



# Pandemic Infrastructure Bundle

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

<https://www.e-janco.com>



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

<https://www.e-janco.com>

# **Disaster Recovery Business Continuity Template**



**2020 Edition**



## Table of Contents

<b>1.0 PLAN INTRODUCTION .....</b>	<b>5</b>
1.1 RECOVERY LIFE CYCLE - AFTER A "MAJOR EVENT" .....	5
1.2 MISSION AND OBJECTIVES .....	7
1.3 DISASTER RECOVERY / BUSINESS CONTINUITY SCOPE.....	18
1.4 AUTHORIZATION.....	18
1.5 RESPONSIBILITY .....	18
1.6 KEY PLAN ASSUMPTIONS.....	19
1.7 DISASTER DEFINITION .....	20
1.8 METRICS.....	20
1.9 DISASTER RECOVERY / BUSINESS CONTINUITY AND SECURITY BASICS .....	22
<b>2.0 BUSINESS IMPACT ANALYSIS .....</b>	<b>27</b>
2.1 SCOPE .....	27
2.2 OBJECTIVES .....	28
2.3 ANALYZE THREATS .....	28
2.4 CRITICAL TIME FRAME .....	30
2.5 APPLICATION SYSTEM IMPACT STATEMENTS .....	30
2.6 INFORMATION REPORTING .....	32
2.7 BEST DATA PRACTICES .....	33
2.8 SUMMARY .....	34
<b>3.0 BACKUP STRATEGY .....</b>	<b>35</b>
3.01 SITE STRATEGY .....	35
3.02 BACKUP BEST PRACTICES .....	35
3.03 DATA CAPTURE AND BACKUPS .....	41
3.04 COMMUNICATION STRATEGY .....	43
3.05 ENTERPRISE DATA CENTER SYSTEMS - STRATEGY .....	47
3.06 DEPARTMENTAL FILE SERVERS - STRATEGY .....	48
3.07 WIRELESS NETWORK FILE SERVERS - STRATEGY .....	49
3.08 DATA AT OUTSOURCED SITES (INCLUDING ISP'S) - STRATEGY .....	50
3.09 BRANCH OFFICES (REMOTE OFFICES & RETAIL LOCATIONS) - STRATEGY .....	51
3.10 DESKTOP WORKSTATIONS (IN OFFICE) - STRATEGY .....	53
3.11 DESKTOP WORKSTATIONS (OFF-SITE INCLUDING AT-HOME USERS) - STRATEGY.....	54
3.12 LAPTOPS - STRATEGY.....	55
3.13 PDA'S AND SMARTPHONES - STRATEGY.....	57
3.14 BYODS - STRATEGY .....	59
3.15 IOT DEVICES - STRATEGY.....	61
<b>4.0 RECOVERY STRATEGY .....</b>	<b>63</b>
4.1 APPROACH .....	63
4.2 ESCALATION PLANS.....	64
4.3 DECISION POINTS .....	65



**5.0 DISASTER RECOVERY ORGANIZATION.....68**

5.1 RECOVERY TEAM ORGANIZATION CHART.....69

5.2 DISASTER RECOVERY TEAM.....71

5.3 RECOVERY TEAM RESPONSIBILITIES .....72

**6.0 DISASTER RECOVERY EMERGENCY PROCEDURES.....83**

6.1 GENERAL .....84

6.2 RECOVERY MANAGEMENT.....85

6.3 DAMAGE ASSESSMENT AND SALVAGE .....87

6.4 PHYSICAL SECURITY .....90

6.5 ADMINISTRATION .....92

6.6 HARDWARE INSTALLATION .....93

6.7 SYSTEMS, APPLICATIONS & NETWORK SOFTWARE .....95

6.8 COMMUNICATIONS .....97

6.9 OPERATIONS.....98

**7.0 PLAN ADMINISTRATION .....99**

7.1 DISASTER RECOVERY MANAGER .....99

7.2 DISTRIBUTION OF THE DISASTER RECOVERY PLAN.....100

7.3 MAINTENANCE OF THE BUSINESS IMPACT ANALYSIS .....101

7.4 TRAINING OF THE DISASTER RECOVERY TEAM.....101

7.5 TESTING OF THE DISASTER RECOVERY PLAN .....101

7.6 EVALUATION OF THE DISASTER RECOVERY PLAN TESTS.....104

7.7 MAINTENANCE OF THE DISASTER RECOVERY PLAN .....105

**8.0 APPENDIX A – LISTING OF ATTACHED MATERIALS .....107**

8.01 DISASTER RECOVERY BUSINESS CONTINUITY – ELECTRONIC FORMS.....107

- Site Evaluation Checklist
- LAN Node Inventory
- Location Contact Numbers
- Off-Site Inventory
- Pandemic Planning Checklist
- Personnel Location
- Plan Distribution
- Remote Location Contact Information
- Server Registration
- Team Call List
- Vendor Contact List
- Vendor / Partner Questionnaire





- 8.02 SAFETY PROGRAM FORMS – ELECTRONIC FORMS .....108
  - 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
  - New Employee Safety Checklist
  - Safety Program Contact List
  - Training Record
- 8.03 BUSINESS IMPACT ANALYSIS – ELECTRONIC FORMS .....108
  - Application and File Server Inventory
  - Business Impact Questionnaire
- 8.04 JOB DESCRIPTIONS .....109
  - Disaster Recovery Manager
  - Manager Disaster Recovery and Business Continuity
  - Pandemic Coordinator
- 8.05 ATTACHED INFRASTRUCTURE POLICIES .....109
  - Backup and Backup Retention Policy
  - Incident Communication Plan Policy
  - Physical and Virtual Server Security Policy
  - Social Networking Policy
- 8.06 OTHER ATTACHMENTS .....109
  - Disaster Recovery Business Continuity Audit Program
- 9.0 APPENDIX B – REFERENCE MATERIALS.....110**
  - 9.01 PREVENTATIVE MEASURES .....110
  - 9.02 SAMPLE APPLICATION SYSTEMS IMPACT STATEMENT .....111
  - 9.03 KEY CUSTOMER NOTIFICATION LIST.....112
  - 9.04 RESOURCES REQUIRED FOR BUSINESS CONTINUITY.....114
  - 9.05 CRITICAL RESOURCES TO BE RETRIEVED.....115
  - 9.06 BUSINESS CONTINUITY OFF-SITE MATERIALS .....117
  - 9.07 WORK PLAN .....119
  - 9.08 AUDIT DISASTER RECOVERY PLAN PROCESS .....122
  - 9.09 DEPARTMENTAL DRP AND BCP ACTIVATION WORKBOOK.....125
  - 9.10 WEB SITE DISASTER RECOVERY PLANNING FORM .....138
  - 9.11 GENERAL DISTRIBUTION INFORMATION.....142
  - 9.12 DISASTER RECOVERY SAMPLE CONTRACT .....144
  - 9.13 RANSOMWARE – HIPAA GUIDANCE .....153
  - 9.14 POWER REQUIREMENT PLANNING CHECK LIST .....155
  - 9.14 COLOCATION CHECKLIST .....156
- 10.0 CHANGE HISTORY .....157**
- 11.0 LICENSE CONDITIONS.....161**

---

## 1.0 Plan Introduction

ENTERPRISE recognizing their operational dependence on computer systems, including the Local Area Network (LAN), Database Servers, Internet, Intranet and e-mail, and the potential loss of revenue and operational control that may occur in the event of a disaster; authorized the preparation, implementation, and maintenance of a comprehensive disaster recovery plan.

The intent of a Disaster Recovery Plan is to provide a written and tested plan directing the computer system recovery process in the event of an interruption in continuous service resulting from an unplanned and unexpected disaster.

The Disaster Recovery Plan preparation process includes several major steps as follows:

- ▶ Identify Systems and Applications currently in use
- ▶ Analyze Business Impact of computer impact and determination of critical recovery time frames
- ▶ Determine Recovery Strategy
- ▶ Document Recovery Team Organization

These steps represent

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

of the Disaster Recovery Plan.

---

## 1.1 Recovery

<https://www.e-janco.com>

We have identified five stages in the recovery life cycle after a major event that requires relocation to a new facility:

1. Survival
2. Support
3. Adjustment
4. Reconciliation
5. Recovery

The first priority will be survival, which involves physiological factors such as physical survival of staff and their families including food and shelter. Next, the focus will be on support from a safety and security perspective. In the following weeks, there will be a period of adjustment, where things should be beginning to settle down, as the organization returns to some form of normality and a sense of belonging returns.

After this will be a period of reconciliation, where the organization and staff begin to accept that things have changed, for example, that there are new offices. The final stage is the recovery phase, during which the enterprise will acknowledge that things will never be exactly the way they were before.

There will be post-event tension. Commonly, it is only when a workplace is back "online" & fully functioning from a technical perspective that the repercussion on personnel is fully recognized. In the

---

## 1.2 Mission and Objectives

The mission of the Disaster Recovery Plan is to establish defined responsibilities, actions, and procedures to recover the ENTERPRISE computer, communication, and network environment in the event of an unexpected and unscheduled interruption. The plan is structured to attain the following objectives:

- ▶ Recover the physical network within the Critical Time Frames<sup>1</sup> established and accepted by the user community
- ▶ Recover the applications within the Critical Time Frames established and accepted by the user community
- ▶ Minimize the impact on the business with respect to dollar losses and operational interference

---

## Compliance

Various compliance frameworks can be used to assess BCP measures—ISO, COBIT, COSO, etc.—but key aspects are similar:

- ▶ COSO requires data center operation controls and transaction management controls in order to ensure data integrity and availability.
- ▶ ISO 1799 has a section entitled Business Continuity Management that requires testing, maintaining, and reassessing a business continuity plan.

As a general rule, knowledgeable individuals other than the BCP team should be involved in the development and process meetings.

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

<https://www.e-janco.com>

Manage

of qualified,  
of the board  
at the BCP plan

- **Implication of Legislated and Industry Standards Requirements**

There<sup>2</sup> are a number of legally mandated and standards mandated issues that need to be covered in the Disaster Recovery / Business Continuity Planning Process.

In addition to the Security & Exchange Commission (SEC) requirements of Sarbanes-Oxley, there are PCI DSS requirements issued by credit card companies, security requirements of HIPAA, and individual state requirements (California and New York) that needed to be considered in the plan.

---

<sup>1</sup> Critical time frames include both the point in time that the recovery will be set to and the point in time that the recovery will be completed and the enterprise can be back in operation.

<sup>2</sup> This section is for informational purposes and can be excluded from the plan.



- **Audit and Examine the Control Processes**

Lastly, the enterprise needs to analyze the effectiveness of controls, optimize them when required, and demonstrate due diligence to both internal and external constituencies.

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

<https://www.e-janco.com>

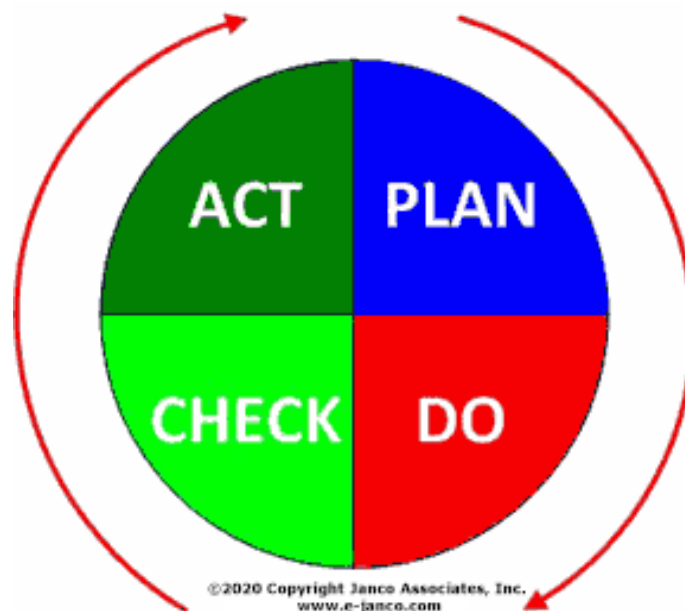
- ▶ Map control information to specific policies in order to provide recommendations for improvements to the control environment; and
- ▶ Collect, integrate, and retain trend analyses and evidentiary information from disparate control mechanisms for audits and documentation requests.

---

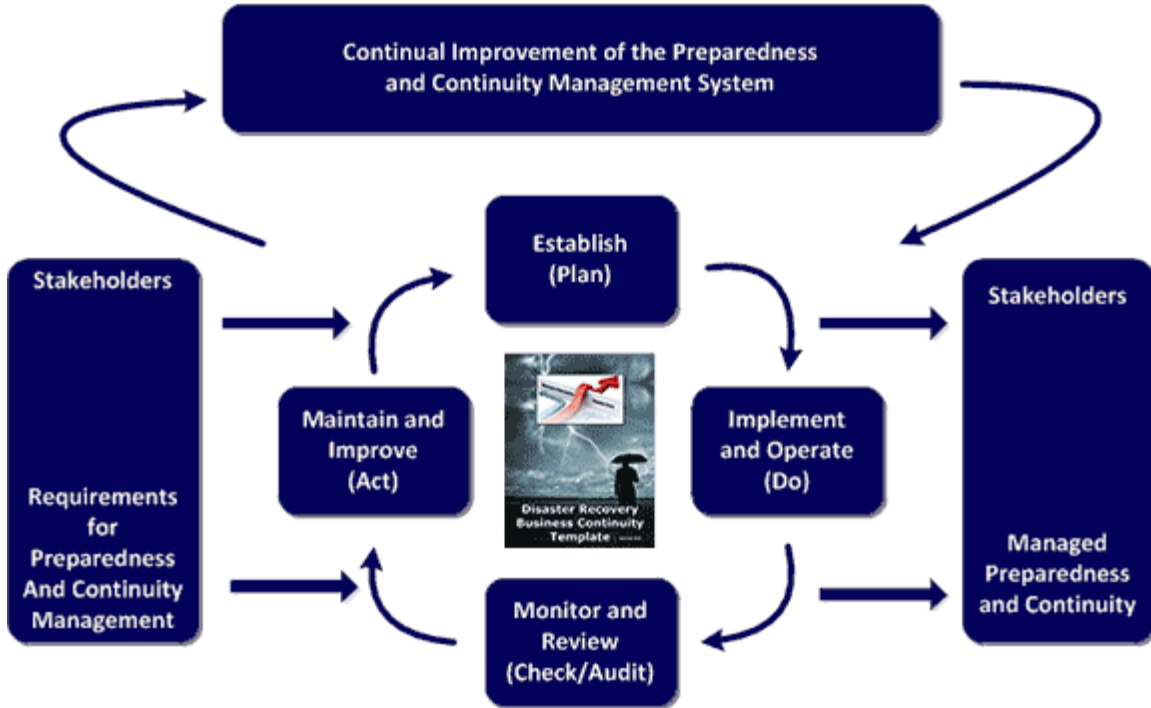
## ISO 27031 Overview

The ISO Standard defines the Information and Communication Technology (ITC) Requirements for Business Continuity (IRBC) program that supports the mandate for an infrastructure that supports business operations when an event or incident with its related disruptions affect the continuity of critical business functions. This includes the security of crucial data as well as enterprise operations.

