Disaster Recovery Plan

v1.0

Jadarah For Dept Collections Co.

This document is a property of **Jadarah For Dept Collections Co.** and contains sensitive and confidential information which should not be disclosed, transmitted, duplicated, and used in whole or part other than for its intended purpose and recipients

Document Control Information

Document Version Control Information				
Version	Date	Author	Reviewer	Approver
1.0	**03 Oct 2024**	Abdulrahman AlJamani	Ahmed Al-Kelani	Misfer Al-Ajmi

Document Change History Information			
Author	Date	Version	Change Description

Contents

Document Control Information **2**
1 Information Technology Statement of Intent **5**
2 Policy Statement **5**
3 Objectives **5**
4 Key Personnel Contact Info **6**
5 Notification Calling Tree **7**
6 External Contacts **8**
7 External Contacts Calling Tree **9**
8 Plan Overview **12**
8.1 Plan Updating 12
8.2 Plan Documentation Storage 12
8.3 Backup Strategy 12
8.4 Risk Management 13
9 Emergency **14**
9.1 Alert, Escalation, and Plan Invocation 14
10 Media **15**
11 Insurance **15**
12 Financial and Legal Issues **16**
13 DRP Exercising **17**
14 Appendices **17**
14.1 Templates Disaster Recovery Plan for <System One> 17
ADDENDUM 19
File Systems 20
14.2 Disaster Recovery Plan for <System Two> 20
ADDENDUM 22
File Systems 23
14.3 Disaster Recovery Plan for Local Area Network (LAN) 23
ADDENDUM 25
File Systems 26
14.4 Disaster Recovery Plan for Wide Area Network (WAN) 26
ADDENDUM 28
Support Systems 29
14.5 Disaster Recovery Plan for Remote Connectivity 29
14.6 29
ADDENDUM 31
Support Systems 32

15 Forms 32
15.1 Damage Assessment Form 32
15.2 Management of DR Activities Form 33
15.3 Disaster Recovery Event Recording Form 34
15.4 Disaster Recovery Activity Report Form 35
15.5 Mobilizing the Disaster Recovery Team Form 35
15.6 Mobilizing the Business Recovery Team Form 36
15.7 Monitoring Business Recovery Task Progress Form 37
15.8 Preparing the Business Recovery Report Form 38
15.9 Communications Form 38
15.10 Returning Recovered Business Operations to Business Unit Leadership 39
15.11 Business Process/Function Recovery Completion Form 39

1 Information Technology Statement of Intent

Jadarah Funders Debt Collection Co recognizes the critical importance of maintaining continuous business operations and protecting our information assets against potential threats and disasters. In alignment with this recognition, our Information Technology (IT) Disaster Recovery Plan (DRP) is established to ensure the resilience of our IT infrastructure and the continuity of our business operations.

The IT DRP outlines our systematic approach to respond to unforeseen incidents that significantly disrupt our IT services, including but not limited to natural disasters, cyber-attacks, system failures, and human errors. Our intent is to minimize the impact of such incidents on our operations, protect the integrity and confidentiality of our data, and ensure the availability of critical services to our clients and stakeholders.

Our mission, through this plan, is to achieve the following:

- **System Uptime:** To ensure our IT systems are operational with minimal downtime.
- **Data Integrity and Availability:** To safeguard our data from loss or corruption and ensure it is available when needed.
- **Business Continuity:** To maintain our critical business functions and services during and after a disaster, facilitating a swift recovery to normal operations.

2 Policy Statement

The management of **Jadarah Funders Debt Collection Co** has endorsed the following policies regarding our IT Disaster Recovery Planning:

- **Comprehensive Planning:** The company commits to developing and maintaining a comprehensive IT disaster recovery plan that addresses all critical and essential infrastructure elements, systems, and networks.
- **Risk Assessment:** A formal risk assessment will be conducted periodically to identify potential threats and vulnerabilities, informing the requirements and strategies of the disaster recovery plan.
- **Coverage and Testing:** The disaster recovery plan will encompass procedures for restoring all critical business activities and IT systems. It will be regularly tested in simulated environments to ensure effectiveness and the readiness of our staff.
- **Staff Awareness and Training:** All employees will be informed about the disaster recovery plan and trained on their specific roles and responsibilities within the plan to ensure a coordinated and efficient response to incidents.
- **Continuous Improvement:** The disaster recovery plan will be reviewed and updated regularly to reflect changes in our business operations, technological advancements, and emerging threats.

3 Objectives

The primary objective of our IT Disaster Recovery Plan is to establish a structured and efficient response mechanism that minimizes the impact of disasters on our business operations. The specific goals of the plan include:

1. **Rapid Recovery:** To resume critical operations within the shortest possible time frame, minimizing the duration of any service outage.
2. **Data Protection:** To prevent data loss and ensure the integrity and confidentiality of sensitive information.
3. **Operational Continuity:** To maintain essential business functions and services during and immediately after a disaster.
4. **Compliance:** To comply with legal, regulatory, and contractual obligations related to business continuity and data protection.
5. **Stakeholder Confidence:** To maintain the trust and confidence of our clients, employees, and partners by demonstrating our commitment to business resilience.
6. **Cost-Effectiveness:** To implement cost-effective disaster recovery measures that balance the need for rapid recovery with the financial implications for the business.

