



IT Infrastructure Policy Bundle



License Conditions

This product is NOT FOR RESALE or REDISTRIBUTION in any physical or electronic format. The purchaser of this template has acquired the right to use it for a SINGLE enterprise in a single county unless they have a multi-use license. Anyone who makes copies of or uses the template or any derivative of it violates the United States and international copyright laws and is 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 any derivative of this template will contain the following words within the first five pages of that document. The words are:

©2024 Copyright Janco Associates, Inc. – ALL RIGHTS RESERVED

All Rights Reserved. No part of this document may be reproduced by any means without the prior written permission of the publisher. No reproduction or derivation of this book shall be re-sold or given away without royalties being paid to the authors. All other publisher's rights under the copyright laws will be strictly enforced.

**Published by: Janco Associates Inc.
Park City, UT 84060**

Email – support@e-janco.com

ISBN13 (978-1881218-48-7)

HandiGuide is a registered trademark of Janco Associates, Inc.

The publisher cannot in any way guarantee the procedures and approaches presented in this book are being used for the purposes intended and therefore assumes no responsibility for their proper and correct use. Also, we are not attorneys and are not providing a legal opinion as to the data that should be retained nor the periods that the data should be retained. The user should check with their own legal counsel to determine the specific requirements for record retention and destruction.

Printed in the United States of America



Table of Contents

This document contains the following policies:

- ✚ Backup and Backup Retention Policy (revised 02/2024)
- ✚ Blog and Personal Web Site Policy (revised 01/2023)
- ✚ BYOD Access and Use Policy (revised 03/2024)
- ✚ Google Glass Policy (revised 03/2023)
- ✚ Incident Communication Policy (revised 01/2023)
- ✚ Internet, Email, Social Networking, Mobile Device, and Electronic Communication Policy (revised 02/2024)
- ✚ Mobile Device Access and Use Policy (revised 04/2024)
- ✚ Outsourcing and Cloud-Based File Sharing Policy (revised 02/2024)
- ✚ Patch Management Version Control (revised 03/2023)
- ✚ Physical and Virtual Server Security (revised 03/2024)
- ✚ Privacy Compliance Policy (revised 03/2024)
- ✚ Record Classification, Management, Retention, and Disposition Policy (revised 03/2024)
- ✚ Safety Program (revised 01/2024)
- ✚ Sensitive Information Policy (revised 03/2024)
- ✚ Service Level Agreement Policy including sample metrics (revised 03/2023)
- ✚ Social Networking Policy (revised 03/2024)
- ✚ Technology Acquisition Policy (revised 03/2023)
- ✚ Text Messaging Sensitive and Confidential Information (revised 03/2024)
- ✚ Travel, Laptop, PDA and Off-Site Meeting Policy (revised 04/2024)
- ✚ Wearable Devices (revised 03/2024)
- ✚ Work From Home (WFH) & Telecommuting Policy (revised 03/2024)

Legend – Highlighted in Yellow updated in 2024

All the job description and electronic forms were reviewed and updated in January 2024

You will receive notifications when the updates are available. If you have not purchased the update service, you will only be able to download these updates for 30 days after the original purchase. To get the update service go to:

- 12 months - https://e-janco.com/session/cart_x.aspx?p=SUB-090-12
- 24 months - https://e-janco.com/session/cart_x.aspx?p=SUB-094-24
- Individual Policies - <https://e-janco.com/updateserviceindividualpolicies.htm>



