IT Backup and Disaster Recovery Plan

(Cloud Disaster Recovery)

In order to maintain the real-time protection and safeguarding of your backed up data, we developed The OVH Backup Kit.

(www.ovhbackupkit.co.za)

(Spider Black Online)

Safe & Secure Data Backup

and

Disaster Recovery Solutions

Confidentiality Caution:

This document is intended only for the use of the individual or entity to which it is addresssed and contains information that is privileged and confidential. If the reader of this document is not the intended recipient, or the employee or agent responsible for delivering the document to the intended recipient, you are hereby notified that any dessemination, distribution or copying of this document is strickly prohibited. If you have received this document in error, please notify us immediately by telephone or email and return the original document to us at the below address at our cost

Legal Disclaimer:

This IT Back-up and Disaster Recovery has been prepared and made available to Spider Black Online authorities for general information purposes only. The information herein does not constitute legal advice, nor should you rely solely on the plan in order to assess risk or make plans.

The content may be, or may become inaccurate or incomplete, and particular facts unique to your situation may render the content inapplicable to your situation. The plan is but one source of information available to you. You may wish to consider multiple sources in order to make plans.

Spider Black Online does not accept liability for any loss or damage arising from, connected with, or relating to the use or reliance on the toolkit by you or any other person. Spider Black Online authorities remain wholly responsible for evaluating the completeness and effectiveness of their own IT disaster recovery plans.

Putting the Plan into Action

Copies of this document need to be provided to all stakeholders (internal and/or external) and all associates or service providers who have responsibilities in the plan. You should create additional hard- and soft-copies for each data center or availability zone that houses your IT systems, including any standby or recovery facilities you have. You will need to ensure that the access to these hard and soft copies is protected to guarantee the integrity of the document.

Additionally, you should schedule time to review the document on a regular basis and to establish periodic tests to ensure continued applicability.

Document Versions Information and Changes

Any changes, edits and updates made to the Disaster Recovery Plan will be recorded in here. It is the responsibility of the Disaster Recovery Lead to ensure that all existing copies of the Disaster Recovery Pla are up to date.

Whenever there is an update to the Disaster Recovery Plan, Spider Black Online requires that the version number be updated to indicate this.

Version	Date	Author	Role	Rationale
1.0	2012-02-01	Eric Mulovhedzi	*IT (DR) Lead*	*First draft*
2.0	2012-07-01	Eric Mulovhedzi	*IT (DR) Lead*	*Procument of the first dedicated server hosting for ABI at Dimension Data.*
2.5	2013-02-25	Eric Mulovhedzi	*IT (DR) Lead*	*Installation of the second, backup, server for ABI data.*
3.0	2013-11-01	Thomas Shirindza	*Consultant*	*Dedicated Firewall Setup (Spider Black)*
3.1	2014-02-01	Seeta Matete	*Systems Administrator*	*Shared Firewall Replacement (Internet Solutions).*
3.6	2014-07-01	Eric Mulovhedzi	*IT (DR) Lead*	*Drafting of new Robust Data Backup and Server Monitoring Policy.*
3.9	2014-09-01	Eric Mulovhedzi	*IT (DR) Lead*	*Implementation of new Robust Data Backup and Server Monitoring Solutions.*
4.0	2015-01-15	Seeta Matete	*Systems Administrator*	*Installation of the third dedicated server for MTN & GSK data.*
4.1	2015-05-15	Eric Mulovhedzi	*IT (DR) Lead*	*Installation of the fourth & fifth dedicated server for Spider Black's SME clients data.*
4.2	2016-02-01	Rudzani Mulovhedzi	*Managing Director*	*Replaced Eric Mulovhedzi as DR Lead.*
4.3	2016-05-01	Rudzani Mulovhedzi	*IT (DR) Lead*	*Revised to include new ERP Platform, OVH Enterprise Framework V2.10.*
4.5	2016-06-01	Rudzani Mulovhedzi	*IT (DR) Lead*	*Procument of the extra 66 sq.metre Office Space. To setup OVH Electronics Laboratory.*

Version	Date	Author	Role	Rationale
4.7	2017-02-01	Eric Mulovhedzi	*Chief Engineer*	*Installation of OVH Server Basement, virtual server managemet application tool in all 5 server assets.*
4.8	2018-06-01	Ultech Solutions	*Contractor*	*Installation of new VoIP Call Centre.*
4.9	2018-08-01	Molatelo Mabelebele	*Lead Researcher*	*Revised to include IoT technologies.*
5.0	2019-02-01	Syllucia Mosima	*Business Analyst*	*Revised to include CCBSA Centralized IT Department.*
5.1	2020-11-25	Morena Maleka	*Lead Developer*	*CCBSA COVID-19 Cyber Security Enhancements.*
5.3	2021-01-27	Eric Mulovhedzi	*Chief Engineer*	*ERP Platform Incorporation of revised Spider Black File Plan and Records Disposal Classifications.*

Table of Contents

INTRODUCTION

AND

OVERVIEW

Our Technology Policy Framework Directive

All Spider Black Online employees, authorities, administrators and other legal professionals have access to appropriate devices, reliable infrastructure, high-speed networks and digital learning environments.

