stored in Oracle and replicated to the Business network through the one way SAN replication process. No external access or internal access from the business network via TCP/IP is allowed into the process control environment. Any files that must be accessed by vendors or other remote users are replicated to the business network. No email or other file transfer mechanisms exist which would utilize TCP/IP protocols. All support activities must be conducted with onsite personnel attached locally to the process control network. All software required for this equipment is loaded on to the business network and using one way SAN replication is replicated into the process control environment.

In order to ensure no external devices are attached to the process control network, Snort intrusion detection devices are attached to the process control network monitoring all IP traffic. Any new devices identified are immediately reported to the main panel operators in the control room and an investigation is initiated.

IT Support personnel or key business employees are provided with company supplied and configured laptops installed with Cisco VPN client software for remote access through cable service providers. Two factor authentication is required for remote access using SecurID tokens supplied by RSA Security. No modem access is allowed into GIAC Enterprises.

The external firewall is configured to only allow HTTP and SMTP protocols as well as VPN connections.

Critical IT resources on the business network include the Oracle data warehouse which houses the Production information replicated from the Process Control network as well as all the business applications such as SAP for maintenance planning, purchasing, financial stewardship, human resource management and production planning.

Engineering applications include Intergraph Intools and Plant Design System(PDS) for plant design, Gensym G2 for process improvements, and Intergraph SmartPlant Foundation for document management.

No business partners or customers have access to the GIAC Enterprises internal business network or process control environment. GIAC Enterprises employees do have full Internet capability on each workstation connected to the business network for outbound access to business partner networks, research, training, and support web sites. All employees also have email accounts for internal and external communication requirements.

1.3. Information Technology Infrastructure

Data Centers

GIAC Enterprises has two data centers within 5 miles of each other located within the perimeter of the company property. The business data center has fiber optic connectivity to most buildings on site and houses the business related information technology infrastructure. The other data center is used to house the process control equipment necessary to control the manufacturing process.

Building access controls utilize the Honeywell Enterprise Building Integrator and the Honeywell Security Manager for controlling access to the more than 50 buildings on the property.

Network Connectivity

GIAC Enterprises has two distinct and separate networks. The business network has fiber optic connectivity to most buildings on site including the business data center. Internet connectivity is provided to the business network.

The Plant Control Network (PCN) controls and collects information related to the widget manufacturing process. Many manufacturing devices in the SCADA (Supervisory Control and Data Acquisition) environment are controlled with Allen-Bradley PLC5 devices and are connected to the PCN network with Modicon protocols. All information is stored in a SAN (Storage Area Network) which replicates information in real time to other SAN devices located approximately 5 miles away in the Business data center.

The business data center contains all of the business applications such as human resources and finance. The business data center also contains the SAP application for control of inventory, maintenance planning, reporting of production status for all equipment associated with the manufacturing process.

No TCP/IP connections are allowed between the Plant Control Network and the business network. Any files required from the Internet for Product updates or maintenance are downloaded to the business data center and then replicated using the SAN one way replication to the Plant Control SAN.

1.3.1. Information Technology Infrastructure

GIAC Enterprises has two infrastructures; one for the Manufacturing operation or Plant Control Network and one for the Business applications.

Business Infrastructure:

Internet Service Providers – Two Internet Service providers are utilized to ensure reliability of service.

Checkpoint Firewalls are deployed for each major network segment. Cisco switches are used to connect the various buildings on the property with fiber optic connections ensuring high speed connectivity.

The service subnet (commonly referred to as DMZ) contains the External DNS server, SMTP mailhub which includes TrendMicro virus scanning, NTP time server, MailMarshal content management, and Apache proxy server. A Cisco 3030 VPN is used for remote access for system administrators to support critical servers as well as key business area support individuals.

The business network is using Microsoft Office products including Exchange 2000 servers for e-mail and scheduling functions. Servers are running

Windows2000 and functions have been split between application servers, print servers, and information storage servers.

Most business applications access Oracle servers running on Tru64 Unix clusters for easy failover. The business applications use a messaging environment for publishing results to the data warehouse which is housed on an EMC Symmetrix enterprise storage area network.

The Engineering workstations are also running Windows2000 on high-end Intel processors.