By adhering to these policies and objectives, **Jadarah Funders Debt Collection Co** aims to enhance its resilience against IT disruptions, ensuring the continuity of operations and the protection of critical business assets.

4 Key Personnel Contact Info

The following table provides the contact information for key personnel crucial to the IT Disaster Recovery Plan (DRP) execution for Jadarah Funders Debt Collection Co. It is imperative that this information is kept up-to-date and securely stored, with access granted only to authorized individuals.

Name, Title	Work	Alternate	Mobile	Home	Email Address	Alternate Email
[General Manager]	[Work No.]	[Alt. No.]	[Mobile No.]	[Home No.]		
[IT Disaster Recovery Manager]	[Work No.]	[Alt. No.]	[Mobile No.]	[Home No.]		
[Head of IT Security]	[Work No.]	[Alt. No.]	[Mobile No.]	[Home No.]		
[HR Manager]	[Work No.]	[Alt. No.]	[Mobile No.]	[Home No.]		
[Facilities Manager]	[Work No.]	[Alt. No.]	[Mobile No.]	[Home No.]		
[Communications Officer]	[Work No.]	[Alt. No.]	[Mobile No.]	[Home No.]		

(Note: Actual contact information needs to be filled out by the company.)

5 Notification Calling Tree

The Notification Calling Tree is a structured system designed to ensure efficient communication among Jadarah Funders Debt Collection Co personnel during a disaster recovery scenario. This calling tree facilitates the rapid dissemination of information and activation of recovery protocols.

1. **Initiation**: The IT Disaster Recovery Manager initiates the calling tree upon identifying a disaster scenario that impacts IT operations.
2. **Sequential Notification**: Each individual in the calling tree has the responsibility to contact the next person on the list. This sequence continues until everyone in the tree has been notified.
3. **Confirmation**: Each recipient must confirm receipt of the message. If confirmation is not received within a specified timeframe, the preceding person attempts to make contact via an alternate method.
4. **Escalation**: In case of unavailability, the calling tree includes designated alternates for each key role to ensure no gaps in communication.

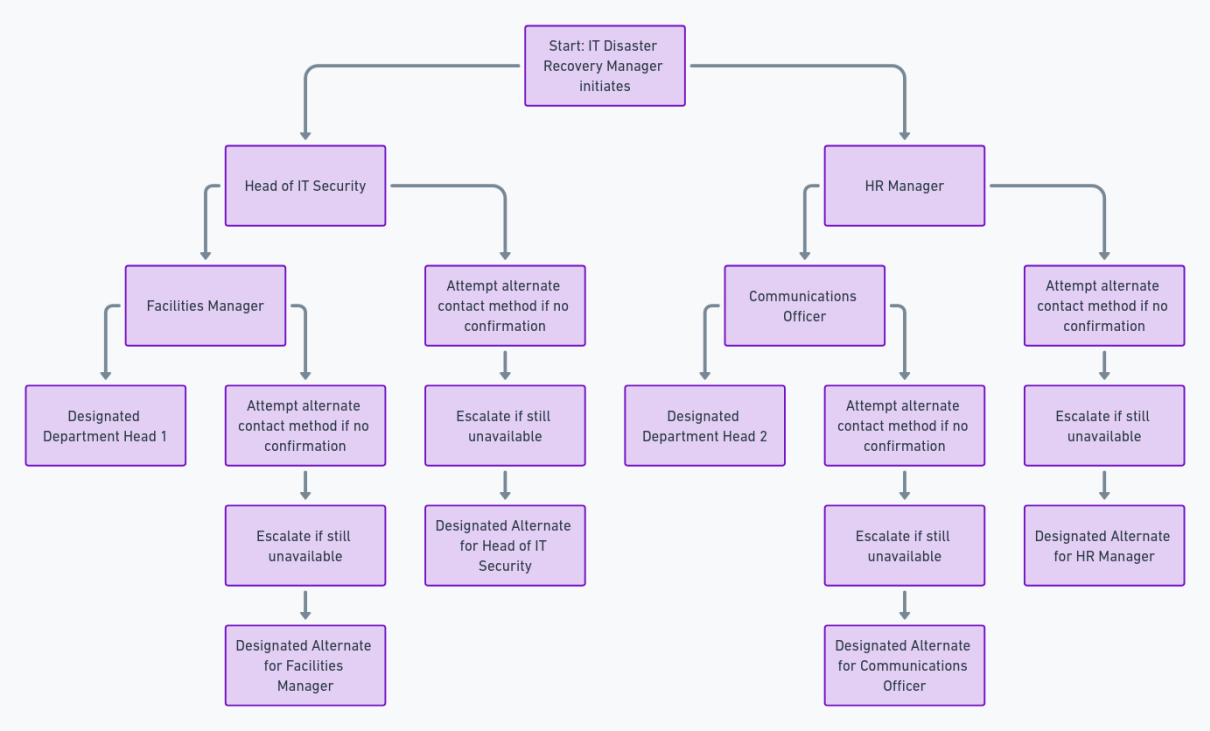
Example Calling Tree Structure:

- **IT Disaster Recovery Manager**
    - Contacts: Head of IT Security and HR Manager
- **Head of IT Security**
    - Contacts: Facilities Manager
- **HR Manager**
    - Contacts: Communications Officer
- **Facilities Manager**
    - Contacts: [Designated Department Head 1]
- **Communications Officer**
    - Contacts: [Designated Department Head 2]
- *[Further branches as required]*

Key Guidelines:

- Always attempt to contact the next individual on the list as soon as possible.
- Utilize all provided contact methods as necessary (e.g., mobile, home, email).
- Document all contact attempts, successful or otherwise, to provide a record of the notification process.
- Remain available for updates or further instructions.

This Notification Calling Tree ensures that all key personnel are promptly informed of the disaster and can commence their designated roles in the disaster recovery process efficiently. Regular updates and revisions to the calling tree are necessary to accommodate changes in personnel or contact information.



6 External Contacts

For the IT Disaster Recovery Plan (DRP) of Jadarah Funders Debt Collection Co, maintaining a current list of external contacts is crucial. These contacts include service providers, vendors, emergency services, and other partners critical to the disaster recovery process. The list should be reviewed and updated regularly to ensure accuracy.

Name, Title	Organization/ Service	Contact Option	Contact Number	Email Address	Notes
	Landlord / Property Manager	Work	[Work No.]	[email@landlord.com]	Responsible for building access
	Power Company	Customer Service	[Customer Service No.]	[service@powercompany.com]	Account No.: [Account Number]

	Telecom Carrier 1	Technical Support	[Support No.]	[support@telecom1.com]	Account No.: [Account Number]
	Hardware Supplier	Account Manager	[Manager No.]	[am@hardwaresupplier.com]	Account No.: [Account Number]
	Insurance Company	Claims Representative	[Claims No.]	[claims@insuranceco.com]	Policy No.: [Policy Number]
	Local Emergency Services	Emergency	911	N/A	Fire, Medical, Police
	Off-Site Data Storage	Account Manager	[Manager No.]	[storage@offsite.com]	Account No.: [Account Number]
	IT Support Services	Technical Support	[Support No.]	[support@itsupport.com]	24/7 support services

(Note: Actual contact information for Jadarah Funders Debt Collection Co needs to be filled out accordingly.)

7 External Contacts Calling Tree

The External Contacts Calling Tree complements the internal Notification Calling Tree by outlining the procedure for contacting external entities critical to the disaster recovery efforts. This calling tree ensures that all necessary external partners are quickly informed and can provide the required support.

Procedure:

1. **Initiation**: The IT Disaster Recovery Manager or designated alternate initiates the external contacts calling tree as part of the disaster response.
2. **Prioritization**: Contacts are prioritized based on the nature of the disaster and immediate needs (e.g., utility services for physical disasters, IT vendors for cyber incidents).
3. **Sequential Notification**: The person initiating the calling tree starts by contacting the most critical external partners first, continuing down the list in order of priority.

4. **Confirmation and Escalation**: For each contact attempt, the initiator must receive confirmation of the message receipt. If unable to reach a critical partner, escalate to an alternate contact or higher-level representative within the partner organization.

5. **Documentation**: All communication attempts, successful or otherwise, are documented for post-disaster review and follow-up.