The ISO standard centers around four areas; Plan, Do, Check, and Act.



## Janco Disaster Recovery Business Continuity Template Compliance with ISO 22301 Business Continuity Standard



### ISO 28000

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

<https://www.e-janco.com>

in implementing and (IS)  
very, aging infrastructure  
Security has become a  
tion to Business Continuity

*"This International Standard (ISO 28000) specifies the requirements for a security management system, including those aspects critical to the security assurance of the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that impact on supply chain security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting goods along the supply chain".*

The business environment is constantly changing – along with threats to a company's survival. Organizations need to be ahead of the game, and an excellent defense can be built around audit of the controls used to support the information security. ISO 28000:2007 is applicable to all sizes of organizations, from small to multinational, in manufacturing, service, storage or transportation at any stage of the production or supply chain that wishes to:

---

## 1.3 Disaster Recovery / Business Continuity Scope

The scope of the plan is to recover computer information services provided by the ENTERPRISE data center and networks located at \_\_\_\_\_

\_\_\_\_\_. The LAN network encompasses the following:

- ▶ General business applications, such as word-processing, spreadsheet and database applications
- ▶ e-Mail
- ▶ File servers supporting all business operations
- ▶ Gateway to the supplier applications and other sites

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

<https://www.e-janco.com>

er grids, telephone switching  
ess transmission sites within a

---

## 1.4 Authorization

The management of ENTERPRISE recognizes the need for a Disaster Recovery Plan for all operations directly or indirectly dependent on data processing. The Chief Information Officer for ENTERPRISE has authorized the development and ongoing maintenance of this plan.

The Disaster Recovery Plan and Process have been reviewed by the executive management of ENTERPRISE and necessary changes in the "BY-LAWS" and or "CHARTER" of ENTERPRISE has been approved by the Board of Directors, Stockholders or other legal entities as required.

---

## 1.5 Responsibility

Responsibility for the development and maintenance of the plan is assumed by the Information Technology group. Specific responsibility for ensuring the plan is maintained and tested rests with the ENTERPRISE DRP Support Group. In consideration of this responsibility, the end-user community is responsible to coordinate with the Project Manager for their information technology requirements.



# Disaster Recovery Business Continuity

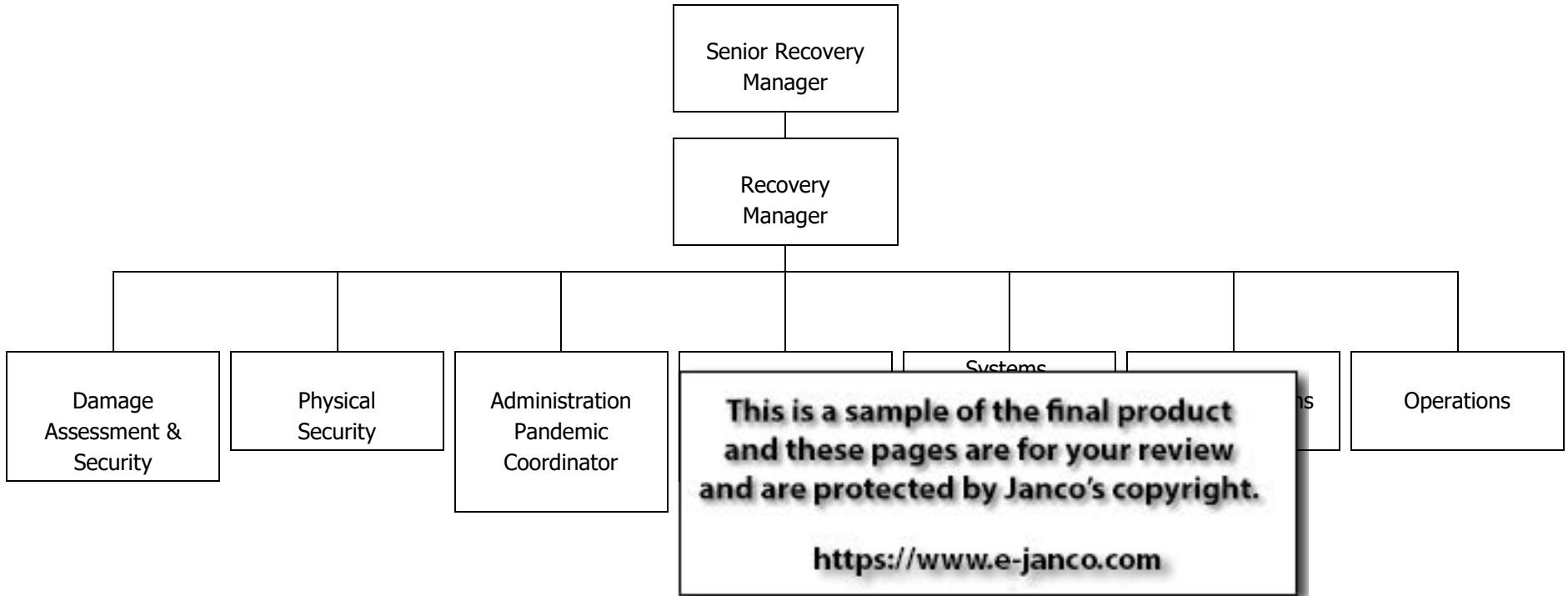
Recovery Strategy	Recovery Time	Advantages	Disadvantages	Comments
<b>Commercial Hot site</b>	24 to 48 Hours	<ul style="list-style-type: none"> <li>Best recovery time</li> <li>Easiest to implement as equipment, application software, data, and OS are in place</li> <li>Easy to test at any point in time</li> <li>The best solution that is available to support on-going operations</li> </ul>	<ul style="list-style-type: none"> <li>Most expensive options duplicate equipment and software plus on-going version control issues</li> <li>Ongoing communication costs to duplicate data very high</li> <li>Term of the agreement can limit the duration of use</li> <li>If you are not the "most important customer" you could be bumped</li> </ul>	Often the most cost-effective strategy for data center recovery strategies. Clear contract terms need to be defined which meets the enterprise service objectives. Consideration should be made for disasters that impact entire regions such as hurricanes and earthquakes.
<b>Internal Hot site</b>	1 to 12 hours	<ul style="list-style-type: none"> <li>Best recovery time</li> <li>Easiest to implement as equipment, application software, data, and OS are in place</li> <li>Easy to test at any point in time</li> <li>The best solution that is available to support on-going operations</li> </ul>	<ul style="list-style-type: none"> <li>Most expensive options duplicate equipment and software plus on-going version control issues</li> <li>Ongoing communication costs to duplicate data very high</li> </ul>	If costs can be shared among multiple facilities within the enterprise, internal provisioning can cost competitive with commercial alternatives. If no appropriate secondary space is available "co-location" facilities providers offer managed raised-floor space at very attractive rates as an alternative to building out secondary sites.
<b>Warm Site</b>	24 to 48 Hours	<ul style="list-style-type: none"> <li>Moderately priced</li> <li>Typically, can be in place for 36 to 72 hours</li> <li>Can be placed in the "parking lot" adjacent to you impacted facility</li> </ul>	<ul style="list-style-type: none"> <li>Recovery time typically is at least 2 to 5 days longer than a hot site.</li> <li>Access to your impacted facility may be hindered because of the event</li> <li>A trailer may not be configured exactly as you need it</li> </ul>	Costs can be shared among multiple facilities within the enterprise, internal provisioning can cost competitive with commercial alternatives. If no appropriate secondary space is available "co-location" facilities providers offer managed raised-floor space at very attractive rates as an alternative to building out secondary sites.
<b>Mobile Site</b>	24 to 48 Hours	<ul style="list-style-type: none"> <li>Moderately priced</li> <li>Typically, can be in place for 36 to 72 hours</li> <li>Can be placed in the "parking lot" adjacent to you impacted facility</li> </ul>	<ul style="list-style-type: none"> <li>Recovery time typically is at least 2 to 5 days longer than a hot site.</li> <li>Access to your impacted facility may be hindered because of the event</li> <li>A trailer may not be configured exactly as you need it</li> </ul>	This approach avoids employee travel issues but has limitations on equipment availability and outbound bandwidth if very small aperture satellite terminal (VSAT) links must be used for communications. If the disaster profile includes events such as hurricanes, floods or toxic spills, these solutions may not be appropriate.
<b>Cold Site</b>	72 plus Hours	<ul style="list-style-type: none"> <li>Lowest cost solution</li> <li>Basic infrastructure power, air, and communication are in place</li> <li>Can rent the facility for a longer-term at lower cost</li> </ul>	<ul style="list-style-type: none"> <li>Longest recovery time</li> <li>All equipment must be ordered, delivered, installed and made operational</li> <li>Worst solution for supporting on-going operations</li> </ul>	"Environmentally appropriate" space can be either provisioned internally or contracted from a commercial facilities service provider. Cold-site strategies are usually based on "quick-ship" delivery agreements to allow server, storage, and communications hardware and network service providers to quickly build out the data center and/or client workspace infrastructure.
<b>Reciprocal Agreement</b>	12 to 48 Hours	<ul style="list-style-type: none"> <li>Least costly solution</li> <li>Better than no strategy</li> </ul>	<ul style="list-style-type: none"> <li>Seldom works</li> <li>Typically, in the same geographic area and a wide range disaster like an earthquake renders it of no use</li> <li>No easy way to test</li> </ul>	This is typically a formal agreement between two trusted, non-competing partners in different industries in which each provides secure sites for the other. This option is the least favorable and has the greatest risk associated with it.
<b>Cloud</b>	0 to 24 Hours	<ul style="list-style-type: none"> <li>Data and applications available immediately</li> <li>Location independent</li> <li>Easy to test</li> </ul>	<ul style="list-style-type: none"> <li>Security</li> <li>May not allow enough time for a daily cycle processing window</li> </ul>	Data should be in place so activation would only be limited by connectivity and network addressing (DNS propagation).

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

<https://www.e-janco.com>



## 5.1 Recovery Team Organization Chart



---

## 7.0 Plan Administration

This Disaster Recovery Plan is a living document. Administration procedures are for the purpose of maintaining the Disaster Recovery Plan in a consistent state of readiness. The procedures specify direct Information Technology administrative responsibilities and coordination responsibilities with users of the data center.

These procedures apply to the continued maintenance, testing, and training requirements of the Disaster Recovery Plan.

They apply to Information Technology management and user management as a whole to promote awareness of the Disaster Recovery Plan and the need for disaster recovery preparedness. The procedures also apply to specific functional areas of Information Technology that have direct responsibility for maintaining the plan current and accurate.

The Manager is responsible for the continued maintenance of the Disaster Recovery Plan. The Manager is responsible for the continued maintenance of the Disaster Recovery Plan.

### 7.1 Disaster Recovery Plan Administration

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

<https://www.e-janco.com>

but it is a member of the Recovery Management Team in the event of a computer disaster.

The areas in which the Manager assumes a leadership position and conducts reviews of effectiveness in the plan administration are as follows:

- ▶ Distribution of the Disaster Recovery Plan
- ▶ Maintenance of the Business Impact Analysis
- ▶ Training of the Disaster Recovery Team
- ▶ Testing of the Disaster Recovery Plan
- ▶ Evaluation of the Disaster Recovery Plan Tests
- ▶ Review, change, and update of the Disaster Recovery Plan



---

## 8.0 Appendix A – Listing of Attached Materials

---

### 8.01 Disaster Recovery Business Continuity – Electronic Forms

These forms come in a separate directory “forms/Disaster Recovery” and as a separate pdf file that contains all the electronic forms In MS Word and PDF formats

The forms included are:

- **Site Evaluation Checklist**
- **LAN Node Inventory**
- **Location Contact Numbers**
- **Off-Site Inventory**
- **Pandemic Planning Checklist**
- **Personnel Location**
- **Plan Distribution**
- **Remote Location Contact Information**
- **Server Registration**
- **Team Call List**
- **Vendor Contact List**
- **Vendor / Partner Questionnaire**

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

**<https://www.e-janco.com>**



---

## 8.02 Safety Program Forms – Electronic Forms

During the recovery period of the disaster safety of all individuals and organizations involved are a primary concern. Attached are all electronic forms from a Safety Program created by Janco to facilitate this. See <https://www.e-janco.com/safetyprogram.htm>.

These forms come in a separate directory “Safety Program Forms”. Forms contained include:

- **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**
- **New Employee Safety Checklist**
- **Safety Program Contact List**
- **Training Record**

---

## 8.03 Business Impact Analysis – Electronic Forms

- **Application and File Server Inventory**
- **Business Impact Questionnaire**

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

**<https://www.e-janco.com>**



---

## 8.04 Job Descriptions

The job descriptions provided complies with the Americans' with Disabilities Act and meet all compliance requirements. They are provided as separate documents in the directory name "Job Descriptions

- **Disaster Recovery Manager**
- **Manager Disaster Recovery and Business Continuity**
- **Pandemic Coordinator**

---

## 8.05 Attached Infrastructure Policies

- **Backup and Backup Retention Policy**
- **Incident Communication Plan Policy**
- **Physical and Virtual Server Security Policy**
- **Social Networking Policy**

---

## 8.06 Other Attachments

- **Disaster Recovery Business Continuity Audit Program**

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

**<https://www.e-janco.com>**



---

## 10.0 Change History

---

### 2020 Edition

- ✚ Restructured the entire plan to be modular with standard electronic forms, infrastructure policies, and job descriptions.
- ✚ Include the Pandemic Planning Checklist as an electronic form
- ✚ Updated all included electronic form
- ✚ Updated all included job descriptions
- ✚ Restructured the template to include all of the electronic forms in a single separate document and files in a separate directory.