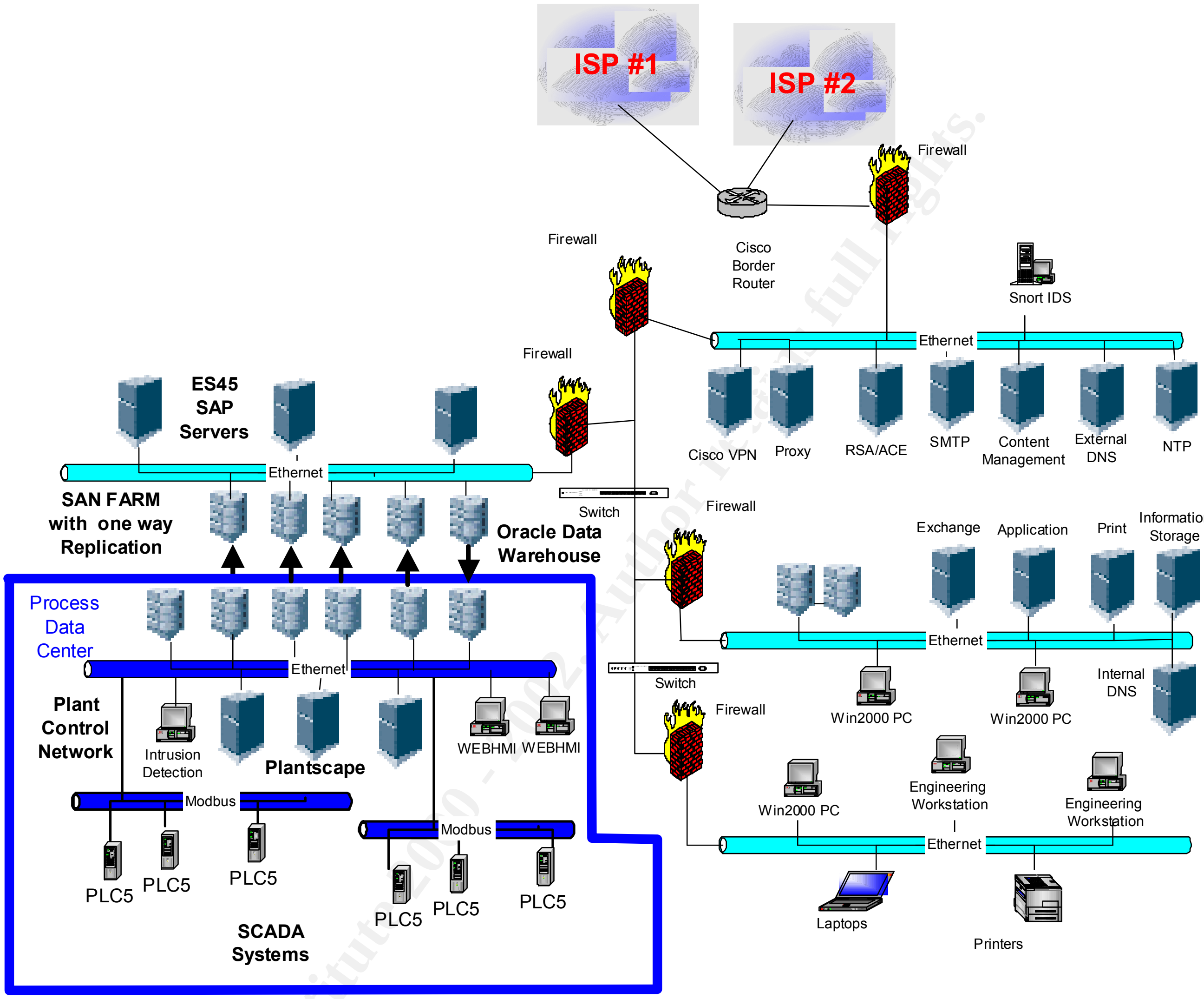
Manufacturing Infrastructure

The Plant Control Network is a separate network without any TCP/IP connectivity to the business network. An EMC SAN device are used as data warehouses between the infrastructures.

Honeywell Plantscape Release 400 is used to manage the manufacturing process. Allen-Bradley PLC5's are used to control most of the devices in the process and are connecting to the Plant Control Network via the Modicon protocol.

HMIWeb stations are used by the panel operators in the main control room for controlling and monitoring the process.

1.3.2. Network Topology



1.3.3. IT Infrastructure Components

Business Network – Hardware components

Function	Manufacturer	Model	Operating System	Quantity
Firewall	Checkpoint	VPN-1/ Firewall-1	HP-UX 11	5
Proxy	HP	rp3405	HP-UX 11	2
DNS	HP	Bind 8.1.2	HP-UX 11	2
NTP	HP	rp3405	HP-UX 11	2
SMTP	HP	rp3405	HP-UX 11	2
Intrusion Detection	Compaq	Proliant DL320	Win2000, SP2	5
Authentication	HP	rp3405	HP-UX 11	2
Exchange	Compaq	Proliant ML530	Win2000, SP2	4
Data Warehouse	HP/DEC	ES45	Tru64 Unix V5.1a	6
Plant Warehouse	HP	rp5470	HP-UX 11	4
Print Servers	Compaq	Proliant ML530	Win2000, SP2	8
Data Servers	Compaq	Proliant ML530	Win2000, SP2	9
App Servers	Compaq	Proliant ML530	Win2000, SP2	18
Workstations	Compaq	Deskpro	Win2000, SP2	1250
Laptops	Toshiba	Satellite Pro 4260	Win2000, SP2	100
Network Router	Cisco	3640	IOS 11.3	1
VPN	Cisco	3030	IOS 12.2	1
Network Switches	Cisco	Catalyst 4006	IOS 12.1	23
Network Switches	Cisco	Catalyst 3550	IOS 12.2	67
SAN	EMC	Symmetrix 8530		1