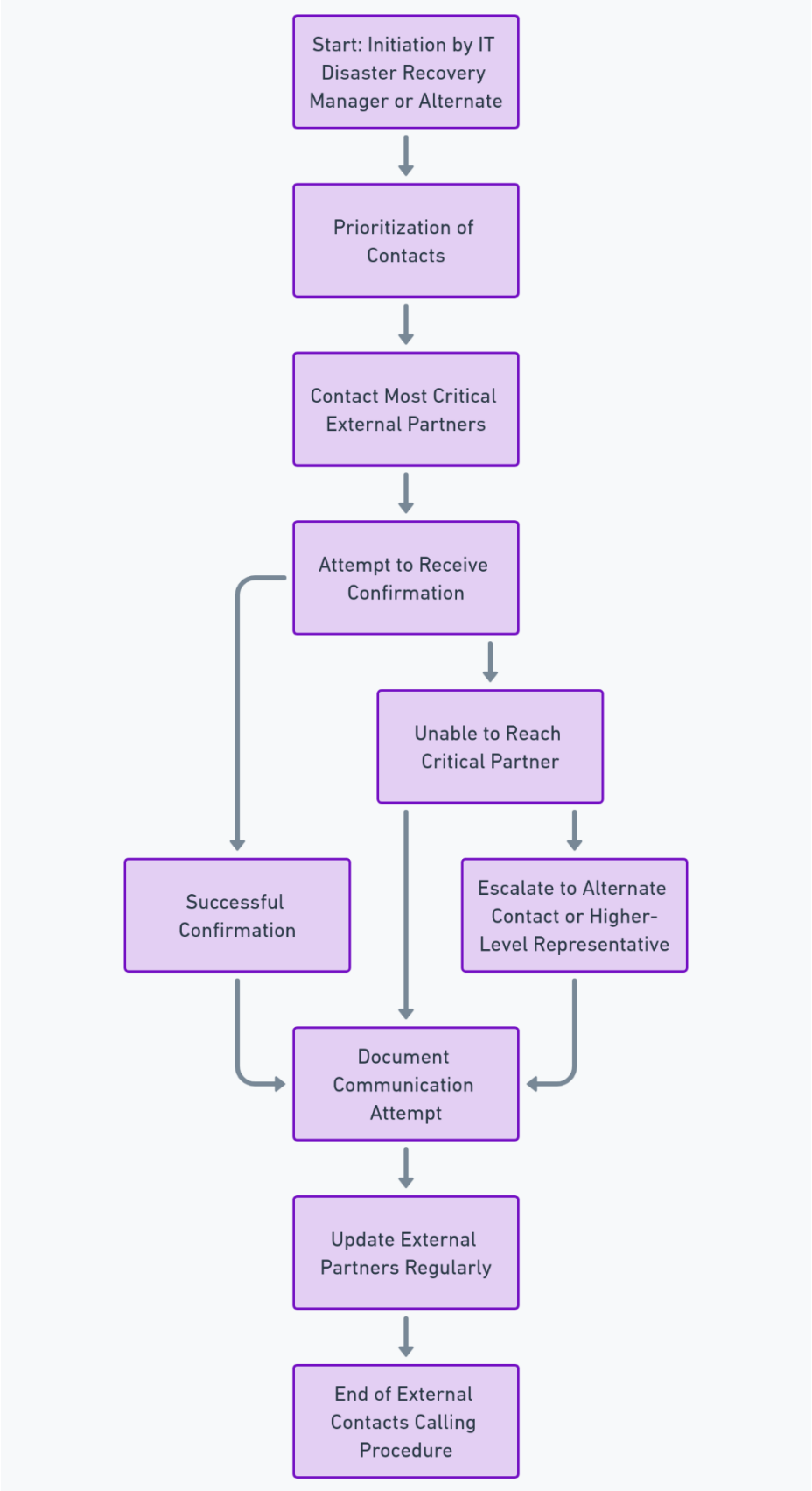
Key Guidelines:

- Use all available contact methods as necessary, starting with the most direct (e.g., mobile phone) to more general (e.g., customer service line).

- Be prepared to provide a concise summary of the disaster situation and specific assistance required from the external contact.

- Update the external partners regularly as the situation evolves and as recovery efforts proceed.

This structured approach to external communication ensures that Jadarah Funders Debt Collection Co can efficiently mobilize the support and resources needed from external partners during a disaster recovery operation.


Start: Initiation by IT Disaster Recovery Manager or Alternate
Prioritization of Contacts
Contact Most Critical External Partners
Attempt to Receive Confirmation
Unable to Reach Critical Partner
Successful Confirmation
Escalate to Alternate Contact or Higher-Level Representative
Document Communication Attempt
Update External Partners Regularly
End of External Contacts Calling Procedure

8 Plan Overview

The IT Disaster Recovery Plan (DRP) for Jadarah Funders Debt Collection Co provides a structured approach for responding to unplanned incidents that disrupt our IT operations, services, and processes. It outlines strategies to recover critical IT systems, ensuring business continuity.

8.1 Plan Updating

Objective: To ensure the DRP remains effective and relevant, reflecting changes in our IT infrastructure, emerging threats, and organizational needs.

Process:

- **Regular Reviews**: The DRP will be reviewed semi-annually or following significant changes to our IT environment or business operations.
- **Change Management**: A formal change management process will be utilized to incorporate necessary updates into the DRP. This process involves assessing the impact of the change, proposing updates, reviewing, and approving by the IT Disaster Recovery Manager and other relevant stakeholders.
- **Documentation**: All updates will be documented, including a revision history with dates, descriptions of changes, and names of individuals making the updates.

8.2 Plan Documentation Storage

Objective: To ensure that the DRP is accessible in the event of a disaster while maintaining its confidentiality and integrity.

Strategy:

- **Primary Location**: A digital copy of the DRP will be stored on a secure, centralized company server with restricted access to authorized personnel only.
- **Off-Site Storage**: A secondary copy will be stored in a secure, off-site location, accessible to the Disaster Recovery Team. This ensures availability if the primary site is compromised.
- **Physical Copies**: Limited physical copies will be maintained in secure, fireproof safes at multiple locations, including the primary business site and off-site recovery location.
- **Encryption and Security**: Digital copies of the plan will be encrypted and password-protected to prevent unauthorized access.

8.3 Backup Strategy

Objective: To minimize data loss and ensure the rapid restoration of IT services in the event of a disaster.

