GDPR Sarbanes-Oxley
California Consumer Privacy Act
PCI-DSS CobiT
ISO 27000 -HIPAA - ITIL
FIPS 199 - NIST SP 800-53

This is a sample of the final product
these pages are for your review only
and are protected by Janco's copyright
PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

Security Manual Template

Version 2021
Ransomware Update

Table of Contents

© 2020 Janco Associates, Inc. – https://www.e-janco.com

© 2021 Janco Associates, Inc. – https://www.e-janco.com

© 2021 Janco Associates, Inc. – https://www.e-janco.com

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Security - Introduction

This document defines 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:

This is a sample of the final product
these pages are for your review only
and are protected by Janco's copyright
PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

- perspective (i.e., the its final
- supporting manual
- procedures for the
- complies with the intent of prevailing privacy legislation regarding safeguards and with certain sections of the foreign corrupt practices act

[1] *This includes manual, Internet and Information technology systems.*

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Scope

The scope of this manual is:

- Provides uniform policy and centralized guidance for dealing with all known and recognized aspects of security affecting ENTERPRISE and its operations
- Provides 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
- Prevents damage to ENTERPRISE business operations due to unauthorized disclosures
- Assures the individual privacy of ENTERPRISE customers and staff members
- Protects funds, supplies, and materials from theft, fraud, misappropriation, or misuse
- Protects the
- Provides for
  administrati
  efficient
- Provides for
  procedures
- Provides for
  stated secu
- Protects contract negotiations and other privileged considerations in dealings with contractors, vendors, media reporters, and others
- Protects staff members from the unnecessary temptation to misuse ENTERPRISE resources while fulfilling their normal duties
- Protects staff members from suspicion in the event of misuse or abuse by others
- Ensures 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
- Ensures the ability of all ENTERPRISE operations to survive business interruptions and to function adequately after recovery
- Protects management from charges of imprudence in the event of a compromise of any security system or disaster

This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Objective

The objective of the ENTERPRISE Security Program is to create an ENTERPRISE environment where, based upon an active and continuous risk analysis program, the following elements of Internet and Information Technology Security can be successfully integrated and implemented:

- Denial of access to the Internet and Information Technology systems resources based upon a defined access requirement
- ENTERPRISE databases
- educate staff
- ual as well as
- ecurity in all Internet
- A program of management reviews and audits to ensure compliance with security controls
- A realistic and exercised contingency plan

This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

Applicability

This manual and the ENTERPRISE Security Program apply to all ENTERPRISE activities, departments, and divisions processing and/or utilizing Internet and Information Technology systems resources.

The provisions of this manual apply to all Internet and Information Technology systems resources regardless of application, functional organization, or source of funding.

Internet and Information Technology systems resources include all computer equipment, remote terminals, peripherals, data, software, associated documentation, contractual services, staff members, suppliers, and facilities.

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Best Practices

To create an environment that is secure, compliant, and efficient many best practices have proven to be very valuable. Best practices that we have identified fall into the following categories:

- Best Practices When Implementing Security Policies and Procedures
- Best Practices Network Security Management
- Best Practices to Meet Compliance Requirements
- Best Practices to Manage Compliance Violations
- Best Practices Data Destruction and Retention
- Best Practices to Protect Against Ransomware

Best Practices When Implementing Security Policies and Procedures

After determining the best security policies and procedures, the implementation and

This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

is not a trivial exercise and derstanding – one that will

ude:

ntation. Every environment ess-critical processes. It is important to understand the unintended results of implementing a security process before making it required.

Upper Management Approval – Upper management must not only be aware of upcoming security initiatives but must support them wholeheartedly. This is critical when human resource policies come into play that could affect personnel. Upper management support will be necessary to enforce a process that may be time-consuming or require additional resources.

