

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

CHEMICAL SPILL > WIND STORM > FIRE > HURRICANE > BLACK OUT > FLOOD > EARTHQUAKE > ICE STORM > S
ILITY OUTAGE > GAS LEAK > DATABASE CORRUPTION > LIGHTNING > TERROR ALERT > TORNADO > SMOKE D

Disaster Recovery & Business Continuity Template

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

Prepared by

Janco

Associates, Inc.
Park City, UT 84060

email - support@e-janco.com

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

Version 5.5

© 2010 Copyright Janco Associates, Inc. ALL RIGHTS RESERVED

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

Table of Contents¹

1.0	Plan Introduction	12
1.1	Mission and Objectives	13
	Compliance.....	13
	Implication of Legislated and Industry Standards Requirements	13
	Sarbanes-Oxley	14
	COSO.....	16
	PCI DSS	17
	COBIT.....	17
	ISO 27000 Compliance Process	18
	Define the Control Environment.....	18
	Control the Environment by Implementation and Management	18
	Audit and Examine the Control Processes.....	19
1.2	Disaster Recovery / Business Continuity Scope	20
1.3	Authorization	20
1.4	Responsibility	20
1.5	Key Plan Assumptions	21
1.6	Disaster Definition.....	22
1.7	Metrics	22
1.8	Disaster Recovery / Business Continuity and Security Basics	24
	Servers.....	24
	Network.....	25
	Clients.....	26
	Recovery Procedures.....	26
	Communication	26
	Designated operators.....	26
	Designated manager	27
	External resources.....	27
	Insurance.....	27
2.0	Business Impact Analysis	28
2.1	Scope.....	28
2.2	Objectives.....	29
2.3	Critical Time Frame	29
2.4	Application System Impact Statements	30

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.

- Essential30
- Delayed30
- Suspended.....30
- 2.5 Information Reporting31
- 2.6 Best Data Practices32
- 2.7 Summary33
- 3.0 Backup Strategy.....34
 - 3.01 Site Strategy34
 - 3.02 Data Capture and Backups37
 - Backup Strategy.....38
 - 3.03 Backup and Backup Retention Policy.....39
 - Policy39
 - Applicability.....39
 - Backup Versus Archive39
 - Archiving Implications Sarbanes-Oxley39
 - SOX – Section 802.....40
 - Record Retention Requirements40
 - Types of Backups.....41
 - Storage Management.....42
 - Minimal Backup Policy42
 - Requirements42
 - Backup Retention43
 - Documentation and Backup Media Labeling.....43
 - Storage.....44
 - Responsibilities.....44
 - Testing and Training.....44
 - System Specific Backup Policy.....45
 - Backup Retention46
 - Documentation and Backup Media Labeling.....46
 - Storage.....47
 - Responsibilities.....47
 - Testing and Training.....47
 - 3.04 Communication Strategy and Policy49
 - DRP / BCP Communication Policy49
 - 3.05 ENTERPRISE Data Center Systems51
 - Backup Files.....51
 - Storage Rotation51
 - ENTERPRISE Data Center.....51
 - Off Site Storage.....51
 - 3.06 Departmental File Servers.....51
 - Backup Files.....52
 - Storage Rotation52
 - Department.....52
 - ENTERPRISE Data Center.....52
 - Off Site Storage.....52
 - 3.07 Wireless Network File Servers.....53
 - Backup Files.....53