Components:

- **Data Prioritization**: Critical data, including customer information, financial records, and operational data, will be identified and prioritized for backup.
- **Backup Frequency**: Critical data will be backed up daily, with incremental backups throughout the day. Non-critical data will be backed up weekly.

- **Off-Site Backups**: In addition to on-site backups, off-site backups will be maintained in a geographically separate location to protect against local disasters.
- **Backup Testing**: Backup processes will be tested quarterly to ensure data integrity and the effectiveness of recovery procedures.

KEY BUSINESS PROCESS	BACKUP STRATEGY
IT Operations	Fully mirrored recovery site
Tech Support - Hardware	Fully mirrored recovery site
Tech Support - Software	Fully mirrored recovery site
Facilities Management	Fully mirrored recovery site
Email	Fully mirrored recovery site
Purchasing	Fully mirrored recovery site
Disaster Recovery	Fully mirrored recovery site
Finance	Fully mirrored recovery site
Contracts Admin	Fully mirrored recovery site
Warehouse & Inventory	Fully mirrored recovery site
Product Sales	Fully mirrored recovery site
Maintenance Sales	Fully mirrored recovery site
Human Resources	Off-site data storage facility
Testing Fully Mirrored Recovery site -	Fully mirrored recovery site
Workshop Fully Mirrored Recovery site -	Fully mirrored recovery site
Call Center	Fully mirrored recovery site
Web Site	Fully mirrored recovery site

8.4 Risk Management

Objective: To identify potential risks to IT operations and implement measures to mitigate these risks, ensuring business continuity.

Approach:

- **Risk Assessment**: Conduct regular risk assessments to identify vulnerabilities in IT infrastructure, data security, and business operations. Assessments will consider natural disasters, cyber threats, hardware failures, and human errors.

- **Mitigation Strategies**: Implement risk mitigation strategies, including robust security measures, redundant systems, employee training, and incident response plans.
- **Insurance Coverage**: Maintain comprehensive insurance policies to cover potential losses from cyber incidents, data breaches, and physical damages to IT infrastructure.
- **Continuous Monitoring**: Establish continuous monitoring mechanisms to detect threats early and adjust risk management strategies accordingly.

Potential Disaster	Probability Rating	Impact Rating	Brief Description Of Potential Consequences & Remedial Actions
Flood	3	4	All critical equipment is located on 1st Floor
Fire	3	4	FM200 suppression system installed in main computer centers. Fire and smoke detectors on all floors.
Tornado	5		
Electrical storms	5		
Act of terrorism	5		
Act of sabotage	5		
Electrical power Failure	3	4	Redundant UPS array together with auto standby generator that is tested weekly & remotely monitored 24/7. UPSs also remotely monitored.
Loss of communications network services	4	4	Two diversely routed T1 trunks into building. WAN redundancy, voice network resilience

This overview establishes a foundational framework for Jadarah Funders Debt Collection Co' approach to disaster recovery planning, ensuring our preparedness to respond effectively to incidents and minimize their impact on our operations.

9 Emergency

9.1 Alert, Escalation, and Plan Invocation

The procedure for alerting key personnel and escalating a disaster situation is as follows:

- **Initial Alert**: Any employee identifying a potential disaster situation immediately notifies the IT Disaster Recovery Manager.
- **Assessment and Escalation**: The IT Disaster Recovery Manager assesses the situation. If deemed a disaster, the Emergency Response Team (ERT) is activated, and the DRP is invoked.
- **Plan Invocation**: The ERT assesses the scope of the disaster and decides on the specific components of the DRP to implement. The team then initiates recovery operations, coordinating with internal and external stakeholders.

10 Media

Media Management in Disasters

During a disaster, managing media interactions is crucial to maintain the company's reputation and ensure accurate dissemination of information.

- **Media Contact**: The Communications Officer is the primary point of contact for all media inquiries. This individual coordinates with the ERT to provide consistent, accurate information.
- **Press Releases**: Prepared by the Communications Officer, press releases outline the nature of the disaster, impacts on operations, and recovery efforts underway. Releases are approved by the IT Disaster Recovery Manager before dissemination.
- **Media Briefings**: Scheduled as needed, media briefings provide updates on the recovery progress. The Communications Officer, along with the IT Disaster Recovery Manager, conducts these briefings.
- **Social Media**: Used to communicate timely updates to customers, employees, and stakeholders. The Communications Officer oversees all social media communications to ensure consistency and accuracy.

Effective media management during a disaster helps to mitigate negative publicity, maintain customer trust, and ensure stakeholders are informed of recovery efforts and impacts on services.

11 Insurance

For Jadarah Funders Debt Collection Co, having comprehensive insurance coverage is a critical component of the IT Disaster Recovery Plan (DRP). This ensures that the company is financially protected against losses resulting from various disasters.

