

Security Manual Template

Prepared by

Janco Associates, Inc.

Park City, UT

email - info@itproductivity.org

Web site – <http://www.e-janco.com> and <http://www.itproductivity.org>

May 2005 – Version 4.0

Sarbanes Oxley



License Conditions:

This product is NOT FOR RESALE or REDISTRIBUTION in any physical or electronic format. The purchaser of this template has acquired the rights to use it for a SINGLE Security Manual template unless they have multi-use license. Anyone who makes copies of or uses the template or any derivative of it is in violation of United States and International copyright laws and subject to fines that are treble damages as determined by the courts. A REWARD of up to 1/3 of those fines will be anyone reporting such a violation upon the successful prosecution of such violators.

The purchaser agrees that derivative of this template will contain the following words within the first five pages of that document. The words are:

Derived from the Security Manual published by Janco Associates.
© 2005 Copyright Janco Associates, Inc. – ALL RIGHTS
RESERVED

Easy use steps:

1. Read this License Conditions
2. Print the first two pages of this template
3. Delete the first two pages.
4. Save As "*your file name*"
5. Edit replace "ENTERPRISE" with your enterprise's name.
6. Edit replace "ENTERPRISE logo" with your enterprise's logo
7. Save As "*your filename.v001*"
8. As you modify the plan continue to save the DRP with a name that has an updated version number.



Table of Contents

I.	Security - Introduction	11
	Scope	11
	Objective.....	13
	Applicability.....	13
	Security General Policy	14
	General Management	14
	Individual Managers And Staff Members	14
	Principles Of Least Privilege And Need-To-Know	14
	Sensitivity And Criticality Of Information And Applications	14
	Critical Applications.....	14
	Sensitive Information and Applications	15
	Safeguarding Resources.....	15
	Safeguarding Resources Traveling or at Off-Site Facility.....	15
	Security Risk Analysis Program	15
	Processing Area Risk Categories.....	15
	Sensitive Staff Member Positions.....	16
	Security Design and Procurement Specifications.....	16
	Software Security.....	16
	Hardware Security.....	16
	Network Security	16
	Logical Access Controls	17
	Software Development Controls.....	17
	Responsibilities.....	18
	Manager, Internet and Information Technology Group.....	18
	Manager, Financial Management & Control Department	18
	Security Committee (SC)	19
	Manager, Internet and Information Technology Security.....	19
	All Enterprise Managers (Enterprise Groups, Departments And Divisions)	20
	Security Representative	20
	Enterprise Staff Members	20
II.	Minimum and Mandated Security Standard Requirements	21
	Gramm-Leach-Bliley (Financial Services Modernization Act of 1999).....	22
	FTC Information Safeguards.....	22
	Sarbanes-Oxley Act	23
	California SB 1386 Personal Information Privacy.....	23
III.	Best Practices to Manage Compliance Violations	25
	Internet Security Myths	25
	SSL (Secure Certificates) Make an Internet Site Secure	25
	Security Is Designed Into The Applications.....	26
	Scan of a Site by Software Reports No Security Issues.....	26
	Firewall (Software and Hardware) Protects Site – Site is Safe.....	27
	Security Audits Are Done Annually – We Have Nothing to Worry About.....	27



IV. Vulnerability Analysis and Threat Assessment	29
Threat and Vulnerability Assessment Tool	30
Demographics and Access	31
Environment, Business and IT Processes.....	32
Evaluate Risk.....	33

V. Risk Analysis – IT Applications and Functions	35
Objective.....	35
Roles and Responsibilities.....	36
General Responsibilities	36
Manager, Financial Management & Control Department.....	36
Internet and Information Technology Security Group	36
Managers, all enterprise user/support departments.....	36
Supporting Responsibilities.....	37
Security Committee.....	37
Program Requirements.....	37
Frequency.....	38
Relationship to Effective Security Design	38
Selection of Safeguards.....	38
Requests for Waiver	38
Program Basic Elements	39
Asset.....	39
Value Analysis.....	39
Threat And Vulnerability Analysis.....	40
Exposure Analysis.....	40
Calculation of Annual Loss Expectancy	40
Countermeasure Evaluation And Selection.....	41
Identification Of Candidate Countermeasures	41
Cost/Benefit Analysis	41
Selection of a Countermeasure.....	41
Management Decision	42
Control Implementation	42
Effectiveness Review	42