---

### 2019 Edition

- ✚ Updated all included job descriptions
- ✚ Updated all included forms
  - Disaster Recovery electronic forms
  - Safety Program electronic forms
- ✚ Added co-location checklist
- ✚ Audit Program Updated
- ✚ Administrative changes
  - Changed core document to exclude job descriptions and forms which are delivered in their own directories
  - Business and IT Impact Questionnaire is delivered in its own and comes as an MS WORD, pdf, and eBook electronic format
  - 3 included job descriptions are delivered in their own directory

---

### Version 8.7

- ✚ Add Disaster Recovery Business Continuity Site Evaluation Checklist Form

---

### Version 8.6

- ✚ Updated to meet EU compliance requirements
- ✚ Updated all the attached electronic forms
- ✚ Updated all the included job descriptions
- ✚ Updated to include references to Mobile Device Data
- ✚ Added Power Requirement 10-point planning checklist



## Version 8.5

- ✚ Update to reflect lessons learned from Hurricane season of 2017
- ✚ Updated references to the cloud and remote backup sites
- ✚ Corrected minor errata

## Version 8.4

- ✚ Updated DR/BC Audit Program to meet the latest mandated requirements
  - Updated to reflect EU and US state requirements for California and Texas
  - IoT audit requirements include an audit program
  - Social media and e-commerce added to audit program
- ✚ Added recovery life cycle after a "Major Event"
- ✚ Added introduction section on Best Practices for Backup
- ✚ Added section of IoT back up
- ✚ Update the electronic MS WORD based forms:
  - Disaster Recovery Business Continuity Bundle (9 forms)
  - Safety Bundle (9 forms)

## Version 8.3

- ▶ Added Ransomware Guidance for HIPAA
- ▶ Updated to meet the latest EU / UK / and the USA mandated compliance requirements

## Version 8.2

- ▶ Updated to meet the latest compliance requirements
- ▶ Updated work plan and deliverables
- ▶ Updated all electronic forms
- ▶ Updated checklists to meet best practices standards

## Version 8.1

- ▶ Updated to meet all of the latest in force and proposed mandated compliance requirements
- ▶ Includes all 9 of the updated Disaster Recovery Plan Electronic Forms
- ▶ Includes all 8 of the updated Safety Program Electronic Forms





## Version 8.0

- ▶ Updated to be compliant with the latest ISO standards
  - Added section on ISO 28000
- ▶ Updated to the latest Business and IT Impact forms (Now included as a separate document for ease of use)
- ▶ Updated to include specific references to mobile users and BYOD devices
- ▶ BYOD back up recovery strategy before and during a disaster defined
- ▶ Updated with the latest electronic forms
- ▶ Updated with the latest Business Impact and Risk Assessment

## Version 7.5

- ▶ Added Physical and Virtual Server Security Policy
- ▶ Added Electronic Form
  - Server Registration

## Version 7.4

- ▶ Updated Recovery Site Strategy for Cloud
- ▶ Updated the CSS Style Sheet for black and white printing
- ▶ Corrected minor errata

## Version 7.3

- ▶ Updated the included files to include Version 1.3 of the Disaster Recovery Business Continuity Audit Program

## Version 7.2

- ▶ Updated responsibilities for team members
- ▶ Added Safety Program references in the core template
- ▶ Added Electronic Safety Program Forms
  - Area Safety Inspection
  - Employee Job Hazard Analysis
  - First Report of Injury
  - Inspection Checklist – Alternative Locations
  - Inspection Checklist – Office Locations
  - New Employee Safety Checklist
  - Safety Program Contact List
  - Training Record

## Version 7.1

- ▶ Updated graphics
- ▶ Updated Business Analysis Impact Section



## Version 7.0

- ▶ Updated for compliance with ISO 22301
- ▶ Added Electronic Forms for Disaster Recovery and Business Continuity Plan Management
  - Plan Distribution Control Log
  - Remote Location Contact Information
  - Team Call List
  - Vendor Contact List
  - Off-Site Inventory
  - LAN Hardware / Software Inventory
  - Personnel Locations

## Version 6.2

- ▶ Added ISO 27031 specific materials
  - Overview
  - Principles – Scope and Objectives
  - Requirements

## Version 6.1

- ▶ Added materials specific to social network communication
- ▶ Added Social network checklist

## Version 6.0

- ▶ Updated Disaster Recovery Audit Program for mandated requirements
- ▶ Updated Business & IT Impact Questionnaire for mandated requirements
- ▶ The updated backup strategy section
- ▶ Added Incident Communication Plan



# Disaster Recovery Business Continuity Electronic

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

<https://www.e-janco.com>



2020

# Disaster Recovery Electronic Forms

---

Forms contained include:

- Disaster Recovery – Business Continuity Site Evaluation Checklist
- Disaster Recovery – Business Continuity LAN Node Inventory
- Disaster Recovery – Business Continuity Location Contact Numbers
- Disaster Recovery – Business Continuity Off-Site Inventory
- Disaster Recovery – Business Continuity Personnel Location
- Disaster Recovery – Business Continuity Plan Distribution
- Disaster Recovery – Business Continuity Remote Location Contact Information
- Disaster Recovery – Business Continuity Server Registration
- Disaster Recovery – Business Continuity Team Call List
- Disaster Recovery – Business Continuity Vendor List
- Pandemic Planning Checklist
- Vendor / Partner Questionnaire

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

**<https://www.e-janco.com>**



# Disaster Recovery Business Continuity Site Evaluation

This form is used to evaluate potential DR/BC sites and in the auditing process of sites that are approved DR/BC locations as defined in the DR/BC Plan

Site Name: \_\_\_\_\_ Location: \_\_\_\_\_

Contact: \_\_\_\_\_ Phone/email: \_\_\_\_\_

Phone at Location: \_\_\_\_\_ Date: \_\_\_\_\_

Describe the Site:

**Power** – Is the power available adequate to meet current and future needs  YES  NO

**Location** - Is the location of the facility beneficial to the enterprise? Are there multiple geographically diverse sites to support future business expansion or disaster recovery site options?  YES  NO

**Resiliency** - What precautions are in place to protect the facility from natural disasters and other threats?  YES  NO

**Security & Protection** - Are security measures in place to protect the facility?  YES  NO

**Carrier Diversity** - Does the facility provide a variety of carriers and do they allow interconnection with other facilities?  YES  NO

**Scalability** - Can the facility support higher density of equipment?  YES  NO

**Service Level Agreement (SLA)** - What level of service is provided?  YES  NO

**Compliance** - Is the facility audited by a third party? Has the audit been reviewed?  YES  NO

**Cost** - Does this facility offer the right combination of price and performance for your future infrastructure needs?  YES  NO

**Support** - Is technical support available 24/7? What is the process for addressing support issues?  YES  NO

**Amenities** - Does the facility offer workspace and conference rooms to enable productivity for employees?  YES  NO

**Environment** - Does the facility adhere to energy-efficient industry standards (LEED, ENERGY STAR, Green Globes)?  YES  NO

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

<https://www.e-janco.com>

Summary Comments \_\_\_\_\_

Signature \_\_\_\_\_ Date \_\_\_\_\_





# PANDEMIC PLANNING CHECKLIST

Electronic form that is filled out as part of the Disaster Recovery and Business Continuity Planning process.



JANCO ASSOCIATES, INC.

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

**<https://www.e-janco.com>**



# Pandemic Planning Checklist

## Impact of a pandemic on enterprise

### Tasks

Identify a pandemic coordinator and/or team with defined roles and responsibilities for preparedness and response planning. The planning process should include input from labor representatives.  Not Started  In Progress  Completed

Identify essential employees and other critical inputs (e.g. raw materials, suppliers, subcontractor services/ products, and logistics) required to maintain business operations by location and function during a pandemic.  Not Started  In Progress  Completed

Train and prepare ancillary workforce (e.g. contractors, employees in other job titles/descriptions, retirees).  Not Started  In Progress  Completed

Develop and plan for scenarios likely to result in an increase or decrease in demand for your products and/or services during a pandemic (e.g. effect of a restriction on mass gatherings, need for hygiene supplies).  Not Started  In Progress  Completed

Determine the potential impact of a pandemic on financials using multiple possible scenarios across product lines and/or production sites.

**This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.**  
<https://www.e-janco.com>

Determine the potential impact of a pandemic on domestic and international travel (e.g. quarantine requirements).

Find up-to-date, reliable pandemic information from community public health, emergency management, and other sources and make sustainable links.  Not Started  In Progress  Completed

Establish an emergency communications plan and revise periodically. This plan includes identification of key contacts (with back-ups), a chain of communications (including suppliers and customers), and processes for tracking and communicating business and employee status.  Not Started  In Progress  Completed

Implement an exercise/drill to test your plan and revise periodically.  Not Started  In Progress  Completed



# Vendor / Partner Questionnaire

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



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

**<https://www.e-janco.com>**

## 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?  Yes  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?  Yes  No

5. If you answered "Yes" to Question (4), what is the expected recovery time for your critical business functions?  0 to 4 hours

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

<https://www.e-janco.com>

6. Does the plan account for interdependencies within your organization?  Yes  No

7. Does the plan cover some, most, or all locations from which you provide your services?  Some  Most  All  NA

8. What percentage of "business as usual" servicing capability is the plan designed to address?

1%-10%  11%-25%  
 26%-50%  51%-75%  
 76%-99%  100%

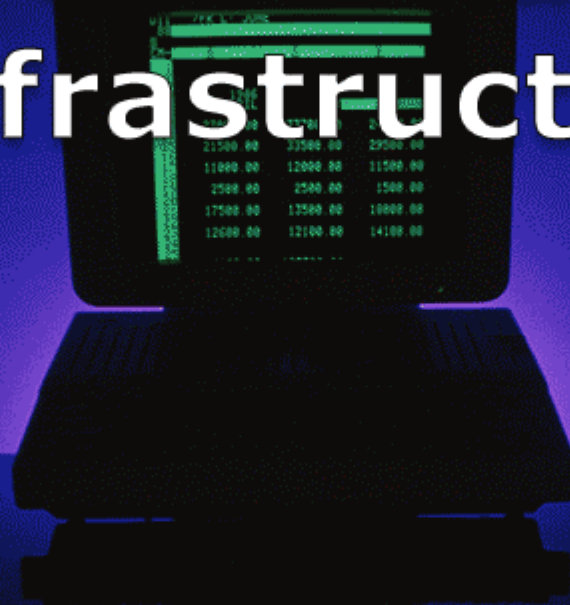
9. Do you have a dedicated team of professionals focused on business continuity and/or IT disaster recovery?  Yes  No

10. If you answered "No" to Question (9), do you use an external BCP/DR service provider to handle your planning needs?  Yes  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?  Yes  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.  Yes  No

# IT Governance Infrastructure



## Infrastructure, Strategy, and Charter Template

**ISO 2700, GDPR, HIPAA, PCI-DSS,  
and CoBit Compliant - Pandemic**

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

<https://www.e-janco.com>

**2020 Edition**







## Table of Contents

<b>IT GOVERNANCE - INFRASTRUCTURE, STRATEGY, AND CHARTER.....</b>	<b>1</b>
Benefits of IT Infrastructure Management .....	1
Base Assumptions and Objectives .....	2
Scope and Applicability .....	2
Operating Philosophy.....	2
Compliance .....	3
International Organization for Standardization .....	3
<b>IT GOVERNANCE - STRATEGY AND CHARTER STATEMENT OF AUTHORITY .....</b>	<b>6</b>
Chief Information Officer (CIO).....	6
Functional IT Group Heads.....	7
IT Management Council .....	8
Users .....	9
<b>IT MANAGEMENT STRUCTURE .....</b>	<b>10</b>
Organizational Approach .....	10
[Enterprise] IT Group .....	11
[Enterprise] IT Resources .....	12
Functional IT Groups .....	13
<b>COMPLIANCE .....</b>	<b>14</b>
Objective .....	14
Responsibilities .....	14
<b>IT JOB FAMILY CLASSIFICATION.....</b>	<b>16</b>
Structure .....	16
<b>PERSONNEL PRACTICES.....</b>	<b>18</b>
Formal Job Descriptions .....	18
Hiring.....	21
Termination.....	21
Training .....	22
[Enterprise] Staff .....	23
Contractor Personnel .....	23
<b>ERP AND OMNI COMMERCE .....</b>	<b>24</b>
Strategy .....	25
<b>CONTROLS .....</b>	<b>27</b>
Types of Controls .....	27
Risks .....	28
Logging and Audit Trails .....	33
<b>SOCIAL NETWORK ENGAGEMENT .....</b>	<b>37</b>
Rules for Social Network Engagement .....	37
<b>APPLICATION DEVELOPMENT STANDARDS .....</b>	<b>39</b>
SAMMY.....	39
Quality Assurance Process .....	41



## IT Governance

### Infrastructure, Strategy, and Charter Template

<b>SERVICE REQUESTS</b> .....	<b>42</b>
Policies .....	42
Process .....	43
Service Request Management .....	44
Equipment/Service Request.....	44
Problem Resolution Process .....	44
<b>LOCAL AREA NETWORKS (LANS) – WI-FI</b> .....	<b>46</b>
Features .....	46
LAN Wi-Fi Standards.....	49
LAN Wi-Fi Councils and Workgroups.....	49
<b>BACKUP &amp; RECOVERY</b> .....	<b>50</b>
Frequency Guidelines.....	50
Data Storage and Media Protection.....	51
Backup Program and Schedule .....	53
<b>DISASTER RECOVERY PLAN</b> .....	<b>56</b>
DRP Description .....	56
Pandemic Considerations.....	57
Planning .....	58
HR Policies.....	58
Technology.....	59
Supply Chain .....	59
Critical Function Analysis .....	60
DRP Procedures for Critical Data .....	60
Backup Criteria .....	60
Backup Procedures.....	61
Storage Criteria .....	61
Business Recovery Procedures.....	62
Requirements for Recovery .....	62
Recovery Guidelines.....	62
Restoring Damaged Equipment .....	63
Recovery Management .....	63
Contingency Planning.....	64
Planning Activities.....	65
<b>SECURITY</b> .....	<b>68</b>
IT Processing Area Classification .....	68
Classification Categories .....	69
Workstations, Remote Terminals, and Wi-Fi Access.....	72
Systems Security .....	73
Staff Member Security .....	74
Responsibilities .....	75
User Sensitive Positions .....	76
Network Security.....	77
Responsibilities .....	77
Violation Reporting and Follow-Up.....	78
<b>ACCESS CONTROL - PHYSICAL SITE</b> .....	<b>79</b>
Separation of Duties.....	79
Least Privilege .....	79



## IT Governance

### Infrastructure, Strategy, and Charter Template

Access Areas.....	80
Definitions of IT Access Control Zones.....	82
Responsibilities .....	83
Badges.....	86
Access Control Methods .....	87
Levels of Access Authority .....	87
Protection of Supporting Utilities .....	88
Resource Protection.....	88
<b>ACCESS CONTROL - SOFTWARE AND DATA .....</b>	<b>92</b>
Resources to Be Protected.....	92
Basic Standards .....	93
Classification Of Data, Software, And Documentation .....	94
Access from Other Facilities.....	95
Authorization Verification.....	98
<b>FACILITY REQUIREMENTS.....</b>	<b>99</b>
Physical Plan Considerations.....	99
Fire .....	103
Power .....	106
Air Conditioning .....	107
<b>OTHER TECHNICAL GUIDES .....</b>	<b>108</b>
<b>APPENDIX .....</b>	<b>109</b>
CIO and CTO Expanded Roles.....	109
HIPAA Audit Program Guide .....	110
ISO 27001 & 27002 Security Process Audit Checklist .....	115
Massachusetts 201 CMR 17 Compliance Checklist.....	136
Job Descriptions .....	139
CIO Job Description	
CIO Job Description (small enterprise)	
Chief Experience Officer (CXO)	
Chief Digital Officer	
Chief Mobility Officer	
Chief Security Officer	
Chief Technology Officer	
Digital Brand Manager	
Electronic Forms .....	140
Employee Termination Checklist	
Pandemic Planning Checklist	
What's News .....	141

#### IT Governance - Infrastructure, Strategy, and Charter

[Enterprise] Information Technology (IT) is a large and diverse organization that manages the information, internet, communication, and computer resources of [Enterprise]. This document

- ✚ Defines the core IT Governance process and guidelines
- ✚ Defines IT responsibilities that are the building blocks of a well-performing organization
- ✚ Highlights the overall guidelines and policies of [Enterprise] IT
- ✚ Provides an understanding of how IT integrates with the enterprise
- ✚ References additional documentation that addresses more tactical standards and guidelines found throughout the company

#### Benefits of IT Infrastructure Management

IT Infrastructure management commonly supports operational functions such as system management, change control, release management, network management, application management, job management, and database management. Across these functions, IT Infrastructure management provides improved service levels, improved

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

<https://www.e-janco.com>

For example, it can increase the number of hardware devices that an individual system or network administrator can manage.