Key Insurance Policies:

1. **Property and Casualty Insurance**: Covers damage to or loss of the physical assets of the company, including buildings, data centers, and equipment.
2. **Business Interruption Insurance**: Provides compensation for lost income and covers operating expenses when the business is unable to operate normally due to a disaster.
3. **Cyber Liability Insurance**: Offers protection against losses resulting from data breaches, cyberattacks, and other cyber security incidents.
4. **General Liability Insurance**: Protects against claims of bodily injury or property damage suffered by others as a result of the company’s operations.

Insurance Management Process:

- **Annual Review**: The insurance portfolio is reviewed annually to ensure that coverage levels are adequate and reflect the current value of the company's assets and the scale of its operations.
- **Claim Filing Procedure**: In the event of a disaster, the designated insurance manager is responsible for promptly notifying the insurance companies and filing claims according to the policies' terms.
- **Documentation**: All insurance policies, contact information for insurance representatives, and claim filing procedures are documented and stored both electronically and in physical form in secure locations.

Policy Name	Coverage Type	Coverage Period	Amount Of Coverage	Person Responsible For Coverage	Next Renewal Date

12 Financial and Legal Issues

Financial Management in Disasters:

1. **Emergency Fund**: COMPANY maintains an emergency fund to cover immediate post-disaster expenses until insurance claims can be processed.
2. **Cash Flow Analysis**: Regular cash flow analysis to ensure liquidity in the event of a disaster.
3. **Financial Obligations**: A plan to prioritize and manage financial obligations, including payroll, taxes, and debts during and after a disaster.

Legal Considerations:

1. **Compliance**: Ensuring that disaster recovery efforts comply with all relevant laws, regulations, and industry standards.
2. **Contracts and Agreements**: Reviewing contracts with vendors, customers, and partners to understand obligations and liabilities in the event of a disaster.
3. **Legal Counsel**: Engaging legal counsel to advise on potential liabilities and legal actions resulting from the disaster, including regulatory fines or litigation.

Record Keeping and Documentation:

- Maintaining accurate and up-to-date records of financial transactions, legal communications, and insurance claims related to the disaster recovery process.

- Documentation to support insurance claims, including photographs of damage, repair invoices, and records of lost income.

By addressing insurance, financial, and legal issues as integral components of the IT Disaster Recovery Plan, Jadarah Funders Debt Collection Co ensures a holistic approach to disaster preparedness, minimizing financial risks and legal liabilities while facilitating a swift recovery.

13 DRP Exercising

Regular exercising of the Disaster Recovery Plan (DRP) is crucial for Jadarah Funders Debt Collection Co to ensure the plan's effectiveness and the staff's readiness in the event of an actual disaster. These exercises help identify any gaps or weaknesses in the plan and provide an opportunity for improvements.

Exercise Types:

1. **Tabletop Exercises**: Simulated disaster scenarios discussed in a meeting format to walk through the plan without activating any actual resources. This helps to familiarize the team with the plan and their roles.
2. **Functional Exercises**: These simulate specific functions such as data recovery from backups, switching to alternate sites, or emergency communications to test the actual capabilities of the recovery teams.
3. **Full-scale Exercises**: Involve activating and mobilizing all components of the DRP as if a real disaster had occurred. This is the most comprehensive form of testing, involving all critical personnel, systems, and external partners.

Exercise Schedule:

- Jadarah Funders Debt Collection Co will conduct tabletop exercises semi-annually.
- Functional exercises will be conducted annually for each critical function identified in the DRP.
- A full-scale exercise will be conducted every two years, involving all aspects of the DRP.

After Action Review (AAR):

Following each exercise, an After Action Review (AAR) meeting will be held to discuss what was successful and what needs improvement. The AAR will result in actionable items that will be tracked to completion to ensure that lessons learned are integrated into the DRP.

Documentation:

All exercises will be documented, including scenarios used, participants, observations, AAR outcomes, and improvements implemented. This documentation will be stored securely and made accessible to the DRP team for future reference.

14 Appendices

14.1 Templates Disaster Recovery Plan for <System One>

SYSTEM	

OVERVIEW	
PRODUCTION SERVER	Location: Server Model: Operating System: CPUs: Memory: Total Disk: System Handle: System Serial #: DNS Entry: IP Address: Other:
HOT SITE SERVER	
APPLICATIONS (Use bold for Hot Site)	
ASSOCIATED SERVERS	

BACKUP STRATEGY **FOR SYSTEM ONE**	
Daily	
Monthly	
Quarterly	

SYSTEM ONE **DISASTER RECOVERY** **PROCEDURE**	
Scenario 1 Total Loss of Data	
Scenario 2 Total Loss of HW	

ADDENDUM

CONTACTS	

File Systems

File System as of Minimal file systems to be created and restored from backup:	**File system Kbytes Used Avail %used Mounted on**
Other critical files to modify	
Necessary directories to create	
Critical files to restore	
Secondary files to restore	
Other files to restore	

14.2 Disaster Recovery Plan for <System Two>

SYSTEM	

OVERVIEW	

PRODUCTION SERVER	Location: Server Model: Operating System: CPUs: Memory: Total Disk: System Handle: System Serial #: DNS Entry: IP Address: Other::
HOT SITE SERVER	
APPLICATIONS (Use bold for Hot Site)	
ASSOCIATED SERVERS	

