XX COMPANY

Information Technology Disaster Recovery

Date

Authored by Andy Ziegler, CBCP

Version #	Authored by	Revision Date	Approved By	Approval Date	Reason for Update
1	Andrew Ziegler - TRM	9/15/2021	TBD	TBD	First draft

1 SECTION 1: INTRODUCTION

1.1 How to use this plan

In the event of a disaster which interferes with XYZ LLP's ability to conduct business from one of its offices, this plan is to be used by the responsible individuals to coordinate the recovery of Information Technology infrastructure and components to support critical functions and/or departments. The plan is designed to contain, or provide reference to, all the information that might be needed at the time of a business recovery.

This plan is not intended to cover the operations of XYZ LLP's separately structured Emergency Response Plan or Business Continuity Plan.

Index of Acronyms:

(EOC) Emergency Operations Center

(EMT) Emergency Management Team

(ERT) Emergency Response Team

(BCP) Business Continuity Plan

(IT) Information Technology

(ISP) Internet Service Provider

(ITDR) Information Technology Disaster Recovery

(ITDRP) Information Technology Disaster Recovery Plan

(ITDRC) Information Technology Disaster Recovery Coordinator

(ITDRT) Information Technology Disaster Recovery Team

Section I, Introduction, contains general statements about the organization of the plan. It also establishes responsibilities for the testing (exercising), training, and maintenance activities that are necessary to guarantee the ongoing viability of the plan.

Section II, Disaster Recovery Strategy, describes the strategy that XYZ LLP will control/implement to maintain IT business continuity in the event of a facility or IT disruption. These decisions determine the content of the action plans, and if they change at any time, the plans should be changed accordingly.

Section III, Recovery Teams, lists the Recovery Team functions, those individuals who are assigned specific responsibilities, and procedures on how each of the team members is to be engaged.

Section IV, Team Procedures, determines what activities and tasks are to be taken, in what order, and by whom in order to affect IT recovery and restoration.

Section V, Appendices, contains all of the other information needed to carry out the plan. Other sections refer the reader to one or more Appendices to locate the information needed to carry out the Team Procedures steps.

1.2 Objectives

The objective of the ITDRP is to coordinate the recovery of IT infrastructure and applications required to perform critical business functions in the event of a facilities (office building) disruption or disaster. This can include short or long-term disasters or other disruptions, such as fires, floods, earthquakes, explosions, terrorism, civil unrest, public health emergencies, tornadoes, extended power interruptions, hazardous chemical spills, and other natural or man-made disasters.

A disaster is defined as any event that renders a business facility inoperable or unusable so that it interferes with the organization's ability to deliver essential business services.

The priorities in a disaster situation are to:

1. Ensure the safety of employees and visitors in the office buildings. (Responsibility of the ERT)

2. Mitigate threats or limit the damage that threats can cause. (Responsibility of the ERT)

3. Have advanced preparations to ensure that critical business functions can continue.

4. Have documented plans and procedures to ensure the quick, effective execution of recovery strategies for critical business functions.

The XYZ LLP Business Continuity Plan includes procedures for all phases of recovery as defined in the Business Continuity Strategy section of the XYZ LLP Business Continuity Plan maintained as a separate reference document by the Business Continuity Team.

1.3 Scope

The ITDRP is limited in scope to the recovery of IT infrastructure and applications to support business continuance from a serious disruption in activities due to non-availability of XYZ LLP's facilities. The ITDRP includes procedures for all phases of recovery as defined in the strategy portion of this document. This plan is separate from XYZ LLP's Business Continuity Plan, which focuses on the overall recovery of all business operations (see Assumption #1 below). Unless otherwise modified, this plan does not address temporary interruptions of duration less than the time frames determined to be critical to business operations.

1.4 Assumptions

The viability of this ITDR is based on the following assumptions:

1. That a viable and tested Business Continuity Plan exists and will be put into operation to ensure the safety and availability of all personnell.