- ✚ **Leveraging of staff resources, leading to increased IT productivity** - Productivity is a measure of how much staff time can be spent on work that brings value to the business - such as deploying new or improved applications to increase competitive advantage. The use of standardized infrastructure management processes can help increase the proportion of staff time that can be used for more productive work that can increase business value in addition to improving the service levels provided by IT.
- ✚ **Higher availability and improved IT Service Management** - With enterprise operations throughout the organization increasingly depending on information systems, system and network availability are key IT and enterprise requirements. While costs vary based on factors such as the nature of the applications, any unplanned downtimes have direct costs that arise from the loss of business opportunity and decreased end-user productivity. The use of infrastructure management processes can reduce downtime, improve application performance, and improve revenue opportunities for the business.

#### IT Governance - Strategy and Charter Statement of Authority

The IT Governance - strategy and charter statement of authority for IT includes all information technology, internet, e-commerce, and communications, which support the business goals of [Enterprise], while:

- ✚ Maintaining production performance at a level that reflects a “Service Excellence” philosophy
- ✚ Seeking out and implementing solutions that effectively satisfy business process requirements and creatively exploit business opportunities

#### Chief Information Officer (CIO)

##### Strategy and Charter

1. Guides the development of the overall Information Technology (IT) strategies and planning
2. Participates as a member of the [Enterprise] executive management team
3. Interacts frequently with senior and functional management on internal

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

<https://www.e-janco.com>

7. Oversees technology and operations group and provides the architectural infrastructure for [Enterprise] systems processes
8. Develops and maintains statements of necessary policies and procedures to assure proper documentation and communication of [Enterprise] IT related activities
9. Participates in the evaluation of IT functions and staff within [Enterprise]
10. Identifies opportunities and provides appropriate guidance for information systems staff career development throughout the organization.
11. Maintains external links to other companies and professional and academic organizations to gain competitive assessments and share information
12. Provides company-wide direction on the use of emerging technologies of IT within the enterprise. Identifies the information technologies to be assimilated, integrated and introduced within the corporation



## IT Job Family Classification

### Structure

#### Other [Enterprise] Resources

- ✓ [Enterprise] Human Resources Representative
- ✓ [Enterprise] Common Office Network and Workstation and PIM Orientation Manual(s)
- ✓ Training & Development Resource Guide
- ✓ IT Job Family Classification - <https://www.e-janco.com/it-Job-Family.html>
- ✓ IT and Internet Job Descriptions - [https://www.e-janco.com/Job\\_Book.htm](https://www.e-janco.com/Job_Book.htm)

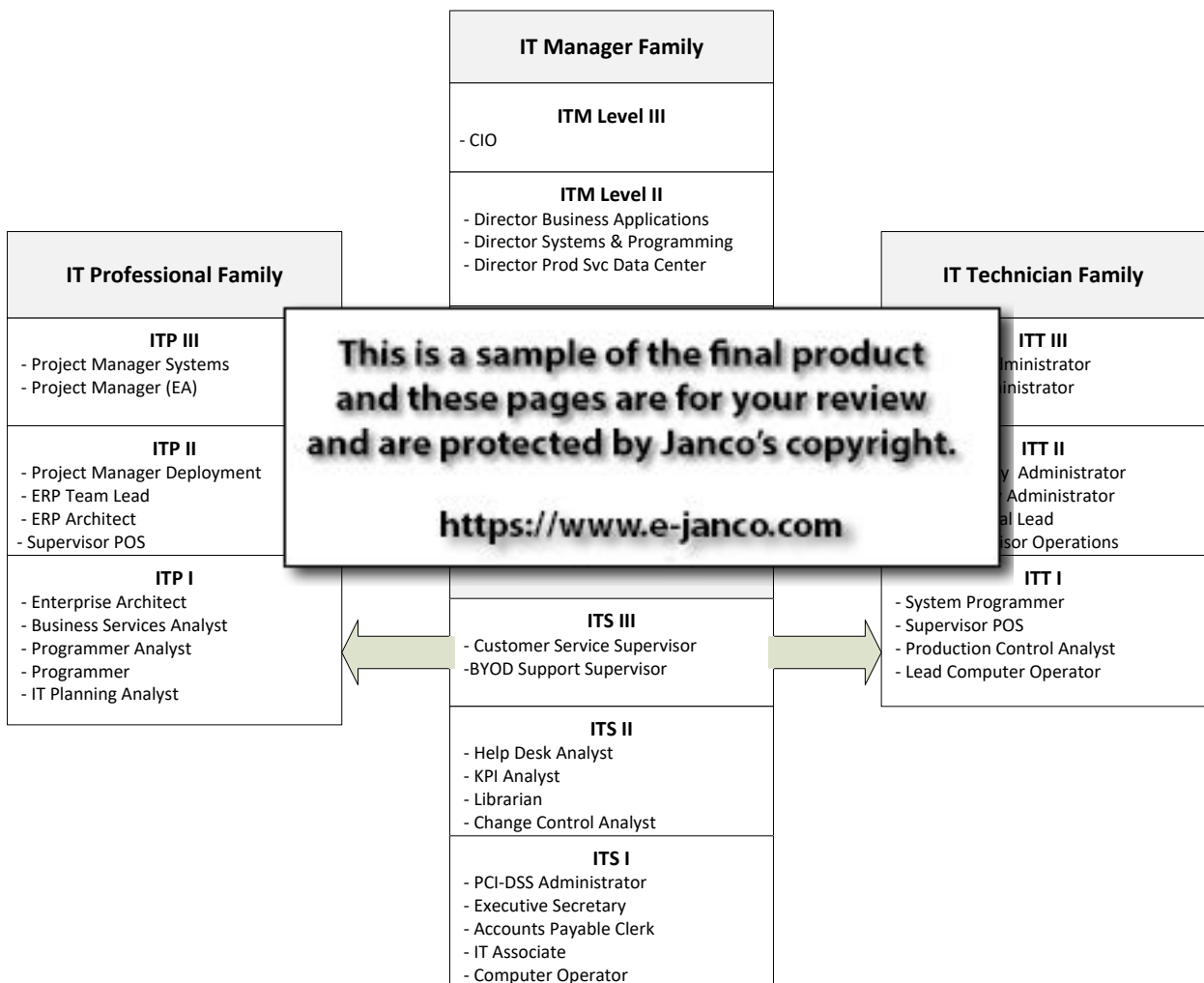
A job family classification system is one that defines how individuals can grow into higher-level positions over time by providing benchmarks milestones that need to be achieved as they advance over time. This in time impacts the compensation that is paid fairly and objectively. A job family is a series of progressively higher, related jobs distinguished by levels of knowledge, skills, and abilities (competencies) and other factors, and providing promotional opportunities over time.

The approach that we have found that works the best has four (4) primary job, families

- **Management Level** – This job family consists of several levels of Information Technology managerial work, which are distinguished based on the complexity and scope of the responsibilities assigned, including the direction of management information programs and services of varying sizes, scope and range of operating systems or subsystems, operating budgets, and other related factors characterized by the applications supported, types of equipment, enterprise considerations and responsibilities and number of staff.
- **IT Professional Level** - This family consists of several levels of Information Technology Professional work – working Professional through Supervisor/Expert. Levels are distinguished based on the complexity and scope of responsibilities, the degree of specialization and the degree of independent functioning. Included within this level are all the development activities.
- **IT Technical Level** - This job family consists of levels of Information Technology Technical work distinguished by the complexity of the responsibilities assigned and characterized by the type of equipment, operating systems or subsystems supported. This job family is distinguished from the Information Technology Professional in that its main emphasis is on installing, maintaining, and troubleshooting network and information technology systems and assisting with their on-going use and operation.

- IT Support/Entry Level** - This job family consists of five levels of Information Technology Consultant work which are distinguished by the complexity of the responsibilities assigned and characterized by the type of equipment, operating systems or subsystems, and interactions with the client users. Positions allocated to this job family differ from those in the professional or technical categories in that assignments are more administrative, involving the completion and coordination of various information services requirements rather than having direct responsibility for the technical aspects of the information system.

### IT Job Families



### Strategy

Over 80% of small to mid-sized businesses (SMB) and all large businesses focus on customer and supplier re-engagement and channel development programs via social media. There are extreme price and value-based competition with this arena. There is a requirement to present the outside world with more choices and interaction capabilities.

To be successful, an ERP and/or Omni commerce implementation must adhere to certain criteria need to be met:

- ✚ The driver for the effort needs to be a member of the “Operational” executive management team or the CEO
- ✚ There needs to be active support and management by a cross-functional team from operations, finance, marketing, distribution, sales and Information Technology (IT)
- ✚ Implementation success should be measured utilizing ROI principles and operational impact (productivity)
- ✚ Closely aligned with the industry and able to grow as a company changes to meet demand

Some businesses feel that ERP and/or Omni Commerce – but they lack the interaction between the different functions.

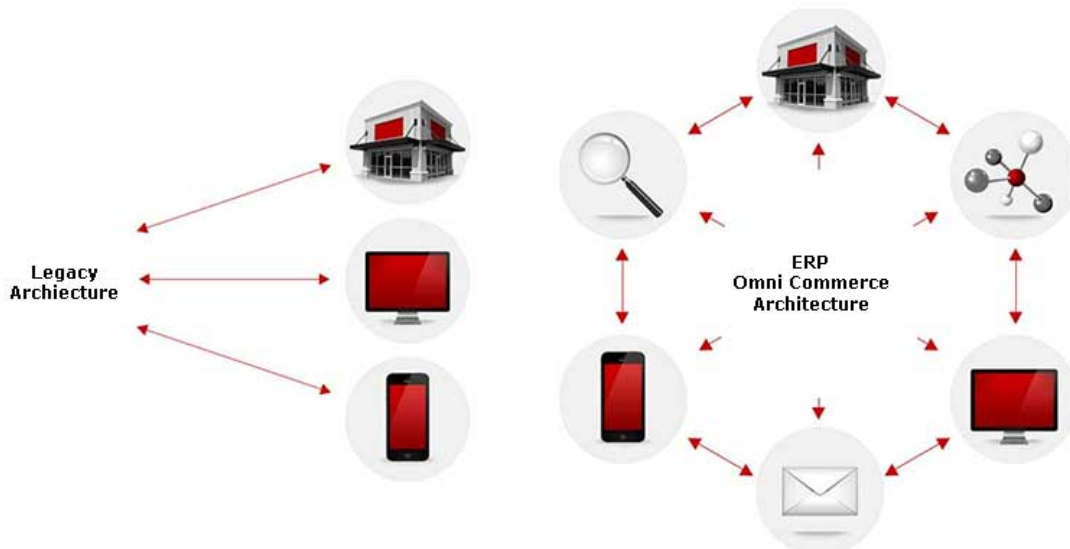
Legacy systems are typically siloed. The graphic below depicts an ERP or Omni Commerce

and or Omni Commerce – but they lack the interaction between the different functions of the IT

single purpose. The graphic below depicts an ERP or Omni Commerce

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

<https://www.e-janco.com>



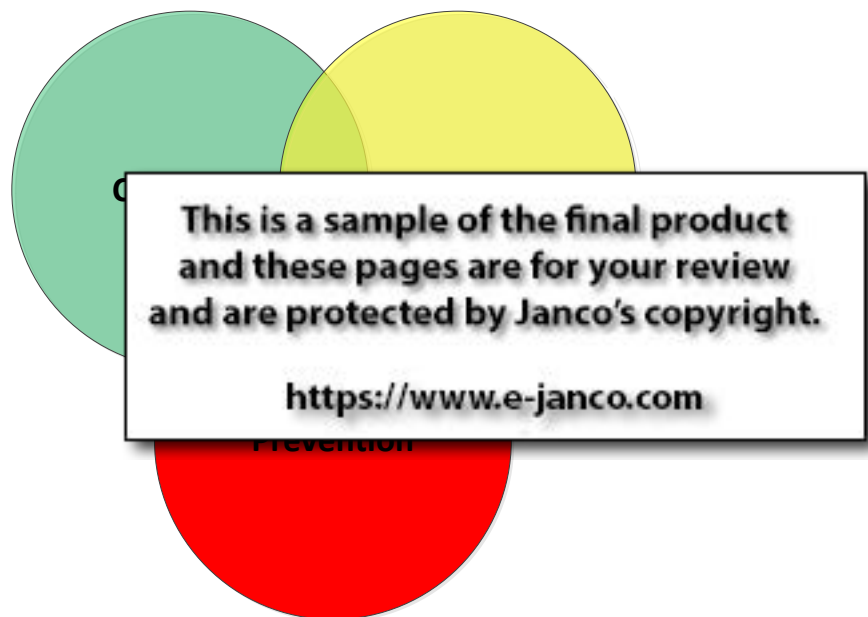
#### Controls

##### Other [Enterprise] Resources

- ✓ Internal Accounting Controls
- ✓ Standard Contracts
- ✓ IT Service Management Policy Template by Janco Associates, Inc. at <https://www.e-janco.com/itsm.htm>
- ✓ Security Manual Template by Janco Associates, Inc. <https://www.e-janco.com/Security.htm>

#### Types of Controls

Information is an organizational asset with associated risks. A good system of internal controls is necessary to protect [Enterprise] from the risks associated with information systems applications and operations. Controls are of three types.



#### Types of Controls

- ✚ **Detection** - notify when a real or potential violation of the control structure has taken place.
- ✚ **Prevention** - provide a way to eliminate the possibility of a violation of the control structure.
- ✚ **Correction** - provide a tool to correct a violation of the control structure.