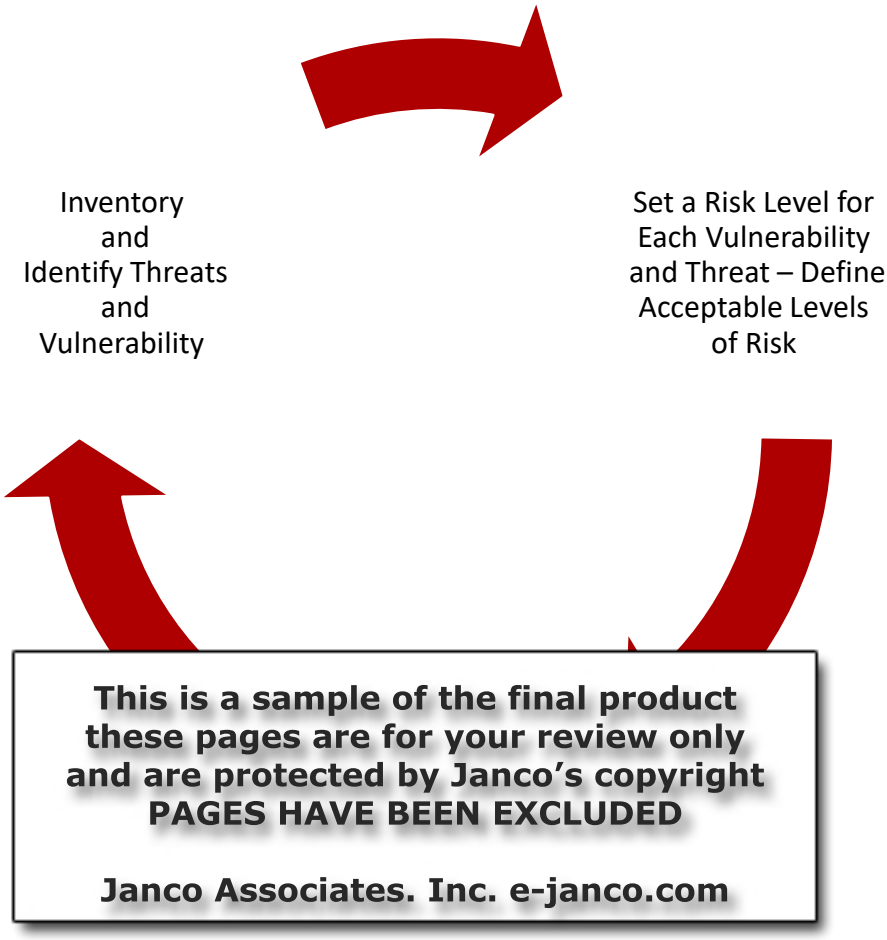
End-User Awareness – End users should be made aware of upcoming changes to security processes. Surprising end-users by changing a process cause fear, confusion, and legitimate frustration. Users should receive awareness as to what is changing and the policies put in place to ensure that the business continues.

Human Resource Policies – Ultimately, human resource policies have to be applied to ensure compliance with security policies. Security processes are often seen as obstructive and employees may try to avoid or circumvent technological solutions. Human resource policies must be in place to discipline these actions.

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Vulnerability Analysis and Threat Assessment

The overall vulnerability analysis and threat assessment process is one that is followed via a structured approach. It is the basis for identifying vulnerabilities and assessing the impacts of existing and new exposures that place ENTERPRISE at risk. The result of this process is to eliminate and/or mitigate unacceptable risk levels within the ENTERPRISE.



This is a sample of the final product
these pages are for your review only
and are protected by Janco's copyright
PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

Threat / Vulnerability / Risk Process

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Evaluate Risk

Risks are at both physical and electronic locations. The result should be a matrix that is used to identify threat areas via vulnerability analysis and business impact analysis tools. The result will be a matrix like the one shown below

Risk Ranking

Impact of Loss	Vulnerability (Probability of Threat)					
	Will Occur over 90%	Extreme 90%< >75%	High 75%< >25%	Moderate 25%< >10%	Low	Under 10%
Catastrophic						
Very High						
Noticeable to ENTERPRISE						
Minor						
None						

Once every risk has been identified and analyzed using the same method of reporting, then ENTERPRISE can understand the existing situation.