- Storage Rotation 53
 - Wireless Network File Server Area 53
 - ENTERPRISE Data Center..... 53
 - Off Site Storage..... 53
- 3.08 Data at Outsourced Sites (including ISP's) 55
 - Backup Files..... 55
 - Storage Rotation 55
 - Outsourced Sites 55
 - ENTERPRISE Data Center..... 55
 - Off Site Storage..... 55
- 3.09 Branch Offices (Remote Offices & Retail Locations) 57
 - Backup Files..... 57
 - Storage Rotation 57
 - Laptop location..... 57
 - ENTERPRISE Data Center..... 58
 - Off Site Storage..... 58
- 3.10 Desktop Workstations (In Office) 59
 - Backup Files..... 59
 - Storage Rotation 59
 - Desktop Workstation location 59
 - ENTERPRISE Data Center..... 59
 - Off Site Storage..... 60
- 3.11 Desktop Workstations (Off site including at home users) 61
 - Backup Files..... 61
 - Storage Rotation 61
 - Desktop Workstation location 61
 - ENTERPRISE Data Center..... 61
 - Off Site Storage..... 62
- 3.12 Laptops 63
 - Backup Files..... 63
 - Storage Rotation 63
 - Laptop location..... 63
 - ENTERPRISE Data Center..... 63
 - Off Site Storage..... 63
- 3.13 PDA's and Smartphones 65
 - Backup Files..... 65
 - Storage Rotation 66
 - Laptop location..... 66
 - ENTERPRISE Data Center..... 66
 - Off Site Storage..... 66
- 4.0 Recovery Strategy 67
 - 4.1 Approach 67
 - 4.2 Escalation Plans 68
 - 4.3 Decision Points 69
 - Plan 1 69
 - Plan 2 70
 - Plan 3 71

5.0	Disaster Recovery Organization	72
5.1	Recovery Team Organization Chart.....	73
5.2	Disaster Recovery Team	75
5.3	Recovery Team Responsibilities	76
5.3.1	Recovery Management	76
	Senior Recovery Manager Responsibilities	76
	Pre-Disaster	76
	Post-Disaster.....	76
	Recovery Manager Responsibilities.....	77
	Pre-Disaster	77
	Post-Disaster.....	77
5.3.2	Damage Assessment and Salvage Team.....	78
	Damage Assessment and Salvage Team Responsibilities	78
	Pre-Disaster	78
	Post-Disaster.....	78
5.3.3	Physical Security	79
	Pre-Disaster	79
	Post-Disaster	79
5.3.4	Administration.....	80
	Pre-Disaster	80
	Post-Disaster	80
5.3.5	Hardware Installation	81
	Pre-Disaster	81
	Post-Disaster	81
5.3.6	Systems, Applications and Network Software.....	82
	Pre-Disaster	82
	Post-Disaster	82
5.3.7	Communications.....	83
	Pre-Disaster	83
	Post-Disaster	83
5.3.8	Operations.....	84
	Pre-Disaster	84
	Post-Disaster	84
6.0	Disaster Recovery Emergency Procedures.....	85
6.1	General.....	86
6.2	Recovery Management	87
6.3	Damage Assessment and Salvage	89
6.4	Physical Security.....	92
6.5	Administration	94
6.6	Hardware Installation.....	95
6.7	Systems, Applications & Network Software.....	97
6.8	Communications	99
6.9	Operations.....	100
7.0	Plan Administration	101
7.1	Disaster Recovery Manager	101
7.2	Distribution of the Disaster Recovery Plan	102
7.3	Maintenance of the Business Impact Analysis	103

7.4	Training of the Disaster Recovery Team	103
7.5	Testing of the Disaster Recovery Plan.....	104
7.6	Evaluation of the Disaster Recovery Plan Tests	106
7.7	Maintenance of the Disaster Recovery Plan	107
8.0	Appendix.....	109
8.01	Plan Distribution.....	110
8.02	ENTERPRISE Sales Offices.....	111
8.03	Disaster Recovery Team Call List.....	112
8.04	Vendor Phone/Address List.....	114
8.05	Off-Site Inventory.....	118
8.06	Personnel Location Form	119
8.07	Hardware/Software Inventory	120
8.08	People Interviewed	121
8.09	Preventative Measures	122
8.10	Sample Application Systems Impact Statement	123
8.11	JOB Descriptions.....	124
	Disaster Recovery Manager	124
	Position Purpose	124
	Problems and Challenges	124
	Essential Position Functions.....	124
	Principal Accountabilities	124
	Authority.....	125
	Contacts.....	125
	Position Requirements	125
	Manager Disaster Recovery and Business Continuity	126
	Position Purpose	126
	Problems and Challenges	126
	Essential Position Functions.....	126
	Principal Accountabilities	126
	Authority.....	127
	Contacts.....	127
	Position Requirements	127
	Pandemic Coordinator	128
	Position Purpose	128
	Problems and Challenges	128
	Essential Position Functions.....	128
	Principal Accountabilities	128
	Authority.....	129
	Contacts	129
	Position Requirements	129
	Career Ladder	130
8.12	Application Inventory and Business Impact Analysis Questionnaire	131
	Facility / Business Function / Application	133
	Sarbanes-Oxley Compliance	134
	ISO – 27000 Compliance - System of Internal Controls	135
	User Environment.....	136
	Operating Environment	138