Actions:

Spider Black Online Management:

- ensure administration of safe and secure networks, infrastructure and technologies
- provide and maintain timely technical support and services
- adopt and maintain effective practices and up-to-date technological standards with respect to Information Technology (IT) governance, IT management and information security management.

Spider Black Online has developed this IT Back-up and Disaster Recovery Plan to be used in the event of a significant disruption to critical IT services at its offices and office premises.

Objectives:

The objectives of this IT Back-up and Disaster Recovery Plan are:

- to ensure business continuity within an appropriate period after an unforeseen incident or disaster has occurred.
- to outline the key recovery steps to be performed during and after a disruption.
- to ensure that operational policies are adhered to within all planned activities.

DEFINITION
OF A
DISASTER

This Disaster Recovery Plan (DR Plan) is the single source for all of the information that describes Spider Black Online's ability to survive and recover from a disaster including the processes that must be followed to accomplish the disaster recovery.

Definition of a Disaster:

A disaster can be caused by many events resulting in Spider Black Online's IT department not being able to perform some or all of their regular roles and responsibilities for a period of time. Spider Black Online 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 DR document to be activated:

- Environmental disaster (Flooding, Hurricane, Fire, etc.)
- Hardware Failure / Server Room Issue
- Power Outage
- Theft
- Deliberate & Terrorist Attack
- Human Error

THE PURPOSE
OF
THE DR PLAN

What the DR Plan Intends and Aims to Achieve

The purpose for this Disaster Recovery Plan document is to inventory all of the IT infrastructure and capture all of the information relevant to the organization's ability to recover its IT from a disaster, and document the steps that the organization will follow in the event that a disaster occurs.

The top priority of Spider Black Online will be to enact the steps outlined in this Disaster Recovery Plan 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 IT assets
- Minimizing downtime related to IT
- Keeping the business running in the event of a disaster

This Disaster Recovery Plan will also detail how this document is to be maintained and tested.

Emergency Contact Form

Full Name	Role / Title	Contact Type	Contact Information
Rudzani Mulovhedzi	*Managing Director*	Work	*+27.87 791 5984*
		Mobile	*079 329 9765*
		Alternate	
		Email	*rudzani@spiderblackonline.co.za*
Eric Mulovhedzi	*Chief Engineer*	Work	*+27.87 791 5984*
		Mobile	*081 716 3886*
		Alternate	
		Email	*eric@spiderblackonline.co.za*
Lwazi Zwane	*Lead Developer*	Work	*+27.87 791 5984*
		Mobile	
		Alternate	
		Email	*lwazi@spiderblackonline.co.za*
Morena Maleka	*Lead Developer*	Work	*+27.87 791 5984*
		Mobile	
		Alternate	
		Email	*morena@spiderblackonline.co.za*

External Contacts

Full Name	Role / Title	Contact Type	Contact Information
Dedicated Server Hosting & Firewall			
Account #	1		
Dimension Data	*Dedicated Hosting*	Tel (Local)	*+27(0)87 365 0055*
		Tel (International)	*+27(0)11 575 0055*
		Email	*support@is.co.za*
Network Provider / Voice Communications Provider			
Account #	2		
Ultech Solutions	*Senior IT Specialist*	Work	
		Mobile	*082 460 8751*
		Email	*support@ultechsolutions.co.za*
Web Hosting / Emails Service Provider			
Account #	3		
Xneelo (Pty) Ltd	*Help Desk*	Tel (Contact Centre)	*0861 0861 08*
		Tel (International)	*+27 21 970 2000*
		Email	*admin@xneelo.com*
Property Manager / Landlord - Midrand			
Account #	4		
		Work	
		Mobile	
		Email	
Property Manager / Landlord			
Account #	5		
		Work	
		Mobile	
		Email	

SCOPE

OF

DISASTER RECOVERY PLAN

SCOPE

The Spider Black Online Disaster Recovery Plan takes all of the following technology areas into consideration:

Service Tier	IT Service / Application Description	RTO	RPO
0	Network Infrastructure	12	24
0	Servers Infrastructure / Firewall Services	12	24
1	Telephony System / Voice Communications / VoIP	24	N/A
0	Information Systems Security	12	24
0	Data Storage and Backup Systems	12	24
0	Data Output Devices	12	24
0	End-User Computing / Desktop Publishing	12	24
0	Organizational Software Systems	12	24
0	Database Systems / Electronic Files	12	24
1	CIC / Customer Interaction Facilities	24	N/A
1	IT Documentation / Document Management System	24	24
1	Email	24	24

NB: This Disaster Recovery Plan does not take into consideration any non-IT, personnel, Human Resources and real estate related disasters.