Backup and Backup Retention Policy



2024



Table of Contents

Table of Contents.....3

Backup and Backup Retention Policy.....4

 Policy.....4

 Applicability4

 Backup Versus Archive.....4

 Archiving Implications Sarbanes-Oxley5

 SOX – Section 8025

 Record Retention Requirements.....5

 Artificial Intelligence Impact on Backup and Recovery.....5

 Types of Backups7

 Storage Management8

 Minimal Backup Policy8

 System Specific Backup Policy13

 Backup Retention.....15

 Documentation and Backup Media Labeling.....15

 Issues to Manage with SLAs for Backup.....17

 Proposed Service Level Agreement Metrics18

Appendix.....19

 EU Safe Harbor Act Compliance and Data Backup Conflicts.....20

 Backup - Best Practices21

 Cloud Backup – Best Practices24

 Mobile Device and Work From Home Users Backup - Best Practices.....25

 Electronic Forms26

 • Outsourcing Security Compliance Agreement

 • Telecommuting Work Agreement

 • Remote Location Contact form

 • Vendor Contact Information form

 • Work From Home Contact Information form

 Job Descriptions.....27

 • Manager Artificial Intelligence

 • Manager Compliance

 • Manager Disaster Recovery and Business Continuity

 • Manager Security and Workstations

 • Manager WFH Support Manager WFH Support

What’s New28



Blog Personal Website Policy

2023 Edition

Table of Contents

Blog and Personal Web Sites Policy	2
Policy	2
Rights to content	3
Option for More Restrictive License Terms	3
Attribution	4
Guidelines	4
Personal Website and Blog Guidelines – Non ENTERPRISE domains	6
Security Standards.....	7
Best Practice Blog Guideline for Publishers.....	8
Blog Best Practices to Improve the Value of Your Blog	9
Issues to Manage with SLAs for Blog and Web Site Security.....	10
Proposed Service Level Agreement Metrics.....	11
Blog Policy Compliance Agreement.....	12
What’s New	13



BYOD Policy Template



JANCO ASSOCIATES, INC.

2024

Table of Contents

Bring Your Own Device (BYOD) Access and Use Policy3

 Overview3

 Components of the BYOD Strategy and Basics for BYOD Policy.....4

 Device Ownership Issues7

 Policy8

 Device Requirements8

 Policy Definitions9

 Access Control.....9

 Security10

 Help & Support11

 Enterprise Mobile Device Infrastructure11

 BYOD Infrastructure.....12

 Disaster Recovery12

 Termination.....12

 Backups12

 Tablet Computer (iPads)13

 Internal Network Access13

 Repair Procedure13

 Upgrade Procedure13

 Patching Policy13

 BYOD Security Best Practices14

 Work From Home - Best Practices.....16

BYOD Metrics and SLA Agreement17

Legal Considerations.....19

Appendix.....22

 BYOD Policy Decision Table23

 Electronic Forms24

 BYOD Access and Use Agreement Form

 Employee Termination Checklist

 Mobile Device Security Access and Use Agreement Form

 Mobile Device Security and Compliance Checklist

 Telecommuting IT Checklist

 Telecommuting Work Agreement

 Work From Home IT Checklist

 Work From Home Work Agreement

 IT Job Descriptions25

 BYOD Support Specialist

 BYOD Support Supervisor

 Manager BYOD Support

 Manager WFH Support

What’s New26



Google Glass Policy Template



Table of Contents

Google Glass Policy	3
<hr/>	
Overview	3
<hr/>	
Policy	3
Google Glass Policy Requirements	4
Policy Definitions	4
Access Control	5
Security	6
Help & Support	7
Work From Home Considerations	7
Ownership of device	7
Ownership of data	7
Enterprise Mobile Device Infrastructure	8
Google Glass Infrastructure	8
Disaster Recovery	9
Backups	9
Google Glass Physical Device	9
Internal Network Access	10
Repair Procedure	10
Upgrade Procedure	10
Patching Policy	10
Google Glass Security Best Practices	11
<hr/>	
Legal Considerations	13
Privacy	13
Record Retention	13
<hr/>	
Appendix – Electronic Forms	16
• Google Glass Access and Use Agreement	16
• Mobile Device Access and Use Agreement	16
• Mobile Device Security and Compliance Checklist	16
• Wearable Device Access and Use Agreement	16
<hr/>	
What’s New	17



Incident Communication Plan Policy



JANCO ASSOCIATES, INC.

2023 Edition



Table of Contents

Incident Communication Plan.....	1
Overview.....	1
Policy	2
Guidelines	3
Request for Information	4
Editorial or Letter to Editor Requests	4
Requests for Interviews	5
Emergency Response.....	5
Pandemic Considerations	6
Unannounced Visit	7
Press Releases.....	8
Business Continuity Communication Lifecycle	9
Pre-event	9
Event Occurrence	10
On-going event impact	11
Resumption of business operation.....	11
Post-event evaluation.....	12
Best Practices	13
News Conference.....	13
Press Release	14
Media Relations	15
Federal Computer Security Incident Handling Requirements	16
Appendix.....	18
Cyber Incident Response Responsibilities	19
Social Networking Checklist.....	20
Job Description	26
Director Media Communications.....	26
Electronic Forms	27
Incident Communication Contact Form	27
Pandemic Planning Checklist Form.....	27
What’s New	28



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



JANCO ASSOCIATES, INC.