Impact of a loss is defined as:

Catastrophic - as a result ENTERPRISE could cease to exist and/or would be placed

This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

s material
to ENTERPRISE's
NTERPRISE's ability

ly and efficiently,

Minor - ENTERPRISE would be affected in a minor way with little productivity and/or service level loss.

None - No impact.

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Impact of Loss	Risk Point Value				
	Will Occur over 90%	Extreme 90%< >75%	High 75%< >25%	Moderate 25%< >10%	Low Under 10%
Catastrophic	8	7	6	5	4
Very High	7	6	5	4	3
Noticeable to ENTERPRISE	6	5	4	3	2
Minor	5	4	3	2	1
None	0	0	0	0	0

Interpretation of scores	
6 to 8	These risks are extreme. Countermeasure actions to mitigate these risks should be implemented immediately.
5	These risks are very high. Countermeasure actions to mitigate these risks should be implemented as soon as possible.
3 to 4	These risks are moderate. Countermeasure actions to mitigate these risks should be implemented in the near term.
1 to 2	These risks are low. Countermeasure actions to mitigate these risks should be implemented as convenient as they will enhance security overall.
0	These currently pose no risk but should continue to be monitored.

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Rights

All Internet and Information Technology systems resources should be assigned to an owner; however, this does not imply full rights of ownership (i.e., the enterprise retains the rights to authorize the sale, distribution, or destruction of a resource).

- The owner is the end-user or person responsible for the assets controlled by a system. Only the identified owner may authorize a user or group of users to access protected resources. Owners of resources are responsible for specifying the:
- A degree of protection for that resource
- Authorized users of that resource
- Access the authority of each user following the policies stated in this manual

		Systems	Applications
Data	Production	Development Group	End Users
	Test	Software Engineering	Application Support Group
Software	Production	Development Group	Development Group
	Test	Software Engineering	Application Support Group
Tra	Test		Application Support Group
Address Space (Capacity)			Development Group
Documentation			Application Support Group

This is a sample of the final product
these pages are for your review only
and are protected by Janco's copyright
PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

Rights Matrix Table

Only the owner of a resource will have the authority to approve a change to the access control restrictions previously specified for that resource. Owners of data are responsible for reviewing access to that data. Owners are also responsible for determining the following resource characteristics:

- Value, importance, and specific business purpose
- Level of classification in one of the classes

[11] *ISP – Internet Service Provider this can be an internal group within the enterprise or an outsourced provider.*

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Ransomware - HIPAA Guidance

A recent U.S. Government report indicates that, on average, there have been 4,000 daily ransomware attacks (a 300% increase over the 1,000 daily ransomware attacks reported last year).

Ransomware exploits human and technical weaknesses to gain access to an organization's technical infrastructure to deny the organization access to its data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and recovering from a ransomware attack. This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.

This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

ckups and ensuring the
nsomware attack. Test
of backed up data and
Because some ransomware
kups, entities should
works.

Email Gateway for Ransomware Attacks

Email cyberattacks are as old as email itself. Ransomware attackers continue developing new tactics as security capabilities continue to become more robust. While 'click-and-run' attacks like spam and mass phishing campaigns still exist, Ransomware cyberattackers do not spend too much time crafting them and they can be effectively blocked with traditional security controls.

Type of Attack	Method	Techniques Used	Payload Delivery
Spam	Mass e-mail	N/A	Malicious Link - executable
Mass Phishing	Mass e-mail	Phishing Kits	Malicious Link - executable
Impersonations	Gmail/Yahoo Look Alike domains	Social Engineering	Ask/request - fake attachment
Financial Fraud	Gmail/Yahoo Look Alike domains	Impersonation and Social Engineering	Ask/request- fake attachment from Bank or agency like IRS
Vendor Fraud	Email from compromised account	Impersonation and Social Engineering	Ask/request - fake attachment from known vendor
Credential Phishing	Email from compromised account	Re-directs, impersonation for login pages	Fake attachments - 0 day links
Account Takeover	Credential phishing attack	Auto-forwarding rules, lateral movement	Fake attachments - 0 day links