Business Network – Software components

Function	Manufacturer	Product	Version
HR, Financial, Maintenance, Purchasing	SAP	SAP R/3	SAP R/3
Engineering	Intergraph	Intools SmartPlant Foundation Plant Design System(PDS)	5.3 1 7
DataBase	Oracle	Oracle9i	
Office	Microsoft	Microsoft Office Professional	Office 2000
Email/scheduling	Microsoft	Exchange2000	SP2
Virus Management	TrendMicro	Interscan VirusWall HP-UX Officescan Corporate Server Protect for NT ScanMail for Exchange	3.6 5.02 5.35 6
Intrusion Detection	Tripwire	Tripwire for Servers	3.0
Content Mgmt	MailMarshal	MailMarshal SMTP and MailMarshal Exchange WebMarshal	5.0 1 2.5
Authentication	RSA Security	ACE server	5.0
Simulation	Gensym	G2	6.2
Proxy	Apache	Apache	2.0.39

Process Control Network – Hardware components

Function	Manufacturer	Model	Operating System	Quantity
Hybrid Controller	Honeywell	C200		2
PLC	Allen-Bradley	PLC5	Concept	53
Servers	Compaq	Proliant	Windows2000	14
Workstations	Compaq	Proliant	Windows2000	62
Production Warehouse	HP/DEC	ES45	Tru64 Unix V5.1a	3
SAN	EMC	Symmetrix 8530		1
Network switches	Cisco	Catalyst 4006	IOS 12.1	14
Network Switches	Cisco	Catalyst 3550	IOS 12.2	64

Process Control Network – Software components

Function	Manufacturer	Product	Version
Operator Panel	Honeywell	HMIWeb	
Process Control	Honeywell	Plantscape 400	1.0
Process Servers	Microsoft	Windows2000	SP2
Intrusion Detection	Snort.org	Snort	1.8.2

2. Areas of Risk

2.1. Threats in general

2002 CSI/FBI Survey[1]

	Responses	**Percent**	**Avg Cost**
Theft of proprietary information	26	5%	$6,571,000
Sabotage of data of networks	28	6%	$541,000
Telecom eavesdropping	5	1%	$1,205,000
System penetration by outsider	59	12%	$226,000
Insider Abuse of Net access	89	18%	$536,000
Financial Fraud	25	5%	$4,632,000
Denial of Service	62	12%	$297,000
Virus	178	35%	$283,000
Unauthorized insider access	15	3%	$300,000
Telecom fraud	16	3%	$22,000
Laptop theft	134	27%	$89,000
Total responses	**503**		

The Computer Security Institute and Federal Bureau of Investigations have completed the 7th annual survey of losses within the Information Security field. Although this survey outlines general threats known in organizations, not all of these threats are relevant to GIAC Enterprises.

GIAC Enterprises is a manufacturing organization with the major threat being the inadvertent shutting down or process disruption of the manufacturing process. A major disruption of the manufacturing process could result in significant losses up to and including company bankruptcy.

GIAC Enterprises needs to address controls associated with the following risks:

1. Integrity and Availability of the Plant Control Network[2] controlling and monitoring the Manufacturing process.
2. The availability of the data warehouse which is used to operate the key business applications that support inventory control and maintenance of key equipment in the manufacturing process.
3. Productivity losses due to the abuse of full Internet access for all employees.

[1] 2002 CSI/FBI survey http://www.gocsi.com/press/20020407.html (6 Oct, 2002)
[2] URL: Honeywell product guide for Plantscape http://www.acs.honeywell.com/ichome/Doc/0/NQ4U1C2E5VAH3AJ2001B69DOBB/PS400ProcessST.pdf (6 Oct, 2002)

The following section will identify the specific threats, impact of the risks, and associated mitigating actions required.

2.2. Integrity of Process Control Environment

Risk: The risks for GIAC Enterprises include the threat of an outsider attack on the manufacturing process. This may occur as a result of some vulnerabilities being exploited that would allow a specific attack to occur. Since some of the equipment in the manufacturing process is Microsoft based, the threat of viruses causing an outage is significant.

Impact: The impact of an outsider being able to alter the process could have significant impact on GIAC Enterprises. The manufacturing process is critical to the financial success of the organization. If someone obtains remote access to the process control infrastructure, modifications could be made to several of the controlling devices such as the Allen-Bradley PLC5's. This could result in process stoppages, quality deviations, or even explosions, which may result in loss of life.

