Pandemic Infrastructure Bundle

Disaster Recovery Business Continuity Template

Janco Associates, Inc.

2020 Edition

Table of Contents

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 repres Recovery Plan.

1.1 Recovery

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[1] 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.

Manage

As a general rule of qualified, knowledgeable i of the board than the BCP tea t the BCP plan and process mee

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

  There[2] 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.

[1] 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.

[2] 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.

onment is how to tie all
of compliance—across all
ols.

tinuing basis;

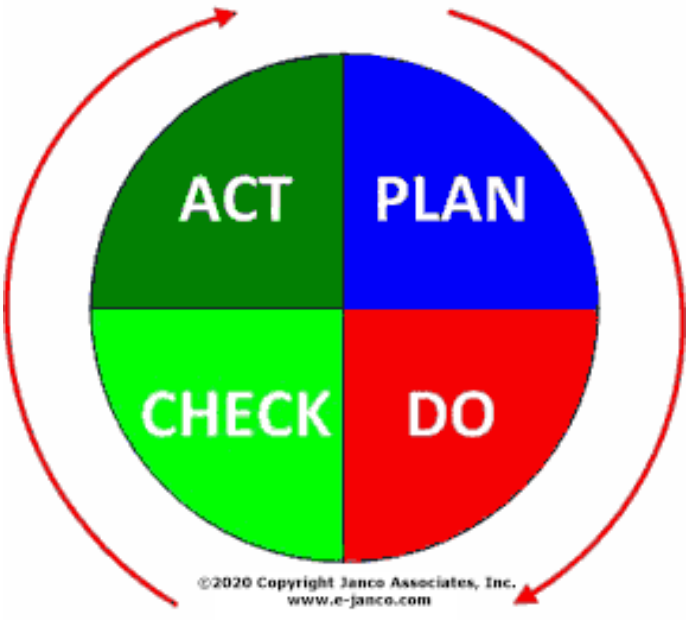
ness of security controls in meeting a variety of standards and regulations and demonstrate due care of compliance.

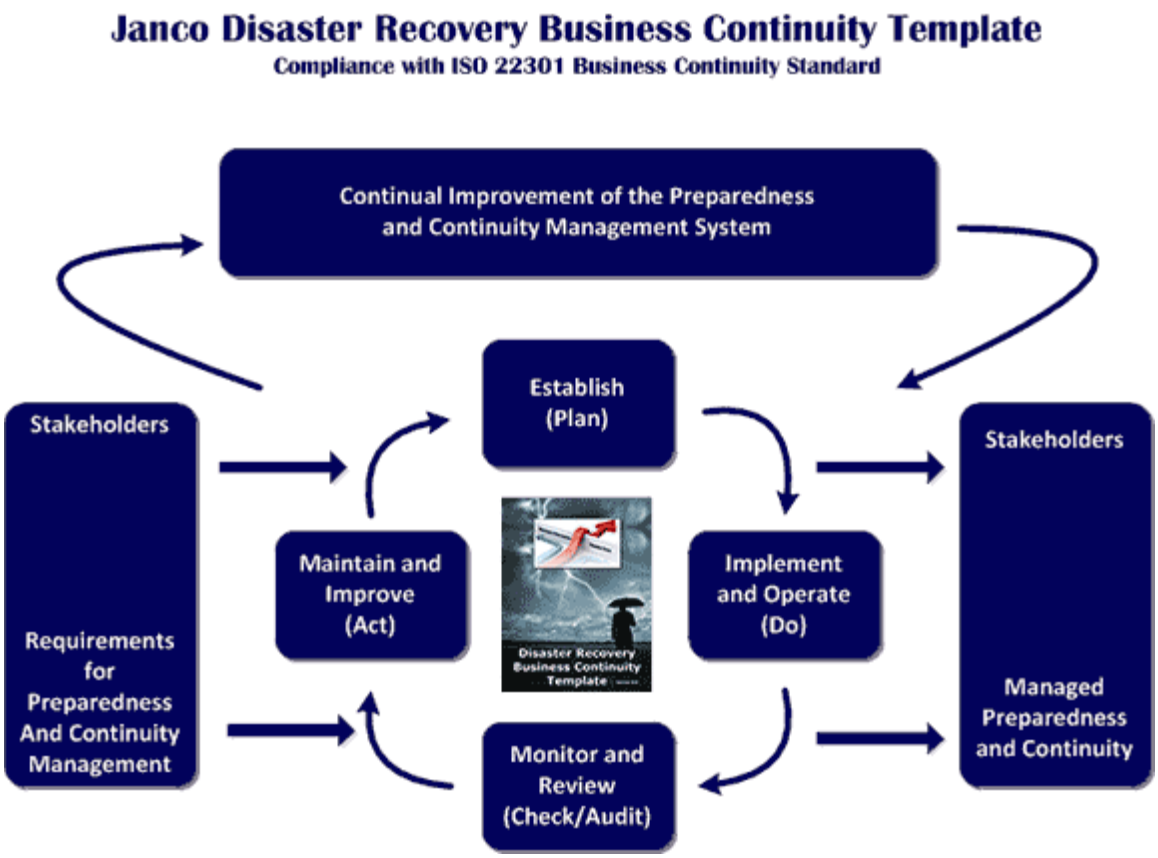
- Map control information to specific policies in order to provide recommendations for improvements to the control environment; and
- Collect, integrate, and retain trend analyses and evidentiary information from disparate control mechanisms for audits and documentation requests.

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.





ISO 28000

n implementing and
MS)

very, aging infrastructure
Security has become a
ion 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

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.

