WHIDBEY
TELECOM

Internet & WiFi • Telephone Services • Security & Alarms

Whidbey Telecom Disaster Recovery Plan

Date
11/2123
Version
1.1

WHIDBEY TELECOM

Internet & WiFi • Telephone Services • Security & Alarms

Table of Contents

Introduction

This Disaster Recovery Plan (DRP) captures, in a single repository, all the information that describes Whidbey Telecom's ability to withstand a disaster as well as the processes that must be followed to achieve disaster recovery.

Definition of a Disaster

A disaster can be caused by man or nature and results in Whidbey Telecom's Technology department not being able to perform all or some of their regular roles and responsibilities for a period of time. Whidbey Telecom defines disasters as the following:

- *One or more vital systems are non-functional*
- *The building is not available for an extended period of time but all systems are functional within it*
- *The building is available but all systems are non-functional*
- *The building and all systems are non functional*

The following events can result in a disaster, requiring this Disaster Recovery document to be activated:

- *Fire*
- *Power Outage*
- *Malware or Ransomware*
- *Core network failure or complete loss of Internet*
- *Complete loss of corporate network or data*
- *Complete loss of voice switching*

Purpose

Note that in the event of a disaster the first priority of Whidbey Telecom is to prevent the loss of life. Before any secondary measures are undertaken, Whidbey Telecom will ensure that all employees, and any other individuals on the organization's premises, are safe and secure.

After all individuals have been brought to safety, the next goal of Whidbey Telecom will be to enact the steps outlined in this DRP to bring all of the organization's groups and departments back to business-as-usual as quickly as possible. This includes:

- *Preventing the loss of the organization's resources such as hardware, data and physical Technology assets*
- *Minimizing downtime related to Technology services*
- *Keeping the business running in the event of a disaster*

This DRP document will also detail how this document is to be maintained and tested.

Scope

The Whidbey Telecom DRP takes all of the following areas into consideration:

- *Network Infrastructure*
- *Servers Infrastructure*
- *Telephone System*
- *Data Storage and Backup Systems*
- *Data Output Devices*
- *End-user Computers*
- *Organizational Software Systems*
- *Database Systems*
- *IT Documentation*

This DRP does not take into consideration any non-Technology, personnel, Human Resources and real estate related disasters.

Version Information & Changes

Any changes, edits and updates made to the DRP will be recorded in here. It is the responsibility of the Disaster Recovery Lead to ensure that all existing copies of the DRP are up to date. Whenever there is an update to the DRP, Whidbey Telecom requires that the version number be updated to indicate this.

Name of Person Making Change	Role of Person Making Change	Date of Change	Version Number	Notes
Wayne Jeffers	*Director of Technology*	*5/19/23*	*1.0*	*Initial version of DR Plan*
Brian Butt	*Sr Systems Admin Supervisor*	*11/13/23*	*1.1*	*Added critical customers, media contacts and crucial vendors and contractors.*

Disaster Recovery Teams & Responsibilities

In the event of a disaster, different groups will be required to assist the IT department in their effort to restore normal functionality to the employees of Whidbey Telecom. The different groups and their responsibilities are as follows:

- *Disaster Recovery Lead(s)*
- *Facilities Team*
- *Network Team*
- *Applications and Servers Team*
- *Operations Team*
- *Management Team*
- *Communications Team*
- *Finance Team*

The lists of roles and responsibilities in this section have been created by Whidbey Telecom and reflect the likely tasks that team members will have to perform. Disaster Recovery Team members will be responsible for performing all of the tasks below. In some disaster situations, Disaster Recovery Team members will be called upon to perform tasks not described in this section.

Disaster Recovery Lead

The Disaster Recovery Lead is responsible for making all decisions related to the Disaster Recovery efforts. This person's primary role will be to guide the disaster recovery process, and all other individuals involved in the disaster recovery process will report to this person in the event that a disaster occurs at Whidbey Telecom, regardless of their department and existing managers. All efforts will be made to ensure that this person be separate from the rest of the disaster management teams to keep his/her decisions unbiased; the Disaster Recovery Lead will not be a member of other Disaster Recovery groups in Whidbey Telecom.

Role and Responsibilities

- *Make the determination that a disaster has occurred and trigger the DRP and related processes.*
- *Initiate the DR Call Tree.*
- *Be the single point of contact for and oversee all of the DR Teams.*
- *Organize and chair regular meetings of the DR Team leads throughout the disaster.*
- *Present to the Management Team on the state of the disaster and the decisions that need to be made.*
- *Organize, supervise, and manage all DRP test and author all DRP updates.*
- *Determine the magnitude and class of the disaster*
- *Determine what systems and processes have been affected by the disaster*
- *Communicate the disaster to the other disaster recovery teams*
- *Determine what first steps need to be taken by the disaster recovery teams*
- *Keep the disaster recovery teams on track with pre-determined expectations and goals*
- *Keep a record of money spent during the disaster recovery process*
- *Ensure that all decisions made abide by the DRP and policies set by Whidbey Telecom*
- *Get the secondary site ready to restore business operations*
- *Ensure that the secondary site is fully functional and secure*
- *Create a detailed report of all the steps undertaken in the disaster recovery process*
- *Notify the relevant parties once the disaster is over and normal business functionality has been restored*

Contact Information

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Wayne Jeffers	*Primary Disaster Lead*	*360.321.0048*	*360.331.7844*	*425.754.7106*
Fred Crandall	*Secondary Disaster Lead*	*360.321.0044*	*360.672.5902*	*425.754.7107*

Facilities Team

The Facilities Team will be responsible for all issues related to the physical facilities that house IT systems. They are the team that will be responsible for setting up standby facilities and for assessing the damage too and overseeing the repairs to the primary location in the event of the primary location's destruction or damage.

Role & Responsibilities

- *Setup standby facility in the event of a loss of the primary facility*
- *Ensure that transportation is provided for all employees working out of the standby facility*
- *Ensure that sufficient food, drink, and other supplies are provided for all employees working out of the standby facility*
- *Assess, or participate in the assessment of, any physical damage to the primary facility*
- *Ensure that measures are taken to prevent further damage to the primary facility*
- *Work with insurance company in the event of damage, destruction or losses to any assets owned by Whidbey Telecom*
- *Ensure that appropriate resources are provisioned to rebuild or repair the main facilities in the event that they are destroyed or damaged*
- *After Whidbey Telecom is back to business as usual, this team will be required to summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

Contact Information

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Barrett Remmen	*Field Operations Manager*	*360.321.0063*		*425.754.0085*
Barney Mills	*Operations Supervisor*	*360.321.0069*		*425.754.7481*

Network Team

The Network Team will be responsible for assessing damage specific to any network infrastructure and for provisioning data and voice network connectivity including WAN, LAN, and any telephony connections internally within the enterprise as well as telephony and data connections with the outside world and customers. They will be primarily responsible for providing baseline network functionality and may assist other Technology DR Teams as required.