The impact of a virus that causes a production upset due to the non availability of a device has been calculated at $350,000 for every hour of production loss.

Mitigation: The Plant Control Network has been completely separated from the Business network. No TCP/IP connections exist between the two networks. No external access is allowed to any devices within this environment. Production and operating parameters are collected within a Oracle Server production data warehouse and stored in a SAN environment. The SAN device is then used to replicate the data in real time to the business data center approximately 5 miles away. Intrusion detection stations are located on the Plant Control network to constantly monitor the known devices and expected network traffic. Tripwire is been used on all Windows2000 servers to ensure the change management process is being followed and no inadvertent changes will impact the availability of the equipment.

2.3. Availability of Data Warehouse

Risk: The major application used on the business network is the SAP Enterprise Resource Planning application. SAP is used to keep track of all orders, inventory widgets, and keep maintenance schedules updated for all of the manufacturing devices.

Impact: Since all business applications publish and subscribe to data in the data warehouse, this information store is critical to the operation of GIAC Enterprises. The data warehouse is running on Oracle databases and most of the applications are using web servers to access the information. The impact of an outage on the warehouse lasting more than one day is calculated at $700,000 per day.

Mitigation: The data warehouse is housed within the EMC Symmetrix Enterprise Storage Area Network and Connectrix Fibre-Channel switches. The servers are located behind a firewall on a separate segment of the network. Only internal TCP/IP traffic is permitted to publish or subscribe to warehouse information. Access controls have been implemented to ensure specific applications can perform publish functions.

2.4. Employee Productivity losses due to network abuse

Risk: GIAC Enterprises has provided all employees with full Internet access on each workstation. The risk is that employees will abuse the access by surfing the Internet for non-business related activities resulting in significant productivity losses.

Impact: GIAC Enterprises has estimated that without monitoring or implementation of any controls or awareness programs, the average employee loss of productivity would be approximately 2 hours per week. Total estimated losses for the year would exceed $3 Million.

Mitigation: In order to mitigate the potential productivity losses, GIAC Enterprises has implemented several controls. The Acceptable Use policy outlines the specifics of acceptable Internet usage. This policy also indicates that the company will be monitoring employees usage of the Internet. For awareness purposes an email is sent to each employee on a daily basis indicating the web sites that the employee has visited in the last 24 hour period. An email content management system has been implemented that restricts audio and video files from being distributed from external sources. This has been implemented using Marshal Software's MailMarshal for SMTP at the gateway and MailMarshal for Exchange for internal control. Web surfing controls are also implemented with the WebMarshal product.

3. Security Policy

3.1. Sample Policy[3]

The following sample policy will be evaluated for effectiveness. This policy was obtained from sample policy provided in the book “Information Security Best Practices” by George L. Stefanek.

Purpose The purpose of establishing this information security policy for CORPORATION X is to protect corporate information and computer assets while allowing:

1. e-mail communication,
2. information transfer, and
3. access to the corporate website and web-based e-commerce server between customers, corporate affiliates, and corporate users.

Also, it defines policies for protecting data within the corporation and addresses the confidentiality, data integrity, availability, accountability, and responsibility issues that each employee must be aware of and comply with while working for this corporation.

Threats

- Virus introduced by e-mail, web browsing, corporate web-site access, floppy, CD, tape, or ftp downloads.
- Denial of service attacks from the internet to corporate servers.
- Unauthorized login into computers by learned or hacked usernames and passwords for the purpose of reading, deleting, removing, or inserting data not approved by the responsible party of the computer resource.
- Unauthorized network access to server and workstation computers for the purpose of reading, deleting, removing, or inserting data not approved by the responsible party of the computer resource.
- Unauthorized physical access to corporate servers that may result in inadvertent or malicious shutoff, damage, or login access to the server.
- Unauthorized access to data by a user because of lack of file protection.
- Loss of data assurance (i.e., receipt of data without traceability) of confidential corporate data during network transfer.
- Loss of data integrity (i.e., data tampered with during transmission) of confidential corporate data during network transfer.
- Theft of disks and tapes.
- Unauthorized tampering with network resources that can lead to the loss of the network.
- Loss of power.

[3] Stefanek, George L., Information Security Best Practices, LLH Technology Publishing, Sample policy or see URL: http://secinf.net/info/misc/Butterworth-Heinemann/ISBPpolicy/css/ISBPpolicy.htm (6 Oct 2002)

- Lightning strike.
- Illness of personnel that may lead to users bypassing information security for the sake of convenience.

Cost/Benefit Analysis

The calculated cost of the e-commerce server being down every minute is $______.
The calculated cost of the network being down every minute is $______.
The calculated cost of removing a virus from a single PC is $______.
The cost for removing a virus from all corporate machines is $______.
The calculated cost of e-mail being down per user per day is $______.
The calculated cost of secret corporate information getting into the hands of a competitor is $______.
These are considered the primary risks due to financial loss for the following information security measures.