## Disaster Recovery Plan

### Other [Enterprise] Resources

- ✓ Business Continuity and DRP Template - <https://www.e-janco.com/drp.htm>
- ✓ Incident Communication Plan <https://www.e-janco.com/Incident-Communication-Plan-Policy.html>
- ✓ Pandemic Planning Checklist – Attached electronic form

## DRP Description

In any business environment, there are inherent risks that must be recognized and addressed. Many of these risks can cause discontinuity of operations and may be quite damaging to [Enterprise] business. To avoid or minimize the impact of discontinuity of operations,

- ✦ Identify areas of risk
- ✦ Assess the potential outcomes associated with each risk
- ✦ Develop internal procedures to minimize the impact should the risks be unavoidable
- ✦ Ensure that personnel are prepared to deal with a variety of situations that could impact operations

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

<https://www.e-janco.com>

This s  
system  
of top

manner

cifically to information  
s a much wider range

- ✦ Ensuring that an environment is created to provide the ability to recover from an extended disruption of service;
- ✦ Making sure that plans are created by the responsible units;
- ✦ Coordinating the testing of applications; and
- ✦ Certifying the status of recovery capability.

Provisions must be made for operational recovery in the event of a disaster. This includes the recovery of critical data on information systems, file servers, workstations, and PIM devices throughout the organization. There is no substitute for advanced planning. Business unit managers must ensure that this planning is done properly and well-coordinated.

All staff members working in IT and support areas should have a thorough knowledge of all emergency procedures and equipment. Staff members should participate in periodic training and drills. These drills should include:

- ✚ How to respond to alarms and report trouble;
- ✚ How to operate fire extinguishers;
- ✚ How to operate automatic and manual alarms, extinguishing systems, controls, etc.;
- ✚ Proper salvage procedures; and
- ✚ How to restore equipment, including air conditioning and power.

All fire alarm and extinguishing systems should be periodically maintained and tested to assure reliability. Systems should be tested according to the following periods:

- ✚ Generators should be run weekly and load tested monthly;

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

<https://www.e-janco.com>

Staff members should assist with testing where possible to remain familiar with the operation of the emergency equipment. All physical security subsystems should be maintained and/or testing

### Pandemic Considerations

Planning for the risks and actions to be taken should occur before an event occurs. Typically travel, people to people contact, and major gatherings will be limited at best. The DR/BC plan and IT Infrastructure policies are impacted.

Business operations will continue only if proper precautions are taken.

1. **Safety and well-being.** Priority should be people – That includes company staff, company partners suppliers and their staff, their staff, and customers/clients. Their safety and wellbeing always come first, and they are best informed with the factual data.
2. **Business impact.** Understand the business impact of any decisions. For example, if a meeting or event is canceled what will the social, scientific, or economic impact be acceptable? What happens if we continue with the meeting or event and participation is reduced? Will this have an impact greater than canceling? What alternatives could be considered? Change of destination, date, or including a virtual element?"
3. **On-site risks.** Risks are typically a combination of the severity of impact vs. likelihood of different scenarios. Use a risk-assessment matrix to the plot, identity, and rank risks to determine and decide on appropriate responses. In times of heightened risks, establish a quick response team.



### Appendix

#### CIO and CTO Expanded Roles

The CIO and CTO have had their roles expanded as more businesses have moved to an Internet-based environment from the traditional “brick and mortar”. The job description for these positions, which are included as separate attachments, has been expanded accordingly.

Responsibility	CIO and CTO Traditional Roles	CIO and CTO Value Added Role
Strategy and Planning	<ul style="list-style-type: none"> <li>Define, update, and implement IT Strategy</li> <li>Manage IT across the enterprise</li> </ul>	<ul style="list-style-type: none"> <li>Align IT objectives and programs with enterprise objectives and strategies</li> <li>Coordinate IT across the enterprise</li> </ul>
Control	<ul style="list-style-type: none"> <li>Align IT, teams, with enterprise performance objectives</li> <li>Control performance objectives</li> <li>Control overall technology budget</li> </ul>	<ul style="list-style-type: none"> <li>Define KP metrics based on overall enterprise objectives</li> <li>Report performance status</li> <li>Coordinate overall technology</li> </ul>
Service	<p><b>This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.</b></p> <p><a href="https://www.e-janco.com">https://www.e-janco.com</a></p>	
Risk Management		
Business Processes	<p>requirements</p> <ul style="list-style-type: none"> <li>Follow IT System Development Methodology (SMD)</li> </ul>	<p>processes</p> <ul style="list-style-type: none"> <li>Define and adjust IT standards and technologies</li> </ul>
Strategic IT Initiatives	<ul style="list-style-type: none"> <li>Plan and manage strategic IT initiatives</li> <li>Manage application portfolio</li> <li>Manage IT projects</li> </ul>	<ul style="list-style-type: none"> <li>Shift decisions to enterprise operational groups</li> <li>Include enterprise process executive in IT governance</li> </ul>
Enterprise Infrastructure & Applications	<ul style="list-style-type: none"> <li>Define standards and architecture</li> <li>Coordinate (consolidate) IT processes across the enterprise</li> </ul>	<ul style="list-style-type: none"> <li>Optimize services through a mix of internal and external services</li> <li>Coordinate security and compliance</li> </ul>

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



## Job Descriptions

The job descriptions are included in a secondary directory (Job Descriptions) and not part of this document, the pdf, nor the ePub versions of it.

**CIO Job Description**

**CIO Job Description (small enterprise)**

**Chief Experience Officer (CXO)**

**Chief Digital Officer**

**Chief Mobility Officer**

**Chief Security Officer**

**Chief Technology Officer**

**Digital Brand Manager**

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

**<https://www.e-janco.com>**



#### Electronic Forms

The electronic forms that are included in a secondary directory (Forms) and not part of this document, the pdf, nor the ePub versions of it.

**Employee Termination Checklist**

**Pandemic Planning Checklist**

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

**<https://www.e-janco.com>**



## What's News

### 2020 Edition

- ✚ Added materials for Pandemic Planning in the DR/BC governance section
- ✚ Updated all included Job Descriptions
- ✚ Updated to meet latest compliance mandates
- ✚ Added electronic forms
  - Employee Termination Checklist
  - Pandemic Planning Checklist

### Version 4.1

- ✚ Added section on Social Network Engagement
- ✚ Added Chief Experience Officer (CXO) job description
- ✚ Updated to comply with the latest mandated security and sensitive information standards.

### Version 4.0

- ✚ Added materials to expand to cover IT Governance
- ✚ Added 3 full Job descriptions
  - Chief Mobility Officer
  - Chief Security Officer
  - Chief Technology Officer
- ✚ Updated all the included job descriptions
- ✚ Updated to meet all compliance requirements including GDPR
- ✚ Added section on Value Added roles of the CIO and CTO

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

**<https://www.e-janco.com>**

---

#### Version 3.5

- ✚ Updated social networking and customer/supplier strategies
- ✚ Added two core Job Descriptions to support the new digital marketplace and Omni-Commerce. Come as a separate MS Word file.
  - Chief Digital Officer
  - Digital Brand Manager
- ✚ Added an eReader version of the IT Infrastructure Strategy, and Charter
- ✚ Updated to meet the latest compliance requirements
- ✚ Updated all Internet HTML links

---

#### Version 3.4

- ✚ Added Job Family Classification
- ✚ Added references to policy, procedures, and electronic forms
- ✚ Updated to meet latest mandated compliance requirements
- ✚ Updated all exhibits

---

#### Version 3.3

- ✚ Updated to add a section on strategy for Omni Commerce and ERP

---

#### Version 3.2

- ✚ Updated to comply with latest ISO requirements
- ✚ Updated graphics

---

#### Version 3.1

- ✚ Added benefits section
- ✚ Updated to comply with CobiT requirements
- ✚ Added Security Management Compliance Checklist
- ✚ Added Massachusetts 201 CMR 17 Compliance Checklist
- ✚ Updated stylesheet elements

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

**<https://www.e-janco.com>**

---

#### Version 3.0

- ✚ Updated stylesheet to be CSS compliant
- ✚ Updated to be HIPAA and PCI compliant
- ✚ Added CIO Job Description
- ✚ Added CIO Small Enterprise Job Description

---

#### Version 2.1

- ✚ Added section defining ISO
- ✚ Added section defining ISO 27000 standard series
- ✚ Updated template to comply with ISO 27001 and 27002
- ✚ Updated Security Process Audit Check List to comply with ISO 27001 and ISO 27002
- ✚ Corrected Errata

---

#### Version 2.0

- ✚ HIPAA Audit Program Added
- ✚ ISO 177799 Security Process Audit Check List Added
- ✚ Office 2007 version Added

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

**<https://www.e-janco.com>**





# CIO IT Infrastructure Policy Bundle



## Table of Contents

This document contains the following policies:

- ✚ Backup and Backup Retention Policy (*revised 05/2019*)
- ✚ Blog and Personal Web Site Policy (*revised 01/2020*)
- ✚ BYOD Access and Use Policy (*revised 03/2019*)
- ✚ Google Glass Policy (*revised 01/2018*)
- ✚ Incident Communication Policy (*revised 03/2020*)
- ✚ Internet, Email, Social Networking, Mobile Device, and Electronic Communication Policy (*revised 02/2020*)
- ✚ Mobile Device Access and Use Policy (*revised 01/2020*)
- ✚ Outsourcing and Cloud-Based File Sharing Policy (*revised 01/2018*)
- ✚ Patch Management Version Control (*revised 10/2018*)
- ✚ Physical and Virtual Server Security (*revised 01/2020*)
- ✚ Privacy Compliance Policy (*revised 03/2019*)
- ✚ Record Classification, Management, Retention, and Disposition Policy (*revised 03/2019*)
- ✚ Safety Program (*revised 1/2020*)
- ✚ Sensitive Information Policy (*revised 1/2020*)
- ✚ Service Level Agreement Policy including sample metrics (*revised 10/2018*)
- ✚ Social Networking Policy (*revised 08/2019*)
- ✚ Technology Acquisition Policy (*revised 10/2018*)
- ✚ Telecommuting Policy (*revised 02/2018*)
- ✚ Text Messaging Sensitive and Confidential Information (*revised 10/2018*)
- ✚ Travel, Laptop, PDA and Off-Site Meeting Policy (*revised 01/2020*)
- ✚ Wearable Devices (*revised 02/2018*)

Shaded items updated in 2019 – All of the policies will be updated within the next several months. 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://www.e-janco.com/session/cart\\_x.aspx?p=SUB-090-12](https://www.e-janco.com/session/cart_x.aspx?p=SUB-090-12)
- 24 months - [https://www.e-janco.com/session/cart\\_x.aspx?p=SUB-094-24](https://www.e-janco.com/session/cart_x.aspx?p=SUB-094-24)
- Individual Policies - <https://www.e-janco.com/updateserviceindividualpolicies.htm>





# **Backup and Backup Retention Policy**

**Version 3.2**



Table of Contents

Backup and Backup Retention Policy.....3

    Policy.....4

    Applicability .....4

    Backup Versus Archive.....4

        Archiving Implications Sarbanes-Oxley .....5

        SOX – Section 802 .....5

        Record Retention Requirements.....5

    Types of Backups .....6

    Storage Management .....7

    Minimal Backup Policy .....7

        Requirements.....8

        Backup Retention .....8

        Documentation and Backup Media Labeling .....9

        Storage .....9

        Cloud Backup.....9

        Responsibilities.....10

        Testing and Training .....11

    System Specific Backup Policy .....12

    Backup Retention.....14

    Documentation and Backup Media Labeling .....14

        Storage .....14

        Responsibilities.....15

        Testing and Training .....15

    Issues to Manage with SLAs for Backup.....16

    Proposed Service Level Agreement Metrics .....17

Appendix .....18

    EU Safe Harbor Act Compliance and Data Backup Conflicts .....19

    Backup - Best Practices .....20

    Cloud Backup – Best Practices .....23

    Mobile Device Backup - Best Practices .....24

    Electronic Forms .....25

        • Disaster Recovery – Remote Location Contact Information .....25

        • Disaster Recovery – Business Continuity Vendor Contact Information Form.....25

        • Outsourcing and Cloud Security Compliance Agreement .....25

        • Remote Location Contact Form .....25

What’s New .....26





# **Blog Personal Website Policy**

**2020 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.

Version 2.1

**Table of Contents**

Bring Your Own Device (BYOD) Access and Use Policy .....	3
Overview .....	3
Components of the BYOD Strategy and Basics for BYOD Policy.....	4
Device Ownership Issues .....	7
Policy .....	8
BYOD Security Best Practices .....	14
BYOD Metrics and SLA Agreement .....	16
Executive management.....	16
Business unit executives .....	16
IT organization .....	16
Legal Considerations.....	18
Privacy.....	18
Record Retention .....	19
Appendix.....	21
BYOD Policy Decision Table .....	22
Electronic Forms.....	23
BYOD Access and Use Agreement Form .....	23
Mobile Device Security Access and Use Agreement Form.....	23
Mobile Device Security and Compliance Checklist .....	23
IT Job Descriptions .....	24
BYOD Support Specialist .....	24
BYOD Support Supervisor .....	24
Manager BYOD Support.....	24
What's New .....	25



# **Google Glass Policy Template**

**Version 1.3**



## Table of Contents

Google Glass Policy .....	3
<hr/>	
Overview .....	3
Policy .....	3
Google Glass Policy Requirements .....	4
Policy Definitions .....	4
Access Control .....	5
Security .....	6
Help & Support .....	7
Enterprise Mobile Device Infrastructure .....	8
Google Glass Infrastructure .....	8
Disaster Recovery .....	8
Backups .....	9
Intellectual Property .....	9
Google Glass Physical Device .....	9
Security .....	9
Supported Problems .....	9
Internal Network Access .....	9
Repair Procedure .....	9
Upgrade Procedure .....	10
Patching Policy .....	10
Google Glass Security Best Practices .....	11
General .....	11
Security Controls .....	11
Remote Google Glass Management .....	11
Access Management Controls .....	12
Google Glass Applications .....	12
<hr/>	
Legal Considerations .....	13
Privacy .....	13
Record Retention .....	13
Record Retention Federal and State Requirements .....	13
Implications Sarbanes-Oxley and Gramm-Leach-Bliley .....	14
Security Requirements .....	14
<hr/>	
Appendix – Electronic Forms .....	16
Google Glass Access and Use Agreement .....	17
Equipment/Expenses .....	17
Confidentiality/Security .....	17
<hr/>	
What’s New .....	18





# Incident Communication Plan Policy



JANCO ASSOCIATES, INC.

2020 Edition



# Table of Contents

Incident Communication Plan.....1  
    Overview.....1  
    Objective.....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  
    Social Networking Checklist .....19  
        Creating Twitter Accounts .....20  
        Creating LinkedIn account .....22  
        Creating and operating a blog .....24  
    Job Description .....26  
        Director Media Communications  
Electronic Forms .....27  
    Incident Communication Contact Form  
    Pandemic Planning Checklist Form  
What’s New.....28





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



JANCO ASSOCIATES, INC.