Role & Responsibilities

- *In the event of a disaster that does not require migration to standby facilities, the team will determine which network services are not functioning at the primary facility*
- *If multiple network services are impacted, the team will prioritize the recovery of services in the manner and order that has the least business impact.*
- *For network services provided by third parties, the team will communicate and co-ordinate with these third parties to ensure recovery of connectivity.*
- *In the event of a disaster that does require migration to standby facilities the team will ensure that all network services are brought online at the secondary facility*
- *Once critical systems have been provided with connectivity, employees will be provided with connectivity in the following order:*
    - *All members of the DR Teams*
    - *All C-level and Executive Staff*
    - *All IT employees*
    - *All remaining employees*
- *Install and implement any tools, hardware, software and systems required in the standby facility*
- *Install and implement any tools, hardware, software and systems required in the primary facility*
- *After Whidbey Telecom is back to business as usual, this team will be summarizing any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

Contact Information

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Fred Crandall	*Secondary Disaster Lead*	*360.321.0044*	*360.672.5902*	*425.754.7107*
Leleng Awi	*ISP & Core Network Engineer*	*360-929-8083*		*360-929-8083*
Landon Gibson	*Network Administrator*	*360.321.0003*		*360.682.7363*

Applications and Servers Team

The Applications and Servers Team will be responsible for ensuring that all enterprise applications operate as required to meet business objectives in the event of and during a disaster. They will be primarily responsible for ensuring and validating appropriate application performance and may assist other Technology DR Teams as required.

Role & Responsibilities

- *In the event of a disaster that does not require migration to standby facilities, the team will determine which applications are not functioning at the primary facility*
- *If multiple applications are impacted, the team will prioritize the recovery of applications in the manner and order that has the least business impact. Recovery will include the following tasks:*
    - *Assess the impact to application processes*
    - *Restart applications as required*
    - *Patch, recode or rewrite applications as required*
- *Setup secondary servers in standby facilities with data copies*
- *Install and implement any tools, software and patches required in the standby facility*
- *Install and implement any tools, software and patches required in the primary facility*
- *After Whidbey Telecom is back to business as usual, this team will be summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

Contact Information

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Brian Butt	*Sr Systems Administrator*	*360.321.0043*	*435.554.8229*	*360.929.8449*
Rodolfo Ramos	*Systems Administrator II*	*360.321.0388*	*509.859.2390*	*360.929.5784*
Tony Annese	*Systems Administrator*	*360.321.0042*		*360.754.7320*
Joshua Land	*Sr Voice Engineer*	*360.321.0035*		*360.320.8631*
Darrell Guenther	*Software Developer*	*360.321.0376*		*425.754.8001*
Juliet Chase	*Business Program Manager*	*360.325.3579*		*360.325.3579*

Operations Team

This team's primary goal will be to provide employees with the tools they need to perform their roles as quickly and efficiently as possible. They will need to provision all Whidbey Telecom employees with the tools that their specific role requires.

Role & Responsibilities

- *Maintain lists of all essential supplies that will be required in the event of a disaster*
- *Ensure that these supplies are provisioned appropriately in the event of a disaster*
- *Ensure sufficient spare computers and laptops are on hand so that work is not significantly disrupted in a disaster*
- *Ensure that spare computers and laptops have the required software and patches*
- *Ensure sufficient computer and laptop related supplies such as cables, wireless cards, laptop locks, mice, printers and docking stations are on hand so that work is not significantly disrupted in a disaster*
- *Ensure that all employees that require access to a computer/laptop and other related supplies are provisioned in an appropriate timeframe*
- *If insufficient computers/laptops or related supplies are not available the team will prioritize distribution in the manner and order that has the least business impact*
- *This team will be required to maintain a log of where all of the supplies and equipment were used*
- *After Whidbey Telecom is back to business as usual, this team will be required to summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

Contact Information

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Brian Butt	*Sr Systems Administrator*	*360.321.0043*	*435.554.8229*	*360.929.8449*
Sam Noyes	*Helpdesk Specialist*	*360.321.0031*		*360.320.0088*
Tony Annese	*Systems Administrator*	*360.321.0042*		*360.754.7320*

Senior Management Team

The Senior Management Team will make any business decisions that are out of scope for the Disaster Recovery Lead. Decisions such as constructing a new data center, relocating the primary site etc. should be made by the Senior Management Team. The Disaster Recovery Lead will ultimately report to this team.

Role & Responsibilities

- *Ensure that the Disaster Recovery Team Lead is help accountable for his/her role*
- *Assist the Disaster Recovery Team Lead in his/her role as required*
- *Make decisions that will impact the company. This can include decisions concerning:*
  - *Rebuilding of the primary facilities*
  - *Rebuilding of data centers*
  - *Significant hardware and software investments and upgrades*
  - *Other financial and business decisions*

Contact Information

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Donna Hilty	*COO*	*360.321.0008*		*206.910.1138*
George Henny	*CO-CEO*	*360.321.0014*		*425.754.8080*
Julia Henny	*CO-CEO*	*360.321.0001*		*425.754.7111*

Communication Team

This will be the team responsible for all communication during a disaster. Specifically, they will communicate with Whidbey Telecom's employees, clients, vendors and suppliers, banks, and even the media if required.

Role & Responsibilities

- *Communicate the occurrence of a disaster and the impact of that disaster to all Whidbey Telecom's employees*
- *Communicate the occurrence of a disaster and the impact of that disaster to authorities, as required*
- *Communicate the occurrence of a disaster and the impact of that disaster to all Whidbey Telecom's vendors and contractors*
- *Communicate the occurrence of a disaster and the impact of that disaster to media contacts, as required*
- *After Whidbey Telecom is back to business as usual, this team will be required to summarize any and all costs and will provide a report to the Disaster Recovery Lead summarizing their activities during the disaster*

Contact Information

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Martha Ford	*Marketing Director*	*360.321.0362*		*360.929.2615*
Jennifer Wilkins	*Marketing Specialist*	*360.321.0364*		*360.499.4020*
Joshua Land	*Sr Voice Engineer*	*360.321.0035*		*360.320.8631*

Finance Team

This team will be responsible for ensuring that all of Whidbey Telecom's finances are dealt with in an appropriate and timely manner in the event of a disaster. The finance team will ensure that there is money available for necessary expenses that may result from a disaster as well as expenses from normal day-to-day business functions.

Role & Responsibilities

- *Ensure there is sufficient cash on-hand or accessible to deal with small-scale expenses caused by the disaster. These can include paying for accommodations and food for DR team members, incremental bills, etc.*
- *Ensure there is sufficient credit available or accessible to deal with large-scale expenses caused by the disaster. These can include paying for new equipment, repairs for primary facilities, etc.*
- *Review and approve Disaster Teams' finances and spending*
- *Ensure that payroll occurs and that employees are paid as normal, where possible*
- *Communicate with creditor to arrange suspension of extensions to scheduled payments, as required*
- *Communicate with banking partners to obtain any materials such as checks, bank books etc. that may need to be replaced as a result of the disaster*
- Contact insurance company
    -

Contact Information

Name	Role/Title	Work Phone Number	Home Phone Number	Mobile Phone Number
Gary Ricketts	*Accounting Manager*	*360.321.0051*		*360.929.2035*
Donna Hilty	*COO*	*360.321.0008*		*206.910.1138*