© 2021 Copyright Janco Associates, Inc. – ALL RIGHTS RESERVED – https://e-janco.com

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Appendix - A

Attached Job Descriptions

Chief Security Officer (CSO)

Chief Compliance Officer (CCO)

Data Protection Officer

Manager Security and Workstation

Manager WFH support

Security Architect

System Administrator

This is a sample of the final product
these pages are for your review only
and are protected by Janco's copyright
PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

Attached Policies

To ensure that you have the latest version of several critical IT Infrastructure policies (when this template updates), they are included as separate documents. However, be aware that you will NOT BE notified when the policies below are updated unless this Template is updated.

These policies are in a sub-directory title "Policy"

Blog and Personal Website Policy

Internet, Email, Social Networking, Mobile Device, and Electronic Communication Policy

Mobile Device Policy

Physical and Virtual File Server Security Policy

Sensitive Information Policy - Credit Card, Social Security, Employee, and Customer Data

Travel and Off-Site Meeting Policy

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Attached Security Forms

To ensure that you have the latest version of several critical Security Management Forms (when this template updates), they are included as separate documents. However, be aware that you will NOT BE notified when the policies below are updated unless this Template is updated.

These policies are in a sub-directory title "Forms"

Application & File Server Inventory
Blog Policy Compliance Agreement
BYOD Access and Use Agreement
Company Asset Em
Email Employee Ag
Employee Termina
FIPS 199 Assessme
Internet Access Re
Internet and Electr
Internet use Approv
Mobile Device Access and Use Agreement
Mobile Device Security and Compliance Checklist
New Employee Security Acknowledgment and Release
Outsourcing and Cloud Security Compliance Agreement
Outsourcing Security Compliance Agreement
Preliminary Security Audit Checklist
Privacy Compliance Policy Acceptance Agreement
Risk Assessment
Security Access Application
Security Audit Report
Security Violation Procedures
Sensitive Information Policy Compliance Agreement
Server Registration
Social networking Policy Compliance Agreement
Telecommuting Work Agreement
Text Messaging Sensitive Information Agreement
Threat and Vulnerability Assessment Inventory
Work From Home Work Agreement

This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Additional Attached Materials

Business and IT Impact Questionnaire

Attached as a separate document

Threat and Vulnerability Assessment Tool

Attached as a separate document

Sarbanes-Oxley Section 404 Check List Excel Spreadsheet

Attached as a separate document

This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Employee Termination Process

After an employee has terminated (voluntary or involuntary) you can find yourself in the middle of a wrongful termination lawsuit. This can cost the company both time and money. If you are unlucky, you may be forced to hire the employee back. Using an employee termination checklist can help ensure you follow all the correct procedures when letting someone go.

As you now know, firing or laying off an employee is not as simple as saying "you're fired" or "you are laid-off." There are legal ramifications and is therefore much more complicated than it appears on the surface.

- ❑ **Compile The Proper Documentation** You or your manager should have the right legal documents in pl
paperwork you
words, make sur
- ❑ **Prepare The Te**
likely have a tem
- ❑ **Create A Severa**
employee severa
Department and
this package ready for the employee during the termination meeting. Include a document for the employee to sign before they get the package, which limits or eliminates their rights to sue the company, its employees, and its agents.
- ❑ **Come Up With Additional Agreements** As an employer you may wish to have the employee sign an employee termination agreement or a non-compete agreement. Make sure whatever your draft is run by either your Human Resources Personnel or your business attorney.
- ❑ **Prepare An Agenda For The Termination Meeting** You must know exactly what you are going to say and how you will say it. Make sure you set up a meeting room ahead of time that is away from the individual's coworkers. Also, have another representative (witness) from the company there. Usually, a member of the Human Resources Department is a good choice.
- ❑ **List Out Those Items The Former Worker Must Return** Employee terminations are stressful for both the employer and the employee. During this time, you may forget to ask the worker to return important company property. Recovering it after the employee is gone will prove difficult.
- ❑ **Conduct An Employee Exit Interview** It is usually best to have a third party do this for you.