2024



TABLE OF CONTENTS

Internet, Email, Social Networking, Mobile Device, and Electronic Communication Policy.....	2
Risks and Costs Associated with Email, Social Networking, Electronic Communication, and Mobile Devices.....	2
Appropriate use of Equipment	2
BYOD Security	2
Overview of electronic communication and data sharing.....	3
Internet Access	4
Tablets, PDAs, and Smartphones.....	4
Federal Rules of Civil Procedures.....	5
Enterprise Acceptable Use Overview for Electronic Communications.....	6
Electronic Mail	6
Retention of Email on Personal Systems	11
Email Forwarding Outside of ENTERPRISE.....	11
Email User Best Practices.....	12
Commercial Email	14
Work From Home	16
Social Networking	17
Copyrighted Materials	20
Ownership of Information	20
Security	20
Skype.....	21
Text Messaging	22
Appendix.....	23
Job Descriptions	23
Manager User Support	
Manager WFH Support	
Forms.....	24
Internet & Electronic Communication - Employee Acknowledgment	
Internet Access Request	
Email Employee Acknowledgment	
Internet Use Approval	
Security Access Application	
Social Networking Policy Compliance Agreement	
Telecommuting IT Check List Form	
Telecommuting Work Agreement	
Text Messaging Sensitive Information Agreement	
Work From Home Contact Information	
Work From Home IT Checklist	
Work From Home Work Agreement	
Reference Section	25
Standard e-mail Reply Responses	25
Canada's Anti-spam Law (CASL), Bill C-28	26
What's News.....	30



Mobile Device Access & Use Policy



Table of Contents

Mobile Access and Use Policy	2
Overview	2
Components of the BYOD Strategy and Basics for BYOD Policy.....	3
Policy.....	6
Policy and Appropriate Use.....	6
Mobile Devices.....	8
Policy Definitions	9
Access Control.....	9
Federal Trade Commission Mobile Policy Guidelines	10
Security	11
Help & Support	12
Enterprise Mobile Device Infrastructure	13
Equipment and Supplies	13
Tablet Computer (iPads and Microsoft Surface).....	14
Mobile Device Security Best Practices	16
Mobile Device Security Best practices	16
Security controls	16
Remote device management	17
Access management controls	17
Tablet and Smartphone applications	17
Appendix.....	18
Electronic Forms.....	19
• BYOD Access and Use Agreement Form	
• Company Asset Employee Control Log	
• Employee Termination Checklist	
• Mobile Device Security Access and Use Agreement Form	
• Mobile Device Security and Compliance Checklist	
• Wearable Device Access and Use Agreement	
• Work From Home Contact Information	
• Work From Home IT Checklist	
• Work From Home Work Agreement	
What’s New	20



Outsourcing & Cloud Based File Sharing Policy

2024 Edition



JANCO ASSOCIATES, INC.



Table of Contents

Outsourcing and Cloud-Based File Sharing Policy.....3

 Outsourcing Cloud-Based File Sharing Management Standard.....3

 Overview3

 Standard3

 Outsourcing Policy4

 Policy Statement4

 Goal4

 Approval Standard5

 Overview5

 Standard5

 Work From Home Considerations.....10

 Responsibilities.....10

 Appendix.....12

 Electronic Forms.....13

 • Outsourcing and Cloud Security Compliance Agreement

 • Outsourcing Security Compliance Agreement

 • Remote Location Contact Information

 • Vendor Contact

 • Work From Home IT Checklist

 • Work From Home Work Agreement

 Job Descriptions14

 • Vice President Strategy and Architecture

 • Manager Cloud Applications

 • Manager Outsourcing

 • Manager User Support

 • Manager Vendor Management

 • Manager WFH Support

 • Cloud Computing Architect

 Audit Program Guide.....15

 Background.....15

 ISO 27001 requirements15

 ISO 27001 implementation requires15

 Planning the Audit.....16

 Audit Scope17

 Audit Objectives17

 Audit Wrap Up.....18

 Top 10 Cloud and Outsourcing SLA Best Practices.....19

 What’s New20



Patch Management Version Control Policy



2023 Edition



Table of Contents

Patch Management Version Control Policy	2
The Patch Management Version Control Process	2
Policy.....	3
Emergency patches.....	7
Critical Patches	7
Version Control Best Practices.....	9
Security Patch Management Best Practices	11
Appendix.....	14
Job Descriptions.....	14
Manager Change Control	
Manager Training and Documentation	
Manager User Support	
Manager WFH Support	
Change Control Supervisor	
Change Control Analyst	
Electronic Form.....	15
Change and Patch Management Control Log	
Work From Home Contact Information	
Work From Home IT Checklist	
What’s New.....	19

Policy that describes the requirements for all application and data servers which are private and public – including Cloud based applications and data

Physical and Virtual Server Security Policy

2023 Edition



Physical and Virtual File Server Security Policy

Table of Contents

Table of Contents	2
Physical and Virtual File Server Security Policy	4
Policy Purpose	4
Policy Statement.....	4
Applicability	4
Terms and Definitions.....	4
Server Requirements	4
Critical Server Requirements	5
General Server Requirements.....	5
Public Server Requirements.....	5
Server Configuration Guidelines.....	6
Forms	7
Server Registration Form	
Application & File Server Inventory	
What's New	8