WHIDBEY TELECOM

Internet & WiFi • Telephone Services • Security & Alarms

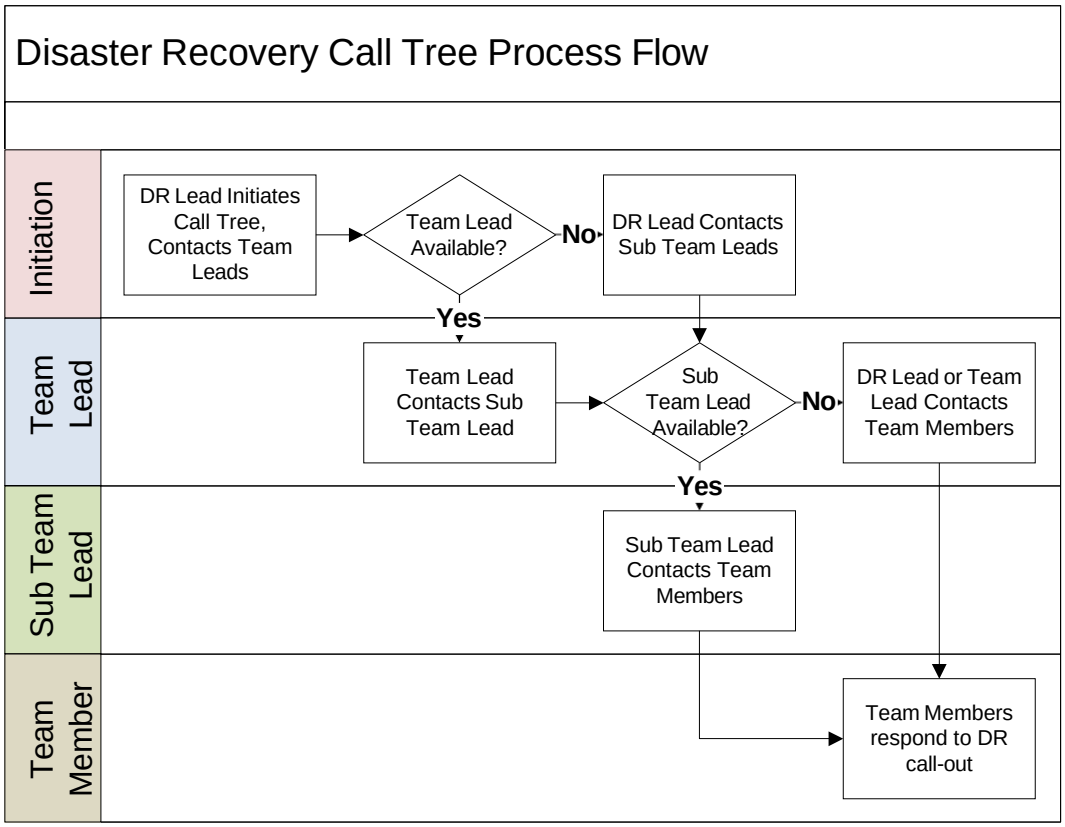
Disaster Recovery Call Tree

In a disaster recovery or business continuity emergency, time is of the essence so Whidbey Telecom will make use of a Call Tree to ensure that appropriate individuals are contacted in a timely manner. Ongoing comunication will flow up and down this tree at regular intervals.

- The Disaster Recovery Team Lead calls all Level 1 Members (Blue cells)
- Level 1 members call all Level 2 team members over whom they are responsible (Green cells)
- Level 1 members call all Level 3 team members over whom they are directly responsible (Beige cells)
- Level 2 Members call all Level 3 team members over whom they are responsible (Beige cells)
- In the event a team member is unavailable, the initial caller assumes responsibility for subsequent calls

Contact	Office	Mobile	Home
DR Lead *Wayne Jeffers*	*360.321.0048*	*425.754.7106*	*360.331.7844*
Management Team Lead *Donna Hilty*	*360.321.0008*	*206.910.1138*	*425.881.1076*
Management Team *George Henny*	*360.321.0014*	*425.754.8080*	
Management Team *Julia Henny*	*360.321.0001*	*425.754.7111*	
Facilities Team Lead *Barrett Remmen*	*360.321.0063*	*425.754.0085*	
Sub Facilities Team Lead *Barney*	*360.321.0069*	*425.754.7481*	
Network Team Lead *Fred Crandall*	*360.321.0044*	*425.754.7107*	*360.672.5902*
Sub Network Team Lead *Leleng Awi*	*360.341.0005*	*360.929.8083*	*360.321.4293*
Network Team *Landon Gibson*	*360.321.0003*	*360.682.7363*	
Applications and Servers Team Lead *Brian Butt*	*360.321.0043*	*360.929.8449*	*435.554.8829*
Sub App & Srv Team Lead *Rodolfo Ramos*	*360.321.0388*	*360.929.5784*	*509.859.2390*

App & Srv Team *Tony Annese*	*360.321.0042*	*360.754.7320*	
App & Srv Team *Joshua Land*	*360.321.0035*	*360.320.8631*	*360.321.4293*
App & Srv Team *Darrell Guenther*	*360.321.0376*	*425.754.8001*	
Operations Team Lead *Brian Butt*	*360.321.0043*	*360.929.8449*	*435.554.8829*
Sub Operations Team Lead *Tony Annese*	*360.321.0042*	*360.754.7320*	
Sub Operations Team Lead *Sam Noyes*	*360.321.0031*	*360.754.7320*	
Communications Team Lead *Martha Ford*	*360.321.0362*	*360.929.2615*	
Sub Comm Team Lead *Jennifer Wilkins*	*360.321.0364*	*360.499.4020*	
Comm Team *Joshua Land*	*360.321.0035*	*360.320.8631*	*360.321.4293*
Finance Team Lead *Gary Ricketts*	*360.321.0051*	*360.929.2035*	
BPO Team *Juliet Chase*		*360.325.3579*	360.341.5412 Low cellular service
Sub BPO Team *Jessica Cooks*	*360.321.0034*	*360.320.5420*	


Disaster Recovery Call Tree Process Flow
Initiation
Team Lead
Sub Team Lead
Team Member
DR Lead Initiates Call Tree, Contacts Team Leads
Team Lead Available?
No
DR Lead Contacts Sub Team Leads
Yes
Team Lead Contacts Sub Team Lead
Sub Team Lead Available?
No
DR Lead or Team Lead Contacts Team Members
Yes
Sub Team Lead Contacts Team Members
Team Members respond to DR call-out

Data and Backups

This section explains where all of the organization's data resides as well as where it is backed up to. Use this information to locate and restore data in the event of a disaster.

Data in Order of Criticality

Rank	Data	Data Type	Back-up Frequency	Backup Location(s)
1	Full SAN Snapshots	All SAN Data	12 hours	Freeland ORM DR SAN
2	OS and Application backup	Veeam	Nightly differential & Weekly full	Freeland ORM BackupNAS
3	O365 Data	Veeam	Nightly	Freeland ORM BackupNAS
4	Meta Switch Backup			

Communicating During a Disaster

In the event of a disaster Whidbey Telecom will need to communicate with various parties to inform them of the effects on the business, surrounding areas and timelines. The Communications Team will be responsible for contacting all of Whidbey Telecom‘s stakeholders.

In the event of a Major Outage as defined by WAC 480-120-412 Whidbey Telecom will need to notify the UTC and submit form 481. Outages that affect any emergency response facility must notify PSAP(s) serving the affected area(s).

