

CHEMICAL SPILL > MIND STORM > FIRE > HURRICANE > BLACK OUT > FLOOD > EARTHQUAKE > ICE STORM  
FACILITY OUTAGE > GAS LEAK > DATABASE CORRUPTION > LIGHTNING > TERROR ALERT > TORNADO > SMOKE

# Disaster Recovery & Business Continuity Template

ISO 22301, 27000, 27031, Sarbanes-Oxley, HIPAA,  
PCI DSS, COBIT, and ITIL Compliant

Prepared by

## Janco

Associates, Inc.

Park City, UT 84060

email - [support@e-janco.com](mailto:support@e-janco.com)

Web sites – <http://www.e-janco.com> - <http://www.it-toolkits.com> -- <http://www.itproductivity.org>

Version 7.1

© 2012 Copyright Janco Associates, Inc. ALL RIGHTS RESERVED

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

[www.e-janco.com](http://www.e-janco.com)

CHEMICAL SPILL > MIND STORM > FIRE > HURRICANE > BLACK OUT > FLOOD > EARTHQUAKE > ICE STORM > SMOKE  
FACILITY OUTAGE > GAS LEAK > DATABASE CORRUPTION > LIGHTNING > TERROR ALERT > TORNADO > SMOKE DAN

# Table of Contents<sup>1</sup>

<b>1.0 Plan Introduction .....</b>	<b>5</b>
1.1 Mission and Objectives .....	6
Compliance .....	6
ISO Compliance Process.....	11
ISO 27031 Overview.....	13
ISO 23301.....	16
1.2 Disaster Recovery / Business Continuity Scope.....	17
1.3 Authorization.....	17
1.4 Responsibility .....	17
1.5 Key Plan Assumptions .....	18
1.6 Disaster Definition .....	19
1.7 Metrics .....	19
1.8 Disaster Recovery / Business Continuity and Security Basics.....	21
Server Requirements .....	21
Network .....	22
Clients .....	23
Recovery Procedures .....	23
Communication.....	23
Role of Social Networking.....	23
Designated operators .....	24
Designated manager .....	24
External resources .....	24
Insurance .....	25
<b>2.0 Business Impact Analysis.....</b>	<b>26</b>
2.1 Scope .....	26
2.2 Objectives .....	27
2.3 Analyze Threats .....	27
2.4 Critical Time Frame.....	28
2.5 Application System Impact Statements .....	28
Essential .....	29
Delayed .....	29
Suspended .....	29
2.6 Information Reporting.....	30
2.7 Best Data Practices .....	31
2.8 Summary .....	32

---

NOTE – Due to incompatibilities between WORD 2003 and WORD 2007 you may need to regenerate the Table of Contents. The Table of Contents was generated using WORD 2007 and if you use this document in any version other than WORD 2007 you will have to update the Table of Contents and all update fields which link to unique pages in this template.

<b>3.0 Backup Strategy .....</b>	<b>33</b>
3.01 Site Strategy .....	33
3.02 Data Capture and Backups .....	35
Backup Strategy .....	36
3.03 Backup and Backup Retention Policy .....	37
Policy .....	37
Applicability .....	37
Backup Versus Archive .....	37
Types of Backups .....	39
Storage Management .....	40
Minimal Backup Policy .....	40
System Specific Backup Policy .....	43
3.04 Communication Strategy and Policy .....	47
DRP / BCP Communication Policy .....	47
Communication with Employees .....	48
Social Networks .....	49
What to Communicate .....	50
3.05 ENTERPRISE Data Center Systems .....	50
Backup Files .....	50
Storage Rotation .....	50
3.06 Departmental File Servers .....	51
Backup Files .....	51
Storage Rotation .....	51
3.07 Wireless Network File Servers .....	53
Backup Files .....	53
Storage Rotation .....	53
3.08 Data at Outsourced Sites (including ISP's) .....	55
Backup Files .....	55
Storage Rotation .....	55
3.09 Branch Offices (Remote Offices & Retail Locations) .....	57
Backup Files .....	57
Storage Rotation .....	57
3.10 Desktop Workstations (In Office) .....	59
Backup Files .....	59
Storage Rotation .....	59
3.11 Desktop Workstations (Off site including at home users) .....	61
Backup Files .....	61
Storage Rotation .....	61
3.12 Laptops .....	63
Backup Files .....	63
Storage Rotation .....	63
3.13 PDA's and Smartphones .....	65
Backup Files .....	65
<b>4.0 Recovery Strategy .....</b>	<b>67</b>
4.1 Approach .....	67
4.2 Escalation Plans .....	68
4.3 Decision Points .....	69