KEY CONTACTS	
Hardware Vendor	
System Owners	
Database Owner	
Application Owners	
Software Vendors	
Offsite Storage	

BACKUP STRATEGY for SYSTEM TWO	
Daily	
Monthly	
Quarterly	

SYSTEM TWO DISASTER RECOVERY PROCEDURE	
Scenario 1 Total Loss of Data	
Scenario 2 Total Loss of HW	

ADDENDUM

CONTACTS	

File Systems

File System as of Minimal file systems to be created and restored from backup:	**File system Kbytes Used Avail %used Mounted on**
Other critical files to modify	
Necessary directories to create	
Critical files to restore	
Secondary files to restore	
Other files to restore	

14.3 Disaster Recovery Plan for Local Area Network (LAN)

SYSTEM	

OVERVIEW	
PRODUCTION SERVER	Location: Server Model: Operating System: CPUs: Memory: Total Disk: System Handle: System Serial #: DNS Entry: IP Address: Other::
HOT SITE SERVER	
APPLICATIONS (Use bold for Hot Site)	
ASSOCIATED SERVERS	

KEY CONTACTS	
Hardware Vendor	
System Owners	
Database Owner	
Application Owners	
Software Vendors	

Offsite Storage	

BACKUP STRATEGY for Local Area Network (LAN)	
Daily	
Monthly	
Quarterly	

Local Area Network (LAN) **DISASTER** **RECOVERY PROCEDURE**	
Scenario 1 Total Loss of Data	
Scenario 2 Total Loss of HW	

ADDENDUM

CONTACTS	

File Systems

File System as of Minimal file systems to be created and restored from backup:	**File system Kbytes Used Avail %used Mounted on**
Other critical files to modify	
Necessary directories to create	
Critical files to restore	
Secondary files to restore	
Other files to restore	

14.3.1.1

14.4 Disaster Recovery Plan for Wide Area Network (WAN)

SYSTEM	

OVERVIEW	
PRODUCTION SERVER	Location: Server Model: Operating System: CPUs: Memory: Total Disk: System Handle: System Serial #: DNS Entry: IP Address: Other::
HOT SITE SERVER	
APPLICATIONS (Use bold for Hot Site)	
ASSOCIATED SERVERS	

KEY CONTACTS	
Hardware Vendor	
System Owners	
Database Owner	
Application Owners	

Software Vendors	
Offsite Storage	

BACKUP STRATEGY for Local Area Network (LAN)	
Daily	
Monthly	
Quarterly	

Local Area Network (LAN) **DISASTER** **RECOVERY PROCEDURE**	
Scenario 1 Total Loss of Data	
Scenario 2 Total Loss of HW	

ADDENDUM

CONTACTS	

Support Systems

Support system	
Critical network assets	
Critical interfaces	
Critical files to restore	
Critical network services to restore	
Other services	

14.5 Disaster Recovery Plan for Remote Connectivity

14.6

SYSTEM	

OVERVIEW	
PRODUCTION SERVER	Location: Server Model: Operating System: CPUs: Memory: Total Disk: System Handle: System Serial #: DNS Entry: IP Address: Other::
HOT SITE SERVER	
APPLICATIONS (Use bold for Hot Site)	
ASSOCIATED SERVERS	

KEY CONTACTS	
Hardware Vendor	
System Owners	
Database Owner	
Application Owners	

Software Vendors	
Offsite Storage	

BACKUP STRATEGY for Local Area Network (LAN)	
Daily	
Monthly	
Quarterly	

Local Area Network (LAN) **DISASTER** **RECOVERY PROCEDURE**	
Scenario 1 Total Loss of Data	
Scenario 2 Total Loss of HW	

ADDENDUM

CONTACTS	

Support Systems

Support system	
Critical network assets	
Critical interfaces	
Critical files to restore	
Critical network services to restore	
Other services	

15 Forms

15.1 Damage Assessment Form

Key Business Process Affected	Description Of Problem	Extent Of Damage

15.2 Management of DR Activities Form

- During the disaster recovery process all activities will be determined using a standard structure;
- Where practical, this plan will need to be updated on a regular basis throughoutthe disaster recovery period;
- All actions that occur during this phase will need to be recorded

Activity Name:
Reference Number:
Brief Description:

Commencement Date/Time	**Completion Date/Time**	**Resources Involved**	**In Charge**

15.3 Disaster Recovery Event Recording Form

- All key events that occur during the disaster recovery phase must be recorded.
- An event log shall be maintained by the disaster recovery team leader.
- This event log should be started at the commencement of the emergency and a copy of the log passed on to the business recovery team once the initial dangers have been controlled.
- The following event log should be completed by the disaster recovery team leader to record all key events during disaster recovery, until such time as responsibility is handed over to the business recovery team.