Confidentiality

- Corporate servers must be located in a secure physical location with access only by authorized personnel via combination lock or access card.
- A firewall must separate corporate computers and servers from the internet.
- All users must have a separate user account and password that must be kept confidential.
- Each server must have an account policy that enforces passwords to be a minimum of 6 alphanumeric characters long.
- Each server must have an account policy that enforces password expiration every 3 months.
- Each server must keep a password history file that saves the history of a user's passwords and does not allow reuse.
- Users cannot share accounts.
- All user accounts will use password-protected screen savers.
- Users may not access another user's data without permission. Each server must have a file protection system that restricts user access to the user's own files. Exceptions include a user belonging to a group that has file access via group file permissions.
- Users must take responsibility to protect their data.
- All corporate confidential data must be encrypted with 128-bit encryption before being transmitted over a public communication channel (e.g., the internet, leased lines, or POTS connections).
- All corporate confidential email must use PGP encryption. Public keys must be posted to the PKI system at the following server ldap://certserver.pgp.com. Day to day email does not have to be encrypted.
- Financial servers and servers with highly classified corporate information must reside on a separate network that is physically separate from any corporate network that is connected to the internet.

- No e-mail or internet access is allowed on corporate financial servers and servers with highly classified corporate information.
- Workstations and servers behind the corporate firewall must not have a modem connection. Modem connections will be handled via an authorized dial-in server

Integrity

- The administrator and alternate administrator account must be the only accounts with access to all files.
- All file transfers of highly confidential data between machines must check for the integrity of the data.
- System files must be read-execute for users.
- Any new data copied onto a server must be done through the server that must log the transaction.
- All systems must have anti-virus software present that scans all disks, floppy drives, incoming IP traffic, and MS Word macros.
- Confidential data must be encrypted during data transfer.
- No unapproved software shall be installed on any workstation without authorization from the corporate MIS department.

Availability

- Dial-in capability will be to a specified dial-in server that will authenticate the user.
- Each server must have an uninterruptible power supply (UPS).
- All servers must be available 24 x 7 x 365.
- Access to e-mail, FTP, and HTTP services must be available 24 hours per day.
- Each server must be in a room with controlled access.
- The servers and workstations in the internal network must have proxy services for designated users coming in outside the firewall. Database servers may be accessed by specific IP addresses that are authorized to access the resources using FTP or HTTP. These addresses must use gateway authentication at the firewall in order to gain access to servers inside the firewall.
- Access to servers on the internal network must be restricted by a firewall that specifies the IP address that may pass and requires authentication.
- If IT personnel are not available during an emergency, then there will be a backup person(s) that will be assigned to the task

Accountability

- All account security events must be logged.
- All confidential file access must be logged.
- All data transfers of confidential data must use authentication between server and client.

- All confidential data sent to another machine must have a digital signature associated with it.
- All new software deployed on either servers or workstations must be authorized by the IT staff. A software log of installed software must be maintained.
- All connections through the firewall must be logged

Recovery

- All server data will be backed up daily using incremental back- ups.
- Full backups will be done once a week.
- Archives will be done monthly.
- Backups and archives must be stored off-site.
- Desktop workstations will use network file services to store corporate data that should be backed up by the server.
- Desktop workstations will have standardized configurations for each department that will include designated versions of the operating system at a specified revision level, anti-virus software, e-mail and groupware software, word processing and spreadsheet software, and other specific departmental software. An image of this software configuration will be made by MIS. This image will be pushed down to the departmental workstation in the event of operating system corruption.

Employee Responsibilities

- Employees must adhere to the stated policy as technology changes and must make best efforts to protect data and not indulge in activities that compromise data.
- Employees should backup any data that they feel is important that is not stored on the corporate file servers.
- Employees must comply with the corporate information security policy.
- Copyrighted software must be used in accordance with the software license.
- Corporate computers cannot be used for personal purposes.
- Corporate e-mail cannot be used for personal purposes.
- The hardware configuration of a desktop workstation cannot be changed without approval from the MIS department.
- Employees are prohibited from transmitting fraudulent, obscene or harassing messages to anyone.
- Employees are prohibited from transmitting programs to anyone that have the intent of compromising information security or disrupting work.

Enforcement

- Any reported abuses of corporate resources will be investigated. During the investigation the company may access the electronic file of its employee. If computer policy has been violated then the employee's privileges may be restricted as decided by the CIO.

- The company will audit resources periodically to ensure that software and computer configurations comply with policy.

Education

- Information security training will be provided by the company once a year.
- Each employee will receive a hard copy of the corporate information security policy and must read it.