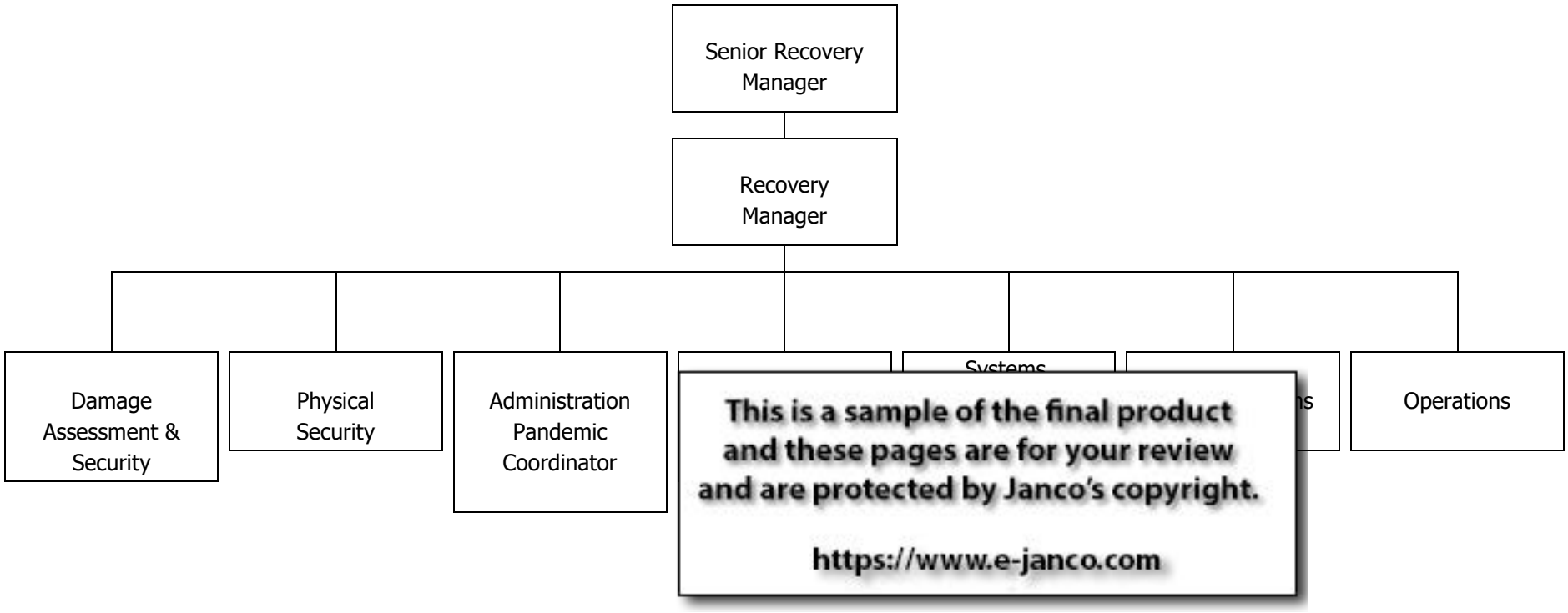
The Disaster Recovery Plan and Process have been reviewed by the executive management of ENTERPRISE and necessary changes in the "BY-LAWS" and or "CHARTER" of ENTERPRISE has been approved by the Board of Directors, Stockholders or other legal entities as required.

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.

Recovery Strategy	Recovery Time	Advantages	Disadvantages	Comments
Commercial Hot site	24 to 48 Hours	• Best recovery time • Easiest to implement as equipment, application software, data, and OS are in place • Easy to test at any point in time • The best solution that is available to support on-going operations	• Most expensive options duplicate equipment and software plus on-going version control issues • Ongoing communication costs to duplicate data very high • Term of the agreement can limit the duration of use • If you are not the "most important customer" you could be bumped	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.
Internal Hot site	1 to 12 hours	• Best recovery time • Easiest to implement as equipment, application software, data, and OS are in place • Easy to test at any point in time • The best solution that is available to support on-going operations	• Most expensive options duplicate equipment and software plus on-going version control issues • Ongoing communication costs to duplicate data very high	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.
Warm Site	24 to 48 Hours	• M • Ba su • Ab im ha so co		osts can be shared among multiple facilities thin the enterprise, internal provisioning can st competitive with commercial alternatives. o appropriate secondary space is available -location" facilities providers offer managed sed-floor space at very attractive rates as an ernative to building out secondary sites.
Mobile Site	24 to 48 Hours	• Moderately priced • Typically, can be in place for 36 to 72 hours • Can be placed in the "parking lot" adjacent to you impacted facility	• Recovery time typically is at least 2 to 5 days longer than a hot site. • Access to your impacted facility may be hindered because of the event • A trailer may not be configured exactly as you need it	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.
Cold Site	72 plus Hours	• Lowest cost solution • Basic infrastructure power, air, and communication are in place • Can rent the facility for a longer-term at lower cost	• Longest recovery time • All equipment must be ordered, delivered, installed and made operational • Worst solution for supporting on-going operations	"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.
Reciprocal Agreement	12 to 48 Hours	• Least costly solution • Better than no strategy	• Seldom works • Typically, in the same geographic area and a wide range disaster like an earthquake renders it of no use • No easy way to test	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.
Cloud	0 to 24 Hours	• Data and applications available immediately • Location independent • Easy to test	• Security • May not allow enough time for a daily cycle processing window	Data should be in place so activation would only be limited by connectivity and network addressing (DNS propagation).

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.

Th he Disaster Recovery M

7.1 Disa

ining the plan in a ifaceted. Not only does g maintenance of the plan, 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**