2. That the current data backups are available to the IT recovery team.

3. That the proper IT infrastructure is in place at the restoration site prior to backup recovery and restoration.

4. That this plan has been properly maintained and updated as required.

5. The ITDRP incorporates disruptions that may occur at any current XYZ LLP facility.

1.5 Changes to the Plan/Maintenance Responsibilities

Maintenance of the XYZ LLP ITDRP is the joint responsibility of the Executive Committee, the IT Director, and the Business Continuity Team.

Executive Committee is responsible for:

1. Periodically reviewing the adequacy and appropriateness of its ITDR strategy.

2. Assessing the impact on the XYZ LLP ITDRP of additions or changes to existing business functions, XYZ LLP procedures, equipment, and facilities requirements.

3. Keeping recovery team personnel assignments current, taking into account promotions, transfers, and terminations.

4. Communicating all plan changes to the Business Continuity Team and IT Director so that the organization's ITDRP can be updated.

IT Director is responsible for:

1. Maintaining and/or monitoring the health and availability of all critical XYZ LLP IT systems, databases, servers, applications, hardware, software and any other critical IT components to meet the predefined XYZ LLP ITDR recovery time frames.

2. Communicating all plan changes to the Business Continuity Coordinator so that the master plan can be updated.

3. Maintaining and updating the ITDRP

4. Planning, executing and reporting yearly ITDR exercises to demonstrate the ability to the predefined XYZ LLP ITDR recovery time frames

The Business Continuity Team is responsible for:

1. Keeping the organization's Business Continuity Plan updated with changes made to XYZ LLP facilities, IT, business or supplier structure.

2. Coordinating changes among plans and communicating to XYZ LLP management when other changes require them to update their plans.

1.6 Plan Testing Procedures and Responsibilities

XYZ LLP Executive Committee is responsible for ensuring the workability of their ITDRP. This should be periodically verified by active or passive testing (See section V for detailed test plans)

1.7 Plan Training Procedures and Responsibilities

The Executive Committee is responsible for ensuring that the personnel who would carry out or be impacted by the ITDRP are sufficiently aware of the plan's details. This may be accomplished in a number of ways including; annual lunch and learn sessions, practice exercises,

participation in tests, and awareness programs conducted by the Business Continuity Coordinator and IT Director.

1.8 Plan Distribution List

The XYZ LLP ITDRP will be provided to all members of the Executive Committee, ITDR Team and Business Continuity Teams in both electronic and hard copy forms. **All recipients of this plan are to ensure the plans remain fully secured and any previous copies are fully destroyed.** Electronic copies are not be sent to or transported on a non-company device (ie personal email/laptop, jump drive, etc)

2 DISASTER RECOVERY STRATEGY

2.1 Introductions

This section of the XYZ LLP Business Continuity Plan describes the strategy devised to maintain availability of systems and applications critical to business continuity in the event of a facilities disruption. This strategy would be invoked should the XYZ LLP primary IT systems somehow be damaged, compromised, or inaccessible.

2.2 Capability Recovery Priorities

The overall goal of the XYZ LLP ITDR strategy is to ensure recovery of critical company operations within X# hours of a declared disruption.

The strategy is to recover critical XYZ LLP IT services at the alternate site location. Information Systems will recover IT functions based on the critical departmental business functions and defined strategies. Business Functions by Location are listed in the XYZ LLP Business Continuity Plan.

“Time Critical Business Functions,” i.e., those of which are of the most critical for immediate recovery at the secondary location are:

1. List critical functions here

2.3 Digital Records Management Infrastructure and Strategy

Describe how your business maintains and stores client and financial records.

2.4 Access Management Infrastructure and Strategy

Describe how you maintain access management: XYZ IT is managed through Active Directory on a dedicated server. Active Directory is maintained via hot/hot VPN replication between both primary and secondary sites, details of which can be found in the XYZ LLP Business Continuity Plan.

2.5 Recovery Time Objectives

The Recovery Time Objective is the goal for how fast to restore technology services after a disruption (based on the acceptable amount of down time and level of performance)1. For example, a recovery time objective of 24 hours with local accessibility for payroll services means that the payroll application must be up and running within 24 hours as well as accessible locally.