Assumptions

This IT Disaster Recovery Plan intends to provide Spider Black Online with the necessary information needed to resume business in a manner that is appropriate and timely for business continuity in the event of the following priority:

- Destruction or Inability to access the office or customer interaction centre or servers facilities
- Loss of Systems (Network Connectivity and or Applications), and Loss of Employees

Furthermore, the detailed recovery procedures as well as recovery strategies, estimated recovery time objectives and recovery point objectives are based on the following general assumptions and will need to be validated:

- Continuous efforts to allocate the space required in the current office to restore information systems in case this site is deemed unavailable
- Continuous efforts to establish the alternate site for the current office in case the data centre is deemed unavailable, and Backups are readily available to initiate restoration efforts.

(A) Networking:

There is ample bandwidth at the recovery facility to connect to the internet. Configuration files can be uploaded to network devices through a laptop or other type of device.

(B) Key Users:

- Key Users will have their laptops or a suitable devices with them during a disaster.
- Key Users will have internet access and telephone/voice communication capability available to work from a remote location.

(C) Staff:

- Key IT staff or their alternates required to assist in the recovery efforts will be available.
- IT staff involved in recovery efforts have the necessary technical skills to restore critical information systems identified in this document.

IT-Backup & DR Plan as a Procurement (Bidding) Requirement

for

Legal Professionals & Law Firms

As a proof of business continuity when bidding, the National Treasury of South Africa clearly states that:

(i) Bidders shall provide proof that they have IT security systems in place to protect private and confidential information while processing information (e.g. anti-virus, firewall, back-ups and/or encryptions, but not limited to the aforementioned)

- Proof to be provided by Bidders(s) that IT security systems are in place to protect private and confidential information while processing information.

NB: Proof of IT security systems must be provided by the Bidder

(ii) Bidders shall provide proof that they have a back-up and disaster recovery plan which should include, but not be limited to, a business continuity plan that reflects on emergency management planning, crisis management and continuation of operations.

What is a Disaster Recovery?

A Disaster Recovery Plan (DR Plan) is a detailed IT document that provides a blueprint for recovering from common IT-based business disruptions such as:

- Ransomware or Other Cyberattacks
- Environmental Catastrophes
- Building Accessibility or Power Disruption
- Employee Errors
- Hardware Failures
- Software Failures

Whether you are managing your DR plan internally or are entrusting your plan to a managed service provider, the document must contain detailed, accurate and up-to-date information about the IT operations of your organization.

The DR Plan must present that information in a clear and coherent format that is easily consumable and, most importantly, actionable during an actual emergency.Your employees or service provider must be able to follow the document and react rapidly so that availability can be restored per the companyÕs established service level requirements.

How our IT Back-up and DR Solution was Developed

Managed Service Provider

Spider Black Online IT Disaster Recovery solutions have been carefully developed to provide cost effective, dependable options for customers to protect their critical business data and ensure recoverability. These cloud-based services provide customers with unmatched data loss prevention and the flexibility to address any RTO and RPO objectives. Driven by each customer's unique needs, our solutions offer backup and recovery protection for:

- Desktops
- Physical Servers
- Operating Systems
- Hypervisors
- Storage

We have designed our Disaster Recovery suite to allow businesses to determine their level of risk and spend accordingly. Our customers not only know where their data is backed up, they also know how and when they will have it restored when a disaster is declared, as defined in their Disaster Recovery Plan.

RECOVERY

PLAN

Facilities and Infrastructure Plan

Facility Requirements:

Requirement	Description
Infrastructure	Office Furniture for about 25 Personnel
Desktop Publishing	End-User Desktop Workstations and a Printer
Network Connectivity	WIFI (100 Mbs)
Backup Network Connectivity	Telkom ADSL/FIBRE (100 Mbs)
Voice Communications	Telephones
Power (Voltage)	Normal 240v
Backup Power Generator	Normal 240v
Office Space Size	200 Square Metres

NB: If the incident manager determines that the primary facility is no longer sufficiently functional or operational to restore normal business operations, the team will be instructed that the recovery of systems will be done at the recovery facility.

Once this determination has been made, the facilities team will be engaged to bring the alternate facility to a functional state. The incident manager will co-ordinate travel and logistics to ensure that the team can operate out of the alternate site.

If the recovery facility is unavailable, the facilities team will contact hotels, other schools or public buildings to see if they can provide the required space and power.