This is a sample of the final product
these pages are for your review only
and are protected by Janco's copyright
PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Employment Termination Checklist

Employee Name: _____

Date: _____

Notify Human Resources

_____ Notify HR: As soon as you are aware of and/or receive a letter from an employee that notifies you of the employee's intention to terminate employment, notify your Human Resources office.

_____ Official Notice: If an employee tells you of their intention to leave your employment, ask them to write a resignation letter that states they are leaving and their termination date. (Companies request a minimum of two weeks' notice, when possible and desirable.)

Permissions Termination

This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

strator: As soon as
r and other
rminate the
es. Arrange for these
ntact with clients
ntry alarm code and

Return of Property

_____ Return of company property: Existing employees are required to turn in all company books and materials, keys, ID badges, computers, cell phones, and any other company-owned items.

_____ Passwords: Employees should provide their supervisors with passwords and other information on accessing computer files and telephone messages. (You may want to keep email and phone accounts active for a while to field customer contacts.) In any case, to meet regulatory guidelines you will need to archive all data that can be considered a "business record."

Status of Benefits

_____ Vacation pay and unused sick time: Terminating employees are paid up to a maximum of 30 days for unused, accrued vacation time. If the employee has used the time not yet accrued, payment to the company for this time is subtracted from the last paycheck. (If your company designates a certain number of sick days and they are accrued, you would also need to pay the employee for the time accrued.)

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Security Management Compliance Checklist

This defines the base level of requirements for compliance with most mandated requirements for the security of sensitive information.

Policy & Process Definition

- ❑ **Provisioning Policies** - Ability to define rule-based policies to determine the list of applications a user should be provisioned to and his or her entitlements in those applications
- ❑ **Denial Policies** - Ability to define what resources and applications should be denied to a user or a set of users, as part of provisioning policies.
- ❑ **Access Policies** - Ability to define rule-based policies to determine who has access to which web resources.
- ❑ **Role-Based Access Control (RBAC)** - Ability to define provisioning entitlements and membership rules to the

This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

at the auditors and
s effective on a given

o applications or
ccess policies.

- ❑ **Approval Policies** - Ability to define the list of approvers for each resource in provisioning requests. Ability to utilize roles in approval policies.
- ❑ **Administrative Policies** - Ability to define rule-based policies for administering various identity entities i.e. roles, organizations, and resources
- ❑ **Segregation of Duty (SOD) Policies** - Ability to define policies that prevent a user from acquiring a conflicting combination of roles, resources, or entitlements in a single resource.

Preventive Controls

- ❑ **Single Sign-On** - Ability to support single sign-on across multiple applications and heterogeneous servers spread across multiple DNS domains extending to partner and consumer applications.
- ❑ **Strong Authentication** - Ability to support advanced authentication mechanisms to prevent authentication attacks such as phishing, trojan, proxy attacks, and other threats.
- ❑ **Real-time Fraud Prevention** - Ability to perform a sophisticated risk analysis to trigger real-time alerts and follow-up actions (for example, challenge the user) to prevent fraudulent transactions in real-time.
- ❑ **Authoritative Source** - Ability to designate a set of resources or applications as the authoritative sources for user provisioning.
- ❑ **Authoritative Reconciliation** - Ability to trigger provisioning workflows based on reconciling with authoritative resources.
- ❑ **User On-Boarding Workflow** - Ability to define automated or approval based workflows based on provisioning policies to create a user's accounts in various applications.

© 2021 Janco Associates, Inc. – https://www.e-janco.com

User/Customer Sensitive Information and Privacy Bill of Rights

Users and customers of the enterprise's systems and networks will have the following rights:

- Enterprise will provide Users/customers of the enterprise's systems a privacy policy regarding the data they collect.
- Users/customers of the enterprise's systems have the right to know what type of personally identifiable information is being collected and how long that personally identifiable information is kept by the enterprise and any other related third party.
- Users/customers of the enterprise's systems can expect that an enterprise or related 3rd party that holds their personally identifiable information in connection with a transaction or service is adequately protecting the personally identifiable information from disclosure to unauthorized persons.