Privacy Compliance Policy



2024



Table of Contents

Privacy Compliance Policy – U.S. and EU Mandated Requirements.....	3
Overview.....	3
Right to Privacy.....	3
California Consumer Privacy Act of 2018.....	4
Consumer’s Right to Know Information that Has Been Captured.....	4
Consumer’s Right to Have Data Removed.....	5
Consumer’s Right to Know How Data is Used.....	6
Consumer’s Rights to Data That is Sold.....	7
Consumer’s Rights for Stopping the Sale of Data.....	8
Consumer’s Rights to Not be Discriminated Due to Opt Out.....	9
Enterprise Reporting Requirements.....	10
Enterprise Internet and WWW requirements.....	12
GDPR.....	13
Why Data is Captured.....	13
User Consent.....	14
Communication.....	15
Third Party Data.....	15
Profiling.....	16
Legacy data.....	16
PCI.....	17
HIPAA.....	20
Gramm-Leach-Bliley (Financial Services Modernization Act of 1999).....	21
Massachusetts 201 CMR 17.00 Data Protection Requirements.....	22
User/Customer Sensitive Information and Privacy Bill of Rights.....	23
Appendix.....	24
Forms.....	24
Privacy Compliance Policy Acceptance Agreement	
Job Descriptions.....	25
Chief Security Officer	
Data Protection Officer	
Manager Compliance	
Manager Security and Workstations	
Security Architect	
Privacy and Security Compliance Implementation Work Plan.....	26
What’s New.....	28



Record Management, Retention, and Disposition Policy



Table of Contents

Record Classification, Management, Retention, and Disposition Policy Statement2
Overview2
Scope3
Work From Home impact3
AI impact3
What is Record Classification and Management4
Regulatory Overview5
What ENTERPRISE Should Do10
Record Classification, Management, Retention, and Disposition Standard11
Email Retention Compliance25
Implementation Interview Checklist30
Record classification, management, retention, and disposition Annual Review Process31
Record Management Best Practices33
Appendix37
Job Descriptions38
Manager – Record Administrator
Manager WFH Support
Record Management Coordinator
Forms39
Personnel Records – sections of this form have been pre-completed for areas that are mandated by US federal laws and are consistent across all industries
Administrative Records
Computer and Information Security Records39
Computer Operations and Technical Support
Data Administration
General Systems and Application Development
Facility Records
Financial Records
Mobile Device Access and Use Agreement
Safety Records
Sales Records
Network and Communication Services
User and Office Automation Support
Document Retention Periods40
Federal Law Record Retention41
Pennsylvania Record Retention50
Massachusetts Record Retention53
I-9 Retention55
Version History58

Safety Program



JANCO ASSOCIATES, INC.

2024



Table of Contents

- Safety Program Policy2
- Safety Goals3
- Responsibilities4
- Internet of Things (IoT)6
- Safety Rules7
- Progressive Disciplinary Program10
- Accident Investigation11
- Hazard Recognition And Control12
 - Job Hazard Analysis (JHA).....12
 - Inspection Procedures.....12
 - Incidental Inspection13
 - Planned Inspection.....13
- Safety Committee14
- Safety Training15
- Communication17
- Record Keeping18
 - Inspection Documentation.....18
 - Accident Investigation -- Accident & Injury Records18
 - Training18
 - Safety Committee.....18
- New Employee Orientation19
- Training20
- Appendix.....22
 - IT Job Descriptions23
 - Manager Safety Program
 - Supervisor Safety Program
 - Forms.....24
 - Area Safety Inspection
 - Employee Job Hazard Analysis
 - First Report of Injury
 - Inspection Checklist – Alternative Locations
 - Inspection Checklist - Computer Server Data Center
 - Inspection Checklist – Office Locations
 - Inspection Checklist – Work From Home Locations
 - New Employee Safety Checklist
 - Safety Program Contact List
 - Training Record
 - OSHA Electronic Forms.....24
 - Instructions
 - OSHA xls Form
 - OSHA 300 Form
 - OSHA 300A Form
 - OSHA 301 Fprm
- Revision History25



Policy

Sensitive Information



JANCO ASSOCIATES, INC.