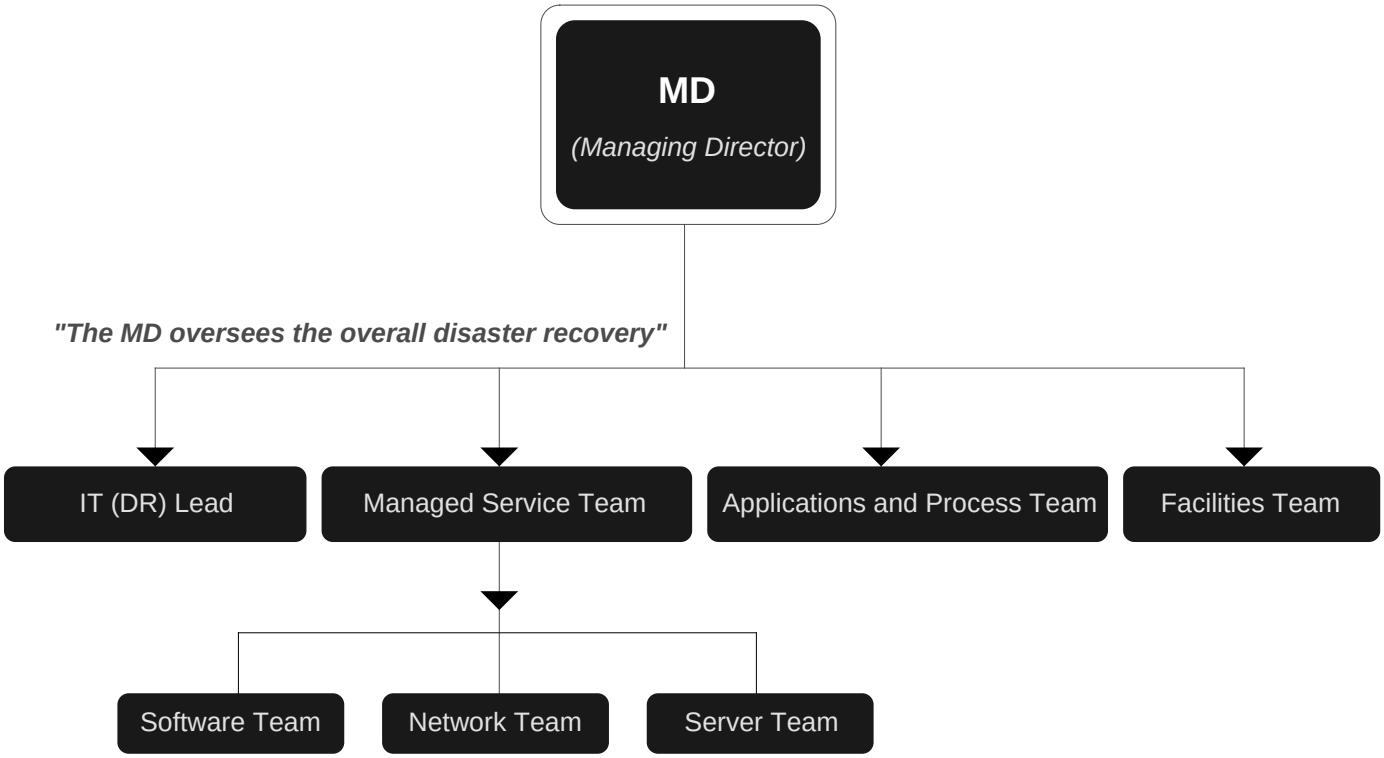
Recovery Plan Responsibility Table

System	Responsibility	Priority	Recovery Strategy and Procedure	Assumptions	RTO & RPO	Recovery Platform
Network Infrastructure	*IT App. Team*	*C*	*- Access backup files from the cloud Restore files to respective computers*	*- Backup of files was done regular to the cloud - Login details to the cloud is available*	*RTO=12 RPO=24*	*Service Provider*
Servers Infrastructure	*IT App. Team*	*C*	*- Access backup files from the cloud Restore files to respective computers*	*- Open Source Licences are always valid*	*RTO=12 RPO=24*	*Linux (Ubuntu)*
Voice Communications	*IT App. Team*	*V*	*- Acquisition of telephones - Contact service provider to*	*- Backup of files was done regular to the cloud - Login details to the cloud is available*	*RTO=24 RPO=N/A*	*Service Provider*
Security Firewall	*IT App. Team*	*V*	*- Contact service provider to reinstall configuration*	*- Dimension Data shared firewall licence*	*RTO=12 RPO=24*	*Service Provider*
End-User Computing	*IT App. Team*	*C*	*- Access backup files from the cloud Restore files to respective computers*	*- Backup of files was done regular to the cloud - Login details to the cloud is available*	*RTO=12 RPO=24*	*Windows & Mac OS*
Legal Software	*IT App. Team*	*C*	*- Reinstall call centre software to server*	*- Backup of Case Management Software and files was done regularly*	*RTO=12 RPO=24*	*Online Cloud Software*
Electronic Files	*IT App. Team*	*C*	*- Access backup files from the cloud system*	*- Backup of files was conducted regular to the cloud - Login details to the cloud is available*	*RTO=12 RPO=24*	*Online Cloud Software*
Email	*IT App. Team*	*N*	*- Reinstall email software to all laptops and workstations - Restoration of configuration data*	*- Login details of email accounts and/or domain control panel are readily available*	*RTO=12 RPO=24*	*Online Cloud Software*

PLAN

IMPLEMENTATION

DISASTER RECOVERY TEAM ORGANIZATIONAL CHART



In the event of a disaster, different teams will be required to assist the IT department or and Managed Service Provide in their effort to restore normal functionality to the employees of Spider Black Online. The above chart depicts the key roles involved in preparing for and responding to a disaster.