Communicating with the Authorities

The Communications Team’s first priority will be to ensure that the appropriate authorities have been notified of the disaster, providing the following information:

- *The location of the disaster*
- *The nature of the disaster*
- *The magnitude of the disaster*
- *The impact of the disaster*
- *Number of E911 customers affected*
- *Assistance required in overcoming the disaster*
- *Anticipated timelines*

Authorities Contacts

Island County	
I-COM 911 Emergency Services	(360) 679 9567
Sheriff	(360) 221-4433
Fire Department	(360) 321-1533
SWF/EMS Ategan Technologies, LLC	(360) 528-3426
Tom Akehurst	(206) 515 3795
Judy Hill Jhill@icom911.org	(360) 720 0052
John "JJ" Jenkins jjenkins@icom911.ortg	(360) 720-3134 help@ategan.com

Whatcom County	
WHAT-COMM Communications Center	(360) 676-6911
FAX	(360) 778-8901
Sheriff	(360) 676-6814
Fire Department	(360) 676-6711
Shelia Hamlin	360 778 8900
Greg Ericsonn Deputy Director	(360) 778 8906
Acct Tech	(360) 778- 8900
Chief Carleton (Fire District #5)	(303) 589-5565
Snohomish County	
SNOCOM	(425)775-5201
FAX	(425) 775-9386
10 Digit Emergency Number	(425) 775-4545
Sheriff	(425) 388-3393
Fire Department	
John "JJ" Jenkins	(360) 720-3134
Lisa Ernst lisa@icom911.org	(360) 320-2118
OPALCO-Rock Island	
(Head Network Tech) Rick Lysen rick@slowdrip.com	(360) 502-5555
(Network Eng.) Seb Ghizzo seb@binarynw.com	(360) 746-1186
San Juan 911 and Information Services	
(IS Net Admin) Norm Varsovia normv@sanjuanco.com	(360) 370-7412
(IT Mgr.) Tony Harrell tonyh@sanjuanco.com	(360) 370-7405
EOC	
Email:	E911Outages@mil.wa.gov
Phone:	800.258.5990
WUTC	
Detailed Report Email	telecom-outage@utc.wa.gov
Phone	(888) 333-9882
Department of Homland Security	
Phone	(360) 945-5211

Communicating with Employees

The Communications Team's second priority will be to ensure that the entire company has been notified of the disaster. The best and/or most practical means of contacting all of the employees will be used with preference on the following methods (in order):

- *E-mail (via corporate e-mail where that system still functions)*
- *Telephone to employee mobile phone number*
- *Telephone to employee home phone number*

The employees will need to be informed of the following:

- *Whether it is safe for them to come into the office*
- *Where they should go if they cannot come into the office*
- *Which services are still available to them*
- *Work expectations of them during the disaster*

Communicating with Customers

After all of the organization's employees have been informed of the disaster, the Communications Team will be responsible for informing customers of the disaster and the impact that it will have on the list below. This will be done with a combination of website postings, social media and physical signage as needed. It is critical that the communications team do as much as possible to manage the company's reputation.

- *Anticipated impact on service offerings*
- *Anticipated impact on delivery schedules*
- *Anticipated impact on security of client information*
- *Anticipated timelines*
- *Recovery status*
- *After event reports for reputation management*

Crucial customers will be made aware of the disaster situation first. Crucial customers will be E-mailed first then called after to ensure that the message has been delivered.

Crucial Customers

Company Name	Point of Contact	Phone Number	E-mail
South Whidbey Fire/EMS	Terry Ney	360-321-2546	ops@swfe.org
Port of South Whidbey	Molly Macleod	360-331-5494	molly@portofsouthwhidbey.com
BNSF Railway	Lisa Horton	817-352-4408	lisa.horton@bnsf.com
South Whidbey School Distr	Ian Turner	360-221-0602	technology@sw.wednet.edu
Whidbey Health	Kati Phips	360-682-2810	phppk@whidbeyhealth.org
Whidbey Medical Center EMS	Robert Huff	253-324-4496	huffro@whidbeyhealth.org
Wave/Divison Holdings	Margret Blackburne	732-715-8940	margaret.blackburne@astound.com
City Of Langley	Alex Cattand	360-221-4214	permittech@langleywa.org

Point Roberts Fire Dept	Christopher Carleton	360-945-3473	chief@wcfd5.com
Whatcom County Fire Distr 5	Christopher Carleton	360-945-3474	chief@wcfd5.com
Is Co Emergency Srvs comm	Lisa Ernst	360-675-3752	lisa@icom911.org
Whatcom County Sherrifs office	Robert Greene	360-778-7166	rgreene@cowhatcom.wa.us
Wholesail Networks	Chet Lange	360-340-1088	chet.lange@astound.com
Port of Coupeville	Chris Michalopoulos	360-222-3151	executivedirector@portofcoupeville.org
Clinton Water District	Adam Lehman	360-341-5487	cwd@whidbey.com
Freeland Water District	Andy Campbell	360-331-5566	gotwater@live.com
Hat Island Water Treatment	Sandy Bettencourt	360-444-6611	hioffice@hatisland.com
Point Roberts Water District #4	Dan Bourks	360-945-4696	prwd@whidbey.com

Communicating with Vendors and Contractors

After all of the organization's employees have been informed of the disaster, the Communications Team will be responsible for informing vendors and contractors of the disaster and the impact that it will have on the following:

- *Adjustments to service requirements*
- *Adjustments to delivery locations*
- *Adjustments to contact information*
- *Anticipated timelines*

Crucial vendors and contractors will be made aware of the disaster situation first. Crucial vendors and contractors will be E-mailed first then called after to ensure that the message has been delivered. All other vendors and contractors will be contacted only after all crucial vendors have been contacted.

Vendors and contractors encompass those organizations that provide everyday services to the enterprise, but also the hardware and software companies that supply the Technology department. The Communications Team will act as a go-between between the DR Team leads and vendor contacts should additional Technology infrastructure be required.

Crucial Vendors and Contractors

Company Name	Point of Contact	Phone Number	E-mail
Astound	*Carrier Support*	*888 317 0488*	
Centurylink/Lumen	Account Contacts	888 678 8080 opt 1 opt 2	wendy.gray@centurylink.com
Bell Canada	Michael Danhelka	604-678-7748	michael.Danhelka@bell.ca
Prime electric			

Communicating with the Media

After all of the organization's employees have been informed of the disaster, the Communications Team will be responsible for informing media outlets of the disaster, providing the following information:

- *An official statement regarding the disaster*
- *The magnitude of the disaster*
- *The impact of the disaster*
- *Anticipated timelines*

Media Contacts

Company Name	Point of Contact	Phone Number	E-mail
Whidbey news group	*Editor*		editor@whidbeynewsgroup.com
Hat Island Community Association			hioffice@hatisland.org
The Northern Light	*Editor*		editor@thenorthernlight.com

Dealing with a Disaster

If a disaster occurs in Whidbey Telecom, the first priority is to ensure that all employees are safe and accounted for. After this, steps must be taken to mitigate any further damage to the facility and to reduce the impact of the disaster to the organization.