	Criticality of Application	140
	Processing Information.....	142
	Application / File Servers.....	143
	Historical Information.....	145
	Database / File Names.....	146
	Documentation.....	147
	Security.....	147
	Application Support and Maintenance.....	147
	Resource Usage	148
	Equipment Requirements by Department	148
	Backups	149
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
	Off Site Stored Materials	155
	Recovery Box	155
8.17	Work Plan.....	157
	Project Initiation	158
	Project Scheduling	158
	Business Impact Analysis	159
	Backup and Recovery Strategy	159
	Initial Implementation.....	160
	Post Implementation.....	160
8.18	Audit Disaster Recovery Plan Process	161
	Audit Program	161
	Audit Program Overview	161
	Suggested interviewees for Audit.....	162
	Objective #1 - Backup Procedures.....	162
	Objective #2 - Off-site Storage Facility	162
	Objective #3 - Disaster Recovery Plan	162
8.19	Vendor Disaster Recovery Planning Questionnaire	163
	Vendor / Partner Information	164
	DRP and Business Continuity Strategy.....	165
	Crisis Communication	167
	Backup Facilities	168
	Testing	170
	Prior DRP and BCP Plan Activations.....	171
	DRP and BCP Support	172
8.20	Departmental DRP and BCP Activation Workbook	173
	Quick Reference Guide.....	174
	Team Alert List.....	175
	Team Responsibilities	177
	Team Leader Responsibilities / Checklist.....	177
	General	177
	Critical Functions	177
	Normal Business Hours Response	178

- After Normal Business Hours Response 178
- Primary Location..... 179
- Alternate Location 179
- Team Recovery 180
 - Business Resumption Plan Copies 180
 - Cellular Phone (TBD)..... 180
 - Team Work Area..... 180
 - Notifications 180
 - Team Recovery Steps..... 180
 - The team leader responsibilities..... 180
 - Departmental Meeting 181
 - Personnel Location Form 181
 - Status Report 181
 - Travel Arrangements 181
- Notification..... 182
 - Notification Checklist..... 182
- Notification Procedure 183
- Notification Call List..... 184
- Project Status Report..... 185
- Planned Activities for the Period 185
- Accomplished Planned Activities 185
- Planned Activities Not Accomplished 185
 - Activity 185
 - Reason..... 185
 - Expected completion..... 185
- Unplanned Activities Performed or Identified..... 185
 - Activity 185
 - Reason..... 185
 - Impact on project..... 185
 - Planned Activities for the Next Period..... 186
 - Cost Data To Date 186
 - Open Issues and Resolutions..... 186
 - Comments 187
- 8.21 Web Site Disaster Recovery Planning Form 188
 - Backup Site 189
 - Backup Site (Secondary) 190
 - Software Required to Operate Web Site 191
- 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
1.a General principles.....	200
1b. Definition of a disaster	201
1c. Period of service	201
Prerequisites	201
Alignment.....	202
3a. Specify kind of system, for example: Broking system	202
3b. Specific data and applications.....	202
3c. Backup facilities	203
Provisions.....	204
4a. Office space	204
4a-a. Work space	204
4a-b. Meeting space	204
4a-c. Storage space	205
4a-d. Safe	205
4b. Office equipment	205
4b-a. Telephone	205
4b-b. Fax	205
4b-c. E-mail.....	205
4b-d. Mail, courier, and messenger services	205
4b-e. Stationery, photocopying, and other facilities.....	205
4c. Computer equipment	205
4c-a. PC.....	206
4c-b. Printer	206
4c-c. Backups (initial data load)	206
4c-d. Backups (within service provision).....	206
4c-e. Specify platform from which data should be backed up	207
4c-f. Periodic processing	207
4c-g. Broking system GUI applications	207
4d. Specialist requirements.....	207
4d-a. Non-standard items.....	207
4d-b. Slips, cover notes, and other documents	207
4e. Restrictions.....	208
Termination Procedure	208
5a. Termination of Service	208
5b. Termination of the agreement.....	208
Responsibilities	208
Testing the Plan	209

