Disaster Recovery Summary Plan

A platform you can build on

Clarity Human Services provides communities with a secure, compliant way to confidently share and collaborate around sensitive data.

Bitfocus Disaster Recovery Plan Summary Document

Note: One of the objectives of our Information Security Department is to establish an IT Disaster Recovery Plan. This Disaster Recovery Plan document was created to assist Bitfocus in the development of consistent and cohesive IT Disaster Recovery Plans. This is a summary document which omits key infrastructure references to protect our Information Security Infrastructure.

Introduction

The purpose of this summary is to document a Disaster Recovery Plan that addresses information resources as they may be affected in the event of a disaster. This document is meant to minimize any of these effects, and enable Clarity Human Services to either maintain, or quickly resume, mission-critical functions. This Disaster Recovery Plan also serves as the primary guide for Bitfocus, Information Technology Services Department in the recovery and restoration of the information technology systems in the event that they are damaged or destroyed as a result of a disaster.

Document Overview

The Disaster Recovery Plan is composed of numerous sections documenting the resources and procedures to be used in the event that a disaster occurs at the data center, which is located at Flexential in Las Vegas, Nevada. Separate sections are devoted to the specific recovery procedures for each supported application or platform. Also included are sections documenting the personnel requirements that are necessary to perform each recovery task. This plan will be updated on a regular basis as changes to the computing and networking systems are made. Due to the very sensitive nature of the information contained in the plan, this summary omits several key references.

PERSONNEL AUTHORIZED TO DECLARE A DISASTER OR RESUME NORMAL OPERATIONS

Robert Herdzik, Founder & CEO
Jeffrey Ugai, Cheif Operating Officer
Tauri Royce, Vice President of Customer Experience

Disaster Recovery Plan Summary

Plan Activation

This plan will be activated in response to internal or external threats to the Information Technology Systems of Bitfocus Internal threats could include fire, bomb threat, loss of power or other utility or other incidents that threaten the staff and/or the facility. External threats include events that put the facility in danger. Examples might include severe weather or a disruptive incident in the community. Once a threat has been confirmed, the plan management team will assess the situation and initiate the plan if necessary.

Resumption of Normal Activities

Once the threat has passed, equipment will be repaired and/or replaced, and/or a new data center will be transitioned. The disaster recovery team will then assess the situation; If the disaster has expired, the team will resume normal operations.

Plan Objectives

The primary objectives of this plan are to protect Silver Spur Systems' computing resources, to safeguard the vital records of which Bitfocus is the custodian, and to guarantee the continued availability of essential IT services. The role of this plan is to document the pre-agreed decisions and to design and implement a sufficient set of procedures for responding to a disaster that involves the data center and its services.

A disaster is defined as the occurrence of any event that causes a significant disruption in IT capabilities. This plan assumes the most severe disaster, the kind that requires moving computing resources to another location. Less severe disasters are controlled at the appropriate management level as outlined in this plan.

The basic approach, general assumptions, and possible sequence of events that need to be followed are stated in the plan. It will outline specific preparations prior to a disaster and emergency procedures immediately after a disaster. The plan is a roadmap from disaster to recovery. Due to the nature of the disaster, the steps outlined may be skipped or performed in a different sequence. The general approach is to make the plan as threat independent as possible. This means that it should be functional regardless of what type of disaster occurs.

For the recovery process to be effective, the plan is organized around a team concept. Each team has specific duties and responsibilities once the decision is made to invoke the disaster recovery mode. The leader of each team and their alternates are key personnel. IT staff will be assigned to multiple teams with specific assignments made according to knowledge, experience and availability. It is also assumed vendors and knowledgeable personnel will be actively enlisted to help during a recovery situation.

The plan represents a dynamic process that will be kept current through updates, testing, and reviews. As recommendations are completed or as new areas of concern are recognized, the plan will be revised to reflect the current IT environment.

Disaster Recovery Phases

The disaster recovery process consists of four phases. They are:

- Phase 1: Disaster Assessment
- Phase 2: Disaster Recovery Activation
- Phase 3: Alternate Site/Data Center Rebuild
- Phase 4: Return Home

Phase 1: Disaster Assessment

The disaster assessment phase lasts from the inception of the disaster until it is under control and the extent of the damage can be assessed. Cooperation with Flexential emergency personnel is critical.