Regardless of the category that the disaster falls into, dealing with a disaster can be broken down into the following steps:

1) Disaster identification and declaration
2) DRP activation
3) Communicating the disaster
4) Assessment of current and prevention of further damage
5) Standby facility activation
6) Establish IT operations
7) Repair and rebuilding of primary facility

Disaster Identification and Declaration

Since it is almost impossible to predict when and how a disaster might occur, Whidbey Telecom must be prepared to find out about disasters from a variety of possible avenues. These can include:

- *First hand observation*
- *System Alarms and Network Monitors*
- *Environmental and Security Alarms in the Primary Facility*
- *Staff*
- *End users*
- *3rd Party*
- *Media reports*

Once the Disaster Recovery Lead has determined that a disaster had occurred, s/he must officially declare that the company is in an official state of disaster. It is during this phase that the Disaster Recovery Lead must ensure that anyone that was in the primary facility at the time of the disaster has been accounted for and evacuated to safety according to the company's Evacuation Policy.

While employees are being brought to safety, the Disaster Recovery Lead will instruct the Communications Team to begin contacting the Authorities and all employees not at the impacted facility that a disaster has occurred.

DRP Activation

Once the Disaster Recovery Lead has formally declared that a disaster has occurred s/he will initiate the activation of the DRP by triggering the Disaster Recovery Call Tree. The following information will be provided in the calls that the Disaster Recovery Lead makes and should be passed during subsequent calls:

- *That a disaster has occurred*
- *The nature of the disaster (if known)*
- *The initial estimation of the magnitude of the disaster (if known)*
- *The initial estimation of the impact of the disaster (if known)*
- *The initial estimation of the expected duration of the disaster (if known)*
- *Actions that have been taken to this point*
- *Actions that are to be taken prior to the meeting of Disaster Recovery Team Leads*
- *Scheduled meeting place for the meeting of Disaster Recovery Team Leads*
- *Scheduled meeting time for the meeting of Disaster Recovery Team Leads*
- *Any other pertinent information*

If the Primary and Secondary Disaster Recovery Leads are unavailable to trigger the Disaster Recovery Call Tree, that responsibility shall fall to the Management Team Lead

Communicating the Disaster

Refer to the “Communicating During a Disaster” section of this document.

Assessment of Current and Prevention of Further Damage

Before any employees from Whidbey Telecom can enter the primary facility after a disaster, appropriate authorities must first ensure that the premises are safe to enter.

The first team that will be allowed to examine the primary facilities once it has been deemed safe to do so will be the Facilities Team. Once the Facilities Team has completed an examination of the building and submitted its report to the Disaster Recovery Lead, the Management, Networks, and Operations Teams will be allowed to examine the building. All teams will be required to create an initial report on the damage and provide this to the Disaster Recovery Lead within one hour of the initial disaster.

During each team’s review of their relevant areas, they must assess any areas where further damage can be prevented and take the necessary means to protect Whidbey Telecom’s assets. Any necessary repairs or preventative measures must be taken to protect the facilities; these costs must first be approved by the Disaster Recovery Team Lead.

Standby Facility Setup and Activation

The Standby Facility will be formally requested when the Disaster Recovery Lead determines that the nature of the disaster is such that the primary facility is no longer sufficiently functional or operational to sustain normal business operations.

Once this determination has been made, the Facilities Team will be commissioned to setup a Standby Facility to functional status after which the Disaster Recovery Lead will convene a meeting of the various Disaster Recovery Team Leads at the Standby Facility to assess next steps. These next steps will include:

1. *Determination of impacted systems*
2. *Criticality ranking of impacted systems*
3. *Recovery measures required for high criticality systems*
4. *Assignment of responsibilities for high criticality systems*
5. *Schedule for recovery of high criticality systems*
6. *Recovery measures required for medium criticality systems*
7. *Assignment of responsibilities for medium criticality systems*
8. *Schedule for recovery of medium criticality systems*
9. *Recovery measures required for low criticality systems*
10. *Assignment of responsibilities for recovery of low criticality systems*
11. *Schedule for recovery of low criticality systems*
12. *Determination of facilities tasks outstanding/required at Standby Facility*
13. *Determination of operations tasks outstanding/required at Standby Facility*
14. *Determination of communications tasks outstanding/required at Standby Facility*
15. *Determination of facilities tasks outstanding/required at Primary Facility*
16. *Determination of other tasks outstanding/required at Primary Facility*
17. *Determination of further actions to be taken*

During Standby Facility activation, the Facilities, Networks, Servers, Applications, and Operations teams will need to ensure that their responsibilities, as described in the “Disaster Recovery Teams and Responsibilities” section of this document are carried out quickly and efficiently so as not to negatively impact the other teams.

Restoring IT Functionality

Should a disaster actually occur and Whidbey Telecom need to exercise this plan, this section will be referred to frequently as it will contain all of the information that describes the manner in which Whidbey Telecom's information system will be recovered.

Current System Architecture

System Architecture Diagram

IT Systems

Rank	IT System	System Components (In order of importance)
1	Hyper-Visor	VMWare UCS clusters, SAN01, SANDR, vCenter70
2	Customer/Public DNS	Nspower, nsmax, nsnew, dns1-2
3	Corporate Email	VESA01, DC1-2016, AAD Sync (CA), Firewall01
4	Customer Email	mailfw1, mailfw2, mailldap, atsql, atsqllog, atdns, passwd, spamd1-5, mailtool, uatsmtp3-5, atstore, webmailadmin, uatmail(1,6,8,9,10), roundcube
5	NISC	51510app, 51510apqa, 51510dbqa, 51510gis, 51510ivr, 51510uss, 51510vlt, 51510vltqa, 51510web
6	Accounting services	FireboxV-Accounting01, DHCP, Veritas01, View01, UAG01, RDgateway01 AccountingFiles01, vm-acct-001-0014, vm-acct-LMcMa, JOHN-GEVAERT
7	Customer Webservers	Dmzldap, dmzsql, ntp, apwsvirt, apwsvirt2
8	Customer Service	Newterm, vm-cc-001-019, UCS-TNS cluster VMs, SharePoint, Alarm Cluster, Manitou1, Manitou2, Stealth1, Stealth2
9	File services	Fileserver01, SharePoint, OneDrive, Veritas01
10	SQL servers	SQL01, SQL2008, Report01
11	Corp VDI VMs	vm-corp-001-027
12	OpenVPN	VPNhost, OpenVPN Access Server, VPN-pfSense
13	Genetec	Security01

Criticality Rank-One Hyper-Visor

System Name	Hyper-Visor
Component Name	Cisco UCS 5108 Chassis 01
Vendor Name	Cisco
Model Number	5108
Serial Number	FOX1420H4XE
Recovery Time Objective	15 minuets
Recovery Point Objective	Have Hardware to run Virtual Machines on

Title: Standard Operating Procedures for Starting UCS cluster
Document No.: Disaster recovery SOP #1

System Name	Hyper-Visor
Component Name	Cisco UCS 5108 Chassis 02
Vendor Name	Cisco
Model Number	5108
Serial Number	FOX1420GC78
Recovery Time Objective	15 minuets
Recovery Point Objective	Have Hardware to run Virtual Machines on

Title: Standard Operating Procedures for Starting UCS cluster
Document No.: Disaster recovery SOP #1