2024



Table of Contents

Sensitive Information Policy - Credit Card, Social Security, Employee, and Customer Data	2
Overview	2
Policy	2
User/Customer Sensitive Information and Privacy Bill of Rights	7
Secure Network Standards	8
Payment Card Industry Data Security Standard (PCI DSS)	8
Install and Maintain a Network Configuration Which Protects Data	12
Wireless & VPN	13
Modify Vendor Defaults	13
Protect Sensitive Data	14
Protect Encryption Keys, User IDs, and Passwords	15
Protect Development and Maintenance of Secure Systems and Applications	16
Manage User IDs to Meet Security Requirements	18
Restrict Physical Access to Secure Data Paper and Electronic Files	19
Regularly Monitor and Test Networks	20
Test Security Systems and Processes	21
Email Retention Compliance	22
Policy	22
Email to be printed	24
Regulations and Industry Impact	25
Keys to Email Archiving Compliance	25
Privacy Guidelines	26
Best Practices	27
Best Practices for Text Messaging of Sensitive Information	27
US government classification system	29
Appendix	32
Job Descriptions	33
• Chief Compliance Officer (CCO)	
• Chief Security Officer (CSO)	
• Manager Data Security	
• Security Architect	
Forms	34
• Sensitive Information Policy Compliance Agreement	
• Work From Home IT Checklist	
HIPAA Audit Program Guide	35
What's New	40