**2020 Edition**



# 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
Social Networking .....	16
Copyrighted Materials .....	19
Ownership of Information .....	19
Security .....	19
Skype.....	20
Text Messaging .....	21
Forms .....	22
Internet & Electronic Communication - Employee Acknowledgment .....	22
Email Employee Acknowledgment.....	22
Internet Use Approval .....	22
Security Access Application.....	22
Social Networking Policy Compliance Agreement .....	22
Telecommuting IT Check List Form .....	22
Telecommuting Work Agreement.....	22
Text Messaging Sensitive Information Agreement .....	22
Reference Section.....	23
Canada's Anti-spam Law (CASL), Bill C-28.....	23
What's News.....	27



# **Mobile Device Access & Use Policy**



**2020 Edition**



## Table of Contents

### Mobile Access and Use Policy

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 .....	8
Access Control.....	8
Federal Trade Commission Mobile Policy Guidelines .....	9
Security .....	11
Help & Support .....	12
Enterprise Mobile Device Infrastructure .....	12
Equipment and Supplies .....	13
Tablet Computer (iPads and Microsoft Surface).....	14
Mobile Device Security Best Practices .....	16
Top 10 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 .....	19
Company Asset Employee Control Log.....	19
Mobile Device Security Access and Use Agreement Form.....	19
Mobile Device Security and Compliance Checklist .....	19
What’s New .....	20





# **Policy – Outsourcing and Cloud-Based File Sharing**

**Version 3.3**



## Table of Contents

<i>Outsourcing and Cloud-Based File Sharing Policy</i> .....	2
Outsourcing Cloud-Based File Sharing Management Standard.....	2
Overview .....	2
Standard .....	2
Service Level Agreements (SLA) .....	2
Responsibility .....	2
Security, Disaster Recovery, Business Continuity, Records Retention and Compliance .....	3
Outsourcing Policy .....	3
Policy Statement .....	3
Goal .....	3
Approval Standard .....	4
Overview .....	4
Standard .....	4
Base Case.....	4
Cloud-Based File Sharing .....	5
Risk Assessment .....	5
Categorization .....	6
Planning.....	6
Retained Costs.....	6
Unit Cost.....	7
Selecting an Outsourcer .....	7
Contract and Confidentiality Agreements.....	7
Contract Negotiation .....	8
Responsibilities.....	9
Appendix.....	11
Outsourcing and Cloud Security Compliance Agreement .....	12
Outsourcing Security Compliance Agreement .....	13
Audit Program Guide.....	14
Background.....	14
ISO 27001 requirements .....	14
Planning the Audit.....	15
Audit Scope .....	16
Audit Objectives .....	16
Audit Wrap Up.....	17
Top 10 Cloud and Outsourcing SLA Best Practices.....	18
Job Description - Manager Outsourcing.....	20
Job Description - Manager Vendor Management.....	23
What's New .....	26





# **Patch Management Version Control Policy**





# Table of Contents

- Patch Management Version Control Policy .....2
- The Patch Management Version Control Process .....2
- Policy.....2
- Vendor Updates.....3
- Concepts .....3
- Responsibility.....3
- Organizational Roles .....4
- Monitoring.....5
- Review and evaluation.....5
- Risk assessment and testing .....6
- Notification and scheduling.....6
- Implementation .....7
- Emergency patches.....7
- Critical Patches .....7
- Auditing, assessment, and verification .....7
- User responsibilities and practices .....7
- Best Practices .....8
- Security Patch Management Best Practices .....10
- Appendix .....13
- Change and Patch Management Control Log .....13
- Job Descriptions .....17
- Manager Change Control (under separate cover) .....17
- Change Control Supervisor (under separate cover) .....17
- Change Control Analyst (under separate cover).....17
- What’s New.....18

**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**

**2020 Edition**



# Physical and Virtual File Server Security Policy

## Table of Contents

<b>Table of Contents</b> .....	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



# 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.....	21
User/Customer Sensitive Information and Privacy Bill of Rights.....	22
Appendix.....	23
Forms.....	23
Privacy Compliance Policy Acceptance Agreement.....	23
Job Descriptions.....	23
Chief Security Officer.....	23
Data Protection Officer.....	23
Manager Compliance.....	23
Manager Security and Workstations.....	23
Security Architect.....	23
Privacy and Security Compliance Implementation Work Plan.....	24
What’s New.....	26





**Record Classification,  
Management,  
Retention, and  
Disposition Policy**



**Table of Contents**

Record Classification, Management, Retention and Disposition Policy Statement .....	3
Overview .....	3
Scope .....	3
What is Record Classification and Management .....	4
Regulatory Overview .....	5
Record Retention Federal and State Requirements .....	5
Record Retention Implications Sarbanes-Oxley Sections 302, 404, and 409 .....	6
SOX - Section 302 .....	6
SOX - Section 404 .....	6
SOX – Section 409 .....	7
SOX – Sections 103a and 801a .....	7
SOX – Section 802 .....	7
Record Retention Requirements and Time Periods .....	7
Primary Classification List of Records to Be Retained .....	8
Record Classification by Device and Location .....	9
What ENTERPRISE Should Do .....	10
Record Classification, Management, Retention and Disposition Standard .....	11
Purpose .....	11
Scope .....	11
Responsibilities .....	12
Record Management .....	14
Record Creation .....	14
Data Security Classification .....	15
Record Retention Designation .....	17
Vital Records .....	19
Record Use .....	21
Record Disposition .....	22
Non-Archival Records .....	22
Archival Records .....	23
Record Destruction .....	23
Compliance and Enforcement .....	24
Legal Definitions .....	24
Email Retention Compliance .....	25
Policy .....	25
Unclassified – Temporary .....	26
Email to Be Deleted .....	26
Email to be maintained .....	27
Email to be printed .....	27
Regulations and Industry Impact .....	28
Keys to Email Archiving Compliance .....	29
Implementation Interview Checklist .....	30
Interviewee Questions .....	30
Records Accessed .....	30
Records Created .....	30





# Record Classification, Management, Retention, and Disposition Policy

---

Record classification, management, retention, and disposition Annual Review Process .....	31
Understand all the requirements for every type record your organization has.....	31
Develop and maintain clear and well-documented Record Management policies.....	31
Get management concurrence on those policies. ....	31
Annually review your Record Management practices.....	31
Review systems, technologies, and facilities, as well as your practices. ....	32
Document the results .....	32

---

Record Management Best Practices.....	33
Engage key managers and record stakeholders .....	33
Define scope, needs, and Objectives.....	33
Implement metrics and monitor processes.....	33
Define meaningful retention periods .....	34
Define search and retrieval core requirements.....	35
Automate the record retention and destruction processes.....	35
Start the process with current records – add old records over time .....	36
Train staff.....	36
Review and update the policy at least annually .....	36

---

Appendix.....	37
Job Descriptions.....	38
Manager – Record Administrator .....	38
Record Management Coordinator.....	38
Record Classification - Electronic Forms.....	38
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	
Facility Records	
Financial Records	
Sales Records	
Computer and Information Security Records	
Computer Operations and Technical Support	
Data Administration	
General Systems and Application Development	
Network and Communication Services	
User and Office Automation Support	
Safety Records	
Document Retention Time Periods.....	39
Federal Law Record Retention.....	40
Pennsylvania Record Retention .....	49
Massachusetts Record Retention .....	52
I-9 Retention .....	54

---

Version History .....	57
-----------------------	----

# Safety Program



JANCO ASSOCIATES, INC.

**2020**



# Table of Contents

- Safety Program Policy .....2
- Safety Goals .....3
- Responsibilities .....4
- Internet of Things (IoT) .....6
- Safety Rules .....7
- Accident Investigation .....11
- Hazard Recognition And Control .....12
  - Job Hazard Analysis (JHA).....12
  - Inspection Procedures.....12
  - Incidental Inspection.....13
  - Planned Inspection.....13
- Safety Committee .....14
- Safety Training .....15
- Communication .....17
- Record Keeping .....18
  - Inspection Documentation.....18
  - Accident Investigation -- Accident & Injury Records .....18
  - Training .....18
  - Safety Committee.....18
- New Employee Orientation .....19
- Training .....20
- Appendix.....22
  - IT Job Descriptions .....23
    - 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
    - New Employee Safety Checklist
    - Safety Program Contact List
    - Training Record
  - OSHA Electronic Forms.....24
    - Instructions
    - OSHA 300 Form
    - OSHA 300A Form
    - OSHA 301 From
- Revision History .....25





# **Policy**

# **Sensitive Information**



JANCO ASSOCIATES, INC.

**2020 Edition**



Table of Contents

Sensitive Information Policy - Credit Card, Social Security, Employee, and Customer Data .....3
Overview .....3
Policy .....3
PCI .....4
HIPAA .....4
California Consumer Protection Act (CCPA) .....5
General Data Protection Regulation (GDPR) .....6
Gramm-Leach-Bliley (Financial Services Modernization Act of 1999) .....6
Massachusetts 201 CMR 17.00 Data Protection Requirements .....7
User/Customer Sensitive Information and Privacy Bill of Rights .....8
Secure Network Standards .....9
Payment Card Industry Data Security Standard (PCI DSS) .....9
Install and Maintain a Network Configuration Which Protects Data .....13
Wireless & VPN .....14
Modify Vendor Defaults .....14
Protect Sensitive Data .....15
Protect Encryption Keys, User IDs, and Passwords .....16
Protect Development and Maintenance of Secure Systems and Applications .....17
Manage User IDs to Meet Security Requirements .....19
Restrict Physical Access to Secure Data Paper and Electronic Files .....20
Regularly Monitor and Test Networks .....21
Test Security Systems and Processes .....22
Email Retention Compliance .....23
Policy .....23
Unclassified – Temporary .....24
Email to Be Deleted .....24
Email to be maintained .....25
Email to be printed .....25
Regulations and Industry Impact .....26
Keys to Email Archiving Compliance .....26
Privacy Guidelines .....27
Best Practices .....27
Best Practices for Text Messaging of Sensitive Information .....28
US government classification system .....29
Appendix .....32
Attached Form .....33
• Sensitive Information Policy Compliance Agreement .....33
HIPAA Audit Program Guide .....34
What’s New .....39





# **Service Level Agreement Policy Template & Sample KPI Metrics**

**Table of Contents**

Table of Contents ..... 1

Service Level Agreement..... 3

    Definition of What a Service Level Agreement is..... 3

    Sample Service Level Agreement..... 4

        Assumptions ..... 4

        Service Stakeholders ..... 5

        Service Scope ..... 5

        IT Provider Responsibility..... 6

        Prioritization..... 6

    Typical Service Level Agreements ..... 7

        Internal IT SLAs ..... 7

        External SLA..... 9

Job Descriptions ..... 13

    Director IT Management and Controls ..... 13

    Manager Metrics ..... 13

    Metrics Measurement Analyst..... 13

    Job Description Structure..... 13

Sample Metrics..... 14

    System Management – Sample Metrics Report ..... 15

    What's New ..... 16

Service Level Agreement Sample Metrics..... 17

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

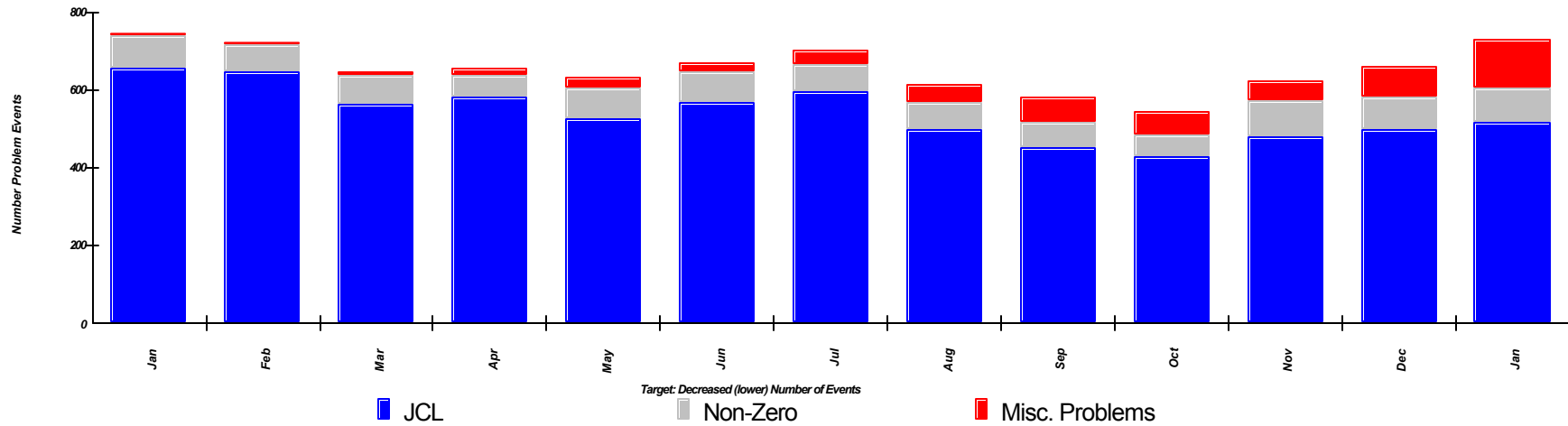
[SMC SRT \(All Summary\)](#)