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**

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**

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

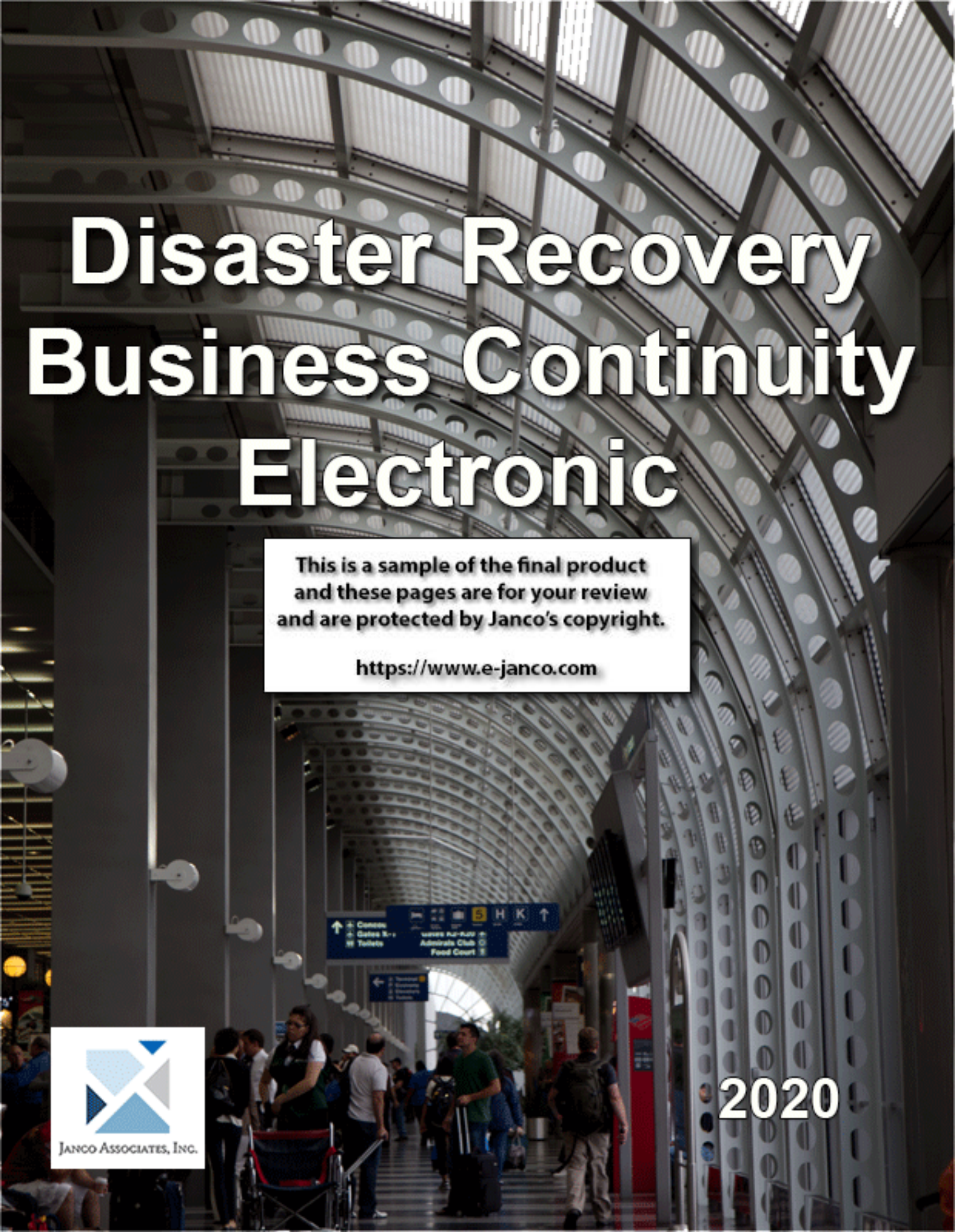
- Added ISO 27031 specific materials
  - Overview
  - Principles – Scope and Objectives
  - Requirements

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

Janco Associates, Inc.

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

JANCO ASSOCIATES, INC.

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 measure		NO
Carrier Diversity - Does the facility provide a they allow interconnection with other faciliti		NO
Scalability - Can the facility support higher d		NO
Service Level Agreement (SLA) - What level		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

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.

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 pande financials using multiple possible scenarios product lines and/or production sites.	pleted
Determine the potential impact of a pande domestic and international travel (e.g. quar	pleted
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

Janco Associates, Inc.

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
6.	Does the plan account for interdependencies your organization?	
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

Janco Associates, Inc.

2020 Edition

Table of Contents

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 Infrastruct ngs, improved service lev

- cedures, and ture alerts and dardization can tions and by aff member. 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

cts for services

oss-functional

pplications

pliance, SAP)

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

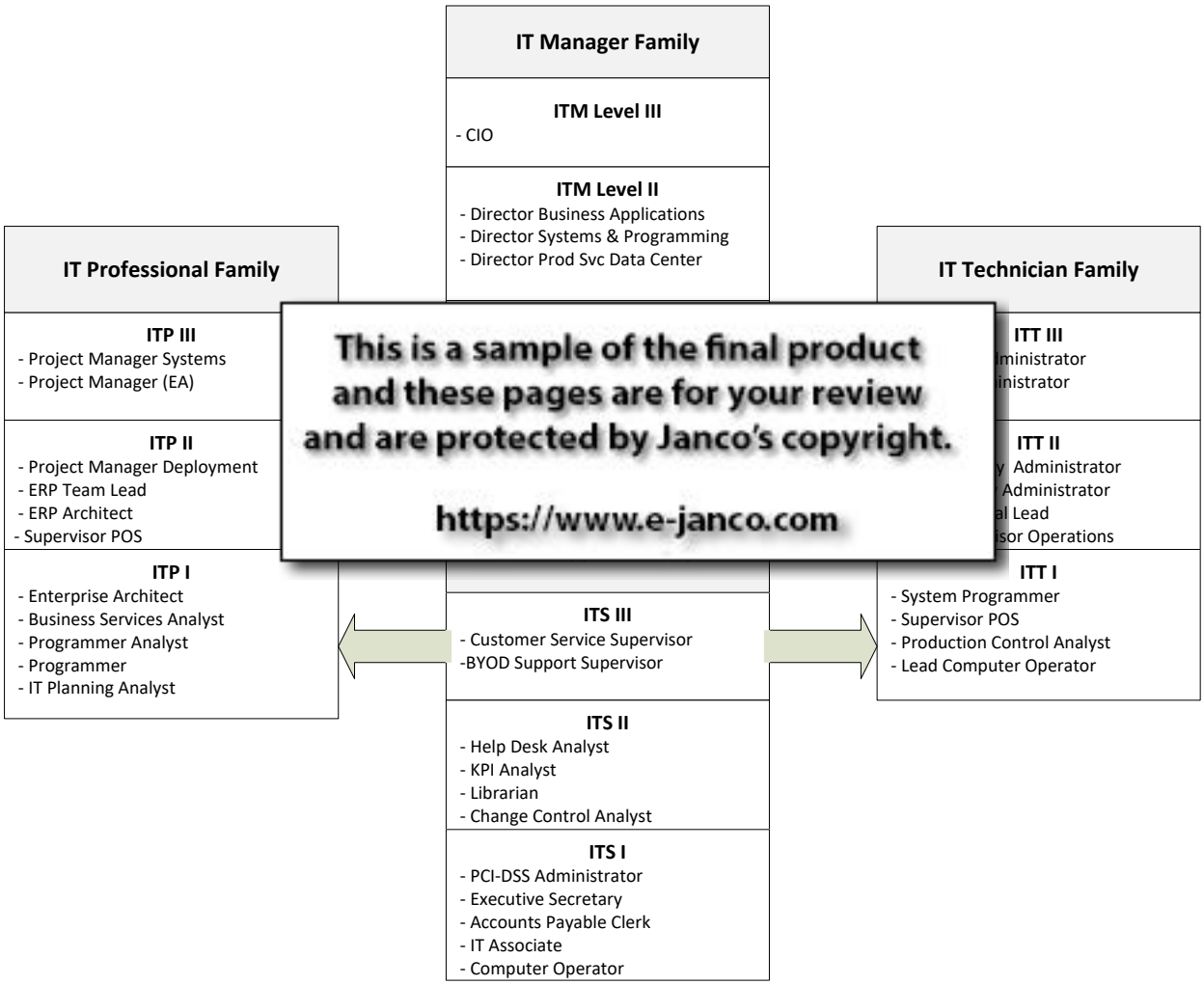
A job family classification system is one that defines how individuals can grow into higher-level positions over time by providing benchmarks milestones that need to be achieved as they advance over time. This in time impacts the compensation that is paid fairly and objectively. A job family is a series 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

