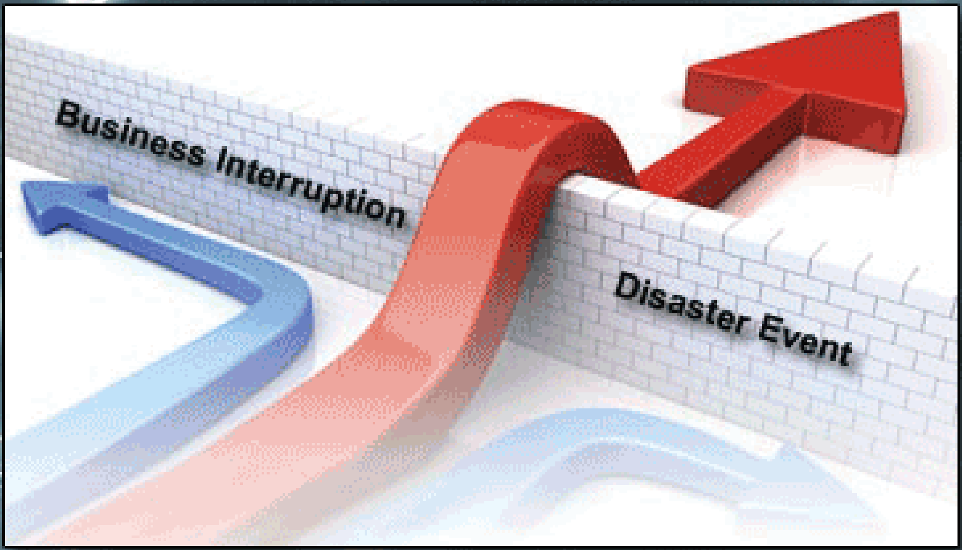


Disaster Recovery Business Continuity Template

2024

Janco Associates, Inc.

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:

critical

- Document Training & Maintenance Procedures

These steps represent the effort required in the preparation of the ENTERPRISE Disaster Recovery Plan.

1.1 Recovery Life Cycle - After a "Major Event"

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 priority will be survival, which involves physiological factors such as the 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.

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 for 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:

agement

at requires

anage

As a general rule, to test BCP/DR compliance within an organization, a team of qualified, knowledgeable internal auditors should be created, reporting to a different member of the board than the BCP team reports to. This team of internal auditors should test to ensure that the BCP plan and process meet the compliance requirements discussed in the following sections.

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

  Many legally mandated and standards-mandated issues 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 need to be considered in the plan.

- **Sarbanes-Oxley**

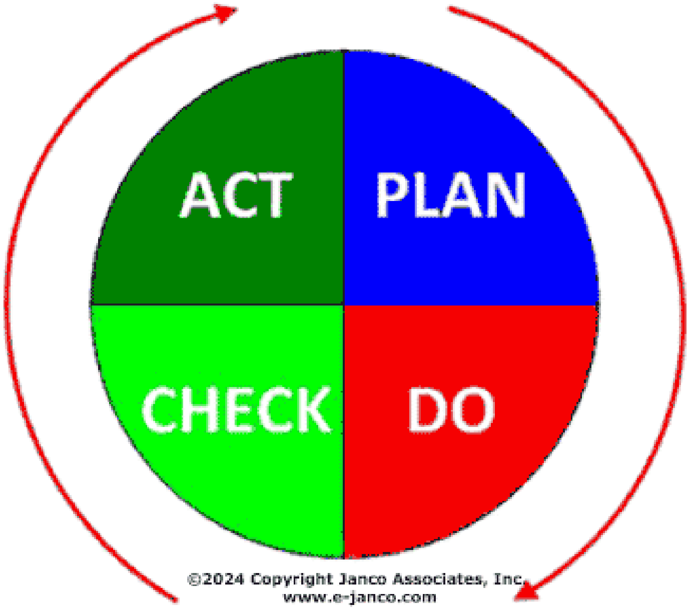
  With the rise of both financial (Sarbanes- Oxley for SEC – US Security and Exchange Commission) and industry ITIL (Version 3 of the Information Technology Infrastructure Enterprise) standards, specific additional

[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.

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 affects 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.