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

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

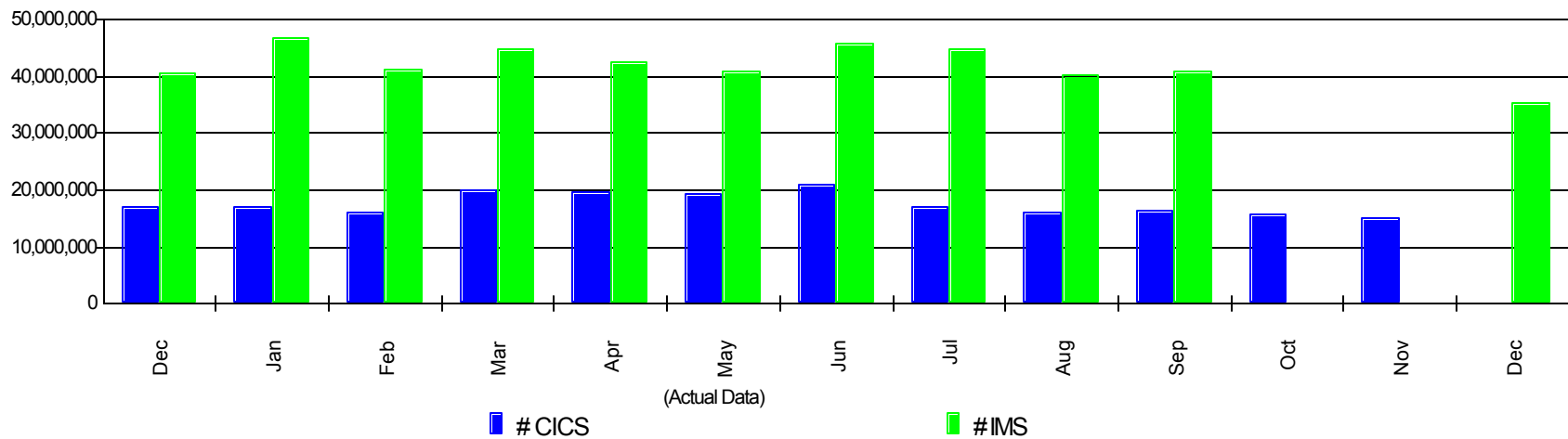
# System Management

## Number Reported Events/Problems - Nightly Batch



## Monthly # IMS/CICS Online Transactions

## All Systems





# **Social Networking Policy**

**Managing and Controlling Employee Social Networks**

**Version 2.2**





# Table of Contents

<b>Social Network Policy.....</b>	<b>3</b>
Definitions .....	3
Overview.....	3
Policy.....	4
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 Relationship.....	19
Steps to Prevent Being Scammed by Social Media .....	20
<b>Appendix.....</b>	<b>21</b>
Job Descriptions	
Job Description – Manager Social Networking .....	22
Job Description – Social Media Specialist .....	22
Electronic Forms	
Internet and Electronic Communication Agreement.....	23
Social Network Policy Compliance Agreement.....	23
Protection from Phishing and Whaling Attacks.....	24
Social Networking Best Practices .....	27
Twitter.....	27
LinkedIn.....	29
Blog .....	31
What’s News.....	33



Any technology that accesses, adds, alters, or deletes any enterprise data is covered by this policy

# Technology Acquisition Policy

---

Version 1.1



# Technology Acquisition Policy

## Table of Contents

Technology Acquisition Policy .....	3
Policy Purpose .....	3
Policy Statement.....	3
Applicability .....	3
Requirements .....	3
Roles .....	4
IT's Role .....	4
For Purchases within IT.....	4
Standard Items.....	5
Non-Standard Items.....	5
Capital Expenditures.....	5
Reimbursable Expenses .....	5
Vendor Evaluation .....	6
Preferred Vendors .....	6
Purchase Approval.....	7
Emergency Purchasing.....	8
Confidentiality .....	8
Conflict of Interest .....	8
Non-Compliance .....	8
Appendix.....	9
Security and Compliance Requirements.....	9





# **Telecommuting Policy Template**

Version 2.1





## Table of Contents

Telecommuting Policy .....2

---

Overview .....2

- Telecommuting resource misuse can have serious implications for an enterprise.....2

Policy .....4

- Policy Definitions .....4
- ENTERPRISE Responsibilities .....5

ENTERPRISE Policy Requirements.....5

- Termination of Agreement .....5
- Terms and Conditions .....5

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 Agreements .....8
- BYOD, Tablets, PDAs, and SmartPhones .....10

---

Appendix .....11

- Employer Legal Workplace Responsibilities .....12
- Position Requirements for Qualification for Telecommuting .....13
  - Determining positions that are appropriate for telecommuting.....13
  - Employee qualities that are appropriate for telecommuting .....13
- Electronic Forms .....14
  - Enterprise Owned Equipment
  - Internet and Electronic Communication Agreement
  - Mobile Device Access and Use Agreement
  - Mobile Device Security and Compliance Checklist
  - Safety Checklist - Work at Alternative Location
  - Security Access Application Mobile
  - Telecommuting IT Checklist
  - Telecommuting Work Agreement

---

What’s New.....15



# **Text Messaging Sensitive and Confidential Information Policy**





## Table of Contents

Text Messaging of Sensitive and Confidential Information Policy .....	2
Policy .....	2
Text Messaging Best Practices .....	3
Policy Specific Requirements .....	4
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 – Form - Text Messaging Sensitive Information Agreement .....	12
Text Messaging Sensitive Information Agreement .....	12
Confidentiality/Security .....	12
Equipment/Expenses .....	12
What’s New .....	13



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

**2020 Edition**



JANCO ASSOCIATES, INC.





## Table of Contents

Travel, Laptop, PDA, and Off-Site Meetings .....	2
Laptop and PDA Security .....	2
BYOD Security .....	2
Service Provider Selection .....	3
Wi-Fi & VPN .....	3
Data and Application Security.....	4
Minimize Attention .....	4
Public Shared Resources – Wireless and Shared Computers.....	5
Off-Site Meeting Special Considerations .....	6
International Travel Best Practices .....	7
Remote Computing Best Practices.....	8
Electronic Meetings .....	10
Best Practices for Electronic Meetings.....	11
Appendix.....	12
Electronic Forms.....	13
Mobile Device Access and Use Agreement	
Mobile Device Security and Compliance Checklist	
Privacy Policy Compliance Agreement	
Telecommuting IT Checklist	
Revision History .....	14



# **Wearable Device Policy**

Version 2.1



## Table of Contents

Wearable Device Policy.....	3
Overview.....	3
Policy.....	3
Wearable Device Policy Requirements.....	4
Policy Definitions.....	4
Access Control.....	5
Security.....	6
Help & Support.....	7
Creating a Wear Your Own Device Strategy (WYOD).....	7
Enterprise Mobile Device Infrastructure.....	8
Wearable Device Infrastructure.....	8
Disaster Recovery.....	8
Backups.....	9
Intellectual Property.....	9
Wearable Device Physical Device.....	9
Security.....	9
Supported Problems.....	9
Internal Network Access.....	9
Repair Procedure.....	10
Upgrade Procedure.....	10
Patching Policy.....	10
Wearable Devices Security Best Practices.....	10
Security Controls.....	10
Remote Wearable Devices Management.....	10
Access Management Controls.....	11
Wearable Device Applications.....	11
Legal Considerations.....	12
Privacy.....	12
Record Retention.....	13
Record Retention Federal and State Requirements.....	13
Implications Sarbanes-Oxley and Gramm-Leach-Bliley.....	13
Security Requirements.....	14
WYOD Management Security Options.....	15
Appendix.....	16
Top 10 WYOD Best Practices.....	17
Electronic Forms.....	18
Wearable Device Access and Use Agreement.....	18
What's New.....	19



# Infrastructure

# Electronic Forms

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

<https://www.e-janco.com>



**2020**



# Infrastructure Electronic Forms

---

## Forms contained include

- Application & File Server Inventory<sup>i</sup>
- Background Check Authorization
- Blog Policy Compliance Agreement
- BYOD Access and Use Agreement
- Change and Patch Management Control Log - (EXCEL)
- Company Asset Employee Control Log
- Disaster Recovery – Business Continuity
  - ▶ DR/BC Site Evaluation Checklist
  - ▶ LAN Node Inventory
  - ▶ Location Contact Numbers
  - ▶ Off-Site Inventory
  - ▶ Pandemic Planning Checklist
  - ▶ Personnel Location
  - ▶ Plan Distribution
  - ▶ Remote Location Contact Information
  - ▶ Server Registration
  - ▶ Team Call List
  - ▶ Vendor List
- Email – Employee Acknowledgement
- Employee Termination Checklist
- Enterprise Owned Equipment Inventory
- FIPS 199 Assessment
- Google Glass Access and Use Agreement
- Incident Communication Contacts
- Internet Access Request
- Internet & Electronic Communication Employee Acknowledgement
- Internet Access Request
- Internet Use Approval
- Interview Questionnaire
- Mobile Device Access and Agreement
- Mobile Device Security and Compliance Checklist
- New Employee Security Acknowledgement and Release
- Outsourcing and Cloud Security Compliance Agreement
- Outsourcing Security Compliance Agreement
- Pandemic Planning Checklist
- Preliminary Security Audit Checklist
- Privacy Compliance Policy Acceptance Agreement
- Retention Schedule
  - Administrative Records
  - Computer and Information Security Records
  - Computer Operations and Technical Support
  - Data Administration
  - Facility Records
  - Financial Records
  - General Systems and Application Development
  - Mobile Device Access and Use Agreement
  - Network and Communication Services
  - Personnel Records
  - Safety Records
  - Sales Records
  - User and Office Automation Support
- Safety Records
  - 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
  - New Employee Safety Checklist
  - Safety Program Contact List
  - Training Record
  - OSHA – 300 Log
  - OSHA – 300A Summary
  - OSHA – 301 Injury and Illness
- Security Access Application
- Security Audit Report
- Security Violation
- Sensitive Information Policy Compliance Agreement
- Social Network Compliance Agreement
- Telecommuting IT Checklist
- Telecommuting Work Agreement
- Text Messaging Sensitive Information Agreement
- Threat and Vulnerability Assessment
- Wearable Device Access and Use Form

---

<sup>i</sup> Partially electronic – currently work in process



## Background Check Authorization

Employee Name \_\_\_\_\_ SS Number \_\_\_\_\_

Former Name \_\_\_\_\_ DL/State \_\_\_\_\_

Address \_\_\_\_\_ DOB \_\_\_\_\_

\_\_\_\_\_  
Telephone \_\_\_\_\_

The information contained in this application is correct to the best of my knowledge.

*I hereby authorize COMPANY NAME and its designated agents and representatives to conduct a comprehensive review of my background report to be generated for employment and/or volunteer purposes. I understand that the scope of the report/ investigative report may include, but is not limited to the following areas: verification of social security number; employment history, education background, character references; drug testing, civil and criminal history records for all state and federal jurisdictions; driving records, birth records, and*

*I further authorize any information, verbal or written, to be used for any and all purposes. I hereby authorize the complete release of any information, firm, corporation, or public agency may have, to include information or data received from other sources. COMPANY NAME and its designated agents and representatives shall maintain all information received from this authorization in a confidential manner in order to protect the applicant's personal information, including, but not limited to, addresses, social security numbers, and dates of birth.*

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

<https://www.e-janco.com>

By signing this form, I affirm my approval to allow COMPANY NAME to conduct a background check on me for purposes of employment.

Signature \_\_\_\_\_

Date [Click here to enter a date.](#)

### Notice to California, Minnesota and Oklahoma Residents:

If you wish to receive a copy of the background check report that is requested.

I wish to receive a copy of any Background Check Report on me that is requested.

## Email - Employee Acknowledgment

If you have questions or concerns about this Policy, contact the ENTERPRISE's CIO before signing this agreement.

I have read the ENTERPRISE's Email Policy and agree to abide by it. In addition I agree to abide with all of the company's other policies relating to its electronic records. I understand violation of any of the above terms may result in discipline, up to and including my termination.

Employee Name \_\_\_\_\_ ID Number \_\_\_\_\_

Job Title \_\_\_\_\_ Location \_\_\_\_\_

Do you need Em



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

**<https://www.e-janco.com>**

liate)

d)

Signature \_\_\_\_\_

Date [Click here to enter a date.](#)

Approval Process			
Supervisor _____	IT Department _____	<input type="checkbox"/>	Approved
Email Address _____	User Level _____	<input type="checkbox"/>	Approved
Comments _____		<input type="checkbox"/>	Basic user
		<input type="checkbox"/>	Supervisor
		<input type="checkbox"/>	Manager
		<input type="checkbox"/>	Administrator



## Employee Job Hazard Analysis Acknowledgement

Employee Name \_\_\_\_\_ ID Number \_\_\_\_\_

Job Title \_\_\_\_\_ Location \_\_\_\_\_

I have complete the Job Hazard Analysis (JHA) programs for this function with the undersigned supervisor and fully understand the safety hazards associated with the function that I perform and how accidents can be prevented. My initials and signature below signify that I understand and will comply with each safety rule and procedure.

Hazards Reviewed -- Employee is to check the boxes for the items reviewed	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

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

**<https://www.e-janco.com>**

Signature \_\_\_\_\_

Supervisor Name \_\_\_\_\_

Position Title \_\_\_\_\_

Company Name \_\_\_\_\_

Email Address \_\_\_\_\_

Phone Number \_\_\_\_\_

# Mobile Device Access and Agreement

Employee Name \_\_\_\_\_ ID Number \_\_\_\_\_

Job Title \_\_\_\_\_ Location \_\_\_\_\_

Employee agrees to adhere to the Mobile Device Access and Use Policy	<input type="checkbox"/> Yes	<input type="checkbox"/> No
ENTERPRISE concurs with employee participation and agrees to support the approved mobile devices	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Copy of the ENTERPRISE Mobile Device Access and Use Policy and the Record Management Policy have been given to and read by the employee	<input type="checkbox"/> Yes	<input type="checkbox"/> No

## Equipment/Expenses

- ✚ An employee who uses ENTERPRISE equipment agrees to protect such equipment in accordance with ENTERPRISE guidelines. Enterprise equipment will be serviced and maintained by the ENTERPRISE.
- ✚ If the employee provides equipment, he/she is responsible for servicing and maintaining it.
- ✚ The ENTERPRISE is not liable for damages to an employee's personal or real property during the course of the performance of work duties or while using enterprise equipment in the workplace.
- ✚ The ENTERPRISE is not liable for damages to an employee's personal or real property during the course of the performance of work duties or while using enterprise equipment in the workplace.
- ✚ The ENTERPRISE is not liable for damages to an employee's personal or real property during the course of the performance of work duties or while using enterprise equipment in the workplace.

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

<https://www.e-janco.com>

## Confidentiality/Security

- ✚ The employee agrees to protect and maintain the confidentiality of all information, including but not limited to, trade secrets, confidential information, and other information that is proprietary to the ENTERPRISE. The employee will not disclose or disseminate such information to any other person, in any form, without the prior written consent of the ENTERPRISE. The employee will comply with the privacy requirements set forth in the ENTERPRISE policy or procedure.

By signing this form, I affirm my willingness to abide by ENTERPRISE's mobile device access and policies, procedures, and guidelines.