Phase 2: Disaster Recovery Activation

This phase begins if the decision to move primary processing to a location is made. The Disaster Recovery Management Team will assemble at the command center and call upon team members to perform their assigned tasks. The most important function is to fully restore operations at a suitable location and resume normal functions. Once normal operations are established at the alternate location, Phase 2 is complete.

Phase 3: Alternate Site Operation/Data Center Rebuild

This phase involves continuing operations at the alternate location. In addition, the process of restoring the primary site will be performed.

Phase 4: Return Home

This phase involves the reactivation of the primary data center at either the original or possibly a new location. The activation of this site does not have town be as rushed as the activation of the alternate recovery center.

At the end of this phase, a thorough review of the disaster recovery process should be taken. Any deficiencies in this plan can be corrected by updating the plan.

Key Disaster Recovery Activities

Declaring a Disaster

Declaring a disaster means:

1. Activating the recovery plan
2. Notifying team leaders & staff
3. Notifying key management contacts
4. Notifying affected customer contacts
5. Securing a new location for the data center
6. Ordering and configuring replacement equipment
7. Reconfiguring the network
8. Restoring Virtual Machine infrastructure from onsite or offsite Backup
9. Keeping management informed
10. Keeping customer contacts informed

Disaster Decision Tree

Event	Decision
Data Center destroyed	Activate disaster recovery plan
Data Center unusable for MORE than 2 days	Activate disaster recovery plan
Data Center unusable for 2 days or LESS	Management Team performs an assessment
Network down	Management Team performs an assessment
Environmental problems (A/C, power, etc)	Management Team performs an assessment

Decision Point	Actions				Category
1. Incident occurs	2. Alarm sounds	3. Begin evacuation	4. Ensure all employees evacuated	5. Meet in designated area	Initiation
7. Determine if incident is real	8. If no, then	9. Recovery plan is not activated	10. Return to normal operations	12. Evaluate evacuation	Determination
	8. If yes, then	9. Switch call handling to an alternate location			Determination
10. Determine scope of incident and assess damage after building access is allowed	11. If small scope with no to minimal damage, then	12. Return and begin clean up and monitor repairs	13. Return calls	14. Return to normal operations	Short Evacuation Required
	11. If moderate to large scope or moderate to severe damage, then	12. Activate alternate computer processing site	13. Activate recovery team	14. Notify management and employees of of situation	Moderate to Severe Damage to Data Center or Infrastructure
16. Assess damage	17. If damage is moderate and will be able to return in 30 days or less	18 Complete repairs as necessary while operating at alternate site	19. Return to data center	20. Return to normal operations	Moderate Severe Damage to Data Center or Infrastructure
	17. If more than 30 days, locate to new facility	18. Order supplies and equipment	19. Set up and operate at new facility while completing repairs	20. Return to normal operations	Severe Data to Data Center or Infrastructure

Recovery Time Objectives (RTO)

The Recovery Time Objectives reflect the estimated recovery times based on current configurations and operations.

Network Service	Recovery Goal
LAN (Local Area Network)	2-3 days estimate
WAN (Wide Area Network)	2 days estimate
Internet	2 days estimate

Application Recovery Tier	Recovery Goal
Infrastructure Servers	Immediately after WAN/Internet restore
Application / SQL Servers	3 days after LAN/WAN restore
Reporting Servers	5 days after LAN/WAN restore

These RTO's should be considered best-case estimates. Bitfocus operates on a VMware virtual environment, with all server tiers fully virtualized. In the event of a disaster, the Disaster Assessment Team would assess the situation to determine if the local VM backups or the offsite VM backups (Amazon S3/Glacier) would be selected for recovery.

Once the assessment is complete, the Disaster Assessment Team will determine which temporary Data Center location to restore to. Current options are identified as Amazon Cloud or our Reno Data Center. Both locations are on standby.

Recovery Point Objectives (RPO)

Recovery Point Objectives (RPO) reflects the estimated point in time to which recovery would be made based on current configurations and operations. the exact recovery point for each server will vary due to the time when the backup takes place and when the disaster occurs. Below are general guidelines for the different types of DR data protection.

Data Protection Type	Recovery Point (Age of Data)
Onsite Backup	Up to 24 hours from disaster period.
Offsite Backup	Up to 7 days from disaster period.

Customers who have purchased additional Disaster Recovery SLA plans may have shorter RPO.