VI. Staff Member Roles	43
Basic Policies	43
Individual Responsibility.....	44
Review Of Positions	44
Violation Procedures.....	44
Dangerous Security Practices.....	44
Security Violations.....	44
Management Action	45
Security - Responsibilities.....	45
Managers, all departments, Internet and Information Technology Group	45
Managers, Personnel Organizations	45
Manager, Legal Department	45
Manager, Internet and Information Technology Contracts/Hardware Services Division.....	45
Manager, Audit Department	45
Internet and Information Technology Security group, Financial Management & Control Department.....	45
Determining Sensitive Internet and Information Technology Systems Positions	46
Personnel Practices.....	47
Hiring Procedures	47
Termination Types	47



Voluntary Termination	47
Job Abandonment.....	48
Involuntary Termination	48
Termination Actions	48
Education and Training.....	49
Contractor Personnel.....	49
<hr/>	
VII. Physical Security.....	51
Information Processing Area Classification	51
Application	52
Processing Backup Capability.....	52
Classification Categories	52
Category I Information Processing Area	52
Category II Information Processing Area	52
Category III Information Processing Area	52
Category IV Information Processing Area	53
Access Control	53
Separation of Duties.....	53
Least Privilege.....	54
Access Areas	54
Individual Accountability.....	54
Access Control Methods	54
Levels of Access Authority.....	55
Permanent Access	55
Temporary Access	55
Access Control Requirements by Category	55
Category I Information Processing Areas.....	55
Category II Information Processing Areas.....	55
Category III Information Processing Areas.....	55
Category IV Information Processing Areas	56
Implementation Requirements.....	56
Protection of Supporting Utilities.....	57
<hr/>	
VIII. Facility Design, Construction and Operational Considerations	59
Building Location	59
External Characteristics.....	60
Location of Information Processing Areas	61
Construction Standards	61
Water Damage Protection	62
Air Conditioning	62
Entrances and Exits.....	63
Interior Furnishings	63
Fire	64
Prevention.....	64
Fire Detection.....	65
Fire Suppression	66
Sprinklers - Category I, II, III and IV Areas.....	66
Halon - Category I and II Areas	66
Emergency Shut Down Control - Category I and II Areas.....	67
Portable Fire Extinguishers - Category I, II, III and IV Areas.....	67
Electrical	67
Category I, II, III and IV Areas.....	67
Uninterruptible Power Supplies	68
Emergency Power.....	68
Air Conditioning	68



Category I, II, III and IV Areas	68
Category I and II Areas	68
Category I Areas	68
Remote Internet and Information Technology Workstations	69
Security Requirements	69
Training, Drills, Maintenance and Testing	69
<hr/>	
IX. Media and Documentation	71
Data Storage and Media Protection	71
Labeling	71
Storage	72
Retention Schedule	72
Disposal Of Sensitive Information	72
Documentation	72
Responsibilities	72
Accountability And Control	73
Storage of Information and Forms	73
Disposal	73
Off-Site Backup Storage	73
Combustible Media	73
<hr/>	
X. Data and Software Security	75
Resources to Be Protected	75
Data	75
Software	75
Basic Standards	76
Classification	77
Sensitive Information	77
Non-Sensitive Information	78
Rights	78
Support Manger	79
Users	79
Access Control	80
Types Of Controls	80
Hardware controls	80
System Software Controls	80
Systems Software Rights Controls	80
Access From Other Sites	80
Controllability	81
Integrity	81
Identification	82
Authentication	82
Techniques	82
Standards For Passwords	82
Authorization Verification	83
Internet / Intranet / Terminal Access	84
Owners	84
Access Control	84
User Accountability	84
Logging And Audit Trails	85
Reporting	85
Network Security	85
Internet / Intranet Security	85
Dial-up Access Security	85
Logging and Audit Trails Requirements	86