Service Classification

Classification	Maximum Recovery Time
Critical	Within 24 hours
Vital	Within 72 hours
Necessary	Within 2 weeks
Desired	Longer than 2 weeks but necessary to return to full business-as-usual operations

2.6 Telecommunications Infrastructure and Strategy

Describe your telecommunication infrastructure and strategy.

EXAMPLE: XYZ LLP is partnered with Sasktel to provide telecommunications service. Both primary and secondary sites house a PBX switch to route calls. Procedures are in place for rerouting XYZ LLP's primary phone number to the secondary site by contacting Saktel and directing them to switch the DID. This is not automatic and would require manual intervention.

2.7 Internet Service Provider Strategy

Describe your ISP and strategy.

EXAMPLE: XYZ LLP is partnered with Sasktel to provide internet access to both primary and secondary locations. The secondary site has a hot

secondary ISP with Shaw Communications and automatic failover capabilities.

2.8 Vital Record Backups

Describe your backup protocols and strategy.

EXAMPLE Full IT point-in-time snapshots are automatically backed up daily for each server at both the primary and secondary site with the primary site storing backups for 30 days and the secondary site storing backups since inception in YEAR.

2.9 IT Redundancy Strategy

Describe your redundancy protocols and strategy (ie hot/cold, hot/warm, hot/hot, hot/rebuild etc).

EXAMPLE XYZ LLP maintains a fully redundant IT infrastructure in the secondary site with a combination of hot/hot and hot/warm failover capabilities. Daily backups are stored at both the primary and secondary site should restoration be required. While active directory is replicated in real time, virtual machine activation would have to be manually executed at the secondary site to allow file server access.

3 RECOVERY TEAMS

3.1 Purpose and Objective

This section of the plan identifies who will participate in the ITDR process for the XYZ LLP ITDRP. The participants are organized into one team of several roles. The team leader is the IT Director or their delegate. Other team members are assigned either to specific responsibilities or as team members to carry out tasks as needed.

3.2 IT Recovery Team Descriptions

BCT – Business Continuity Team: Directs and coordinates all activities documented in the XYZ LLP Business Continuity Plan

ITDRC – Information Technology Disaster Recovery Coordinator: Responsible for the leading the ITDRT

ITDRT – Information Technology Disaster Recovery Team: Responsible for executing tasks in the ITDRP including:

- Activating the IT Technology Recovery Plan
- Managing the IT disaster response and recovery procedures.
- Mobilizing and managing IT resources.
- Coordinating all communications related activities, as required, with telephone & data communications, PC, server support, and other IT related vendors.
- Assisting, as required, in the acquisition and installation of equipment at the recovery site.
- Ensuring that cellular telephones, and other special order equipment and supplies are delivered to teams as requested.
- Participating in testing equipment and facilities.
- Participating in the transfer of operations from the alternate site as required.
- Coordinating telephone setup at the EOC and recovery site.
- Coordinating and performing restoration or replacement of all desktop PCs, LANs, telephones, and telecommunications access at the damaged site.
- Coordinating Disaster Recovery/IT efforts between different departments in the same or remote locations.
- Training Disaster Recovery/IT Team Members

3.3 IT Recovery Team Assignments

ITDRC-IT Director and Team Leader: member of the Business Continuity Team. Responsible for coordinating all activities and communicating to the Business Continuity Team and Executive Committee. Also responsible for planning and coordinating disaster recovery tests. Responsible for maintaining the ITDRP and all infrastructure required to ensure recovery objectives are met and training of ITDRT members.

- Information Availability-completes and validates the restoration of and employee access to critical company data
- Telecommunications-completes and validates the continued operation, restoration or redirection of phone systems and ISP availability

- End user testing and support-supports testing all end user functions, validates user access to critical systems to ensure full operational capability for all impacted employees and serves as a point of contact for employees to trouble shoot access issues
- Secondary site coordinator-coordinates and directs all secondary site functions related to ITDR

3.4 Team Contacts

Name	Role	Email	Cell phone
?	?	?	?
?	?	?	?
?	?	?	?