This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

e from an enterprise or
r is reasonably believed to
ult in identity theft or

hat to the enterprise's

e from the enterprise in
reasonable delay" (never later than 60 days after a breach, unless a criminal investigation is potentially affected.)

- Service providers that have obtained personally identifiable from the enterprise will send a notification regarding a data breach of protected information that is held by them, under mandated laws such as SOX, PCI, HIPPA, and other mandated requirements.
- Users/customers of the enterprise's systems will receive a general description of the actions taken by the enterprise to restore the security and confidentiality of the personally identifiable information involved in a data breach.
- Users/customers of the enterprise's systems will be provided at least 12 months of identity theft protection at the enterprise's expense.
- Enterprise will notify users/customers of a summary of the breach as victims of identity theft under the Fair Credit Reporting Act.

© 2021 Janco Associates, Inc. – https://www.e-janco.com

General Data Protection Regulation (GDPR) - Checklist

The General Data Protection Regulation (GDPR) sets specific compliance requirements on how your business does business with enterprises and individuals in the EU.

The EU requires that enterprises need to have consent or legitimate interests to use personal data. Whether you rely on consent or legitimate interests for your marketing, you need to do similar things to make sure you are GDPR compliant:

- ❑ Be clear with individuals why you need their data at the point of collection
- ❑ Always use clear and concise language appropriate for your target audience
- ❑ Provide information at the point the data is collected. It cannot be hidden in small print.
- ❑ Give individuals control over their data. They should be able to decide whether to share their data with you or not.

This is a sample of the final product these pages are for your review only and are protected by Janco's copyright PAGES HAVE BEEN EXCLUDED

Janco Associates. Inc. e-janco.com

- ❑ Validated that legitimate interests are the most appropriate lawful basis for processing
- ❑ Communicate how or why there is a need for an individual's data when it is collected
- ❑ Utilize a layered privacy notice/policy - A layered privacy notice puts the most important information up front and then there is a more detailed privacy policy underneath it
- ❑ Inform Individuals on what the plan is for their data when it is collected
- ❑ Allow individuals to "opt-out" of marketing
- ❑ Collect the minimum data necessary and delete records after use
    - Data needed for a suppression file can be kept.
    - Have a valid reason to process an individual's data using your legal legitimate interests. For example, an individual may have acquired a product, therefore, the business can market similar products to the customer

© 2021 Janco Associates, Inc. – https://www.e-janco.com

Revision History

Version 2021 - Ransomware Update

- Updated the Internet, Email, Social Networking, Mobile Device, and Electronic Communication Policy to highlight Ransomware gateway email threats

Version 2021

- Updated to meet the latest compliance mandates including CCPA and GDPR
- Updated to meet WFH security requirements
- Updated all 28 included electronic forms
- Added form
  - Work From Home Work Agreement
- Added job descriptions
  - Data Protection Officer
  - Manager Security and Workstation
  - Manager WFH support
  - Security Architect
  - System Administrator
- Updated job descriptions
  - Chief Security Officer (CSO)
  - Chief Compliance Officer (CCO)

Version 2020

- Updated to meet the latest compliance mandates including CCPA
- Included job descriptions
  - Chief Security Officer (CSO)
  - Chief Compliance Officer (CCO)
- Included Policy – Internet, Email, Social Networking, Mobile Device, and Electronic Communication Policy as a standalone item.
- Updated all electronic forms to current versions
- Updated all attached policies to current versions

Version 2019

- Updated to meet the latest compliance mandates
- Updated forms as a separate attached PDF file
- Updated all attached policies as separate items

Version 2018 - 07

- Added section to cover the New California Consumer Privacy Act – Defines consumer rights and business responsibilities.
- Change the Version numbering system for the Security Manual Template

© 2021 Janco Associates, Inc. – https://www.e-janco.com