3.2. Evaluation of Policy

Purpose: The purpose of the policy is stated in terms of performing very specific activities listing three examples but then goes on to identify a list of general control areas for protecting data. The purpose is lacking the fundamental reason for the policy and that is the protection controls required to minimize losses to the corporation associated with information management. It discusses controls but not the rationale. It does not specifically outline who the policy applies to although at the end of the policy is does indicate under the education section that all employees must read the policy.

Background: The policy identifies several threats associated with the loss of Information Systems and suggests methods for calculating the loss. The list of threats provides the reader with a good awareness of possible threats. The cost/benefit analysis does not belong in a policy but should be identified as a reference to a procedure that is used to consistently value losses related to Information Systems.

Scope: The statements in the policy assume the risk is the same for all systems and that controls are therefore required to be the same for all the systems. In practice, different systems will have a different impact on the organization and therefore some controls need to be applied differently depending on the risk.

Controls should be identified as preventative controls or detection controls. Preventative controls are put into place to attempt to prevent the risk from occurring. Detection controls are the logging features or auditing features to assess the effectiveness of the preventative controls. Both types of controls need to be identified within the policy.

Policy Statement: The policy contains a number of good suggestions on controlling risks to corporate information systems.

The statements associated with Integrity reference confidentiality and are therefore are located in the incorrect category.

The Education section should be included within the Employee responsibilities. The Employee responsibility section should be created as a separate "Acceptable Use" policy.

Responsibility: The owner of this policy is not clearly identified although enforcement of any violation of the policy has been designated as the CIO. The owner needs to be identified so that suggestions for change or improvements can be forwarded to the identified party. Although the CIO is responsible for enforcement of any violations, no responsibility is assigned to individuals within the company for identifying the violations or implementing the actions associated with enforcement of the violations.

Action: Although this policy identifies several actions to be done by the user, the system administrator is not specifically mentioned in ensuring proper controls are in place when performing system management related activities. No timeline is provided for a corporate review of the policy. The policy does not contain an effective date. Some dates are provided in the policy which include education; once per year, backups done daily, weekly, and monthly; password expiry every 3 months.

3.3. *Revised Security Policy*

POLICY01 – Information Systems Protection and Detection Controls

Purpose: The purpose of this policy is to protect GIAC Enterprises from the loss of any corporate information system.

This policy is the responsibility of the Chief Information Security Officer of GIAC Enterprises.

Rationale: This policy is in place to ensure the risks associated with the following examples of possible threats are mitigated.

Availability Threats

- Virus introduced by e-mail, web browsing, corporate web-site access, floppy, CD, tape, or ftp downloads.
- Denial of service attacks from the internet to corporate servers.
- Unauthorized tampering with network resources that can lead to the loss of the network.
- Loss of power.
- Lightning strike.

Integrity Threats

- Unauthorized login into computers by learned or hacked usernames and passwords for the purpose of reading, deleting, removing, or inserting data not approved by the responsible party of the computer resource.
- Unauthorized network access to server and workstation computers for the purpose of reading, deleting, removing, or inserting data not approved by the responsible party of the computer resource.
- Unauthorized physical access to corporate servers that may result in inadvertent or malicious shutoff, damage, or login access to the server.
- Loss of data integrity (i.e., data tampered with during transmission) of confidential corporate data during network transfer.

Confidentiality Threats

- Unauthorized access to data by a user because of lack of file protection.
- Loss of data assurance (i.e., receipt of data without traceability) of confidential corporate data during network transfer.
- Theft of disks and tapes.
- Illness of personnel that may lead to users bypassing information security for the sake of convenience.

Scope: This policy covers all business systems and process control systems in GIAC Enterprises.

Policy: Each information system in use within GIAC Enterprises must have a documented risk assessment completed and updated yearly by the information system owner. Each owner will review the confidentiality, integrity, and availability risks. Based on the level of risk associated with each information system, various protection and detection controls are required to be in place. An audited review of the expected controls based on the risk classification for each Medium or High risk information system must be done in conjunction with the Information Security organization within GIAC Enterprises at least bi-annually.

RISK	Low	Medium	High
Protection Controls - Minimum Specifications			
Authentication[4]	Onsite – Unique LANID and password. Generic Ids for approved functions. Offsite – Access token plus password. Admin Ids need complex password and changed every 90 days.	Onsite - Unique LANID and password. No generic LANID's. Offsite – Access token plus password. Password history verified to prevent reuse.	Unique LANID, and Token for onsite access. Userid unique to domain and not authenticated on Business LAN Digital signature associated with data.