- **Plan** - Establish a Disaster Recovery Business Continuity policy. with objectives, metrics, and processes relevant to managing risk and improving Information and Communication Technology's ability and readiness to operate at the level
  recovery and

  ss Continuity

  d by the Disaster
  municate the

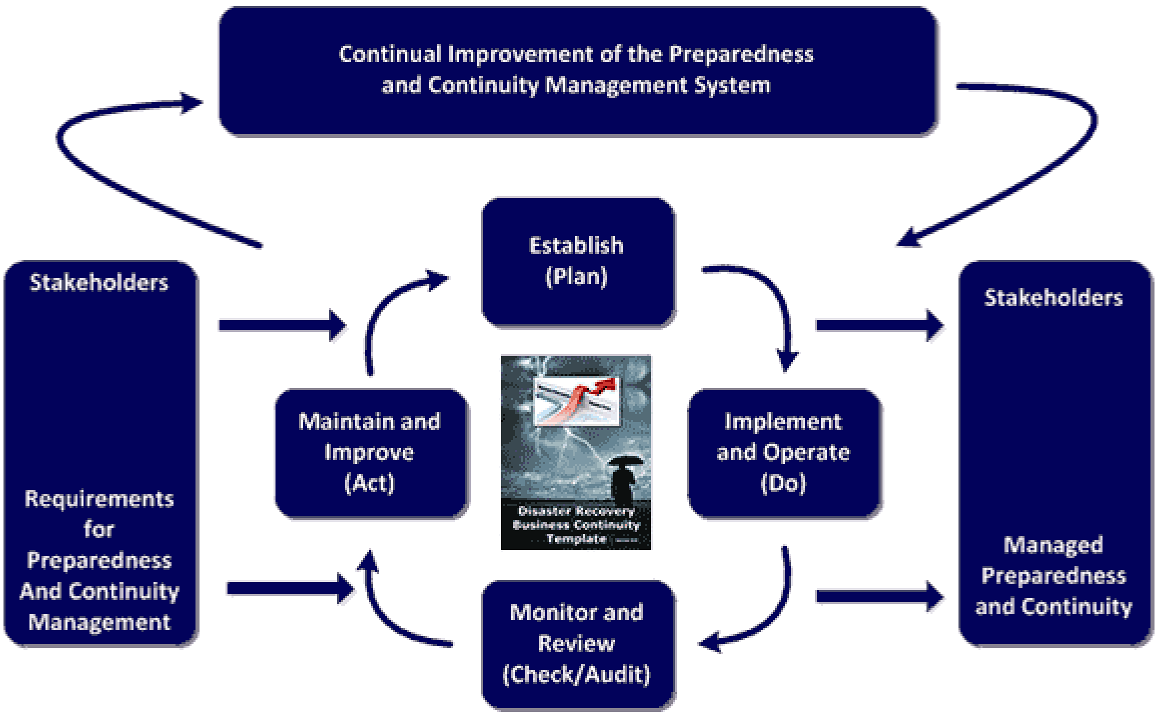
- **Act** - Modify the Disaster Recovery and Business Continuity policies, procedures, and metrics based on the "Check" to improve the Disaster Recovery and Business Continuity Policy.

ISO 22301

ISO 22301 is the latest ISO Business Continuity standard. It is called "Societal security – Business continuity management systems – Requirements". Although societal security may sound a little strange with business continuity, here is how ISO defines it: … standardization around societal security, aimed at increasing crisis management and business continuity capabilities, i.e. through improved technical, human, organizational, and functional interoperability as well as shared situational awareness, amongst all interested parties.

Janco Disaster Recovery Business Continuity Template

Compliance with ISO 22301 Business Continuity Standard


Continual Improvement of the Preparedness and Continuity Management System
Stakeholders
Requirements for Preparedness And Continuity Management
Establish (Plan)
Maintain and Improve (Act)
Disaster Recovery Business Continuity Template
Implement and Operate (Do)
Monitor and Review (Check/Audit)
Stakeholders
Managed Preparedness and Continuity