Accountability	86
Reconstruction Of Events	86
Information to Be Recorded	86
Tracing Transactions.....	87
Support Information.....	87
Retention Period Documentation / Audit Trail Data.....	87
Audit Log Requirements.....	87
Job-Related Data Log	87
Program-related log	87
File-Related Log	88
Transaction-Related Log.....	88
Message-Related Log.....	88
Data Base-related Log.....	89
Satisfactory Compliance	89
Violation Reporting and Follow-Up	90
Detection.....	90
Violation Logging.....	90
Follow-Up On Violation Reporting	90
<hr/>	
XI. Network Security	91
Vulnerabilities	91
Exploitation Techniques.....	91
Unauthorized Interception	91
Unauthorized Insertion of Information	91
Unauthorized Denial of Service.....	91
Unauthorized Intrusion	92
Goal	92
Responsibilities.....	92
Owners.....	92
Application Support Organizations	92
Network Services	93
Internet and Information Technology Security.....	93
Resource Protection	93
Network Components.....	93
Wire Closets.....	94
Remote Devices.....	94
Configuration Management	94
Dial-Up Controls	95
Message Authentication	95
Encryption.....	96
Standards.....	96
Key Management.....	97
Rules.....	97
Exceptions	98
Network Contingency Planning.....	98
<hr/>	
XII. Internet and Information Technology Contingency Planning	99
Responsibilities.....	99
Manager, Internet and Information Technology Group.....	99
Manager, Financial Management & Control Department	99
Managers, Information Processing Areas	99
Manager, Contingency Planning	99
Managers, All Departments.....	100
User Organizations	100
Information Technology	100



Disaster Recovery Planning	100
Contingency Planning.....	101
Development Activities	101
Documentation	101
Contingency Plan Activation and Recovery	102
<hr/>	
XIII. Insurance	103
Objectives.....	103
Responsibilities.....	103
Risk Manager	103
Contracts/Hardware Services Manger	103
Managers, All Departments, Internet and Information Technology Group	104
Internet and Information Technology Security Group And The Risk Manager	104
Filing A Proof Of Loss.....	104
Risk Analysis Program.....	104
Purchased Equipment and Systems.....	104
Leased Equipment and Systems	105
Media.....	105
Business Interruption.....	106
Staff Member Dishonesty	106
Errors and Omissions	107
<hr/>	
XIV. Outsourced Services	109
Responsibilities.....	109
Managers, All Departments, Internet and Information Technology Group	109
Managers, All Other ENTERPRISE Departments	110
Internet and Information Technology Systems Contract Personnel And Organizations	110
Manager, Internet and Information Technology Contracts/Hardware Services Division.....	110
Internet And Information Technology Security Group	111
Manager, Audit Department	111
Outside Service Providers	111
Contract Terms And Operating Policies	111
<hr/>	
XV. Travel and Off-Site Meetings	113
Maximize Data and Application Security.....	113
Minimize Attention	114
Carefully Use Shared Resources.....	114
Off-Site Meeting Special Considerations	115
<hr/>	
XVI. Waiver Procedures.....	117
Purpose and Scope	117
Policy.....	117
Definition.....	117
Responsibilities.....	117
Procedure	118
<hr/>	
XVII. Incident Reporting Procedure.....	119
Purpose & Scope.....	119
Definitions.....	119
Responsibilities.....	119
Procedure	120
Analysis/Evaluation.....	121