<b>5.0 Disaster Recovery Organization .....</b>	<b>73</b>
5.1 Recovery Team Organization Chart.....	74
5.2 Disaster Recovery Team .....	76
5.3 Recovery Team Responsibilities .....	77
5.3.1 Recovery Management .....	77
5.3.2 Damage Assessment and Salvage Team .....	79
5.3.3 Physical Security .....	80
5.3.4 Administration .....	81
5.3.5 Hardware Installation .....	82
5.3.6 Systems, Applications and Network Software .....	83
5.3.7 Communications .....	84
5.3.8 Operations .....	85
<b>6.0 Disaster Recovery Emergency Procedures .....</b>	<b>86</b>
6.1 General .....	87
6.2 Recovery Management .....	88
6.3 Damage Assessment and Salvage .....	90
6.4 Physical Security .....	93
6.5 Administration .....	95
6.6 Hardware Installation .....	96
6.7 Systems, Applications & Network Software .....	98
6.8 Communications.....	100
6.9 Operations.....	101
<b>7.0 Plan Administration .....</b>	<b>102</b>
7.1 Disaster Recovery Manager.....	102
7.2 Distribution of the Disaster Recovery Plan.....	103
7.3 Maintenance of the Business Impact Analysis .....	104
7.4 Training of the Disaster Recovery Team.....	104
7.5 Testing of the Disaster Recovery Plan .....	105
7.6 Evaluation of the Disaster Recovery Plan Tests .....	107
7.7 Maintenance of the Disaster Recovery Plan .....	108
<b>8.0 Appendix.....</b>	<b>110</b>
8.01 Disaster Recovery – Business Continuity Plan Distribution.....	111
8.02 Disaster Recovery – Business Continuity Remote Location Contact Information .....	112
8.03 Disaster Recovery – Business Continuity Team Call List.....	113
8.04 Disaster Recovery – Business Continuity Team Vendor Contacts .....	114
8.05 Disaster Recovery – Business Continuity Off-Site Inventory .....	115
8.06 Disaster Recovery – Business Continuity Personnel Location Form.....	116
8.07 Disaster Recovery – Business Continuity LAN Hardware/Software Inventory .....	117
8.08 People Interviewed .....	118
8.09 Preventative Measures.....	119
8.10 Sample Application Systems Impact Statement.....	120
8.11 JOB Descriptions.....	121
Disaster Recovery Manager .....	121
Manager Disaster Recovery and Business Continuity.....	123
Pandemic Coordinator .....	125
8.12 Application Inventory and Business Impact Analysis Questionnaire .....	128
8.13 Key Customer Notification List .....	150
8.14 Resources Required for Business Continuity.....	152