The lists of roles and responsibilities in this section have been created by Spider Black Online 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.

IT Lead / IT Disaster Recovery Lead

The IT Disaster Recovery Lead is responsible for making all decisions related to the IT 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 Spider Black Online, 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. As a result, the Disaster Recovery Lead will not be a member of other Disaster Recovery groups in Spider Black Online.

Roles and Responsibilities:

- Make the determination that the organization is declaring that a disaster has occurred and trigger the Disaster Recovery Plan and related processes.
- Initiate the Disaster Recovery Notification Network.
- Be the single point of contact for and oversee all of the Disaster Recovery Teams.
- Organize and chair regular meetings of the Disaster Recovery Team leads throughout the disaster.
- Present to the Management Team including MD (Managing Director) on the state of the disaster and the decisions that need to be made.
- Organize, supervise and manage all Disaster Recovery Plan test and author all Disaster Recovery Plan updates.

Contact Information:

Name	Role / Title	Work Phone No.	Home Phone No.	Mobile Phone No.
Rudzani Mulovhedzi	*Primary DR Lead*	*+27.87 791 5984*		*079 329 9765*
Lwazi Zwane	*Secondary DR Lead*	*+27.87 791 5984*		
Dimension Data	*Dedicated Hosting*	*+27(0)87 365 0055*		*+27(0)11 575 0055*

Managed Service Team - Software Team

Managed Service Provider

The Cloud Software Team, Spider Black Online, in this case, is responsible for safeguarding the well-being of all software applications that Spider Black Online utilizes on a daily,weekly and monthly bases. This include (but is not limited to) Cloud-based Applications and Mobile Applications.

Also, this team has to ensure that all Spider Black Online's data requisition processes are in a format that meets international data quality standards.

It also supports Spider Black Online's workflow processes management system, administration business processes system, and its financial management complementary system.

Roles and Responsibilities:

- Vendor and Support of Workflow Management Solution System
  - Master Data Management System (MDM) Module
    - System Support
    - After-care Customer Service
  - Dedicated Server Support
  - Third-party Integration Support
- Customizable Business Processes Workflow Automation.
- Artificial Intelligence and Big Data Management Software.
- Asset Tracking and Fleet Management Software.
- Software Project Managemet for new modules that Spider Black Online may require as their organization's goals and needs change.

Managed Service Team - Software Team, Contact Information

Managed Service Provider

Contact Information:

Name	Role / Title	Work Phone No.	Email Address
Rudzani Mulovhedzi	*CFO*	*087 701 5384*	*accounts@spiderblackonline.co.za*
Lwazi Zwane	*Lead Developer*	*087 701 5384*	*support@spiderblackonline.co.za*
Morena Maleka	*Lead Developer*	*087 701 5384*	*support@spiderblackonline.co.za*
Eric Mulovhedzi	*Chief Engineer*	*087 701 5384*	*support@spiderblackonline.co.za*

Physical Address:

Unit A1, A2, A3, Halfway Gardens Office Park

Cnr Fred Verseput & Asparagus Road

Midrand

Gauteng

South Africa

Managed Service Team - 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, VoIP, and any telephony connections internally within the organization as well as telephony and data connections with the outside world.

They will be primarily responsible for providing baseline network functionality and may assist other IT Disaster Recovery Teams as required.

Roles and Responsibilities:

- In the event of a disaster, the team will determine which network services are not functioning at the primary availability zones
- 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.
- If network services are 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 system migration, the team will ensure that all network services are brought online at the secondary availability zones.
- Once critical systems have been provided with connectivity, employees will be provided with connectivity in the following order:
    - All members of the Disaster Recovery 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 availability zone.
- Install and implement any tools, hardware, software and systems required in the primary availability zone.
- After Spider Black Online 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.

Managed Service Team - Network Team, Contact Information

Name	Role / Title	Work Phone No.	Email Address
Ultech Solutions	*Senior IT Specialist*	*082 460 8751*	*support@ultechsolutions.co.za*

Managed Service Team - Server Team

Managed Service Provider

The Server Team will be responsible for providing the physical server infrastructure required for the organization to run its IT operations and applications in the event of and during a disaster.

They will be primarily responsible for providing baseline server functionality and may assist other IT Disaster Recovery Teams as required.

Roles and Responsibilities:

- In the event of a disaster that does not require migration, the team will determine which servers are not functioning at the primary availability zone.
- If multiple servers are impacted, the team will prioritize the recovery of servers in the manner and order that has the least business impact. Recovery will include the following tasks:
  - Assess the damage to any servers
  - Restart and refresh servers if necessary
- Ensure that secondary servers located in other zones are kept up-to-date with system patches.
- Ensure that secondary servers located in other availability zones are kept up-to-date with data copies.
- Ensure that the secondary servers located in the standby availability zones are backed up appropriately.
- Ensure that all of the servers in the standby availability zones abide by Spider Black Online's server policy.