ISO 28000

ISO 28000:2007 is necessary for the support of an organization implementing and

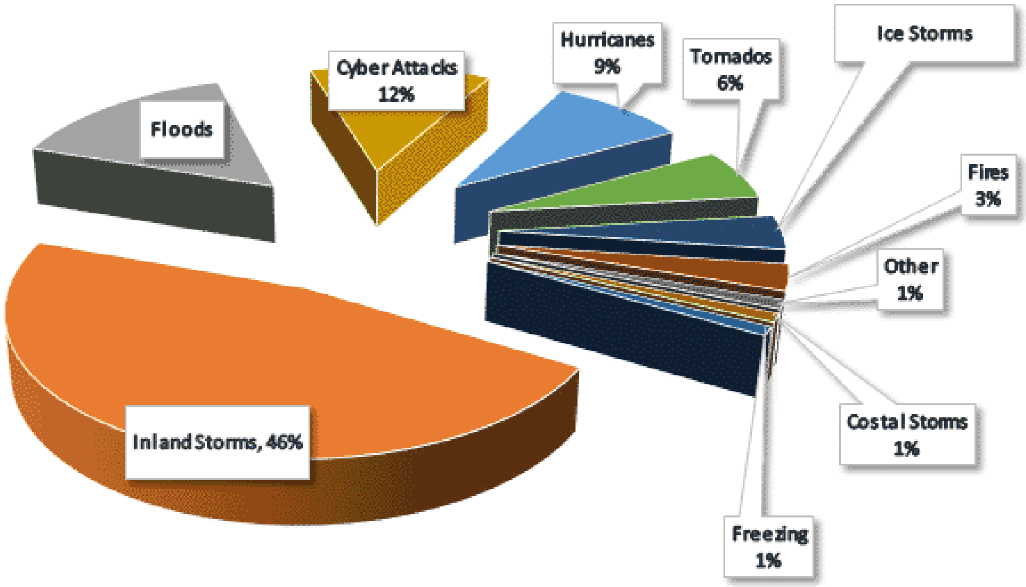
nfrastructure,

s become a

tinuity

"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

Events Causing Disasters



© 2024 Copyright Janco Associates, Inc. – https://e-janco.com

Look at the impact of an event:

- Lost revenue: Even the loss of a single mission-critical service, such as e-mail or

in revenue.

recovery plan in

ption in services

firm's viability in

sonal

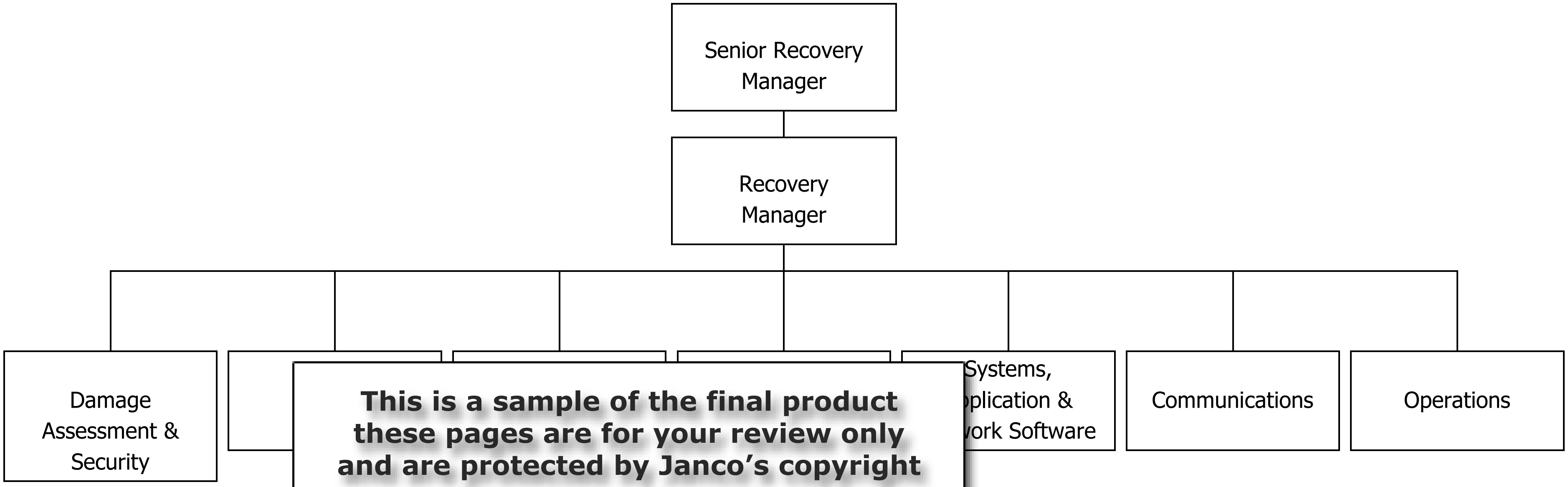
sses found to be

in a state of noncompliance could be subjected to lawsuits, fines, and penalties.

- Staff confidence and effectiveness: As technology becomes an even greater part of business operations, users have come to rely more and more on services and technologies to do their jobs. When those services or technologies become unavailable, even for short periods, users suffer major productivity losses. In addition to the direct costs of lost productivity, long-term damage can result in low staff morale and confidence in the organization, extending the monetary damages well into the future, even after services have been restored.