8.15	Critical Resources to Be Retrieved .....	153
8.16	Business Continuity Off-Site Materials.....	155
8.17	Work Plan .....	157
8.18	Audit Disaster Recovery Plan Process .....	161
	Audit Program.....	162
8.19	Vendor Disaster Recovery Planning Questionnaire .....	163
8.20	Departmental DRP and BCP Activation Workbook .....	173
	Planned Activities for the Period .....	185
	Accomplished Planned Activities .....	185
	Planned Activities Not Accomplished .....	185
	Unplanned Activities Performed or Identified .....	185
8.21	Web Site Disaster Recovery Planning Form .....	188
8.22	General Distribution Information.....	192
	What to do after an Explosion - Terrorist Attack.....	193
	How to Clean Up After a Disaster .....	194
8.23	Business Pandemic Planning Checklist .....	196
	Plan for the impact of a pandemic on your business.....	196
	Plan for the impact of a pandemic on your employees and customers .....	197
	Establish policies to be implemented during a pandemic .....	198
	Allocate resources to protect your employees and customers during a pandemic .....	198
	Communicate to and educate your employees.....	199
	Coordinate with external organizations and help your community: .....	199
8.24	Disaster Recovery Sample Contract .....	200
	Overview .....	200
	Prerequisites .....	201
	Alignment.....	202
	3c. Backup facilities.....	203
	Provisions.....	204
	4c. Computer equipment.....	205
	4d. Specialist requirements .....	207
	Termination Procedure.....	208
	Responsibilities .....	208
	Testing the Plan .....	209
8.25	Incident Communication Plan .....	210
	Overview .....	210
	Objective.....	210
	Guidelines .....	211
	News Conference Best Practices .....	214
	Media Relations Best Practices.....	215
<b>8.26</b>	<b>Social Networking Checklist .....</b>	<b>216</b>
	Creating Twitter Accounts .....	216
	Creating LinkedIn account .....	217
	Creating and operating a blog .....	218
<b>9.0</b>	<b>Change History .....</b>	<b>221</b>

---

## 1.0 Plan Introduction

ENTERPRISE recognizing their operational dependency 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
- Document Recovery Team Responsibilities
- Develop and Document Emergency Procedures
- Document Training & Maintenance Procedures

These steps were conducted and this document represents the completed effort in the preparation of the ENTERPRISE Disaster Recovery Plan.

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

[www.e-janco.com](http://www.e-janco.com)

---

## 1.1 Mission and Objectives

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

- Recover the physical network within the Critical Time Frames<sup>2</sup> established and accepted by the user community
- Recover the applications within the Critical Time Frames established and accepted by the user community
- Minimize the impact on the business with respect to dollar losses and operational interference

---

### Compliance

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

- COSO requires data center operation controls and transaction management controls in order to ensure data integrity and availability.
- ISO 1799 has a section entitled Business Continuity Management that requires testing, maintaining, and reassessing a business continuity plan.
- ISACA's COBIT requires uninterruptible power supplies under its Manage Facilities section.
- NIST requires contingency and continuity plans and management.

As a general rule, in order 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*

There<sup>3</sup> are a number of legally mandated and standards mandated issues that need to be covered in the Disaster Recovery / Business Continuity Planning Process.

---

<sup>2</sup> Critical time frames include both the point in time that the recovery will be set to and the point in time that the recovery will be completed and the enterprise can be back in operation.

<sup>3</sup> This section is for informational purposes and can be excluded from the plan.

---

### 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 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, processes relevant to managing risk and improving Information and Communication Technology's ability and readiness to operate at the level defined within the parameters of the enterprises overall disaster recovery and business continuity objectives.
- **Do** - Implement and operate the Disaster Recovery and Business Continuity policies, procedures, controls an processes.
- **Check** - Assess and monitor the performance metrics as defined within the Disaster Recovery and Business Continuity policy and metrics and communicate the results to the management of the enterprise.
- **Act** - Modify the Disaster Recovery and Business Continuity policies, procedures and metrics based on the "Check" in order to improve the Disaster Recovery and Business Continuity Policy.