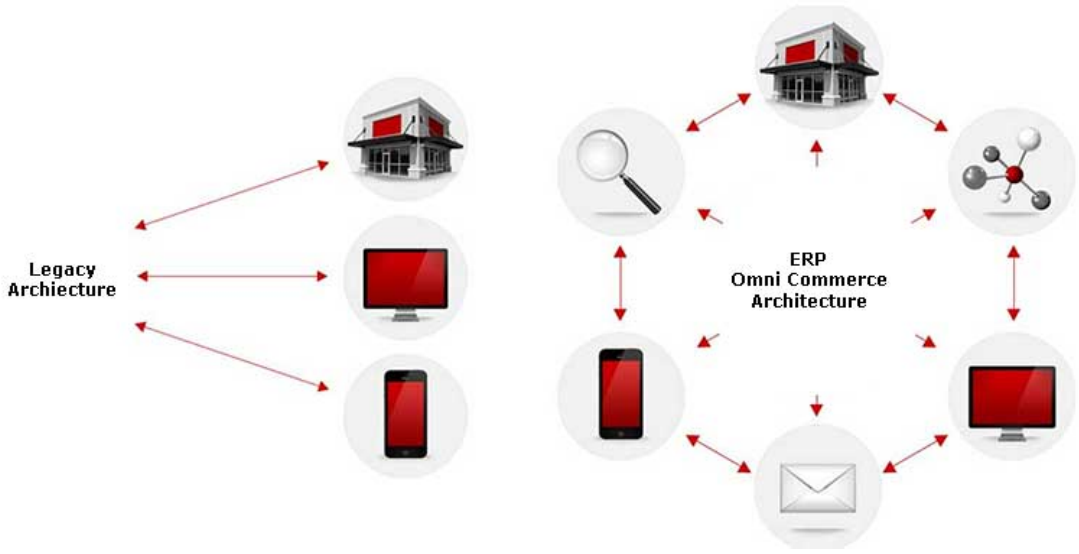
Over 80% of small to mid-sized businesses (SMB) and all large businesses focus on customer and supplier re-engagement and channel development programs via social media. There are extreme price and value-based competition with this arena. There is a requirement to present the outside world with more choices 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 t and or Omni Commerce – but they nd direct interaction between th of the IT function.

Legacy systems are typ single purpose. The graphic below dep cation versus an ERP or Omni Comm



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

manner

This s cifically to information syste s a much wider range of top

- 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;

be load tested monthly;

nually; and

rly.

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.** Priory 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	• Define, update, and implement IT Strategy • Manage IT across the enterprise	• Align IT objectives and programs with enterprise objectives and strategies • Coordinate IT across the enterprise
Control	• Align IT, teams, with enterprise performance objectives • Control performance objectives • Control overall technology budget	• Define KP metrics based on overall enterprise objectives • Report performance status • Coordinate overall technology
Service		versus provider
Risk Managem		with ement
Business Processes	requirements • Follow IT System Development Methodology (SMD)	rise processes • Define and adjust IT standards and technologies
Strategic IT Initiatives	• Plan and manage strategic IT initiatives • Manage application portfolio • Manage IT projects	• Shift decisions to enterprise operational groups • Include enterprise process executive in IT governance
Enterprise Infrastructure & Applications	• Define standards and architecture • Coordinate (consolidate) IT processes across the enterprise	• Optimize services through a mix of internal and external services • Coordinate security and compliance
© 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

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

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

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

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

CIO
IT Infrastructure Policy Bundle

2020-02

Jancо Associates, Inc.

Table of Contents

This document contains the following policies:

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
- 24 months - https://www.e-janco.com/session/cart_x.aspx?p=SUB-094-24
- Individual Policies - https://www.e-janco.com/updateserviceindivdualpolicies.htm

Backup and Backup Retention Policy

Version 3.2

Table of Contents

Blog Personal Website Policy

2020 Edition

Jango Associates, Inc.

Table of Contents

BYOD Policy Template

Janco Associates, Inc.

Version 2.1

Table of Contents

Google Glass Policy Template

Version 1.3

Table of Contents

Incident Communication Plan Policy

JANCO ASSOCIATES, INC.

2020 Edition

Table of Contents

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

Jancq Associates, Inc.

2020 Edition

TABLE OF CONTENTS

Mobile Device Access & Use Policy

Janco Associates, Inc.