System Name	Hyper-Visor
Component Name	Cisco UCS 5108 Chassis 03
Vendor Name	Cisco
Model Number	5108
Serial Number	FOX1421GMC5
Recovery Time Objective	15 minuets
Recovery Point Objective	Have Hardware to run Virtual Machines on

Title: Standard Operating Procedures for Starting UCS cluster
Document No.: Disaster recovery SOP #1

System Name	Hyper-Visor
Component Name	Cisco UCS 5108 Chassis 04
Vendor Name	Cisco
Model Number	5108
Serial Number	<<>>
Recovery Time Objective	15 minuets
Recovery Point Objective	Have Hardware to run Virtual Machines on

Title: Standard Operating Procedures for Starting UCS cluster
Document No.: Disaster recovery SOP #1

System Name	Hyper-Visor
Component Name	Cisco UCS 5108 Chassis 05
Vendor Name	Cisco
Model Number	5108
Serial Number	<<>>
Recovery Time Objective	15 minuets
Recovery Point Objective	Have Hardware to run Virtual Machines on

Title: Standard Operating Procedures for Starting UCS cluster
Document No.: Disaster recovery SOP #1

System Name	Hyper-Visor
Component Name	SAN01
Vendor Name	Dell
Model Number	PowerStore 1000T
Serial Number	862XCJ3
Recovery Time Objective	15 minuets
Recovery Point Objective	Restore Virtual disks for the Virtual Machines

Title: Standard Operating Procedures for Starting Dell SAN
Document No.: Disaster recovery SOP #2

System Name	Hyper-Visor
Component Name	SANDR
Vendor Name	Dell
Model Number	PowerStore 1000T
Serial Number	762XCJ3
Recovery Time Objective	15 minuets
Recovery Point Objective	Restore Virtual disks for the Virtual Machines

Title: Standard Operating Procedures for Starting Dell SAN
Document No.: Disaster recovery SOP #2

System Name	Hyper-Visor
Component Name	vCenter70
Vendor Name	VMWare
Model Number	VMware Photon OS
Serial Number	N/A
Recovery Time Objective	15 minuets
Recovery Point Objective	Restore VMWare functions

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

Criticality Rank-Two Customer/Public DNS

System Name	Customer/Public DNS
Component Name	nspower
Vendor Name	Debian
Model Number	Debian 9
Serial Number	N/A
Recovery Time Objective	10 Minutes
Recovery Point Objective	VM to start

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

System Name	Customer/Public DNS
Component Name	nsmax
Vendor Name	CentOS
Model Number	CentOS 9
Serial Number	N/A
Recovery Time Objective	10 Minutes
Recovery Point Objective	VM to start

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

System Name	Customer/Public DNS
Component Name	Nsnew
Vendor Name	CentOS
Model Number	CentOS 9
Serial Number	N/A
Recovery Time Objective	10 Minutes
Recovery Point Objective	VM to start

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

System Name	Customer/Public DNS
Component Name	DNS1-2
Vendor Name	Debian
Model Number	Bebian 11
Serial Number	N/A
Recovery Time Objective	10 Minutes
Recovery Point Objective	VM to start

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

Criticality Rank-Three Corporate Email

System Name	O365 Email
Component Name	VESA01
Vendor Name	Cisco
Model Number	AsyncOS Version: 14.0.2-020
Serial Number	N/A
Recovery Time Objective	15 Min
Recovery Point Objective	Allow inbound email to be scanned and sent on to office365

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

System Name	O365 Email
Component Name	DC1-2016
Vendor Name	Cisco
Model Number	Windows Server 2016
Serial Number	N/A
Recovery Time Objective	20
Recovery Point Objective	Sync active directory credentials to Office365

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

System Name	O365 Email
Component Name	Firewall01
Vendor Name	Cisco
Model Number	Windows Server 2016
Serial Number	N/A
Recovery Time Objective	15 Min
Recovery Point Objective	Allow email and AD traffic to route to the internet

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

Criticality Rank-Four Customer Email

System Name	Customer Email
Component Name	mailfw1-2
Vendor Name	Firewall
Model Number	N/A
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Mail firewalls to allow for mail flow

Title: Standard Operating Procedures for Restoring VM Appliance from backup
Document No.: Disaster recovery SOP #3

System Name	Customer Email
Component Name	mailldap
Vendor Name	Debian
Model Number	Debian 10
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore email flow

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

System Name	Customer Email
Component Name	atsql
Vendor Name	Debian
Model Number	Debian 10
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore email flow

Title: Standard Operating Procedures for Restoring VM Appliance from backup
Document No.: Disaster recovery SOP #3

System Name	Customer Email
Component Name	atsqllog
Vendor Name	Debian
Model Number	Debian 10
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore email flow

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

System Name	Customer Email
Component Name	atdns
Vendor Name	Debian
Model Number	Debian 10
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore email flow

Title: Standard Operating Procedures for Restoring VM Appliance from backup
Document No.: Disaster recovery SOP #3

System Name	Customer Email
Component Name	passwd
Vendor Name	Debian
Model Number	Debian 10
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore email flow

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

System Name	Customer Email
Component Name	spamd1-5
Vendor Name	Debian
Model Number	Debian 10
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore email flow

Title: Standard Operating Procedures for Restoring VM Appliance from backup
Document No.: Disaster recovery SOP #3

System Name	Customer Email
Component Name	mailtool
Vendor Name	Debian
Model Number	Debian 10
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore email flow

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

System Name	Customer Email
Component Name	uatsmtp3-5
Vendor Name	Debian
Model Number	Debian 10
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore email flow

Title: Standard Operating Procedures for Restoring VM Appliance from backup
Document No.: Disaster recovery SOP #3

System Name	Customer Email
Component Name	atstore
Vendor Name	Debian
Model Number	Debian 10
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore email flow

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

System Name	Customer Email
Component Name	webmailadmin
Vendor Name	Debian
Model Number	Debian 10
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore email flow

Title: Standard Operating Procedures for Restoring VM Appliance from backup
Document No.: Disaster recovery SOP #3

System Name	Customer Email
Component Name	uatmail(1,6,8,9,10)
Vendor Name	Debian
Model Number	Debian 10
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore email flow

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

System Name	Customer Email
Component Name	roundcube
Vendor Name	Debian
Model Number	Debian 10
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore email flow

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

Criticality Rank-Five NISC

System Name	NISC
Component Name	51510app
Vendor Name	NISC
Model Number	SUSE Linux Enterprise 12
Serial Number	N/A
Recovery Time Objective	30 Min
Recovery Point Objective	Restore core business functions

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

System Name	NISC
Component Name	51510apqa
Vendor Name	NISC
Model Number	SUSE Linux Enterprise 12
Serial Number	N/A
Recovery Time Objective	30 Min
Recovery Point Objective	Restore core business functions

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

System Name	NISC
Component Name	51510dbqa
Vendor Name	NISC
Model Number	SUSE Linux Enterprise 12
Serial Number	N/A
Recovery Time Objective	30 Min
Recovery Point Objective	Restore core business functions

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

System Name	NISC
Component Name	51510gis
Vendor Name	NISC
Model Number	Microsoft Windows Server 2016
Serial Number	N/A
Recovery Time Objective	30 Min
Recovery Point Objective	Restore core business functions