## **Requirements**

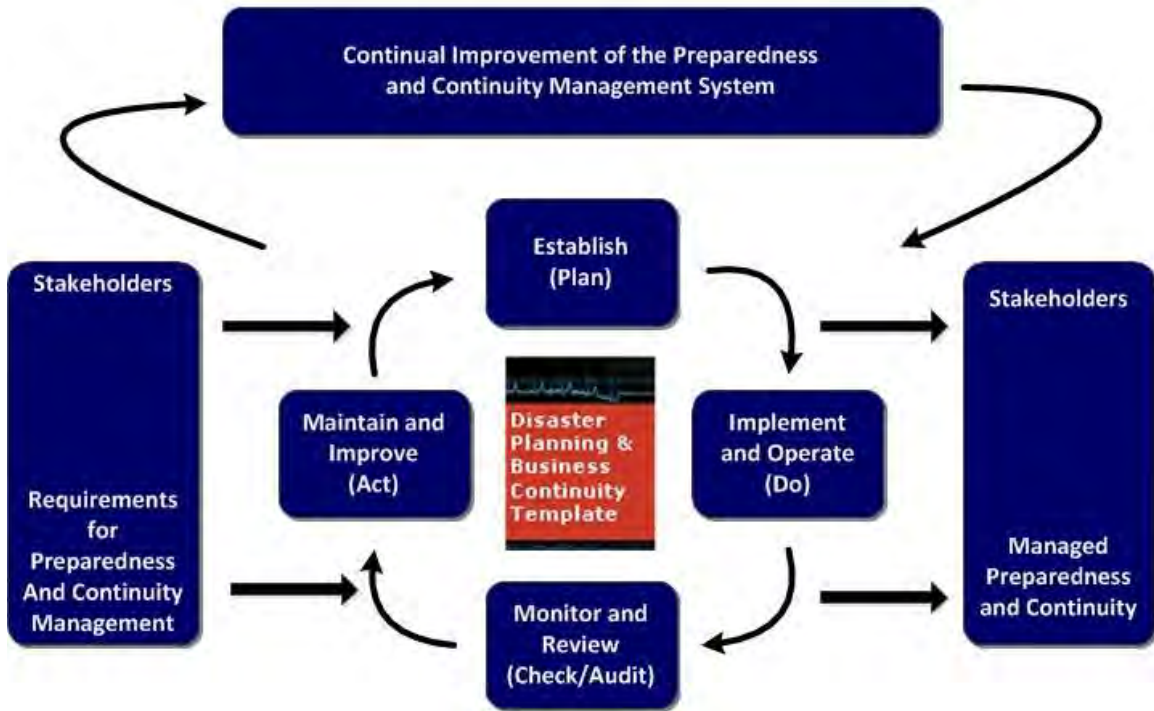
In order to be compliant with ISO 27031 there are a number of elements that that are required and this template meets all of those requirements.

- Staffing with appropriate skills, knowledge, and execution ability
  - Organization Chart (Section 5)
  - Plan Distribution (Appendix)
  - DRP Management Job Descriptions (Appendix)
  - Disaster Recovery Team List (Appendix)
  - Key Customer Contact List (Appendix)
  - Personnel Location List (Appendix)
  - Detail Job Descriptions for 15 key team members (Premium Edition of the template)
- Facilities for both the existing and recovery operation
  - Operational Facilities (Section 3 and Appendix)
  - Recovery Facilities (Appendix – Sample Contract)
  - Off-Inventory (Appendix)
- Technology definition
  - Hardware – Hardware Inventory (Section 3 and Appendix)
  - Network – Network Inventory (Section 3 and Appendix)
  - Software – Software Inventory (Section 3 and Appendix)
  - Resources required for continuity process (Appendix)
  - Business Continuity off-site materials (Appendix)
  - Critical Resources to be retrieved (Appendix)
- Data Identification
  - Application Inventory and Business Impact Questionnaire (Appendix)
  - Application data (Appendix)
  - Voice data (Appendix)
  - Other (Appendix)
- Processes
  - DRP and Activation Workbook (Appendix)
  - General Distribution Materials (Appendix)
  - Web Site Disaster Planning Form (Appendix)
  - Work Plan (Appendix)
  - Incident Communication Plan (Appendix)
  - Social Networking checklist (Appendix)
  - Pandemic Checklist (Appendix)
  - Preventative Measures (Appendix)
  - Audit Plan Process (Appendix)
- Suppliers
  - Vendor and Supplier Disaster Recovery Questionnaire (Appendix)
  - Disaster Recovery Sample Contract (Appendix)

**ISO 23301**

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 in relation to business continuity, here is how ISO defines it: ... standardization in the area of 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



---

## 2.2 Objectives

The Business Impact Analysis is completed to determine the Critical Time Frame in which the application system capabilities and functionality must be available after an interruption in service to minimize the operational loss of control and potential loss of revenue. In addition, the Business Impact Analysis assists in identifying alternative manual procedures which may be used during an interruption in service. Therefore, the objectives of the Business Impact Analysis are:

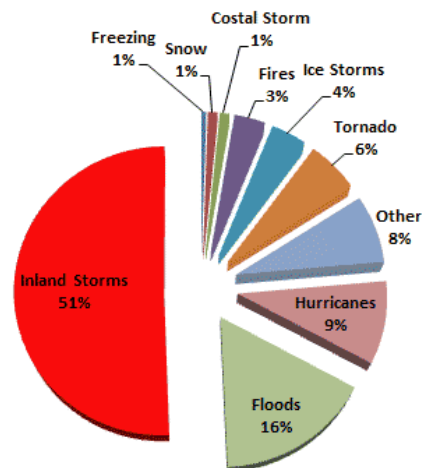
- Educate user on the need for a disaster recovery plan
- Identify the Critical Time Frames for each application by user
- Identify alternative manual procedures which may temporarily minimize impact due to an interruption in computer service
- Identify the shortest Critical Time Frame for each application

---

## 2.3 Analyze Threats

Disasters and business interruptions vary widely in more than duration. As you design your plan, consider the probability of threats that are:

- Chronicled — events that have occurred (Power outages, earthquakes, hurricanes)
- Human — events likely from carelessness, malicious intent, fatigue, or lack of training
- Geographical — events likely as a result of the location of your business (floods, storms, lightning strikes, earthquakes, typhoons, tsunamis)
- Localized — events due to system malfunctions (assembly line failures, computer crashes, sprinkler activations, chemical spills)
- Planned — scheduled events (software upgrades, system tests) that go awry



Typical Disaster Declaration - Historical Data  
© 2012 Janco Associates, Inc.

---

### 3.0 Backup Strategy

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

[www.e-janco.com](http://www.e-janco.com)

certain disastrous events can have (large scale hurricanes, etc.) it has become a standard practice. However, when a business interruption occurs, it is critical to recover key information as quickly as possible. This includes personal desktops, laptops, and PDA<sup>11</sup> in addition to servers. A strategy for backing widely scattered information. Based on the size of the operation and the need for recovery of the data the following backup strategy should be implemented. Strategies for each are discussed in the sections that follow for:

- Communication Strategy and Policy
- ENTERPRISE Data Center Systems
- Departmental File Servers
- Wireless Network File Servers
- Data at Outsourced Sites (including ISP's)
- Desktop Workstations (In Office)
- Desktop Workstations (Off site including at home users)
- Laptops
- PDA's

---

#### 3.01 Site Strategy

Most organizations have more than one recovery site strategy in place, since different business processes have different cost factors and service-level requirements. For example, for data center operations with large capital investments in hardware required for a secondary site, a shared-cost commercial hot-site service provider may be the most effective option. In contrast, provisioning of client-side alternate workspace may be more economically and effectively provisioned internally. Recovery time objectives ("How quickly do I need to be back online?") and data currency objectives ("How much data can the enterprise afford to lose?") will often place restrictions on recovery site options (see Chart 1).