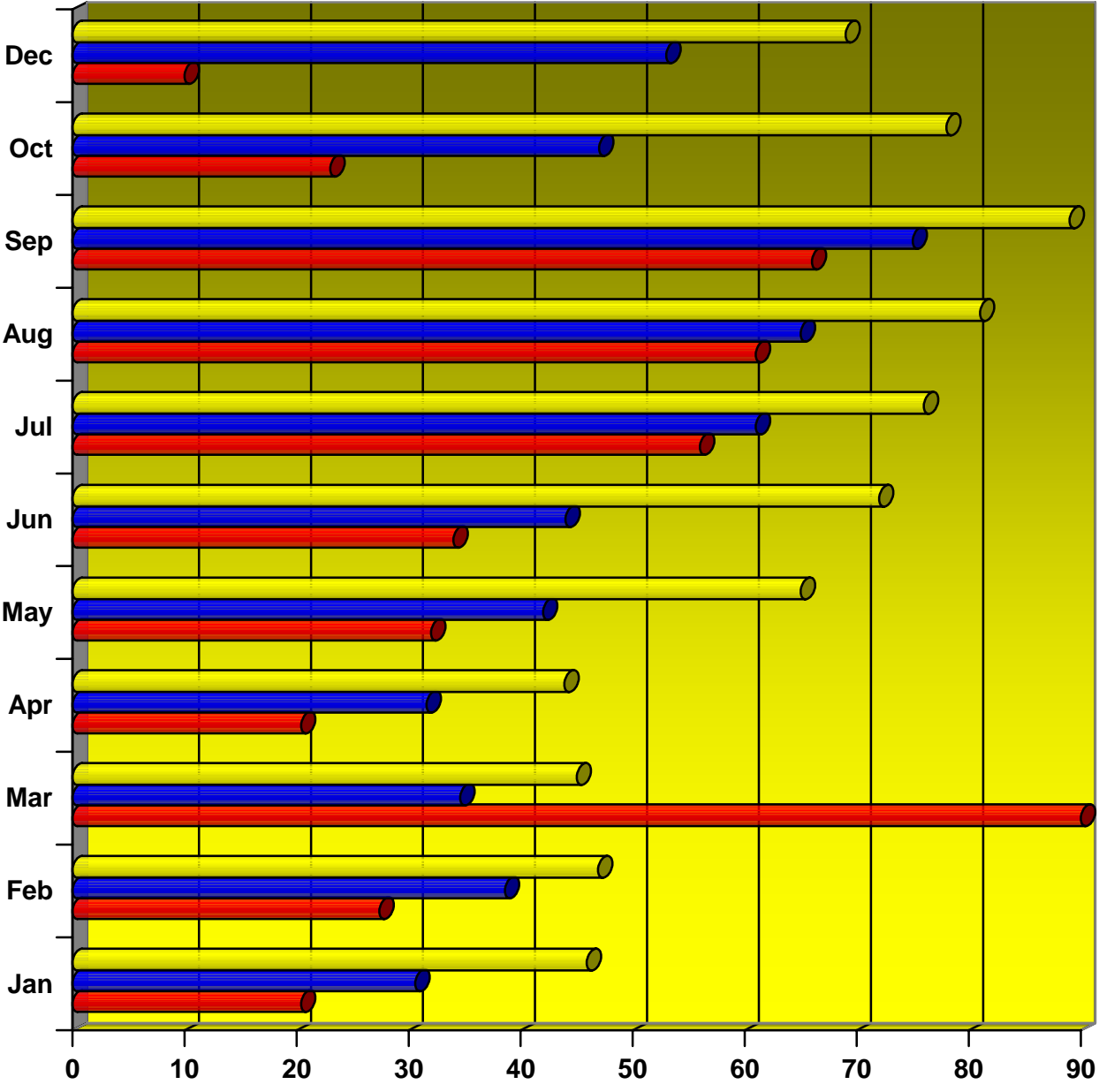
Lorem Ipsum

Service Level Agreement Policy Template & Sample KPI Metrics

Table of Contents

- Table of Contents 2
- Service Level Agreement 5
 - Definition of What a Service Level Agreement is 5
 - Sample Service Level Agreement 6
 - Assumptions 6
 - Service Stakeholders 7
 - Service Scope 7
 - IT Provider Responsibility 8
 - Prioritization 8
- Typical Service Level Agreements 9
 - Internal IT SLAs 9
 - External SLA 11
- Sample Metrics 15
 - Work From Home – KPI Metrics 16
 - System Management – KPI Metrics 17
- What's New 19
- Appendix 18
 - Job Descriptions
 - Director IT Management and Controls
 - Manager KPI Metrics
 - Manager Metrics
 - Metrics Measurement Analyst
 - SEO Specialist

Service Level Agreement and Policy Template with Sample Metrics



Sample SLA Metrics

Service Levels

[System Management](#)

[Weekly Call Volumes](#)

[Response Times](#)

[Desktop - Mean Time To Repair](#)

Problem Analysis

[Ticket Volumes by Group](#)

[Tickets by Severity](#)

Infrastructure

[Infra Notes](#)

[Infra Comm 1](#)

[Infra Comm 2](#)

[Internet Usage](#)

Abend Analysis

[Tracking Abends](#)

[Abend Impact](#)

Applications

[Application Development](#)

System Monitoring Center

[1st SMC Group](#)

[2nd SMC Group](#)

[3 rd SMC Group](#)

[4th SMC Group](#)

[5th SMC Tape Rpt Aging](#)

[Dataset Aging Example Metrics](#)

[SMC SRT \(Cars.IW, M&D, DATool\)](#)

[SMC SRT \(All Summary\)](#)

[SMC SRT \(MAPS, OfficeV\)](#)

[SMC SA \(CARS,MAPS, IW, M&D\)](#)



Social Networking Policy

Managing and Controlling Employee Social Networks



JANCO ASSOCIATES, INC.

2024



Table of Contents

Policy – Social Networking	3
Definitions	3
Overview.....	3
Rights to content	8
Rules for Social Network Engagement	11
Social Network Best Practices and Guidelines	13
Security Standards.....	16
BYOD Security.....	17
Protect Sensitive Data	17
Disaster Recovery and Business Continuity.....	18
Best Practices in Managing Social Networks and Social Relationships	19
Steps to Prevent Being Scammed by Social Media	20
Appendix.....	21
Job Descriptions	22
• Chief Experience Officer	
• Manager Social Networking	
• Social Media Specialist	
Electronic Forms.....	23
• Internet and Electronic Communication Agreement	
• Social Network Policy Compliance Agreement	
Protection from Ransomware, Phishing, and Whaling Attacks.....	24
Social Networking Best Practices	28
Twitter.....	28
Truth Social	30
LinkedIn.....	31
Blog	33
What's New	36



Technology Acquisition Policy



JANGO ASSOCIATES, INC.

2023

Technology Acquisition Policy

Table of Contents

Policy - Technology Acquisition	3
Policy Statement.....	3
Applicability	3
Roles	4
Vendor Evaluation	6
Purchase Approval.....	7
Emergency Purchasing.....	8
Confidentiality	8
Conflict of Interest.....	8
Non-Compliance	8
Appendix.....	9
Security and Compliance Requirements.....	10
Electronic Forms	11
• Vendor Partner Contact Form	
• Vendor Partner Questionnaire	
Job Descriptions.....	12
• Manager Contracts and Pricing	
• Manager Outsourcing	
• Manager Vendor Management	
• Contract Management Administrator	
What's New	13



Vendor Partner Checklist

Electronic Form that is provided to vendors and partners as part of the Disaster Recovery and Business Continuity Planning process