- Install and implement any tools, hardware, and systems required in the standby availability zones.
- Install and implement any tools, hardware, and systems required in the primary availability zones.
- After Spider Black Online 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.

Managed Service Team - Dedicated Server Team, Contact Information

Managed Service Provider

Contact Information:

Name	Role / Title	Work Phone No.	Email Address
Morena Maleka	*Lead Developer*	*087 701 5384*	*support@spiderblackonline.co.za*
Eric Mulovhedzi	*CEO/Chief Engineer*	*087 701 5384*	*support@spiderblackonline.co.za*
Dimension Data	*Server Engineer*	*+27(0)87 365 0055*	*support@is.co.za*

Physical Address:

Unit A1, A2, A3, Halfway Gardens Office Park

Cnr Fred Verseput & Asparagus Road

Midrand

Gauteng

South Africa

Applications and Processes Team

The Applications and Processes Team will be responsible for ensuring that all organization 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 IT Disaster Recovery Teams as required.

Roles and Responsibilities:

- In the event of a disaster that does not require migration, the team will determine which applications are not functioning at the primary availability zones.
- 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
- Ensure that the following IT processes are followed when managing applications:
  - Incident Management and Change Management;
  - Access provisioning and Security Standards are adhered to
- Ensure that secondary servers located in other availability zones are kept up-to-date with application patches.
- Ensure that secondary servers located in other availability zones are kept up-to-date with data copies.
- Install and implement any tools, software and patches required in the standby availability zones.
- Install and implement any tools, software and patches required in the primary availability zones.
- After Spider Black Online 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.

Applications and Processes Team, Contact Information

Name	Role / Title	Work Phone No.	Email Address
Eric Mulovhedzi	*Program Manager*	*087 701 5384*	*support@spiderblackonline.co.za*
Lwazi Zwane	*System Admin*	*087 701 5384*	*support@spiderblackonline.co.za*

Facilities Team

The facilities team is responsible for all issues related to the physical facilities including both the primary and recovery facilities.

They also are responsible for assessing the damage and overseeing the repairs to the primary location in the event of the primary location's destruction or damage thereof.

Roles and Responsibilities:

- Assess physical damage to the primary facility.
- Ensure that the recovery facility is maintained in normal working order.
- Ensure transportation, sufficient supplies, food and water and sleeping arrangements are provided for all employees working at the recovery facility.
- Ensure that measures are taken to prevent further damage to the primary facility and appropriate resources are provisioned to rebuild or repair the main facilities if necessary.

Disaster Response Process

Responding to a disaster occurs in several phases as shown below. After an event occurs, the team assesses the event and determines whether to declare a disaster. If a disaster has occurred, the team initiates recovery of the IT service(s), in an alternate location if necessary. Once the required IT services are up and running, the team can focus on resuming normal operations. The final phase is to conduct a post-event review to discuss lessons learned.

STEP 1: EVENT OCCURS

- 2. Assess
  - Detect Incidents
  - Assess Severity
  - Escalate
  - Assess Impact
- 3. Recover
  - Notify Team
  - Initiate Recovery
  - Communicate Progress
  - Support Recovery Team
- 4. Resume Normal Operations
  - Initiate Project
  - Communicate Plans
- 5. Review
  - Conduct Post-Event Review

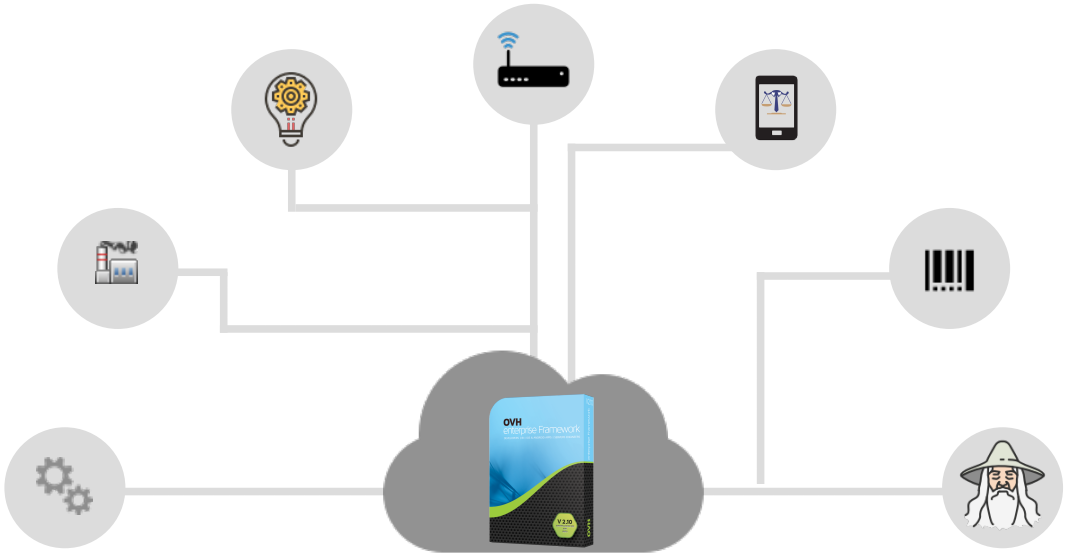
PLAN

TESTING AND MAINTENANCE

OUR 4IR CLOUD FACILITIES

While efforts were made initially to construct this IT back-up and disaster recovery plan were as complete and accurate as possible, it is essentially impossible to address all possible problems at any one time. Additionally, over time the Disaster Recovery needs of the organization will change. As a result of these two factors this plan will need to be tested.