2020 Edition

Table of Contents

Policy – Outsourcing and Cloud-Based File Sharing

Version 3.3

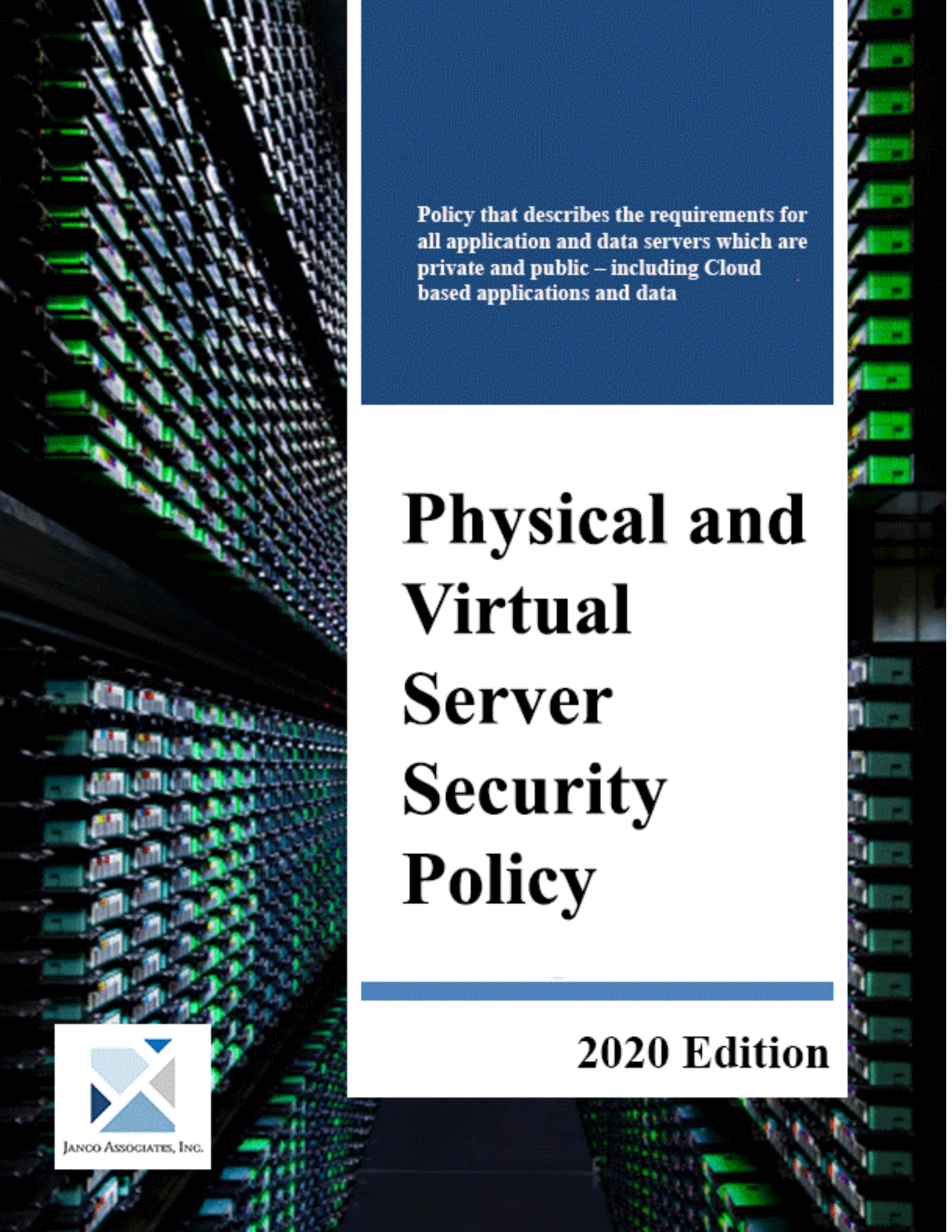
Table of Contents

Patch Management Version Control Policy

Janco Associates, Inc.

Version 2.3

Table of Contents



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

Janco Associates, Inc.

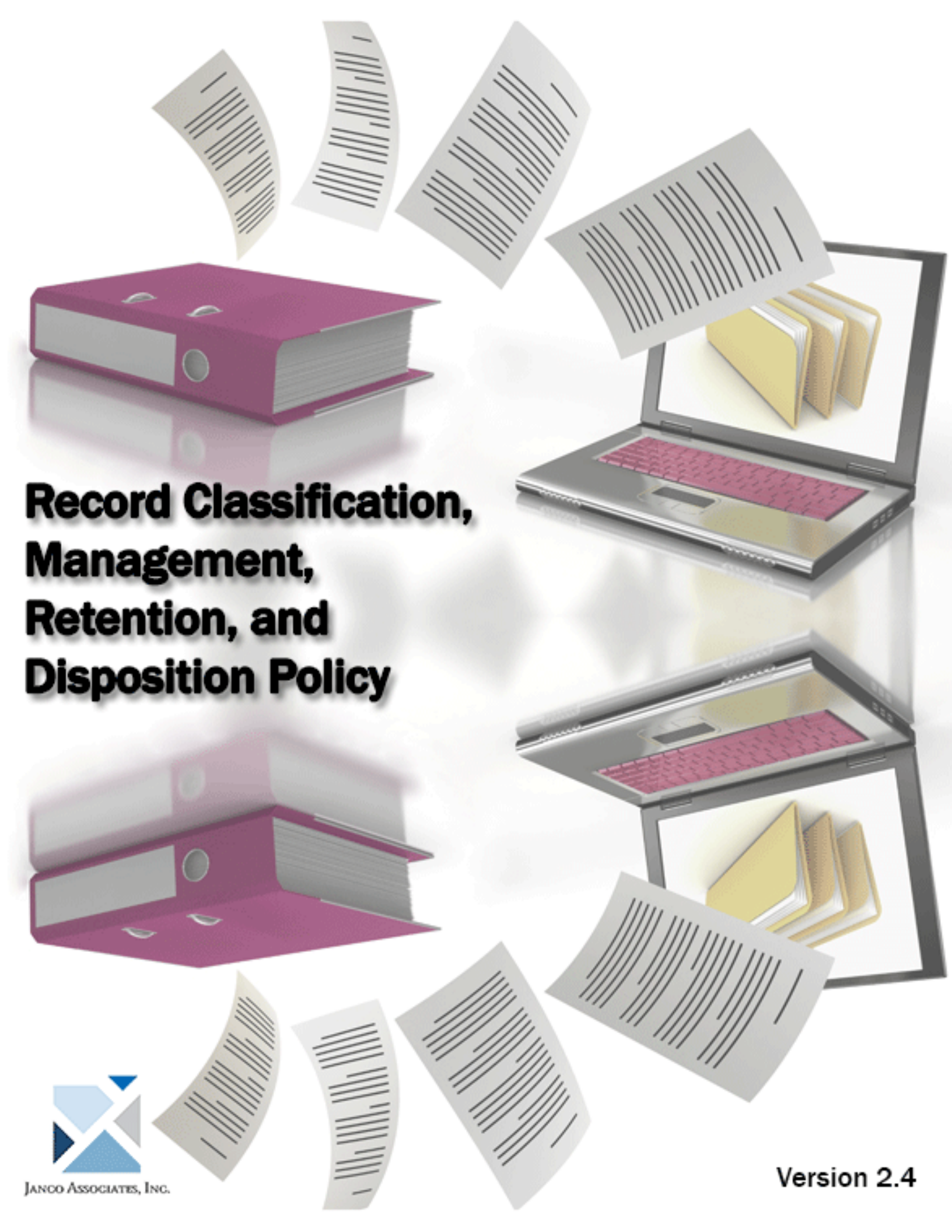
Table of Contents

Privacy Compliance Policy

Janco Associates, Inc.

2019

Table of Contents



Record Classification, Management, Retention, and Disposition Policy

Version 2.4

Janco Associates, Inc.

Table of Contents

Safety Program

Janco Associates, Inc.

2020

Table of Contents

Policy
Sensitive Information

Janco Associates, Inc.