9.0 Change History210

- Version 5.5 – Release date January 2010210
- Version 5.4 – Release date May 18, 2009210
- Version 5.3 – Release date January 2, 2009.....210
- Version 5.2 – Release date August 1, 2008.....210
- Version 5.1 – Release date July 1, 2008.....210
- Version 5.0 – Release date February 21, 2008210
- Version 4.5 – Release date November 2, 2007211
- Version 4.4 – Release date September 1, 2007211
- Version 4.3 – Release date July 26, 2007211
- Version 4.2 – Release date February 1, 2007211
- Version 4.1 – Release date August 28, 2006.....211
- Version 4.0 - Release date March 5, 2006211
- Version 3.1 - Release date January 2, 2006211
- License Conditions213

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.

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 Frames² 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

There³ are a number of legally mandated and standards mandated issues that need to be covered in the Disaster Recovery / Business Continuity Planning Process.

² 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.

³ This section is for informational purposes and can be excluded from the plan.

Site Strategy	Recovery Time	Comments
Commercial Hot Site	24 to 48 hours	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.
Mobile Data Center / Office Space	24 to 48 hours	Pre-configured mobile resources for data center or client workspace recovery. 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. Businesses also typically assume that they can be placed in the parking lot of the affected site, so if the disaster profile includes events such as hurricanes, floods or toxic spills, these solutions may not be appropriate.
Internal Hot Site	1 to 12 hours	<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>
Cold Site	72 plus hours	"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
Reciprocal Site	12 to 48 hours	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.

Backup Strategy

Backups can be accomplished locally, centrally or both. There are advantages and disadvantages to each. The table below lists some of the advantages and disadvantages of each.

Disaster Recovery Backup Alternatives	Advantage	Disadvantage
Local Backup	<ul style="list-style-type: none"> • Backup quicker • Minimal bandwidth usage • Quicker restore in minor recovery situation 	<ul style="list-style-type: none"> • More hardware required • More staff required • Security risks increased • Riskier restore in a major recovery situation.
Central Backup	<ul style="list-style-type: none"> • Hardware requirement less • Less staff required • Less training • Quicker restore in a major recovery situation. • Security risks lower 	<ul style="list-style-type: none"> • More bandwidth required • Backup takes longer to complete • Restore takes longer in minor recovery situation
Coordinated Local and Central Backup	<ul style="list-style-type: none"> • Recovery time eased • Enterprise risks reduced • Easier to coordinate DRP and Business Continuity Plans 	<ul style="list-style-type: none"> • More hardware required • More staff required • More training required • More bandwidth required

3.03 Backup and Backup Retention Policy

Policy

The purpose of this policy is to define the need for performing periodic computer system backups to ensure that mission critical administrative applications, data and archives and applications, users' data and archives are adequately preserved and protected against data loss and destruction. Each ENTERPRISE unit responsible for providing and operating a mission critical application must document and perform System Specific Data Backup or at least Minimal Data Backup on a periodic basis.

Computer systems that create or update mission critical ENTERPRISE data on a daily basis need to be backed up on a daily basis to minimize the exposure to loss of mission critical data. The unit responsible for providing and operating such systems must conduct a systematic and detailed investigation of all the influencing factors leading to the compilation of a comprehensive System Specific Data Backup Policy. System specific backup policies must at least fulfill the requirements of the Minimal Data Backup Policy.