1. **Plan Maintenance**
2. **Plan Testing**



Spider Black Online Software Platform

Maintenance

The IT back-up and disaster recovery plan will be updated three(3) months or any time a major system update or upgrade is performed, whichever is more often. The IT 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:

- Ensuring that all team lists are up to date
- Ensuring that all call lists are up to date
- Reviewing the plan to ensure that all of the instructions are still relevant to the organization
- Making any major changes and revisions in the plan to reflect organizational shifts, changes and goals
- Ensuring that the plan meets any requirements specified in new laws

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

Spider Black Online is committed to ensuring that this Disaster Recovery Plan is functional. The Disaster Recovery Plan should be tested every three(3) months in order to ensure that it is still effective. Testing the plan will be carried out as follows:

Disaster Recovery Rehearsal:

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 Disaster Recovery Plan Lead to make appropriate changes to the plan. Spider Black Online staff should be familiar with procedures, equipment, and all technologies (if required).

Failover Testing:

Under this scenario, servers and applications are brought online in an isolated environment. ThereÕs no impact to existing operations or uptime. Systems administrators ensure that all operating systems come up cleanly.Application administrators validate that all applications perform as expected.

Live-Failover Testing:

A live-failover test activates the total DR Plan. The test will disrupt normal operations, and therefore should be approached with caution. Ensure you have completed several iterations of steps 1 and 2 before proceeding with this step.Additionally, communicate all expected disruptions well in advance of performing this test.

Each period (every three months), a table top walkthrough, disaster simulation, full Failover Testing will be executed.

And, once a year, a full Live-Failover Testing will be conducted too.