Roles of the Disaster Recovery Coordinator

The function of the Disaster Recovery Coordinator is vitally important to maintaining the plan in a consistent state of readiness. The Recovery Coordinator's role is multifaceted. Not only does the Coordinator assume a lead position in the ongoing life of the plan, but the Coordinator is a member of the Continuity Management Team in the event of a computer disaster.

The primary responsibilities of the Disaster Recovery Plan Coordinator are as follows:

- Distribution of the Disaster Recovery Plan
- Training the Disaster Recovery Teams
- Testing of the Disaster Recovery Plan
- Evaluation of the Disaster Recovery Plan Tests
- Review, change and update the Disaster Recovery Plan

In a disaster situation, the Disaster Recovery Plan Coordinator will:

- Facilitate communication between technical and non-technical staff
- Act as a Project Manager to coordinate the efforts of:
  - » Technical Staff
  - » Business Staff
  - » Vendors
  - » Other personnel as needed

The Disaster Recovery Coordinator for Bitfocus is Robert Herdzik. The alternate Disaster Recovery Plan Coordinator is Yanis Guenane.

General Recovery Information

Items Stored Offsite

1. Router / VPN Firmware and Export Settings.
2. A current copy of this disaster recovery plan.
3. A copy of Veeam Backup & Recovery 7 extract utility.
4. Weekly backups of full VMware Virtual Machine files of entire infrastructure and data.

All standard security and privacy precautions apply to offsite storage. The offsite storage facility is equipped with surge protectors and natural disaster protective measures.

Onsite backup includes all of the above, including nightly full Virtual Machine incremental backups of entire infrastructure and data.

Server Recovery

These procedures outline the steps required to restore any Bitfocus servers. Recovery for the servers assume that:

- Good backup data exists and can be retrieved from either onsite or offsite storage
- Replacement servers are on standby or Amazon Cloud servers are on standby
- Network connectivity is established

A decision must be made as to where the recovery will take place (Amazon Cloud or Reno Data Center). This decision is not made ahead of time since the specifics of the incident requiring recovery is not known.

Disaster Recovery Plan Maintenance

The disaster recovery plan is a "living" document. Failure to keep it current could severely impact Bitfocus' ability to successfully recover in the event of a disaster.

Some information contain in the plan is more dynamic than other information. A matrix of events and recommended maintenance schedule is included in this section. It is important to document changes to the plan and ensure that all copies of the plan are updated.

Changes to the plan could occur more frequently than the time frames listed in the following table. Major hardware upgrades might affect business recovery contracts as well as this plan. Software changes, personnel changes and other changes that affect the plan should be updated as soon as possible, not just when the recommended intervals occur.

Period	Action
Quarterly	Review all job changes and update plan with new personnel assignments
	Have any new application servers been implemented? If so, have all disaster recovery implication been addressed?
	Have there been any major changes to existing applications? If so, update the recovery plan accordingly
	Has the hardware configuration changed? If the changes affect your ability to recover, make appropriate changes to the recovery configuration
	Update the Network Configuration Diagrams / Infrastructure Wiki
	Visit the off-site storage location and ensure documentation is available and current
	Ensure all team assignments are still valid
Semiannually	Test the plan and update it based on the results of the test
Annually	Review Amazon / Azure retention requirements
	Review Insurance coverage

Testing the Disaster Recovery Plan

The Disaster Recovery Coordinator is responsible for testing of the disaster recovery plan at least annually to ensure the viability of the plan. On an on-going basis this frequency appears to be adequate considering the systems involved. However, special tests are to be given consideration whether there has been a major revision to the plan or significant changes in the software, hardware or data communications have occurred.

The objectives of testing the disaster recovery plan are as follows:

- Simulate the conditions of an ACTUAL Business Recovery situation.
- Determine the feasibility of the recovery process.
- Identify deficiencies in the existing procedures.
- Test the completeness of the business recovery information stored at the Offsite Storage Location.
- Train members of the disaster recovery teams.

The initial test of the plan will be in the form of a structured walk-through and should occur within two months of the disaster recovery plan's acceptance. Subsequent tests should be to the extent determined by the Disaster Recovery Coordinator that are cost effective and meet the benefits and objectives desired.

Sample Recovery Test Agenda

1. What is the purpose of the test?
2. What are the test objectives?
3. How will the successful achievement of these objectives be measured?
4. At the conclusion of the test, collect test measurements from all participants.
5. Evaluate the test results. Determine if the test was successful or not.
6. Determine the implications of the test results. Does success for this test imply success in all recovery scenarios?
7. Update the plan based on results of the test.