2020 Edition

Table of Contents

Service Level Agreement Policy Template & Sample KPI Metrics

Version 2.2

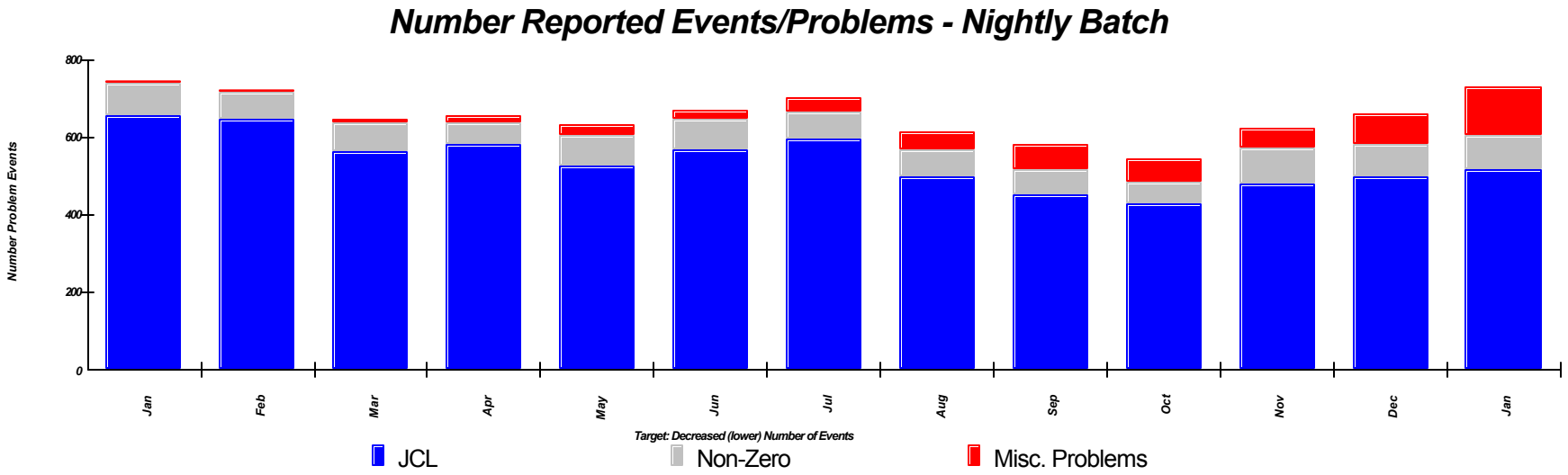
Jancc Associates, Inc.

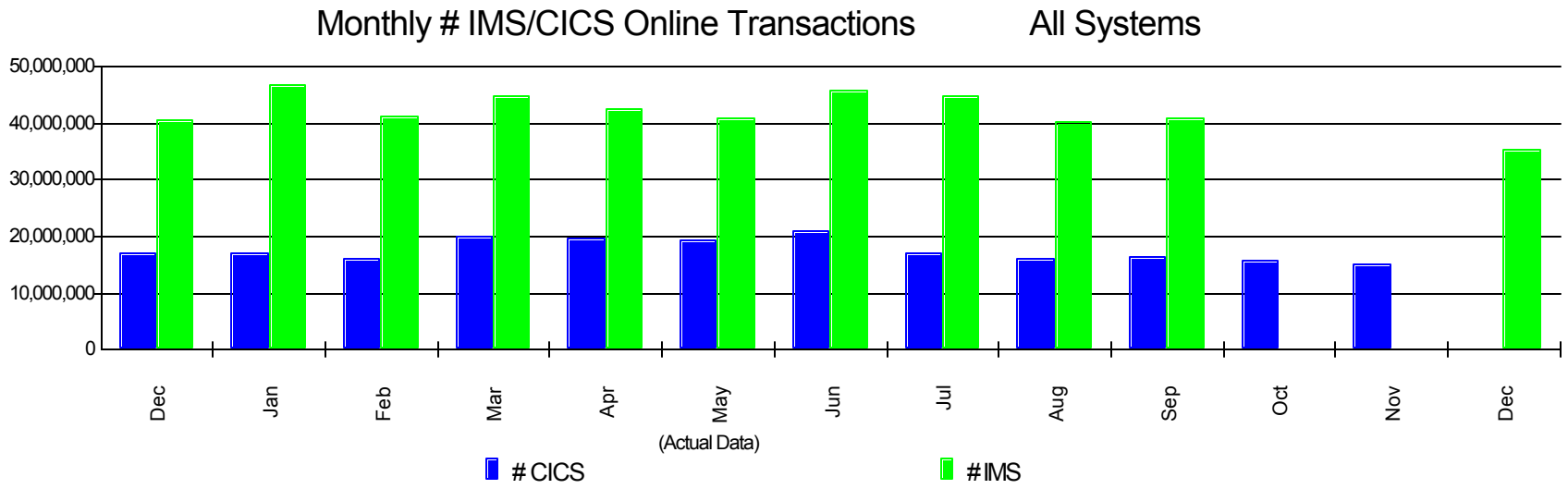
Table of Contents

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





Social Networking Policy

Managing and Controlling Employee Social Networks

Version 2.2

Table of Contents

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

Technology Acquisiton Policy

Version 1.1

Jayco Associates, Inc.

Technology Acquisition Policy

Table of Contents

Telecommuting Policy Template

Version 2.1

Table of Contents

Text Messaging Sensistive and Confidential Information Policy

JANCO ASSOCIATES, INC.