DRP and Business Continuity Strategy	
1. In the event of a disaster or significant disruption, does your organization have documented plans for business continuity and IT disaster recovery?	<input type="radio"/> Yes <input type="radio"/> No
2. What type of failure scenarios or outages do you plan for?	
3. What duration of time is assumed for each type of failure scenario or outage you plan for?	
4. Does the plan establish critical business functions with recovery priorities?	<input type="radio"/> Yes <input type="radio"/> No
5. If you answered “Yes” to Question (4), what is the expected recovery time for your critical business functions?	<input type="radio"/> 0 to 4 hours <input type="radio"/> 4 to 8 hours <input type="radio"/> 8 to 24 hours <input type="radio"/> 1 to 2 days <input type="radio"/> More than 2 days
6. Does the plan account for interdependencies both internal and external to your organization?	<input type="radio"/> Yes <input type="radio"/> No
7. Does the plan cover some, most, or all locations from which you provide your services?	<input type="radio"/> Some <input type="radio"/> Most <input type="radio"/> All <input type="radio"/> NA
8. What percentage of “business as usual” servicing capability is the plan designed to address?	<input type="radio"/> 1%-10% <input type="radio"/> 11%-25% <input type="radio"/> 26%-50% <input type="radio"/> 51%-75% <input type="radio"/> 76%-99% <input type="radio"/> 100%
9. Do you have a dedicated team of professionals focused on business continuity and/or IT disaster recovery?	<input type="radio"/> Yes <input type="radio"/> No
10. If you answered “No” to Question (9), do you use an external BCP/DR service provider to handle your planning needs?	<input type="radio"/> Yes <input type="radio"/> No
11. Is your main IT facility or data center located in the same building or office complex occupied by your main business or operations staff?	<input type="radio"/> Yes <input type="radio"/> No
12. Please provide an illustration or schematic of how your organization’s primary, secondary, and/or tertiary servicing centers are set up to provide redundant services to ENTERPRISE.	<input type="radio"/> Yes <input type="radio"/> No



Text Messaging Sensitive and Confidential Information Policy



JANCO ASSOCIATES, INC.

2024



Table of Contents

Text Messaging of Sensitive and Confidential Information Policy	2
Overview	2
Policy	2
Text Messaging Best Practices	3
Policy Specific Requirements	4
Work From Home Considerations	5
Secure Text Message Requirements	6
Authentication methods	6
Password management	6
Administrator rights	7
Login monitoring and auditing	7
Automatic logoff	7
Access control	7
Account Management	8
Protection of data on the mobile device	8
Backup processes	8
Secure photo and screen capture sharing	9
Notifications & read receipts	9
Remote wipe for lost or stolen devices	9
Tracking & Monitoring	10
Text Message Marketing	10
Best Practices	11
Appendix	12
Electronic Forms	13
• Text Messaging Sensitive Information Agreement	
Job Descriptions	14
• Chief Compliance Officer	
• Chief Mobility Officer	
• Compliance Security Auditor Officer	
What's New	15



Travel, Laptop, PDA, and Off-Site Meeting Policy

2024



JANCO ASSOCIATES, INC.



Table of Contents

Travel, Laptop, PDA, and Off-Site Meetings	3
Laptop and PDA Security	3
BYOD Security	3
Service Provider Selection	4
Wi-Fi & VPN	4
Data and Application Security.....	5
Minimize Attention	5
Public Shared Resources – Wireless and Shared Computers.....	6
Off-Site Meeting Special Considerations	7
Pandemic Issues.....	8
International Travel Best Practices	8
Remote Computing Best Practices.....	9
Electronic Meetings	11
Best Practices for Electronic Meetings.....	12
Appendix.....	13
Job Description.....	14
Chief Experience Officer	
Chief Mobility Officer	
Manager Help Desk Support	
Manager Telecommuting	
Manager WFH Support	
Electronic Forms.....	15
Mobile Device Access and Use Agreement	
Mobile Device Security and Compliance Checklist	
Privacy Policy Compliance Agreement	
Telecommuting IT Checklist	
Telecommuting Work Agreement	
Work From Home IT Checklist	
Work From Home Work Agreement	
Revision History	16



Wearable Device Policy



2024



Table of Contents

- Wearable Device Policy.....3
- Overview.....3
- Policy.....3
- Creating a Wear Your Own Device Strategy (WYOD)7
- Enterprise Mobile Device Infrastructure8
 - Wearable Device Infrastructure.....8
 - Disaster Recovery8
 - Backups.....9
 - Wearable Device Physical Device9
 - Internal Network Access9
 - Repair Procedure10
 - Upgrade Procedure.....10
 - Patching Policy.....10
 - Ownership of device10
 - Ownership of data10
- Wearable Devices Security Best Practices12
 - Security Controls.....12
 - Remote Wearable Devices Management12
 - Access Management Controls.....13
 - Wearable Device Applications13
- Legal Considerations.....14
 - Privacy.....14
 - Record Retention15
- WYOD Management Security Options.....17
- Appendix.....18
 - Top 10 WYOD Best Practices19
 - Electronic Forms.....20
 - Mobile Device Access and Use Agreement
 - Mobile Device Security and Compliance Checklist
 - Wearable Device Access and Use Agreement
 - What’s New21