[4] Pipkin, Donald L., Information Security Protecting the Global Enterprise, Upper Saddle River, New Jersey, Prentice Hall, 2000, Chapters 7-20

Authorization	Permissions assigned to files and folders. Default is read access for all LANID's. Restrictions on update access.	Access can be provided to groups of individuals assigned to specific roles. Default is restricted access to designated roles.	Data restricted to write access. Read access provided at lower level. Access restricted to specific individuals. No groups defined.
Remote Access	Unique LANID, physical token, and password. Two factor authentication required for remote access. System admin requires VPN for remote access.	No remote access without current virus software signature file installed and local firewall. Remote access requires encryption of all transmission.	Physical control of all access points. No modem access. Separate network –. No remote access even for Administrative purposes.
Network Controls	Firewall must separate Internet and Internal network. Network Address Translation in use for all external communication. No modem connectivity directly to workstation.	Additional access controls implemented through devices such as firewalls, routers, and proxy servers. .	Separate Firewall with very restricted controls on isolated separate network. Unique Domain.
Anti-virus	All systems and networks to contain anti-virus software.	Signature files to be updated within 1 hour of being available from vendor.	No TCP/IP connectivity allowed to other systems.

RISK	**Low**	**Medium**	**High**
Protection Controls – Confidentiality			
Access Controls	Knowledge of information but may not have access to it. Password protected screen savers activated after 15 mins of non use.	Individual files protected by authorization and password or encryption.	Individual files protected by 128-bit Encryption and Passwords. Public keys must be posted in corporate server.
Non disclosure agreements	Approved by Contracting.	Approved by Contracting and Legal	Approved by Executive Committee.
Information Storage		Disposal of electronic media requires a verified process.	Proof of controls required including disposal.
Protection Controls – Integrity			
Accuracy/Integrity		Each data base must use rollback support.	Physical separation between write and read access.
Concurrent applications			No e-mail system installed in this environment.

Transmission of information between Systems		Remote access must be encrypted.	Proof of controls required including disposal.

Protection Controls – **Availability**			
Information Storage	All data must be stored on network drives.		
Recovery	Restoration to be done to last day.	Restoration to be done to last transaction. Outage not to exceed one day	No outage acceptable. Availability 24 X 7 X365 days per year.
Data sharing	All software installations require MIS department approval.	Must be authorized by department management.	NO TCP/IP connections with other Information Systems.
Operating System maintenance	Current within 1 year of manufacturer release	Current within 6 months of release, patches as required.	Current within 3 months of release, patches at least monthly.
Implementation Process	Change management procedures followed.	Risk assessment documented with change management.	Full impact assessment and disaster recovery test.

RISK	**Low**	**Medium**	**High**
Detection Controls - Minimum Specifications			
Authentication	All logons, successful and unsuccessful. All accounts reviewed monthly for expiration.	Yearly review of physical token possessions. Accounts reviewed monthly for employees changing function.	Admin passwords changed immediately when individual transfers to another function or leaves organization. Connection origin must be verified.
Frequency of review	Monthly – managed departmentally	Weekly – centrally managed Alerts daily	Daily by Information Security team. Alerts in real time
Physical Controls	Servers located in secure computer rooms. Access via card lock system.		Physical access monitored with cameras and entry logs.
Network Controls	All connections through firewalls must be logged.	Network Intrusion Detection in place.	7 X 24 network intrusion monitoring.
Accountability	Ability to identify individual/program that caused an event.	All Admin access must be logged.	No use of shared accounts.

Detection Controls – Confidentiality			
Access Control	Logging done for change of permissions, Unsuccessful access to restricted information.	Log all file access, both successful and unsuccessful. Organization changes reviewed by central group on weekly basis.	Information can be viewed on screen but can not be printed or copied except by Owner.
Detection Controls – Integrity			
Operating System controls		Operating system compromise verification. . (Hourly)	Operating system compromise verification. (Notification within 1 minute)
Detection Controls - Availability			
Stewardship	Monitoring of failure events.	Stewardship of service level agreements.	Complete redundancy of equipment.
Auditing	Testing of failure procedures at least every two years.	Testing of failure procedures at least once per year.	Testing of failure procedures every 3 months.

Enforcement: Any employee or worker using GIAC Enterprises computing resources that is found in violation of this policy may be subject to disciplinary action, which may include termination of employment.

Procedures: see SEC01, SEC02

Revision History: Version 1.0 – October 06, 2002

The GIAC Enterprises Information Security committee must approve all revisions to this policy.

4. Security Procedure

4.1. SEC01 Procedure – Risk Classification of Information Systems

Purpose: This procedure is used to assess the risk level associated with each Information System in GIAC Enterprises. The following table will be used as a guide to classify the risk level associated with Confidentiality, Integrity, and Availability of information. This procedure is used in conjunction with policy POLICY01 and procedure SEC02. The classification of each system is required in order to determine the appropriate level of controls required to manage the risks within GIAC Enterprises.

RISK	Low	Medium	High
Confidentiality	Slight embarrassment within one department.	Embarrassment across company. May involve some litigation.	If information disclosed externally, incident would cause media attention. Company stock impacted > 5%
Integrity	Incorrect information may result in production loss or recovery costs < $100K.	Incorrect information may result in production loss or recovery costs > $100K	Incorrect information may result in production loss or recovery costs > $1 M
Availability[5]	Unavailability of information for 1 week would result in < $100K in loss.	Unavailability of information for 1 week would result in > $100K in loss.	Unavailability of information for 1 week would result in > $1 M in loss.