Version 1.3

Table of Contents

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

2020 Edition

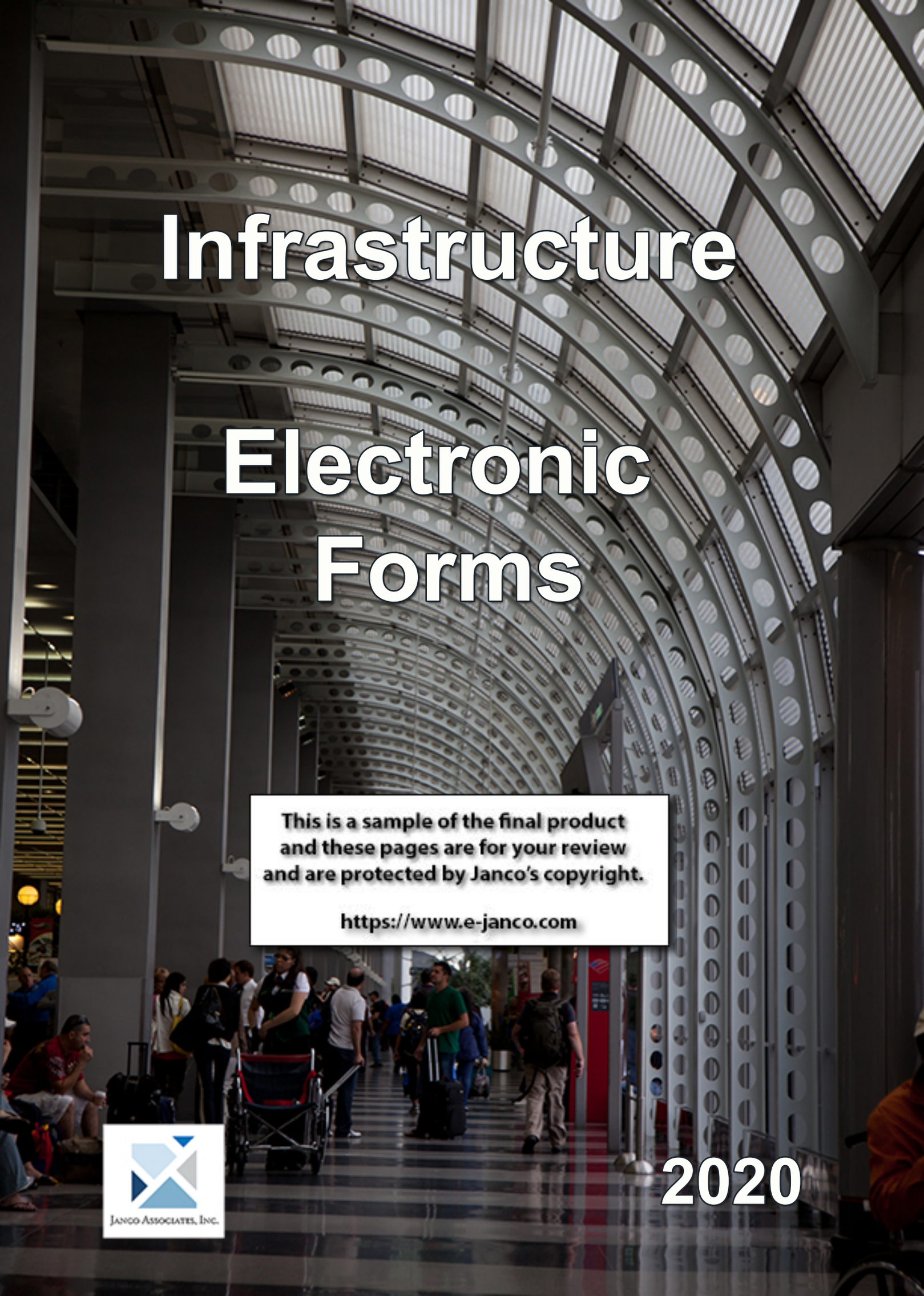
Janco Associates, Inc.

Table of Contents

Wearable Device Policy

Version 2.1

Table of Contents



Infrastructure Electronic Forms

Janco Associates, Inc.

2020

JANCO ASSOCIATES, INC.

Infrastructure Electronic Forms

Forms contained include

- Application & File Server Inventory[i]
- 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

[i] Partially electronic – currently work in process

Administrative Records

This Schedule applies to records in all media, unless otherwise specified.

- Items – a sample listing of items found within a series. Other related records not listed may also be part of a series.
- Disposition – all dispositions are minimum requirements and include, where applicable, transfer to the custody of ENTERPRISE Archives for appraisal and final disposition.
- Destruction – takes place in the office. Any record with confidential or sensitive information shall be properly destroyed by shredding or by means to ensure that the records cannot be physically recreated.
- Original and Reference Copy – original copy (also known as a record copy) is the official authorized copy kept by the office charged with creating or maintaining the record copy. Reference copies (also known as convenience copies) are preserved for the convenience of reference or ease of access.

No destruction of records may take place if litigation or audits are pending or reasonably anticipated or foreseeable.

Class ID	Class Title	Class Description	Items	Disposition

JANCO ASSOCIATES, INC.

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 f… …nty jurisdictions; driving records, birth records, an…

I further authorize any in… …e any and all information, verbal or wr… …ther authorize the complete release of any r… …, 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.

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.

JANCO ASSOCIATES, INC.

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

☐ liate)

☐ d)

Signature _____ Date Click here to enter a date.

Approval Process

Supervisor _____

☐ **Approved**

Email Address _____

Comments

IT Department _____

☐ **Approved**

User Level

☐ **Basic user**

☐ **Supervisor**

☐ **Manager**

☐ **Administrator**

JANCO ASSOCIATES, INC.

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
☐
☐
☐
☐
☐
☐
☐
☐
☐
☐

Signature _____

Supervisor Name _____

Position Title _____

Company Name _____

Email Address _____

Phone Number _____

JANCO ASSOCIATES, INC.

Mobile Device Access and Agreement

Employee Name _____ ID Number _____

Job Title _____ Location _____

Employee agrees to adhere to the Mobile Device Access and Use Policy	☐ Yes	☐ No
ENTERPRISE concurs with employee participation and agrees to support the approved mobile devices	☐ Yes	☐ 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	☐ Yes	☐ 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 i
- The ENTERPR y other incidental co e as an alternate wo

Confidentiality/Security

- The employe m unauthorized disclosure or damage and 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*

JANCO ASSOCIATES, INC.

Mobile Device Security and Compliance Checklist

Employee Name _____ ID Number _____

Job Title _____ Location _____

Device Type ☐Phone ☐Tablet ☐Other Description _____

Security Controls

Yes	No	
☐	☐	256 bit AES encryption per file at rest, 30-day rotating encryption key
☐	☐	256 bit SSL encryption data transfer
☐	☐	SSAE 16 Type II compliant, redundant data centers and DR policy
☐	☐	99.9% SLA Uptime Guarantee

Remote Device Management

Yes	No	
☐	☐	Auto-timed screen logout on mobile devices
☐	☐	Custom 4-digit pass code
☐	☐	Immediate access restriction on device
☐	☐	Auto login to end user accounts for remote wipe

Access Management Controls

Yes	No	

Compliance

and use forms

☐	☐	Is this device included in the Disaster Recovery Business Continuity Plan
☐	☐	Does this device meet the compliance requirements for the record management process
☐	☐	Has the user of this device completed all necessary training

Audit Trail

Yes	No	
☐	☐	All global files can be accessed directly from central admin console
☐	☐	Usage statistics tracked for files, individual users and groups
☐	☐	Complies with record management policy
☐	☐	Downloads, uploads, previews
☐	☐	Tracked by IP Address

Employee Signature *Date*

OSHA's Form 300 (Rev. 01/2004)

Log of Work-Related Injuries and Illnesses

Attention: This form contains information relating to employee health and must be used in a manner that protects the confidentiality of employees to the extent possible while the information is being used for occupational safety and health purposes.