Applicability

This policy applies to all units operating of ENTERPRISE. This backup policy is defined to protect against the following situations:

- Destruction of data media by force majeure, e.g. fire or water
- Deliberate and/or accidental deletion of files with computer-viruses etc
- Inadvertent deletion or overwriting of files
- Technical failure of storage device (head crash)
- Faulty data media
- Demagnetization of magnetic data media due to ageing or unsuitable environmental conditions (temperature, air moisture)
- Interference of magnetic data media by extraneous magnetic fields
- Uncontrolled changes in stored data (loss of integrity)

Backup Versus Archive

A backup process takes periodic or real-time images of active data in order to provide a method of recovering records that have been deleted or destroyed. Most backups are retained only for a few days or weeks as later backup images supersede previous versions.

A backup is designed as a short-term insurance policy to facilitate disaster recovery, while an archive is designed to provide ongoing access to decades of business information. Archived (historical) records are placed outside the traditional backup cycle for a long period of time, while backup operations protect active data that's changing on a frequent basis.

Archiving Implications Sarbanes-Oxley

A record is essentially any material that contains information about ENTERPRISE's plans, results, policies or performance. In other words, anything about ENTERPRISE that can be represented

5.0 Disaster Recovery Organization

The effectiveness and operability of the Disaster Recovery Plan is dependent on the knowledge and expertise of the personnel who develop and execute the plan. It is essential to determine which talents are required and to assign personnel who meet those requirements.

A recovery from a disaster is best conducted by teams of personnel that are formed to perform specific functions (e.g., hardware acquisition, hardware installation, operations). The number and types of teams are dictated by the size and type of computer processing capabilities and facility the plan is being developed to recover.

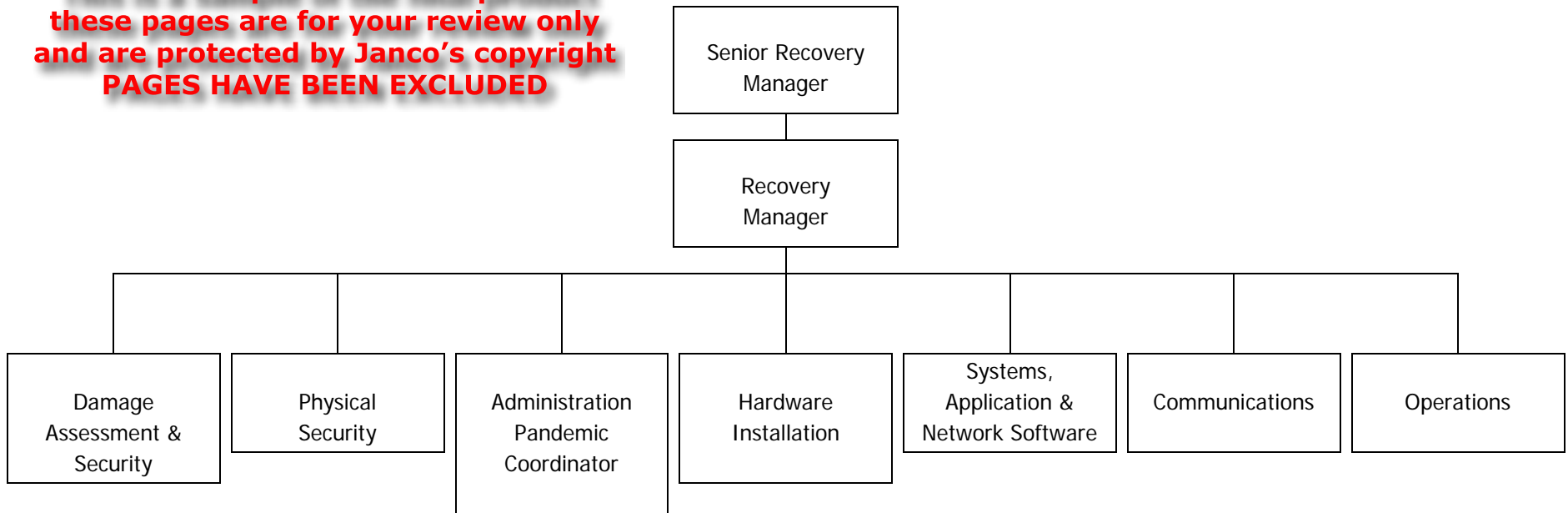
The organization of the staff to recover the system is designed for the worst case situation. The worst case, requiring a move to the alternative site, must be executed by a coordinated team to minimize the operational impacts to end-users, senior management and ENTERPRISE as a whole.