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

System Name	NISC
Component Name	51510ivr
Vendor Name	NISC
Model Number	SUSE Linux Enterprise 12
Serial Number	N/A
Recovery Time Objective	30 Min
Recovery Point Objective	Restore core business functions

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

System Name	NISC
Component Name	51510uss
Vendor Name	NISC
Model Number	SUSE Linux Enterprise 12
Serial Number	N/A
Recovery Time Objective	30 Min
Recovery Point Objective	Restore core business functions

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

System Name	NISC
Component Name	51510vlt
Vendor Name	NISC
Model Number	SUSE Linux Enterprise 12
Serial Number	N/A
Recovery Time Objective	30 Min
Recovery Point Objective	Restore core business functions

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

System Name	NISC
Component Name	51510vltqa
Vendor Name	NISC
Model Number	SUSE Linux Enterprise 12
Serial Number	N/A
Recovery Time Objective	30 Min
Recovery Point Objective	Restore core business functions

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

System Name	NISC
Component Name	51510web
Vendor Name	NISC
Model Number	SUSE Linux Enterprise 12
Serial Number	N/A
Recovery Time Objective	30 Min
Recovery Point Objective	Restore core business functions

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

Criticality Rank-Six Accounting services

System Name	Accounting services
Component Name	FireboxV-Accounting01
Vendor Name	Linux
Model Number	4.x or later Linux
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore firewall for the accounting services

Title: Standard Operating Procedures for Restoring VM Appliance from backup
Document No.: Disaster recovery SOP #3

System Name	Accounting services
Component Name	DHCP
Vendor Name	Microsoft
Model Number	Windows Server 2016
Serial Number	N/A
Recovery Time Objective	1 Hour
Recovery Point Objective	Restore DHCP

Title: Standard Operating Procedures for Restoring VM server from backup
Document No.: Disaster recovery SOP #4

System Name	Accounting services
Component Name	View01
Vendor Name	VMware
Model Number	Windows Server 2016
Serial Number	N/A
Recovery Time Objective	1 hour 30 min
Recovery Point Objective	Restore terminal services

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

System Name	Accounting services
Component Name	UAG01
Vendor Name	VMware
Model Number	VMware Photon OS
Serial Number	N/A
Recovery Time Objective	1 hour 30 min
Recovery Point Objective	Restore terminal services

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

System Name	Accounting services
Component Name	RDgateway01
Vendor Name	Microsoft
Model Number	Microsoft Windows Server 2016
Serial Number	N/A
Recovery Time Objective	1 hour 30 min
Recovery Point Objective	Restore terminal services

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

System Name	Accounting services
Component Name	Veritas01
Vendor Name	Dell
Model Number	PowerEdge R640
Serial Number	6TJJG73
Recovery Time Objective	1 hour
Recovery Point Objective	Have server for restoring backups

Title: Standard Operating Procedures for Restoring Physical Server from backup
Document No.: Disaster recovery SOP #5

System Name	Accounting services
Component Name	vm-acct-001 -014,
Vendor Name	VMWare/Microsoft
Model Number	Windows 10
Serial Number	N/A
Recovery Time Objective	1 Hour
Recovery Point Objective	Restore virtual desktops accounting users

Title: Standard Operating Procedures for Restoring VDI cluster
Document No.: Disaster recovery SOP #6

System Name	Accounting services
Component Name	vm-acct-LMcMa,
Vendor Name	Microsoft
Model Number	Windows 10
Serial Number	N/A
Recovery Time Objective	1 Hour
Recovery Point Objective	Restore virtual desktop for Lei McManus

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

WHIDBEY TELECOM

Internet & WiFi • Telephone Services • Security & Alarms

System Name	Accounting services
Component Name	JOHN-GEVAERT
Vendor Name	Microsoft
Model Number	Windows 10
Serial Number	N/A
Recovery Time Objective	1 Hour
Recovery Point Objective	Restore virtual desktop for John Gevaert

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

Criticality Rank-Seven Customer Webservers

System Name	Customer Webservers
Component Name	Dmzldap
Vendor Name	Debian
Model Number	Debian
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore customer webserver authentication

Title: Standard Operating Procedures for Restoring VM Appliance from backup
Document No.: Disaster recovery SOP #3

System Name	Customer Webservers
Component Name	dmzsql
Vendor Name	Debian
Model Number	Debian
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore customer webserver database

Title: Standard Operating Procedures for Restoring VM Appliance from backup
Document No.: Disaster recovery SOP #3

System Name	Customer Webservers
Component Name	ntp
Vendor Name	symetricom
Model Number	SSU2000
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore customer network time server

Title: Standard Operating Procedures for Restoring VM Appliance from backup
Document No.: Disaster recovery SOP #3

System Name	Customer Webservers
Component Name	apwsvirt
Vendor Name	Debian
Model Number	Debian 9
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore customer webserver hoasting

Title: Standard Operating Procedures for Restoring VM Appliance from backup
Document No.: Disaster recovery SOP #3

System Name	Customer Webservers
Component Name	Apwsvirt2
Vendor Name	Debian
Model Number	Debian 11
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore customer webserver hoasting

Title: Standard Operating Procedures for Restoring VM Appliance from backup
Document No.: Disaster recovery SOP #3

Criticality Rank-Eight Customer Service

System Name	Customer Service
Component Name	Newterm
Vendor Name	Dell
Model Number	PowerEdge R740
Serial Number	582J513
Recovery Time Objective	1 hour 30 min
Recovery Point Objective	Restore terminal services

Title: Standard Operating Procedures for Restoring Physical Server from Backup
Document No.: Disaster recovery SOP #5

System Name	Customer Service
Component Name	vm-cc-001-019
Vendor Name	VMWare/Microsoft
Model Number	Windows 10
Serial Number	N/A
Recovery Time Objective	1 hour 30 min
Recovery Point Objective	Restore Virtual desktops for customer service agents

Title: Standard Operating Procedures for Restoring VDI cluster
Document No.: Disaster recovery SOP #6

System Name	Customer Service
Component Name	MsDCM1
Vendor Name	Meta Switch
Model Number	CentOS 6
Serial Number	N/A
Recovery Time Objective	1 hour 30 min
Recovery Point Objective	Enable voice calling

Title: Standard Operating Procedures for Restoring Meta Switch VMs
Document No.: Disaster recovery SOP #7

System Name	Customer Service
Component Name	MsEAS
Vendor Name	Meta Switch
Model Number	CentOS 7
Serial Number	N/A
Recovery Time Objective	1 hour 30 min
Recovery Point Objective	Enable voice calling

Title: Standard Operating Procedures for Restoring Meta Switch VMs
Document No.: Disaster recovery SOP #7

System Name	Customer Service
Component Name	alarm-01
Vendor Name	Dell
Model Number	PowerEdge R730
Serial Number	DMKJKB2
Recovery Time Objective	1 hour 30 min
Recovery Point Objective	Restore Hosts for Alarm Monitoring Software

Title: Standard Operating Procedures for Restoring VMWare hosts
Document No.: Disaster recovery SOP #8

System Name	Customer Service
Component Name	alarm-02
Vendor Name	Dell
Model Number	PowerEdge R730
Serial Number	JYVRHB2
Recovery Time Objective	1 hour 30 min
Recovery Point Objective	Restore Hosts for Alarm Monitoring Software