Year _____

U.S. Department of Labor
Occupational Safety and Health Administration

You must record information about every work-related injury or illness that involves loss of consciousness, restricted work activity or job transfer, days away from work, or medical treatment beyond first aid. You must also record significant work-related injuries and illnesses that are diagnosed by a physician or licensed health care professional. You must also record work-related injuries and illnesses that meet any of the specific recording criteria listed in 29 CFR 1904.8 through 1904.12. Feel free to use two lines for a single case if you need to. You must complete an injury and illness incident report (OSHA Form 301) or equivalent form for each injury or illness recorded on this form. If you're not sure whether a case is recordable, call your local OSHA office for help.

Form approved OMB no. 1218-0176

Establishment name _____

City _____ State _____

Identify the person				Describe the case		Classify the case											
						CHECK ONLY ONE box for each case based on the most serious outcome for that case:				Enter the number of days the injured or ill worker was:		Check the "injury" column or choose one type of illness:					
(A) Case No.	(B) Employee's Name	(C) Job Title (e.g., Welder)	(D) Date of injury or onset of illness (mo./day)	(E) Where the event occurred (e.g. Loading dock north end)	(F) Describe injury or illness, parts of body affected, and object/substance that directly injured or made person ill (e.g. Second degree burns on right forearm from acetylene torch)	Death	Days away from work	Remained at work		Away From Work (days)	On job transfer or restriction (days)	(M) Injury	Skin Disorder	Respiratory Condition	Poisoning	Hearing Loss	All other illnesses
								Job transfer or restriction	Other record-able cases								
						(G)	(H)	(I)	(J)	(K)	(L)	(1)	(2)	(3)	(4)	(5)	(6)
					Page totals	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*

Be sure to transfer these totals to the Summary page (Form 300A) before you post it.

	Injury	Skin Disorder	Respiratory Condition	Poisoning	Hearing Loss	All other illnesses
	(1)	(2)	(3)	(4)	(5)	(6)

Public reporting burden for this collection of information is estimated to average 14 minutes per response, including time to review the instruction, search and gather the data needed, and complete and review the collection of information. Persons are not required to respond to the collection of information unless it displays a currently valid OMB control number. If you have any comments about these estimates or any aspects of this data collection, contact: US Department of Labor, OSHA Office of Statistics, Room N-3644, 200 Constitution Ave, NW, Washington, DC 20210. Do not send the completed forms to this office.

PANDEMIC PLANNING CHECKLIST

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

Janco Associates, Inc.

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 w other job titles/descriptions,	ress ○ Completed
Develop and plan for scenari decrease in demand for your pandemic (e.g. effect of a rest hygiene supplies).	ress ○ Completed
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

JANCO ASSOCIATES, INC.

Risk Assessment Matrix

Location _____ Function _____

Department _____ Manager _____

	High = 5	4	3	2	Low = 1	Score
Organizational Uncertainty	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	
Technical Uncertainty	No knowledge or experience	Emerging area	Some experience	Understood in a different area	Understood	
Skills Required	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	
Hardware Dependencies	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	
Software Dependencies	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	
Application Software	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	
Total Technical Uncertainty Score						
Infrastructure Uncertainty	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	
Total Risk Score						

JANCO ASSOCIATES, INC.

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)	☐YES	☐NO
• Printer	☐YES	☐NO
• Microphone / headset	☐YES	☐NO
• Camera for video conference	☐YES	☐NO
• Scanner	☐YES	☐NO
• Shredder	☐YES	☐NO
Communication Requirements		
• Landline – linked to enterprise auto attendant	☐YES	☐NO
• Internet broadband	☐YES	☐NO
• VPN	☐YES	☐NO
• Email	☐YES	☐NO
• Instant Messaging	☐YES	☐NO
• File Sharing	☐YES	☐NO
• Records retention and destruction policies	☐YES	☐NO
Security and Compliance Requirements		
• Two factor access (password plus biometrics)	☐YES	☐NO
• Enciphering	☐YES	☐NO
• Disaster Recovery Business Continuity plan	☐YES	☐NO
• Physical Security of all electronic assets located remotely	☐YES	☐NO
• User access to admin functions blocked	☐YES	☐NO
• Media copying blocked (CD/DVD/USB connectivity)	☐YES	☐NO
• Training for telecommuter	☐YES	☐NO
Other Considerations		
• Reimbursement policy for telecommuters work related expenses	☐YES	☐NO
• Policy for non-business use of enterprise assets	☐YES	☐NO
• Inventory of data and enterprise physical assets	☐YES	☐NO
• Rules for audit and termination procedures for employees	☐YES	☐NO

Employee Signature *Date*

Supervisor *Date*

JANCO ASSOCIATES, INC.

Telecommuting Work Agreement

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

Employee Signature *Date*

Supervisor *Date*

Employee agrees to participate in telecommuting and to adhere to applicable guidelines and policies. This is not a guarantee of continued employment.	☐YES	☐NO
Employee agrees to participate in telecommuting for an initial period not to exceed one year, beginning _____ and ending _____. 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.	☐YES	☐NO
ENTERPRISE concurs with employee participation and agrees to adhere to applicable guidelines and policies.	☐YES	☐NO
Copies of the ENTERPRISE Telecommuting Policy and Record Management have been given to and read by the employee.	☐YES	☐NO

Work Location – Schedule

Employe

Employe

Describe

At the ce to

on the fo

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

Dept. Head _____ ☐ **Approved**

Signature _____

Comments

Date:

IT Department _____

☐ **Approved**

User Level

☐ **Basic user**

☐ **Supervisor**

☐ **Manager**

☐ **Administrator**

JANCO ASSOCIATES, INC.

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	☐ Yes	☐ No
ENTERPRISE concurs with employee need to text message sensitive and/or confidential information	☐ Yes	☐ No
Copies of the ENTERPRISE Text Messaging Sensitive and Confidential Information and Record Management Policy have been given to and read by the employee	☐ Yes	☐ 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

for servicing and maintaining
ns to ENTERPRISE's text
y.

ee's personal or real property
prise equipment in the
employee's residence.

- 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 F ◯ ◯ No

Category II - High Fina ◯ ◯ No

Category III - Medium ◯ ◯ 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%
Catastrophic					
Very High					
Noticeable to ENTERPRISE					
Minor					
None					

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

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

JANCO ASSOCIATES, INC.

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	☐ Yes	☐ No
ENTERPRISE concurs with employee participation and agrees to support the approved mobile devices	☐ Yes	☐ 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	☐ Yes	☐ No

Equipment/Expenses

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

sonal or real property during the course of
nt in the employee's residence.

aintenance, or any other incidental costs
sidence as an alternate work location.

ntal costs associated with connectivity
se 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*