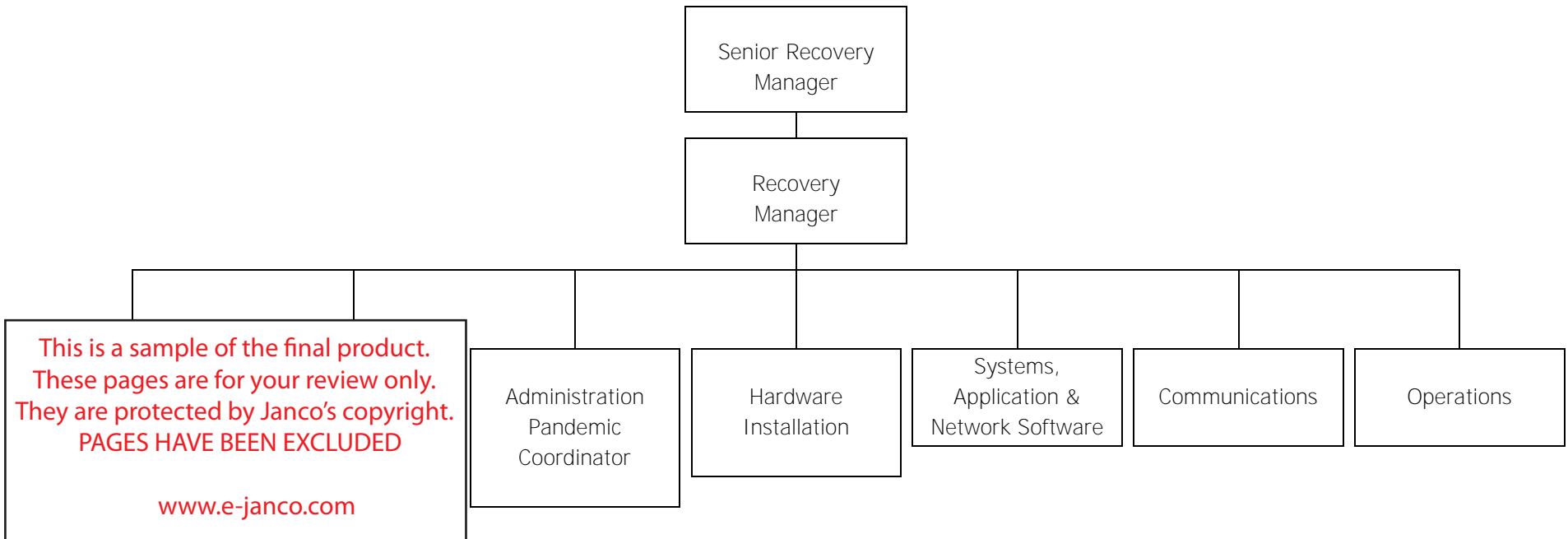
---

<sup>10</sup> Internet Service Providers and other "outsourced" service providers.

<sup>11</sup> Personal Digital Assistants

Site Strategy	Recovery Time	Comments
<b>Commercial Hot Site</b>	<b>24 to 48 hours</b>	Often the most cost effective strategy for data center recovery strategies. This is a market dominated by SunGard and IBM Global Services. Clear contract terms need to be defined which meets the enterprise service objectives. Consideration should be made for disasters which impact entire regions such as hurricanes and earthquakes.
<b>Mobile Data Center / Office Space</b>	<b>24 to 48 hours</b>	<div style="border: 1px solid black; padding: 5px; text-align: center; color: red; font-weight: bold;"> <p>This is a sample of the final product.                      These pages are for your review only.                      They are protected by Janco's copyright.                      PAGES HAVE BEEN EXCLUDED</p> <p><a href="http://www.e-janco.com">www.e-janco.com</a></p> </div> <p>or client workspace es but has limitations on if very small aperture munications. Businesses the parking lot of the nts such as hurricanes, t be appropriate.</p>
<b>Internal Hot Site</b>	<b>1 to 12 hours</b>	<p>This is typically the most expensive option since there is an added cost for internal provisioning of the necessary excess capacity. If costs can be shared among multiple facilities within the enterprise, internal provisioning can be cost competitive with commercial alternatives. In light of legislation such as Sarbanes –Oxley and the need for protection of sensitive information this is often the best solution.</p> <p>Organizations with strict data currency needs and aggressive recovery-time objectives have found internal hot-site strategies to be the only viable option. If no appropriate secondary space is available within existing property, suppliering and “co-location” facilities providers offer managed raised-floor space at very attractive rates as an alternative to building out secondary sites.</p>
<b>Cold Site</b>	<b>72 plus hours</b>	"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. In the case of an extensive disaster such as a hurricane or earthquake this option is less favorable
<b>Reciprocal Site</b>	<b>12 to 48 hours</b>	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.