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 ongoing operations	• The most expensive options are duplicate equipment and software plus ongoing version control issues • Ongoing communication costs to duplicate data are very high • The 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 meet 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 ongoing operations	• The most expensive options are duplicate equipment and software plus ongoing version control issues • Ongoing communication costs to duplicate data are very high	If costs can be shared among multiple facilities within the enterprise, internal provisioning can be 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	• Moderately priced • Basic infrastructure is in place to support recovery operations • Ability imple hardw softwa comm	• Not easy to test • Recovery time is longer than with a hot site and is controlled by the time to locate and restore applications	If costs can be shared among multiple facilities within the enterprise, internal provisioning can be cost-competitive with commercial alternatives. riate secondary space is available " facilities providers offer sed-floor space at very attractive lternative to building out tes.
Mobile Site	24 to 48 Hours	• Mode • Typica 72 hou • Can be placed in the "parking lot" adjacent to your impacted facility	be hindered because of the event • A trailer may not be configured exactly as you need it	h avoids employee travel issues ations on equipment availability d bandwidth if small aperture inal (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 a lower cost	• Longest recovery time • All equipment must be ordered, delivered, installed, and made operational • Worst solution for supporting ongoing 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 of disasters 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 are 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 to maintain 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 coordination of the Disaster Recovery Plan is the responsibility of the Disaster Recovery Manager.

7.1 Disaster Recovery Manager

The function of the Disaster Recovery Manager is critical to maintaining the plan in a
eted. Not only does
intenance of the plan,
nt of a computer
n and conducts

- 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 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 separate files that contain 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**
- **Work From Home Contact Information**

8.02 Safety Program Forms – Electronic Forms

During the recovery period from the disaster safety of all individuals and organizations involved is a primary concern. Attached are all electronic forms from a Safety Program created by Janco to facilitate this.
See https://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 comply 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**
- **Chief Compliance Officer**
- **Chief Experience Officer**
- **Chief Mobility Officer**
- **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**
- **WFH and Telecommuting PolicyPolicy**

8.06 Other Attachments

- **Disaster Recovery Business Continuity Audit Program**

9.15 Colocation Checklist

One of the options in Disaster Recovery Planning is to have a colocation facility for operations when a disaster or other critical event occurs. This checklist helps enterprise management validate that important questions that will affect colocation services and your eventual commitment are asked and answered.

- Space - How many cabinets and/or racks do you require to hold your equipment?
- Power - How much power in kW do you require for each footprint? Be sure to consider your current power usage as well as planned future usage.
- Location
    - Is the location of the data center strategically beneficial to your business?
    - Does the provider have multiple geographically diverse sites to support future business expansion or disaster recovery site options?
- Resiliency - What precautions are in place to protect the data center from natural disasters and other threats?
- Security & Protection - What security measures does the facility have in place to control access to your footprint?
- Carrier Diversity

?

eet Me Rooms?

figurations?

use the facility?

    - What percentage of capacity is contracted for already and potentially?
- Hybrid Capabilities
    - Is the data center designed to accommodate hybridization?
    - While many organizations do not require this initially, the ability to hybridize across different environments often becomes important as the business scales.
- Service Level Agreement (SLA) - What level of availability does the provider guarantee? Do they offer proactive credits for SLA violations?
- Compliance
    - Is the facility audited by a third party?
    - If so, how often?
    - Does the provider offer access to the report?
- Cost - Does this facility offer the right combination of price and performance for your future infrastructure needs?
- Support
    - Is technical support available 24/7?
    - What is the process for addressing support issues?
- Amenities - Does the facility offer workspace and conference rooms to enable productivity for your employees?
- Environment - Does the provider adhere to energy-efficient industry standards (LEED, ENERGY STAR, Green Globes)?

10.0 Change History

2024

- Added Job Description
    - Chief Experience Officer
- Updated implications of new mandated requirements including 28000 – Supply Chain Management
- Updated all included 2024 electronic forms
- Updated all included 2024 job descriptions
- Updated all included latest infrastructure policies

2023 Update

- Added Job Descriptions
    - Chief Compliance Officer
    - Chief Mobility Officer

2023

- Updated implications of new mandated requirements including 28000 – Supply Chain Management
- Updated all included 2022 electronic forms
- Updated all included 2022 job descriptions
- Updated all included latest infrastructure policies

2022

- Updated all included 2022 electronic forms
- Updated all included 2022 job descriptions
- Updated all included latest infrastructure policies
- Updated to address WFH implications
- Added WFH & Telecommuting Policy

2021

- Updated to include the option for DR/BC via the cloud
- Updated all included electronic forms
- Updated all included job descriptions
- Updated all included infrastructure policies
- Updated to address WFH implications