Work From Home & Telecommuting Policy

2024



Table of Contents

Work From Home (WFH) & Telecommuting Policy	2
Overview	2
Telecommuting resource misuse can have serious implications for an enterprise.....	3
Policy	4
Compensation and Benefits	5
Hours of Work	5
Attendance at Meetings	6
Sick Leave and Time Off.....	6
Workers’ Compensation and Safety Program Liability	6
Equipment and Supplies	6
Record Management Process and BCP.....	7
BYOD Security	7
Telecommuting costs.....	8
Work From Home	10
Appendix.....	13
Employer Legal Workplace Responsibilities	14
Position Requirements for Qualification for WFH & Telecommuting	15
Top 10 Best Practices.....	16
Job Description	17
Manager Telecommuting	
Manager Work From Home Support	
Electronic Forms	18
Company Asset Control Log	
Inspection Checklist Alternative Location	
Internet and Electronic Communication Agreement	
Mobile Device Access and Use Agreement	
Mobile Device Security and Compliance Checklist	
Privacy Policy Compliance Agreement	
Remote Location Contact Information	
Safety Checklist - Work at Alternative Location	
Security Access Application Mobile	
Sensitive Information Policy Compliance Agreement	
Social Networking Policy Compliance Agreement	
Telecommuting IT Checklist	
Telecommuting Work Agreement	
Text Messaging Sensitive Information Agreement	
Work From Home Contact Administration	
Work From Home IT Checklist	
Work From Home Work Agreement	
What’s New	19



This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

<https://e-janco.com>

Job Descriptions



Table of Contents

Thirty eight (38) job descriptions included in this document

Chief AI Officer
Chief Compliance Officer
Chief Experience Officer
Chief Information Security Officer
Chief Security Officer
Vice President Strategy and Architecture
Data Protection Officer
Director IT Management and Controls
Director Media Communications
Manager BYOD Support
Manager Change Control
Manager Cloud Applications
Manager Compliance
Manager Contracts and Pricing
Manager Metrics
Manager Outsourcing
Manager Record Administration
Manager Security and Workstations
Manager Social Networking
Manager Telecommunications
Manager Telecommuting
Manager User Support
Manager Vendor Management
Manager WFH Support
BYOD Support Specialist
BYOD Support Supervisor
Change control Analyst
Change Control Supervisor
Cloud Computing Architect
Compliance Security Auditor
Content Management Administrator
Metrics Measurement Analyst
Records Management Coordinator
Security Architect
Social Media Specialist
Word Processing Lead Operator
Word Processing Operator
Word Processing Supervisor

**This is a sample of the final product
and these pages are for your review
and are protected by Janco's copyright.**

<https://e-janco.com>

Chief AI Officer (CAIO)

Position Purpose

The Chief AI Officer (CAIO) is a C-suite executive responsible for overseeing a company's overall strategy, acquisition, implementation, and monitoring of AI and Machine Learning (ML) technology. This role requires a deep understanding of the business, technical expertise, and regulatory awareness. The CAIO must be capable of communicating AI-related information effectively across the organization. However, the role is not solely technical; it demands diverse skills, including AI ethics, understanding, and implementation awareness.

This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.

<https://e-janco.com>

are now using data to determine new as well as how to be more efficient, more to break down barriers that remain operational manager. As the role is of AI and machine learning across the the responsibilities are set by the organization's board of directors or other authority, depending on the organization's legal structure. The CAIO is responsible for AI across the entire enterprise and its operations.

Problems and Challenges

The major challenge for this individual is defining the AI solutions and data architecture of the enterprise while balancing data assets and computing services with financial and marketing needs. This is accomplished with the use of AI technology that supports both enterprise growth and productivity. Seamless integration of AI from the customer, through product and service design, financial statements, and management reporting is a primary concern.

For the CAIO, the application of AI is the focal point. As such, it is extremely important to the enterprise's current and future business operations. The Chief AI Officer (CAIO) ensures the continued success of these areas while simultaneously minimizing costs and maximizing equipment and employee performance.

CAIO is a C-suite executive responsible for overseeing a company's overall strategy, acquisition, implementation, and monitoring of AI technology. This role requires a deep understanding of the business, technical expertise, and regulatory awareness. The CAIO must be capable of communicating AI-related information effectively across the organization. However, the role is not solely technical; it demands diverse skills, including AI ethics, understanding, and implementation awareness.

Challenges include:

- ▶ Earning company-wide commitment - Getting everyone on board with the AI and machine learning vision is a major endeavor task with internal politics and an ever-changing digital landscape.
- ▶ Developing an AI strategy mission statement – CAIO is responsible for end-to-end strategy, design, and implementation of the company's AI roadmap.
- ▶ Creating the bridge between AI and ML solutions and business operations - the CAIO focus is the relationship between AI/ML and productivity.
- ▶ Maintaining links with experts.