## 5.1 Recovery Team Organization Chart



### 8.03 Disaster Recovery – Business Continuity Team Call List

This call list should be updated at least monthly and whenever there is any organizational changes or new personnel assume any of these roles

Role	Individual	Office Phone	Email	Mobile	Alternate Email	Credit Card Issued
Recovery Manager Senior						<input type="checkbox"/> Yes <input type="checkbox"/> No
Recovery Manager						<input type="checkbox"/> Yes <input type="checkbox"/> No
Damage Assessment						<input type="checkbox"/> Yes <input type="checkbox"/> No
Physical Security						<input type="checkbox"/> Yes <input type="checkbox"/> No
Administration						<input type="checkbox"/> Yes <input type="checkbox"/> No
Hardware						<input type="checkbox"/> Yes <input type="checkbox"/> No
Network						<input type="checkbox"/> Yes <input type="checkbox"/> No
Application Software						<input type="checkbox"/> Yes <input type="checkbox"/> No
Communication						<input type="checkbox"/> Yes <input type="checkbox"/> No
Operations						<input type="checkbox"/> Yes <input type="checkbox"/> No
Customer Relations						<input type="checkbox"/> Yes <input type="checkbox"/> No
Supplier Relations						<input type="checkbox"/> Yes <input type="checkbox"/> No
Vendor Relations						<input type="checkbox"/> Yes <input type="checkbox"/> No
Media Communications						<input type="checkbox"/> Yes <input type="checkbox"/> No

This is a sample of the final product.  
 These pages are for your review only.  
 They are protected by Janco's copyright.  
 PAGES HAVE BEEN EXCLUDED  
  
[www.e-janco.com](http://www.e-janco.com)

Completed by:

Department:

Date:

## 8.04 Disaster Recovery – Business Continuity Team Vendor Contacts

Vendor Contacts	
Vendor Name	
Product / Service	
Damage Assessment	
Mailing Address	
City/State/Zip	
<b>Contacts</b>	
Primary Contact	Name: Phone: Email: FAX: Mobile:
	This is a sample of the final product. These pages are for your review only. They are protected by Janco's copyright. PAGES HAVE BEEN EXCLUDED  <a href="http://www.e-janco.com">www.e-janco.com</a>
Primary Contact	Name: Phone: Email: FAX: Mobile:
Comments:	
Secure location to get UserIDs and Passwords:	

Completed by:

Department:

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

Application / File Servers

Provide the following information for each application and file server:

- Host name
- IP address and mask for the server
- Administrative contact for the server and security contact (i.e. primary user or department head name and phone number)
- User Types
- Operating system including version number
- Application Software including version number
- Review status (Yes/No, Date, Reviewer)
- Connectivity (Internet, Intranet, modem In, modem out, other)
- Physical location (Address / phone number for contact)

Host Name: _____		Reviewer Name: _____		Date: _____
IP Address / Mask	User Types	Administrative Contact	Connectivity	Physical Location
_____ _____ (mask)	<input type="checkbox"/> Public <input type="checkbox"/> Customers <input type="checkbox"/> Employees <input type="checkbox"/> Groups Emp <input type="checkbox"/> Specific Em <input type="checkbox"/> _____	Name: _____	<input type="checkbox"/> Internet <input type="checkbox"/> Intranet <input type="checkbox"/> Modem In Bound <input type="checkbox"/> Modem Out Bound <input type="checkbox"/> _____	Address: _____ Contact: _____ Phone: _____
IP Address Range	Operating S	Application	App Version / Reviewed	
_____ _____ to _____	<input type="checkbox"/> Windows W <input type="checkbox"/> Windows Se <input type="checkbox"/> Unix <input type="checkbox"/> Lynx. <input type="checkbox"/> Other	Ver: _____ <input type="checkbox"/> Yes <input type="checkbox"/> No Ver: _____ <input type="checkbox"/> Yes <input type="checkbox"/> No	Ver: _____ <input type="checkbox"/> Yes <input type="checkbox"/> No Ver: _____ <input type="checkbox"/> Yes <input type="checkbox"/> No Ver: _____ <input type="checkbox"/> Yes <input type="checkbox"/> No Ver: _____ <input type="checkbox"/> Yes <input type="checkbox"/> No	

This is a sample of the final product.  
 These pages are for your review only.  
 They are protected by Janco's copyright.  
 PAGES HAVE BEEN EXCLUDED  
  
[www.e-janco.com](http://www.e-janco.com)