The Disaster Recovery Team Organization, therefore, is set up to accomplish:

- Expeditious and efficient recovery of computer processing;
- Intermediate and minor impact/expenditure decisions within the Information Technology personnel during the recovery process;
- Major impact/expenditure decisions at the management level; and
- Streamline reporting of recovery progress from recovery teams upward to senior management and end-users.

5.1 Recovery Team Organization Chart

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



ENTERPRISE
Business and IT Impact Questionnaire

The purpose of this questionnaire is to determine the criticality of the applications used at ENTERPRISE. The information provided will be used to develop a Application Inventory that can be used in the Disaster Recovery Plan that minimizes the impact of the loss of this application in the event of a disaster. **(PLEASE USE ADDITIONAL BLANK PAPER OR ATTACHMENTS WHEREVER NECESSARY)**

Facility / Business Function / Application

Name: _____

Provide a brief description/purpose – mission: _____

What are the main functions? _____

Was this developed in-house or purchased from a vendor? If purchased from a vendor, do you hold the plans, source code etc. _____

If the application is a purchased package, are there extensive modifications to this application (briefly describe modifications): _____

What programming language was used to create the application? _____

How old is this application (maturity)? _____

Who is the owner of this application (i.e. Joe Smith of Accounting)? _____

ENTERPRISE

Business and IT Impact Questionnaire

Application / File Servers

Provide the following information for each application and file server:

- Supplier 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)

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

Supplier 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 Employees <input type="checkbox"/> Specific Employees <input type="checkbox"/> _____	Name: _____ Email: _____ Phone: _____	<input type="checkbox"/> Internet <input type="checkbox"/> Intranet <input type="checkbox"/> Modem In Bound <input type="checkbox"/> Modem Out Bound <input type="checkbox"/> Other: _____	Address: _____ Contact: _____ Phone: _____
IP Address Range	Operating System	Version / Reviewed	Application	Version / Reviewed
_____ _____ to _____	<input type="checkbox"/> Windows WS <input type="checkbox"/> Windows Server <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	<input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____ <input type="checkbox"/> _____	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

Comments: _____

ENTERPRISE Vendor Disaster Recovery Planning Questionnaire

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? (NOTICE: <i>if your firm has no plan in place and has not intention of implementing a plan then your firm should be aware that our vendor / partnership relationship is subject to cancellation</i>)	Yes _____	or	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?	_____ (please specify # and hours, days, weeks, months, etc. for each type)			
4	Does the plan establish critical business functions with recovery priorities?	Yes _____	or	No _____	
5	If you answered "Yes" to Question (4), what is the expected recovery time for your critical business functions?	0 – 4 hours _____			
		4 – 8 hours _____			
		Within one day _____			
		1 – 2 days _____			
		More than 2 days _____			
		Other (please specify) _____			
		N/A _____			
6	Does the plan account for interdependencies both internal and external to your organization?	Yes _____	or	No _____	

Disaster Recovery Planning Service Agreement

8.24 Disaster Recovery Sample Contract

Overview

1.a General principles

_____ (Supplier) located at _____ has agreed with _____ (Client) located at _____ to have a arrangement for disaster recovery. \$ _____ dollars have been paid.³⁶

Definition of terms

- **Supplier**, to indicate the company that is providing facilities;
- **Client**, to indicate the company using these facilities;
- **Plan**, to indicate the disaster recovery business continuity plan; and
- **Service**, to indicate all facilities within the provision.