Description of Disaster:
Commencement Date:
Date/Time DR Team Mobilized:

Activities Undertaken by DR Team	**Date and Time**	**Outcome**	**Follow-On Action Required**

Disaster Recovery Team's Work Completed: <Date>
Event Log Passed to Business Recovery Team: <Date>

15.4 Disaster Recovery Activity Report Form

- On completion of the initial disaster recovery response the DRT leader should prepare a report on the activities undertaken.
- The report should contain information on the emergency, who was notified and when, action taken by members of the DRT together with outcomes arising from those actions.
- The report will also contain an assessment of the impact to normal business operations.
- The report should be given to business recovery team leader, with a copy to senior management, as appropriate.
- A disaster recovery report will be prepared by the DRT leader on completion of the initial disaster recovery response.
- In addition to the business recovery team leader, the report will be distributed to senior management

The report will include:

- A description of the emergency or incident
- Those people notified of the emergency (includingdates)
- Action taken by members of the DRT
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Assessment of the effectiveness of the BCP and lessons learned
- Lessons learned

15.5 Mobilizing the Disaster Recovery Team Form

- Following an emergency requiring recovery of technology infrastructure assets, the disaster recovery team should be notified of the situation and placed onstandby.
- The format shown below can be used for recording the activation of the DR team once the work of the damage assessment and emergency response teams has been completed

Description of Emergency:

Date Occurred:
Date Work of Disaster Recovery Team Completed:

Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required
Relevant Comments (e.g., Specific Instructions Issued)					

15.6 Mobilizing the Business Recovery Team Form

- Following an emergency requiring activation of the disaster recovery team, the business recovery team should be notified of the situation and placed on standby.
- The format shown below will be used for recording the activation of the business recovery team once the work of the disaster recovery team has been completed.

Description of Emergency:
Date Occurred:
Date Work of Business Recovery Team Completed:

Name of Team Member	Contact Details	Contacted On (Time / Date)	By Whom	Response	Start Date Required

Relevant Comments (e.g., Specific Instructions Issued)					

15.7 Monitoring Business Recovery Task Progress Form

- The progress of technology and business recovery tasks must be closely monitored during this period of time
- Since difficulties experienced by one group could significantly affect other dependent tasks it is important to ensure that each task is adequately resourced and that the efforts required to restore normal business operations have not been underestimated

Note: A priority sequence must be identified although, where possible, activities will be carried out simultaneously.

Recovery Tasks (*Order of Priority)*	**Person(s) Responsibl e**	**Completion Date**		**Milestone s Identified**	**Other Relevant Information**
		Estimated	Actual		
1.					
2.					
3.					
4.					
5.					
6.					

7.					

15.8 Preparing the Business Recovery Report Form

- On completion of business recovery activities the BRT leader should prepare a report on the activities undertaken and completed
- The report should contain information on the disruptive event, who was notified and when, action taken by members of the BRT together with outcomes arising from those actions
- The report will also contain an assessment of the impact to normal business operations
- The report should be distributed to senior management, as appropriate

The contents of the report shall include:

- A description of the incident
- People notified of the emergency (including dates)
- Action taken by the business recovery team
- Outcomes arising from actions taken
- An assessment of the impact to normal business operations
- Problems identified
- Suggestions for enhancing the disaster recovery and/or business continuityplan
- Lessons learned

15.9 Communications Form

- It is very important during the disaster recovery and business recovery activities thatall affected persons and organizations are kept properly informed
- The information given to all parties must be accurate and timely
- In particular, any estimate of the timing to return to normal working operations should be announced with care
- It is also very important that only authorized personnel deal with media queries

Groups of Persons or Organizations Affected by Disruption	**Persons Selected To Coordinate Communications to Affected Persons / Organizations**		
	Name	**Position**	**Contact Details**
Customers			
Management & Staff			

Suppliers			
Media			
Stakeholders			
Others			

15.10 Returning Recovered Business Operations to Business Unit Leadership

- Once normal business operations have been restored it will be necessary to return the responsibility for specific operations to the appropriate business unit leader
- This process should be formalized in order to ensure that all parties understandthe change in overall responsibility, and the transition to business- as-usual
- It is likely that during the recovery process, overall responsibility may have been assigned to the business recovery process lead
- It is assumed that business unit management will be fully involved throughout the recovery, but in order for the recovery process to be fully effective, overall responsibility during the recovery period should probably be with a business recovery process team

15.11 Business Process/Function Recovery Completion Form

The following transition form should be completed and signed by the business recovery team leader and the responsible business unit leader, for each process recovered.

A separate form should be used for each recovered business process.

Name Of Business Process	
Completion Date of Work Provided by Business Recovery Team	
Date of Transition Back to Business Unit Management ***(If different than completion date)***	

I confirm that the work of the business recovery team has been completed in accordance with the disaster recovery plan for the above process, and that normal business operations have been effectively restored.

Business Recovery Team Leader Name: _____ Signature:_____ Date: _

(Any relevant comments by the BRT leader in connection with the return of this business process should be made here.)

I confirm that above business process is now acceptable for normal working conditions. Name:_ Title:__ Signature: ___

Date: __