Performed by:	Actions	Timing
Information System Owner	Request Information Security facilitate a risk assessment with all stakeholders using the above matrix as a guide.	The risk assessment must be completed before the information system is implemented into production status.
Information Security	Perform the risk assessment.	This must be completed within two weeks of receipt of the request.
Information System Owner	Accept the risk classification. Identify actions to be completed to implement controls (see SEC02)	This must be completed before production implementation and reviewed on a yearly basis.
Information Security	Provide a summary of the classification of all information systems in an annual report.	Annual Information Security report is due March 30 of every year.

Responsibility: The Information Security Officer of GIAC Enterprises is the owner of this procedure.

Policy and Procedure References: See POLICY01 and procedure SEC02.

Procedure Verification: It is the responsibility of the Information Security Officer of GIAC Enterprises to ensure each Information System owner in GIAC Enterprises has completed a Risk classification. The Information Security Officer must provide an annual report, which includes the risk classification of all GIAC Enterprises information systems in March of each year.

[5] Krause, Micki, Tipton, Harold F., Handbook of Information Security Management – 1999, Boca Raton, Auerbach, 1999, pg 450-451

Revision History: Version 1.0, October 15, 2002.
The GIAC Enterprises Information Security committee must approve all revisions to this policy.
------------------------------------ End of Procedure --------------------------------------

4.2. SEC02 Procedure – Implement Risk Controls based on the Classification of Information Systems

Purpose: This procedure is used to ensure appropriate controls have been implemented for each information system within GIAC Enterprises once a risk classification has been performed. This procedure is used in conjunction with policy POLICY01 and procedure SEC01. The controls identified in POLICY01 are implemented commensurate with the identified risk. These controls will include Minimum Preventative controls for Confidentiality, Integrity and Availability; and Minimum Detection controls for Confidentiality, Integrity and Availability. Additional Preventative and Detection controls may be required for Confidentiality, Integrity and Availability based on the risk classification.

Performed by:	Actions	Timing
Information System Owner	Using the risk classification (sec SEC01), identify the appropriate controls from POLICY01 to be implemented for the Information System.	The identified controls must be implemented before the information system is turned over into production status.
Infrastructure Support Group	Identify and recommend configuration options and technology choices for implementation of controls.	Timeframes for implementation of each control must be identified.
Information Security	Review and approve the recommended implementation plans for the necessary controls. A copy of the plan must be filed by the Information Security organization.	Timeframes for implementation will be reviewed monthly.
Information System Owner	The Information Security Committee must approve any exceptions to the recommended controls.	This must be completed before production implementation and reviewed on a yearly basis.
Information Security Committee	Review rationale for exceptions and approve or deny the exceptions.	During regularly scheduled monthly meetings.
Information System Owner	Provide a status update to the Information Security committee on actions taken to mitigate the risks.	Status is provided on a monthly basis.

Information Security	Initiate an audit of the controls implemented for the information system whenever a loss of >$50K has been identified.	Within one month of receiving the loss report.
Information Security	Initiate and maintain an audit schedule for Medium and High risk Information Systems.	An audit review is required to be performed every two years for identified systems.

Responsibility: The Information Security Officer of GIAC Enterprises is the owner of this procedure.

Policy and Procedure References: See POLICY01 and procedure SEC01.

Procedure Verification: This procedure is verified in one of two ways. If an information System has an event, which results in a loss exceeding $50K, the Information Security organization will initiate an audit of the controls for the Information system. An audit of the controls are required to be done every two years for Medium and High risk systems.

Revision History: Version 1.0, October 15, 2002.
The GIAC Enterprises Information Security committee must approve all revisions to this policy.
------------------------------------- End of Procedure ---------------------------------------

5. Bibliography

2002 CSI/FBI survey http://www.gocsi.com/press/20020407.html (6 Oct, 2002)

Krause, Micki, Tipton, Harold F., Handbook of Information Security Management – 1999, Boca Raton, Auerbach, 1999, pg 450-451

Pipkin, Donald L., Information Security Protecting the Global Enterprise, Upper Saddle River, New Jersey, Prentice Hall, 2000, Chapters 7-20

Stefanek, George L., Information Security Best Practices, LLH Technology Publishing, Chapter 4 or see URL: http://secinf.net/info/misc/Butterworth-Heinemann/ISBPpolicy/css/ISBPpolicy.htm (6 Oct 2002)

URL: http://www.acs.honeywell.com/ichome/Doc/0/NQ4U1C2E5VAH3AJ2001B69DOBB/PS400ProcessST.pdf (6 Oct, 2002)