Title: Standard Operating Procedures for Restoring VMWare hosts
Document No.: Disaster recovery SOP #8

System Name	Customer Service
Component Name	Manitou1
Vendor Name	Microsoft
Model Number	Windows server 2012
Serial Number	N/A
Recovery Time Objective	1 hour 30 min
Recovery Point Objective	Restore VM for Alarm Monitoring

Title: Standard Operating Procedures for Restoring Alarm Monitoring VM
Document No.: Disaster recovery SOP #9

System Name	Customer Service
Component Name	Manitou1
Vendor Name	Microsoft
Model Number	Windows server 2012
Serial Number	N/A
Recovery Time Objective	1 hour 30 min
Recovery Point Objective	Restore VM for Alarm Monitoring

Title: Standard Operating Procedures for Restoring Alarm Monitoring VM
Document No.: Disaster recovery SOP #9

System Name	Customer Service
Component Name	Stealth1
Vendor Name	Microsoft
Model Number	Windows server 2012
Serial Number	N/A
Recovery Time Objective	1 hour 30 min
Recovery Point Objective	Restore VM for Alarm Monitoring

Title: Standard Operating Procedures for Restoring Alarm Monitoring VM
Document No.: Disaster recovery SOP #9

System Name	Customer Service
Component Name	Stealth2
Vendor Name	Microsoft
Model Number	Windows server 2012
Serial Number	N/A
Recovery Time Objective	1 hour 30 min
Recovery Point Objective	Restore VM for Alarm Monitoring

Title: Standard Operating Procedures for Restoring Alarm Monitoring VM
Document No.: Disaster recovery SOP #9

Criticality Rank-Nine File Services

System Name	File Services
Component Name	Fileserver01
Vendor Name	Microsoft
Model Number	Microsoft Windows Server 2016
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore Windows file shares

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

Criticality Rank-Ten SQL Servers

System Name	SQL Servers
Component Name	SQL01
Vendor Name	Microsoft
Model Number	Windows Server 2016
Serial Number	N/A
Recovery Time Objective	1 hour 30 Min
Recovery Point Objective	Restore Databases

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

System Name	SQL Servers
Component Name	SQL2008
Vendor Name	Microsoft
Model Number	Windows Server 2019
Serial Number	N/A
Recovery Time Objective	1 hour 30 Min
Recovery Point Objective	Restore Mapping Database

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

System Name	SQL Servers
Component Name	Report01
Vendor Name	Microsoft
Model Number	Windows Server 2016
Serial Number	N/A
Recovery Time Objective	1 hour 30 Min
Recovery Point Objective	Restore reporting services

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

Criticality Rank-Eleven Corp VDI VM's

System Name	Corp VDI VMs
Component Name	VDI VMs vm-corp-001-027
Vendor Name	VMware/Microsoft
Model Number	Windows 10
Serial Number	N/A
Recovery Time Objective	1 hour
Recovery Point Objective	Restore virtual desktops for corporate users

Title: Standard Operating Procedures for Restoring VDI cluster
Document No.: Disaster recovery SOP #6

Criticality Rank-Twelve OpenVPN

System Name	OpenVPN
Component Name	VPNHost
Vendor Name	Dell
Model Number	VEP-4600-V930
Serial Number	2T5R363
Recovery Time Objective	2 hours
Recovery Point Objective	Restore inbound VPN for remote work

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

System Name	OpenVPN
Component Name	OpenVPN Access Server
Vendor Name	OpenVPN
Model Number	Ubuntu Linux
Serial Number	N/A
Recovery Time Objective	2 hours
Recovery Point Objective	Restore inbound VPN for remote work

Title: Standard Operating Procedures for Restoring VM Appliance from Backup
Document No.: Disaster recovery SOP #3

System Name	OpenVPN
Component Name	VPN-pfSense
Vendor Name	pfSense
Model Number	Virtual Machine
Serial Number	
Recovery Time Objective	
Recovery Point Objective	

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

Criticality Rank-Thirteen Genetec

System Name	Genetec
Component Name	Security01
Vendor Name	Microsoft
Model Number	Windows Server 2016
Serial Number	N/A
Recovery Time Objective	2 hours
Recovery Point Objective	Enable the door locks to work with keycards

Title: Standard Operating Procedures for Restoring VM Server from Backup
Document No.: Disaster recovery SOP #4

Plan Testing & Maintenance

While efforts will be made initially to construct this DRP is as complete and accurate a manner as possible, it is essentially impossible to address all possible problems at any one time. Additionally, over time the Disaster Recovery needs of the enterprise will change. As a result of these two factors this plan will need to be tested on a periodic basis to discover errors and omissions and will need to be maintained to address them.

- Make Sure the DRP is Ready for a Disaster

Maintenance

The DRP will be updated annually or any time a major system update or upgrade is performed, whichever is more often. The Disaster Recovery Lead will be responsible for updating the entire document, and so is permitted to request information and updates from other employees and departments within the organization in order to complete this task.

Maintenance of the plan will include (but is not limited to) the following:

1. *Ensuring that call trees are up to date*
2. *Ensuring that all team lists are up to date*
3. *Reviewing the plan to ensure that all of the instructions are still relevant to the organization*
4. *Making any major changes and revisions in the plan to reflect organizational shifts, changes and goals*
5. *Ensuring that the plan meets any requirements specified in new laws*
6. *Other organizational specific maintenance goals*

During the Maintenance periods, any changes to the Disaster Recovery Teams must be accounted for. If any member of a Disaster Recovery Team no longer works with the company, it is the responsibility of the Disaster Recovery Lead to appoint a new team member.

Testing

Whidbey Telecom is committed to ensuring that this DRP is functional. The DRP should be tested every 3months in order to ensure that it is still effective. Testing the plan will be carried out as follows:

1) **Walkthroughs**- Team members verbally go through the specific steps as documented in the plan to confirm effectiveness, identify gaps, bottlenecks or other weaknesses. This test provides the opportunity to review a plan with a larger subset of people, allowing the DRP project manager to draw upon a correspondingly increased pool of knowledge and experiences. Staff should be familiar with procedures, equipment, and offsite facilities (if required).
2) **Simulations**- A disaster is simulated so normal operations will not be interrupted. Hardware, software, personnel, communications, procedures, supplies and forms, documentation, transportation, utilities, and alternate site processing should be thoroughly tested in a simulation test. However, validated checklists can provide a reasonable level of assurance for many of these scenarios. Analyze the output of the previous tests carefully before the proposed simulation to ensure the lessons learned during the previous phases of the cycle have been applied.
3) **Parallel Testing**- A parallel test can be performed in conjunction with the checklist test or simulation test. Under this scenario, historical transactions, such as the prior business day's transactions are processed against preceding day's backup files at the contingency processing site or hot site. All reports produced at the alternate site for the current business date should agree with those reports produced at the alternate processing site.
4) **Full-Interruption Testing**- A full-interruption test activates the total DRP. The test is likely to be costly and could disrupt normal operations, and therefore should be approached with caution. The importance of due diligence with respect to previous DRP phases cannot be overstated.

Any gaps in the DRP that are discovered during the testing phase will be addressed by the Disaster Recovery Lead as well as any resources that he/she will require.

.