Comments: \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

# Disaster Recovery Planning General Distribution Information

## How to Clean Up After a Disaster

What do you do to clean things up? Some tips on disaster recovery and business continuity clean up are:

- **Wet objects (electronic)** - Disconnect from the power source and do not turn it on. In the case of disk drives or other electronic storage devices - inventory all of them and label them. Create a log of all objects recovered, actions taken, and location. Have a disaster clean-up specialist be the one who looks at what can be recovered.
- **Wet objects (non-electronic)** - Rinse with clear water or a fine hose spray. Clean off dry silt and debris with soft brushes or dab with damp cloths. Try not to grind debris into objects; overly energetic cleaning will cause scratching. Dry with a clean, soft cloth. Use plastic or rubber gloves for your own protection.
- **Water damage to paper** - Paper can have serious health consequences such as respiratory problems, skin and eye irritation, and infections. The use of protective gear, including a respirator with a particulate filter, disposable plastic gloves, goggles or protective eyewear, and coveralls or a lab coat, is therefore essential. In order to inhibit the growth of mold and mildew you must reduce humidity. Increase air flow with fans, open windows, air conditioners, and dehumidifiers. Moderate light exposure (open shades, leave lights on in enclosed areas) can also reduce mold and mildew. Remove heavy deposits of mold growth from walls, baseboards, floors, and other household surfaces with commercially available disinfectants. Avoid the use of disinfectants on historic wallpapers. Follow manufacturers' instructions, but avoid splattering or contact with objects and wallpapers as disinfectants may damage objects.
- **Broken Objects** - If objects are broken or begin to fall apart, place all broken pieces and detached parts in clearly labeled, open containers. Do not attempt to repair objects until completely dry or, in the case of important materials, until you have consulted with a professional conservator.
- **Paper Materials** - Documents, books, photographs, and works of art on paper are extremely fragile when wet; use caution when handling. Free the edges of prints and paper objects in mats and frames, if possible. These should be allowed to air dry. Rinse mud off wet photographs with clear water, but do not touch surfaces. Wet books and papers should also be air dried or kept in a refrigerator or freezer until they can be treated by a professional conservator.
- **Office Furniture** - Furniture finishes and painting surfaces may develop a white haze or bloom from contact with water and humidity. These problems do not require immediate attention; consult a professional conservator for treatment. Textiles, leather, and other "organic" materials will also be severely affected by exposure to water and should be allowed to air dry. Shaped objects, such as garments or baskets, should be supported by gently padding with toweling or un-inked, uncoated paper.

This is a sample of the final product.  
These pages are for your review only.  
They are protected by Janco's copyright.  
PAGES HAVE BEEN EXCLUDED  
  
www.e-janco.com

# Pandemic Planning Checklist

## 8.23 Business Pandemic Planning Checklist

### Plan for the impact of a pandemic on your business

Tasks	Not Started	In Progress	Completed
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.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Identify essential employees and other critical inputs (e.g. raw materials, suppliers, sub-contractor services/ products, and logistics) required to maintain business operations by location and function during a pandemic.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Train and prepare ancillary workforce (e.g. contractors, employees in other job titles/descriptions, retirees).	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
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 restriction on mass gatherings, need for hygiene supplies).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Determine potential impact of a pandemic on company business financials using multiple possible scenarios that affect different product lines and/or production sites.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Determine potential impact of a pandemic on business-related domestic and international travel (e.g. quarantines, border closures).	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Find up-to-date, reliable pandemic information from community public health, emergency management, and other sources and make sustainable links.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<div style="border: 1px solid black; padding: 10px; width: fit-content;"> <p style="color: red; font-weight: bold;">This is a sample of the final product. These pages are for your review only. They are protected by Janco's copyright. PAGES HAVE BEEN EXCLUDED</p> <p style="color: red; text-align: center;">www.e-janco.com</p> </div>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<div style="border: 1px solid black; padding: 10px; width: fit-content;"> <p>revise periodically. This (back-ups), chain of (rs), and processes for ee status.</p> </div>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<div style="border: 1px solid black; padding: 10px; width: fit-content;"> <p>revise periodically.</p> </div>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>