XVIII. Access Control Guidelines	123
Purpose & Scope.....	123
Objectives	123
Definitions of Access Control Zones	123
Public Areas	123
Controlled Areas	124
General Areas.....	124
Restricted Areas	124
Responsibilities.....	124
Internet and Information Technology Security Group.....	124
Access Control Operations Center.....	124
Requesting Manager Responsibilities	125
Authorizing Managers	126
Security Guards	126
Staff Members.....	127
Audit Department	127
Badge Issuance.....	128
Permanent Badge/Permanent Staff Member	128
Permanent Badge/Temporary Staff Member	128
Temporary Badge/Permanent Staff Member	128
Temporary Badge/Temporary Staff Member.....	129
Temporary Badge/Non-staff Members	129

XIX. Forms	131
Security Violation Form.....	133
Security Audit Report Form	141
Inspection Check List.....	143
General	143
Employees	143
Office Equipment / computers.....	144
Security Procedures.....	145
New Employee Security Form	147
Background Release.....	147
Security Access Application Form	149
1. Business and IT Impact Questionnaire.....	150
2. Threat and Vulnerability Assessment Tool	150

XX. What's New	153
Version 4.0	153



I. Security - Introduction

This document implements a formal, ENTERPRISE wide program intended to protect Information and data, including Internet and Information Technology systems, resources and assure their availability to support all ENTERPRISE operations.

All elements of the ENTERPRISE Security Program should be structured to minimize or prevent damage, which might result from accidental or intentional events, or actions that might breach the confidentiality of ENTERPRISE records, result in fraud or abuse, or delay the accomplishment of ENTERPRISE operations.

The objective of the ENTERPRISE Security Program is to achieve an effective and cost beneficial security posture for the enterprise's Internet and Information Technology systems. Attainment of this objective requires a balanced combination of problem recognition, resources and policy to implement an effective program.

The information in this manual:

- Applies to all systems¹ and must be considered from a total-system perspective (i.e., the protection of information must be considered from its origination to its final destruction, to include all processes affecting the information)
- Should be considered as the minimum standard for all systems and supporting manual activities
- Establishes security policies, assigns responsibilities and prescribes procedures for the development and maintenance of ENTERPRISE wide security
- Describes the ENTERPRISE security program
- Complies with the intent of prevailing privacy legislation regarding safeguards and with certain sections of the foreign corrupt practices act

Scope

The scope of this manual is to:

- Provide uniform policy and centralized guidance for dealing with all known and recognized aspects of security affecting ENTERPRISE and its operations

¹ This includes manual, Internet and Information technology systems.



- Provide realistic guidance to ensure that all sensitive information handled by ENTERPRISE automated and manual systems is protected commensurate with the risk of inadvertent or deliberate disclosure, fraud, misappropriation, misuse, sabotage or espionage

NOTE: For the purposes of this document sensitive information includes, but is not restricted to, that information which must be safeguarded so as to:

- *Prevent damage to ENTERPRISE business operations due to unauthorized disclosures*
 - *Assure the individual privacy of ENTERPRISE customers and staff members*
 - *Protect funds, supplies and materials from theft, fraud, misappropriation or misuse*
 - *Protect property and rights of contractors, vendors and other organizations*
 - *Provides for the documented, justified selection of physical, technical and administrative security controls which are cost-effective, prudent and operationally efficient*
 - *Provides for the monitoring of the implementation of selected security controls and procedures*
 - *Provides for the auditing and reviewing functions necessary to ensure compliance with stated security requirements*
 - *Protect contract negotiations and other privileged considerations in dealings with contractors, vendors, correspondents and other organizations*
- Protect staff members from unnecessary temptation to misuse ENTERPRISE resources while fulfilling their normal duties
 - Protect staff members from suspicion in the event of misuse or abuse by others
 - Ensure the integrity and accuracy of all ENTERPRISE information assets
 - Protect ENTERPRISE information processing operations from incidents of hardware, software or network failure resulting from human carelessness, intentional abuse or accidental misuse of the system
 - Ensure the ability of all ENTERPRISE operations to survive business interruptions and to function adequately after recovery
 - Protect management from charges of imprudence in the event of compromise of any security system or disaster



XX. What's New

Version 4.0

- ◆ New section on Travel and Off-Site Meetings
- ◆ Updated Inspection Check List Form