This contract allows for the following:

- Provision of _____ (Location) - based office facilities for up to _____ staff for a _____ period.
- Provision of access to _____ (Specify system) and local area network facilities for _____ staff.
- Periodic testing and checking of the plan.
- Access to facilities in _____ (location.

It is understood that:

- Both parties will agree to confidentiality of data, clients, and business practices.
- Neither party will seek compensation from the other should any problems or difficulties arise from the service provided unless there is a breach of this agreement.
- The plan will be shown supplier their comments will be incorporated into the plan.
- Each party to this agreement will ensure that all items to be used in this plan will be maintained and kept in good working order.

³⁶ Note: We are not attorneys and are not providing any legal advice. This document is intended as only set of guidelines that should be review in its entirety by anyone using it and must be review and approved by your legal counsel.

Version History

9.0 Change History

Version 5.5 – Release date January 2010

- Updated to comply with CobiT requirements
 - Sample Disaster Recovery Plan Service Agreement
-

Version 5.4 – Release date May 18, 2009

- Added Pandemic Coordinator job description
 - Added Business Pandemic Planning Checklist
 - Updated organization chart to include Pandemic Coordinator
 - Corrected minor errata
-

Version 5.3 – Release date January 2, 2009

- Updated backup and backup retention section
 - Updated style sheet to be CSS Style sheet format
 - Added Disaster Recovery Business Continuity General Distribution Information
 - What to do after an explosion / terrorist attack
 - How to clean up after a disaster
-

Version 5.2 – Release date August 1, 2008

- Updated style sheet to WORD 2007 format
 - Updated forms and charts
-

Version 5.1 – Release date July 1, 2008

- Added sample Backup and Backup Retention Policy
 - Minor formatting changes
-

Version 5.0 – Release date February 21, 2008

- Updated Disaster Recovery / Business Continuity Plan Audit Program to be compliant with ISO 27000 Series (ISO 27001 and ISO 27002)
- Added a section on Communication Strategy and Policy to be implemented when the Disaster Recovery / Business Continuity Plan is activated
- Added a section on Disaster Recovery / Business Continuity and Security basics
- Added Personnel Location Report
- Added Project Status Report Form

Version History

Version 4.5 – Release date November 2, 2007

- Added Disaster Recovery / Business Continuity Plan Audit Program
- Updated excel work plan to refer to sections versus pages

Version 4.4 – Release date September 1, 2007

- Section added on implications of Sarbanes-Oxley, Treadway Commission, and PCI DSS requirements
- Disaster Planning Branch Offices added
- Backup strategy table added
- Backup strategy for PDA's updated to reflect Smartphones

Version 4.3 – Release date July 26, 2007

- Defined generic metrics for DR/BC success
- Business & IT Impact Analysis Questionnaire Updated
- Updated references to DRP card
- Updated formatting to meet WORD 2007 requirements

Version 4.2 – Release date February 1, 2007

- Added Section defining the ISO 17799 compliance requirements
- Review and modified entire DRP/BCP template to ensure compliance with ISO 17799
- Business & IT Impact Questionnaire updated to meet ISO 17799 compliance requirements
- Corrected errata
- Added Best Data Retention and Destruction Practices Section

Version 4.1 – Release date August 28, 2006

- Department DRP / BCP Activation Workbook Updated in the appendix
- Correct work plan formatting and numbering for project initiation
- Web Site Disaster Recovery Planning Form added to the appendix

Version 4.0 - Release date March 5, 2006

- Vendor Disaster Recovery Planning Questionnaire added to the appendix
- Department Disaster Recovery Planning Workbook added to the appendix
- Vendor Phone List form updated
- Key Customer Notification List form added
- Critical Resources to be Retrieved form added
- Business Continuity Off-Site Materials form added

Version 3.1 - Release date January 2, 2006

- Site Strategy section added (Section 3.1) all other section numbers in Chapter 3 were increased to adjust for this modification.

Enterprise logo here

Version History

- Audit Disaster Recovery Plan Process added (Section 8.13)
- Manager Disaster Recovery and Business Continuity job description added
- Entire template reviewed to validate compliance with Sarbanes-Oxley