Employee Signature \_\_\_\_\_ Date \_\_\_\_\_

Supervisor \_\_\_\_\_ Date \_\_\_\_\_

# Mobile Device Security and Compliance Checklist

Employee Name	_____	ID Number	_____
Job Title	_____	Location	_____
Device Type	<input type="checkbox"/> Phone <input type="checkbox"/> Tablet <input type="checkbox"/> Other	Description	_____

## Security Controls

Yes	No	
<input type="checkbox"/>	<input type="checkbox"/>	256 bit AES encryption per file at rest, 30-day rotating encryption key
<input type="checkbox"/>	<input type="checkbox"/>	256 bit SSL encryption data transfer
<input type="checkbox"/>	<input type="checkbox"/>	SSAE 16 Type II compliant, redundant data centers and DR policy
<input type="checkbox"/>	<input type="checkbox"/>	99.9% SLA Uptime Guarantee

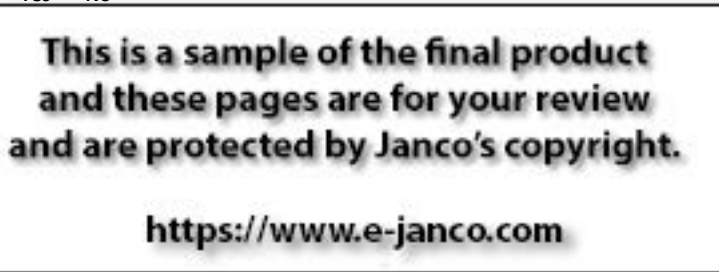
## Remote Device Management

Yes	No	
<input type="checkbox"/>	<input type="checkbox"/>	Auto-timed screen logout on mobile devices
<input type="checkbox"/>	<input type="checkbox"/>	Custom 4-digit pass code
<input type="checkbox"/>	<input type="checkbox"/>	Immediate access restriction on device
<input type="checkbox"/>	<input type="checkbox"/>	Auto login to end user accounts for remote wipe

## Access Management Controls

Yes No

Compliance



<input type="checkbox"/>	<input type="checkbox"/>	Is this device included in the Disaster Recovery Business Continuity Plan
<input type="checkbox"/>	<input type="checkbox"/>	Does this device meet the compliance requirements for the record management process
<input type="checkbox"/>	<input type="checkbox"/>	Has the user of this device completed all necessary training

## Audit Trail

Yes	No	
<input type="checkbox"/>	<input type="checkbox"/>	All global files can be accessed directly from central admin console
<input type="checkbox"/>	<input type="checkbox"/>	Usage statistics tracked for files, individual users and groups
<input type="checkbox"/>	<input type="checkbox"/>	Complies with record management policy
<input type="checkbox"/>	<input type="checkbox"/>	Downloads, uploads, previews
<input type="checkbox"/>	<input type="checkbox"/>	Tracked by IP Address

Employee Signature \_\_\_\_\_

Date \_\_\_\_\_







# PANDEMIC PLANNING CHECKLIST

Electronic form that is filled out as part of the Disaster Recovery and Business Continuity Planning process.



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

**<https://www.e-janco.com>**



# Pandemic Planning Checklist

## Impact of a pandemic on enterprise

### Tasks

Identify a pandemic coordinator and/or team with defined roles and responsibilities for preparedness and response planning. The planning process should include input from labor representatives.  Not Started  In Progress  Completed

Identify essential employees and other critical inputs (e.g. raw materials, suppliers, subcontractor services/ products, and logistics) required to maintain business operations by location and function during a pandemic.  Not Started  In Progress  Completed

Train and prepare ancillary workers for other job titles/descriptions,  Not Started  In Progress  Completed

Develop and plan for scenarios such as a decrease in demand for your products during a pandemic (e.g. effect of a restaurant closure on hygiene supplies).  Not Started  In Progress  Completed

**This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.**  
<https://www.e-janco.com>

Determine the potential impact of a pandemic on company business financials using multiple possible scenarios that affect different product lines and/or production sites.  Not Started  In Progress  Completed

Determine the potential impact of a pandemic on business-related domestic and international travel (e.g. quarantines, border closures).  Not Started  In Progress  Completed

Find up-to-date, reliable pandemic information from community public health, emergency management, and other sources and make sustainable links.  Not Started  In Progress  Completed

Establish an emergency communications plan and revise periodically. This plan includes identification of key contacts (with back-ups), a chain of communications (including suppliers and customers), and processes for tracking and communicating business and employee status.  Not Started  In Progress  Completed

Implement an exercise/drill to test your plan and revise periodically.  Not Started  In Progress  Completed



# Risk Assessment Matrix

Location \_\_\_\_\_ Function \_\_\_\_\_  
 Department \_\_\_\_\_ Manager \_\_\_\_\_

	High = 5	4	3	2	Low = 1	Score
<b>Organizational Uncertainty</b>	The business unit has no plan. Management is uncertain about responsibility there is no business sponsor	The business unit has no specific and has designated, but not committed, resources to the initiative	The business unit has a plan but has not committed resources	The business unit has no specific plan but has committed resources	The business unit has a plan and has committed resources	
<b>Technical Uncertainty</b>	No knowledge or experience	Emerging area	Some experience	Understood in a different area	Understood	
<b>Skills Required</b>	Extensive new skills for both staff & management	Extensive new skills for staff; some new skills for management	Some new skills required for both staff & management	Some new skills for staff; none for management	No new skills for staff & management	
<b>Hardware Dependencies</b>	Hardware is immature; just emerging from vendor labs	Hardware exists but is not yet used within the organization	Hardware exists and has been tested, but is not yet operational	In use in a different application	In use in similar applications	
<b>Software Dependencies</b>	Non-standard software with complex interfaces	Non-standard software	Standard software; multiple interfaces and dependencies exist	Standard software; complex programming is required	Standard software; routine programming is required	
<b>Application Software</b>	No package or solution exists. Complex design and development is required	Programs available commercially, but highly complex. Complex design and development	Programs available commercially with extensive modifications OR Programs can be developed in-house with moderate complexity	Programs available commercially with minimal modifications OR Programs can be developed in-house with minimal complexity	Programs exist & need minimal modification	
<b>Total Technical Uncertainty Score</b>						
<b>Infrastructure Uncertainty</b>	Major changes to the existing infrastructure are needed	Significant changes to the existing infrastructure are needed	Moderate changes to the existing infrastructure are needed	Small changes are required to the existing infrastructure. Investment is needed	The solution will use existing infrastructure and services no investment is required	
<b>Total Risk Score</b>						

# Telecommuting IT Checklist

Both the employee and supervisor should initial each piece of equipment in the issued box and returned box with the equipment is issued or returned.

Employee:	Department:
Location:	Supervisor:
Phone at Location:	Date:

The alternate work location is located (check one):

in home  
 not in home

---

### Hardware Requirements

- |   |                              |                             |
|---|------------------------------|-----------------------------|
| • Base Platform (e.g. laptop, desktop with monitor, tablet) | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Printer   | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Microphone / headset                                      | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Camera for video conference                               | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Scanner   | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Shredder  | <input type="checkbox"/> YES | <input type="checkbox"/> NO |

---

### Communication Requirements

- |  |                              |                             |
|--|------------------------------|-----------------------------|
| • Landline – linked to enterprise auto attendant | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Internet broadband                             | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • VPN  | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Email  | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Instant Messaging                              | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • File Sharing                                   | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Records retention and destruction policies     | <input type="checkbox"/> YES | <input type="checkbox"/> NO |

---

### Security and Compliance Requirements

- |   |                              |                             |
|---|------------------------------|-----------------------------|
| • Two factor access (password plus biometrics)                | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Enciphering   | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Disaster Recovery Business Continuity plan                  | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Physical Security of all electronic assets located remotely | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • User access to admin functions blocked                      | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Media copying blocked (CD/DVD/USB connectivity)             | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Training for telecommuter                                   | <input type="checkbox"/> YES | <input type="checkbox"/> NO |

---

### Other Considerations

- |  |                              |                             |
|--|------------------------------|-----------------------------|
| • Reimbursement policy for telecommuters work related expenses | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Policy for non-business use of enterprise assets             | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Inventory of data and enterprise physical assets             | <input type="checkbox"/> YES | <input type="checkbox"/> NO |
| • Rules for audit and termination procedures for employees     | <input type="checkbox"/> YES | <input type="checkbox"/> NO |

---

Employee Signature Date

---

Supervisor Date



# Telecommuting Work Agreement

The following constitutes an agreement on the terms and conditions of telecommuting on (Date) between:

Employee Signature	Date
--------------------	------

Supervisor	Date
------------	------

<b>Employee agrees to participate in telecommuting and to adhere to applicable guidelines and policies. This is not a guarantee of continued employment.</b>	<input type="checkbox"/> YES	<input type="checkbox"/> NO
<b>Employee agrees to participate in telecommuting for an initial period not to exceed one year, beginning _____ and ending _____.</b> <b>This agreement may be extended beyond the initial one year period, if agreeable to the ENTERPRISE and to the employee. If extended, the terms of this agreement should be reviewed and updated as necessary. This agreement can be terminated at any time by ENTERPRISE without notice.</b>	<input type="checkbox"/> YES	<input type="checkbox"/> NO
<b>ENTERPRISE concurs with employee participation and agrees to adhere to applicable guidelines and policies.</b>	<input type="checkbox"/> YES	<input type="checkbox"/> NO
<b>Copies of the ENTERPRISE Telecommuting Policy and Record Management have been given to and read by the employee.</b>	<input type="checkbox"/> YES	<input type="checkbox"/> NO

## Work Location – Schedule

Employee \_\_\_\_\_  
 Employee \_\_\_\_\_  
 Describe \_\_\_\_\_  
 At the ce \_\_\_\_\_ to  
 on the fo \_\_\_\_\_

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

<https://www.e-janco.com>

At the alternate work location, employee's work hours will normally be from \_\_\_\_\_ to \_\_\_\_\_  
 on the following days:

Employee's time and attendance will be recorded the same as performing official duties at the central workplace.

Supervisors will maintain a copy of employee's work schedule, and employee's time and attendance will be recorded the same as if performing official duties at the central workplace.

Approval Process			
<b>Dept. Head</b>	_____	<b>IT Department</b>	_____
	<input type="checkbox"/> <b>Approved</b>		<input type="checkbox"/> <b>Approved</b>
<b>Signature</b>	_____	<b>User Level</b>	<input type="checkbox"/> <b>Basic user</b>
<b>Comments</b>			<input type="checkbox"/> <b>Supervisor</b>
			<input type="checkbox"/> <b>Manager</b>
<b>Date:</b>			<input type="checkbox"/> <b>Administrator</b>

# Text Messaging Sensitive Information Agreement

Employee Name \_\_\_\_\_ ID Number \_\_\_\_\_

Job Title \_\_\_\_\_ Location \_\_\_\_\_

Employee agrees to adhere to the Text Messaging Sensitive and Confidential Information Policy	<input type="checkbox"/> Yes	<input type="checkbox"/> No
ENTERPRISE concurs with employee need to text message sensitive and/or confidential information	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Copies of the ENTERPRISE Text Messaging Sensitive and Confidential Information and Record Management Policy have been given to and read by the employee	<input type="checkbox"/> Yes	<input type="checkbox"/> No

### Confidentiality/Security

- Employee who text messages ENTERPRISE’s sensitive and/or confidential information agrees to protect such information in accordance with ENTERPRISE guidelines. Such information remains the property of ENTERPRISE.
- Employee will apply approved safeguards to protect ENTERPRISE records from unauthorized disclosure or damage and will comply with the privacy requirements set forth in the ENTERPRISE policy or procedure.

Equ

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

<https://www.e-janco.com>

employee’s residence.

for servicing and maintaining  
ns to ENTERPRISE’s text  
y.  
ee’s personal or real property  
prise equipment in the

- The ENTERPRISE is not responsible for operating costs, home maintenance, or any other incidental costs (e.g., utilities) associated with the use of the employee’s residence as an alternate work location.

By signing this form, I affirm my willingness to abide by ENTERPRISE’s Text Messaging Sensitive and Confidential Information Policy.

Employee Signature \_\_\_\_\_ Date \_\_\_\_\_

Supervisor \_\_\_\_\_ Date \_\_\_\_\_



# Threat and Vulnerability Assessment Physical and Electronic Sites - Page 1

Prepared by \_\_\_\_\_

Date

Location Type      Company      Residence      Multi-Tenant      Public Access

Address

Main Phone      Facility Manager

Assets at facility      Head count at Facility      Primary Functions Performed

Power Grid Distribution Point

Telephone CO Location

Backup Power      Yes      No      Length of Support Hrs

Safety Program      Yes      No      Date of Last Review     

DRP/BCP      Yes      No      Date of Last Test     

Internet Access

Category I - Extreme Financial Impact      **This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.**      No

Category II - High Financial Impact      **https://www.e-janco.com**      No

Category III - Medium Financial Impact      **https://www.e-janco.com**      No

Category IV - Low Financial Impact      Any Cat IV in Facility      Yes      No

Public Access      Yes      No      Security Badges      Yes      No

Reception Desk      Yes      No      Card Key      Yes      No

Guards      Yes      No      Fenced      Yes      No

Armed      Yes      No      Guard Gate      Yes      No

Guest Escorted      Yes      No      Gate Manned      Yes      No

Cameras      Yes      No      24/7 Security      Yes      No

RT Monitoring      Yes      No      After Hours Contact

# Threat and Vulnerability Assessment Physical and IT / Electronic Sites

## 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%
<i>Catastrophic</i>					
<i>Very High</i>					
<i>Noticeable to ENTERPRISE</i>					
<i>Minor</i>					
<i>None</i>					

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

Interpretation of scores	
<b>6 to 8</b>	These risks are extreme. Countermeasure actions to mitigate these risks should be implemented immediately.
	These risks are very high. Countermeasure actions should be implemented as
	Countermeasure actions should be implemented in the
	actions to be implemented as
	convenient as they will enhance security overall.
<b>0</b>	These currently pose no risk but should continue to be monitored.

**This is a sample of the final product and these pages are for your review and are protected by Janco's copyright.**  
  
<https://www.e-janco.com>

# Wearable Device Access and Use Agreement

Employee Name \_\_\_\_\_ ID Number \_\_\_\_\_

Job Title \_\_\_\_\_ Location \_\_\_\_\_

Employee agrees to adhere to the Google Glass and Mobile Device Access and Use Policy	<input type="checkbox"/> Yes	<input type="checkbox"/> No
ENTERPRISE concurs with employee participation and agrees to support the approved mobile devices	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Copies of the ENTERPRISE Google Glass, Mobile Device Access and Use and Record Management Policy have been given to and been read by the employee	<input type="checkbox"/> Yes	<input type="checkbox"/> No

## Equipment/Expenses

- Employee agrees to protect such equipment in accordance with ENTERPRISE guidelines.
- Employee is responsible for servicing and maintaining their own equipment.

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

<https://www.e-janco.com>

personal or real property during the course of  
 ent in the employee's residence.  
 maintenance, or any other incidental costs  
 sidence as an alternate work location.  
 ental costs associated with connectivity  
 use on ENTERPRISE network or

## Confidentiality/Security

- Employee will apply approved safeguards to protect ENTERPRISE records from unauthorized disclosure or damage and will comply with the privacy requirements set forth in the ENTERPRISE policy or procedure.
- Employee will respect the privacy of all employees, associates, suppliers, customers and others they encounter while using or wearing the Google Glass.

By signing this form, I affirm my willingness to abide by ENTERPRISE's Google Glass access policies, procedures and guidelines.

Employee Signature \_\_\_\_\_ Date \_\_\_\_\_

Supervisor \_\_\_\_\_ Date \_\_\_\_\_