4 RECOVERY PROCEDURES

4.1 Purpose and Objective

This section of the plan describes the specific activities and tasks that are to be carried out in the ITDR process for XYZ LLP. Given the ITDR Strategy outlined in Section II, this section transforms those strategies into a very specific set of action activities and tasks organized by infrastructure area in scope

The description for each recovery area begins on a new page. Each activity is assigned to one of the ITDR team members. Each activity has a designated team member who has the primary assignment to complete the activity. Most activities also have an alternate team member assigned. The activities will only generally be performed in this sequence.

The finest level of detail in the Recovery Procedures is the task. All plan activities are completed by performing one or more tasks. The tasks are numbered sequentially within each activity, and this is generally the order in which they would be performed.

This is where you will create your step by step processes for various types of recovery activities that may be necessary. The Pre Plans listed below are for example purposes only.

4.2 Data Recovery – DR Site Available

Activity: Redirect all IT capabilities to DR site

Activation criteria: Business Continuity Team determines that services need to be redirected to secondary site

Tasks:

The below tasks are examples, you must craft the task to fit your own IT infrastructure and procedures:

4.2.1 ITDRC activates the ITDRT via physical and/or virtual means

4.2.2 Team members gather to assess the situation and identify any barriers to execution of data recovery tasks

4.2.3 Instruct the business continuity team to communicate systems outage an ETA to all employees

4.2.4 Ensure secondary site coordinator is in place at secondary site or en route

4.2.5 Disable VPN access to the primary site from the secondary location to ensure accidental overwrite does not occur

4.2.6 Disable user access to primary site, if available, to ensure end users are only accessing the new primary file system to be located at the secondary site

4.2.7 If latest backup is not restored to secondary site file server, execute restore tasks to replicate latest backup to secondary site file server

4.2.8 Suggest putting step by step instructions here

4.2.9 Check logs to ensure latest version of file server is in place

4.2.10 Perform user testing to ensure access to file server is as expected

4.2.11 If issues are encountered, report to ITDRT for trouble shooting

4.2.12 Once access to file systems and proper operation are confirmed, turn on virtual machines at secondary location so end users can access

4.2.13 Validate VM's are activated and working as anticipated

4.2.14 Direct the business recovery team to communicate to employees that they can now access company systems and resume operations and any potential data loss that may have occurred between the latest backup and the point in time where access to the primary file server was lost.

4.2.15 End user testing and support to trouble shoot user issues and escalate issues to ITDRT

4.2.16 ITDRT to continue to monitor secondary site IT infrastructure for health and provide updates to and coordinate actions with business continuity team

4.2.17 If primary site is a complete loss (fire, flood, storm, etc) ITDRC to establish a team to begin planning replacement location and infrastructure needs to establish a new primary or DR site with urgency. In addition, ITDRC will immediately establish a daily cloud based backup of all systems should the secondary site also become unavailable.

4.3 Employee Interface Recovery

Activity: Restore employee equipment and access to critical systems

Activation criteria: Business Continuity Team determines that employees have lost access to desktops, laptops and telephones and need to be replaced.

Tasks:

4.3.1 ITDRC activates the ITDRT via physical and/or virtual means

4.3.2 Team members gather to assess the situation and identify any barriers to execution of data recovery tasks

4.3.3 End user testing and support team member works with business continuity team to identify employees impacted, locations and equipment needs inventory

4.3.4 Spare equipment is deployed first to those with the most critical needs and senior roles in the company

4.3.5 Replacement equipment is ordered from primary or secondary suppliers with fastest shipping available

4.3.6 As replacement equipment arrives, engage other team members to assist in configuration and delivery/sourcing of all replacement equipment to employees

4.3.7 Troubleshoot employee access/equipment issues as needed

4.4 Telecommunications Rerouting Procedures

Activity: Redirect service of company main phone number and extension to secondary site

Activation criteria: Business Continuity Team determines that access to primary site is lost and need to re-direct phone numbers to secondary site telecommunications infrastructure

Tasks:

4.4.1 ITDRC activates the ITDRT via physical and/or virtual means

4.4.2 Team members gather to assess the situation and identify any barriers to execution of telecommunications redirection

4.4.3 Ensure secondary site coordinator is in place at secondary site or en route

4.4.4 Telecommunications coordinator contacts Sasktel at (contact information) and direct them to switch DID to (insert specific instructions here)

4.4.5 Once main phone number has been re-routed, confirm expected operation with secondary site coordinator

4.4.6 Determine next steps to redirect extensions to employees at secondary site in coordination with business continuity team

4.4.7 Coordinate additional handsets and other equipment needs with business continuity team

5 ITDR TEST PLANS

5.1 Data Recovery to Primary and Secondary Sites

Purpose: outline the steps required to test data recovery at the primary (lab environment) and secondary site (production environment)

5.1.1 Coordinate test frequency and timing with executive committee and business continuity team

5.1.2 Identify disaster recovery test team and develop project plan

5.1.3 Schedule date of test execution

5.1.4 Prepare primary lab environment or secondary production environment for data backup restore

5.1.5 Develop step by step plan for promotion of backup data including timelines, checkpoints and communication protocols

5.1.6 Develop IT validation test script

5.1.7 Craft end user test script and take steps to provide a test workstation to simulate end user access

5.1.8 Develop back out plans

5.1.9 Table top DR test with test team 3 weeks and week prior to execution

5.1.10 Execute data recovery test

5.1.11 Perform after action report including lessons learned and opportunities for improvement with test team

5.1.12 Gather results and report to executive committee and business continuity team

5.2 Remote Access Testing

Purpose: Ensure availability of users to access the primary and secondary sites remotely

5.2.1 If multiple users connect and perform their job functions on a reoccurring basis, a test will not be necessary, but poll those employees for satisfaction and suggestions.

5.2.2 If users do not regularly connect remotely, identify a population from different teams and request the connect remotely to perform their job functions on a quarterly basis. Report results to IT Director.

5.3 Telecommunications to DR Site

Purpose: outline the steps required to test rerouting of telecommunications to secondary site and back

5.3.1 Coordinate test frequency and timing with executive committee and business continuity team

5.3.2 Identify disaster recovery test team and develop project plan

5.3.3 Coordinate with telcomm provider (Sasktel)

5.3.4 Schedule date of test execution

5.3.5 Develop step by step plan for switch of DID to secondary location executed by Sasktel including timelines, checkpoints and communication protocols

5.3.6 Develop IT validation test script

5.3.7 Craft end user test script and take steps to provide test handsets at the secondary location

5.3.8 Develop back out plans

5.3.9 Table top DR test with test team 3 weeks and week prior to execution

5.3.10 Execute telecommunications redirection test

5.3.11 Upon completion of test, restore service to original configuration

5.3.12 Execute validation test to ensure service is restored

5.3.13 Perform after action report including lessons learned and opportunities for improvement with test team

5.3.14 Gather results and report to executive committee and business continuity team

5.4 ISP Failover

Purpose: outline the steps required to test failover from primary to secondary ISP

5.4.1 Coordinate test frequency and timing with executive committee and business continuity team

5.4.2 Identify disaster recovery test team and develop project plan

5.4.3 Coordinate with primary and secondary ISP provider

5.4.4 Schedule date of test execution

5.4.5 Develop step by step plan for disabling of primary ISP, monitor for secondary ISP failover and restore to primary ISP

5.4.6 Develop IT validation test script

5.4.7 Craft end user test scripts

5.4.8 Develop back out plans

5.4.9 Table top DR test with test team 3 weeks and week prior to execution

5.4.10 Execute ISP failover test

5.4.11 Upon completion of test, restore service to original configuration

5.4.12 Execute validation test to ensure service is restored

5.4.13 Perform after action report including lessons learned and opportunities for improvement with test team

Gather results and report to executive committee and business continuity team

WHERE DO YOU STORE YOU POLICIES AND PROCEDURES?

CAN YOUR EMPLOYEES EASILY ACCESS THEM AT ALL TIMES