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

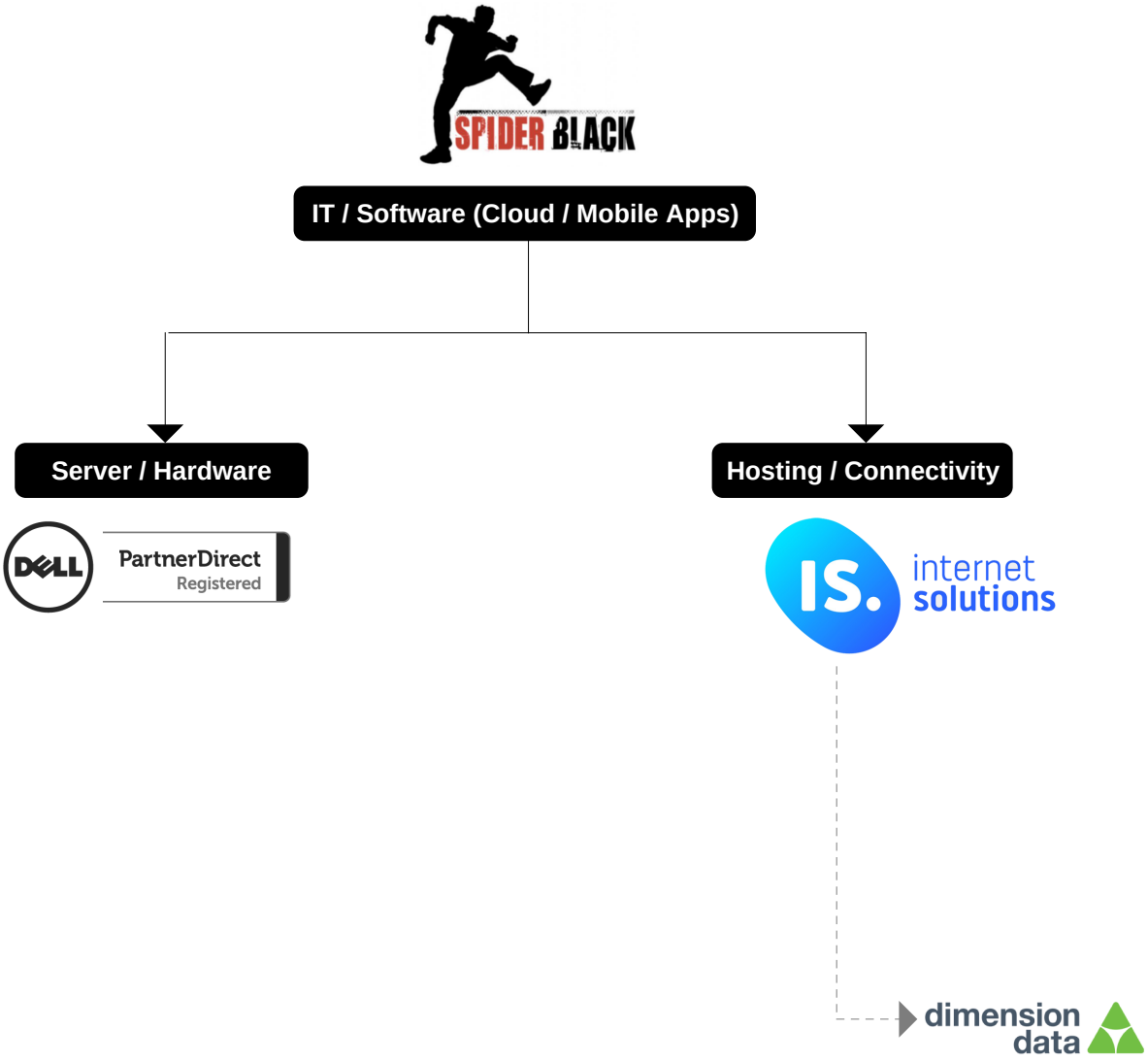
OUR

CLOUD TECHNOLOGY PARTNERS

WHERE WE HOST & MANAGE OUR DATA

PARTNERSHIPS:

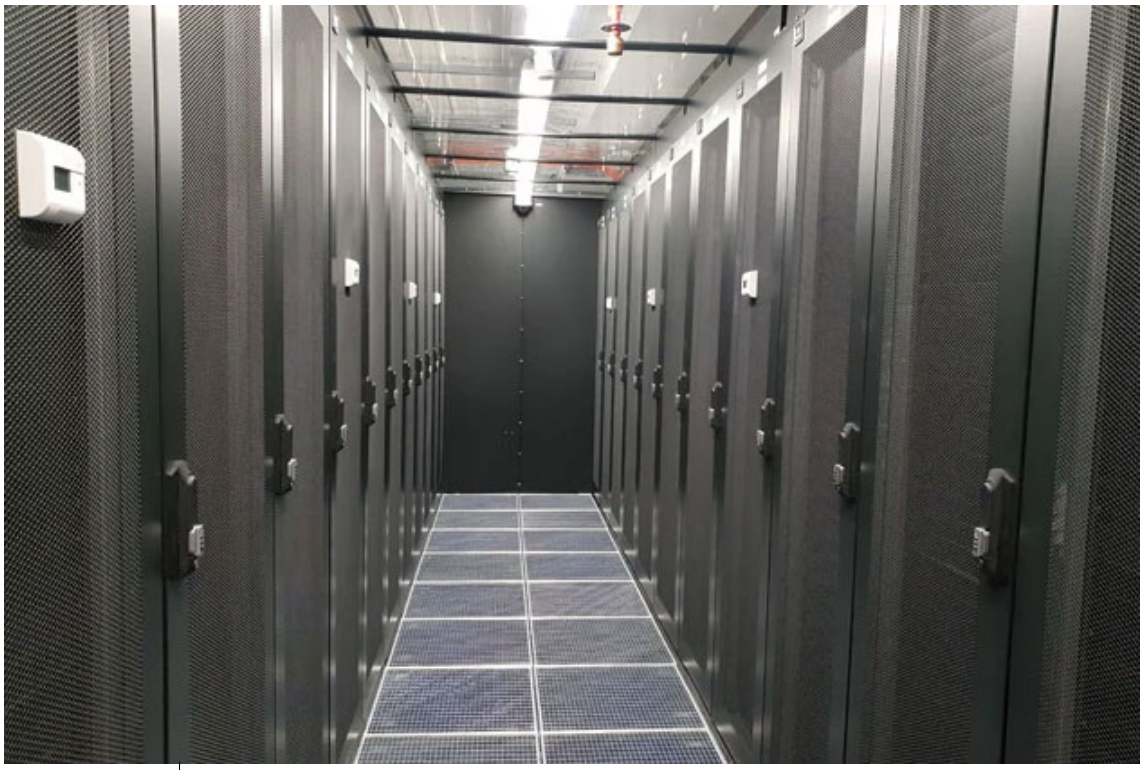
In order to meet all our IT back-up and disaster recovery plans, goals, and objectives to ensure seamless business continuity in case of unforseen crisis or disaster, Spider Black Online has partnered with the following reputable technology companies:



Our Heavy-Duty Mechanical Evidence Locker Room (Data Centre)

Your digital and electronic items will be placed in a heavy-duty mechanical evidence locker room. Fingerprint security system into the room allows that both deposit and retrieval can only be performed by pre-authorized individuals whose prints have already been entered into the system.

Lockers are divided into readily identifiable compartments, which are opened and closed with the user-friendly button locks. A heavy-duty steel structure, with welding at the ends to reinforce the strength of the doors. The doors themselves incorporate robust load-bearing hinges and rubber stops to ensure smooth closure. The digital lockers are also enhanced with detection sensors and LED panels that display valuable information at a glance. (Internet Solutions Data Centre)

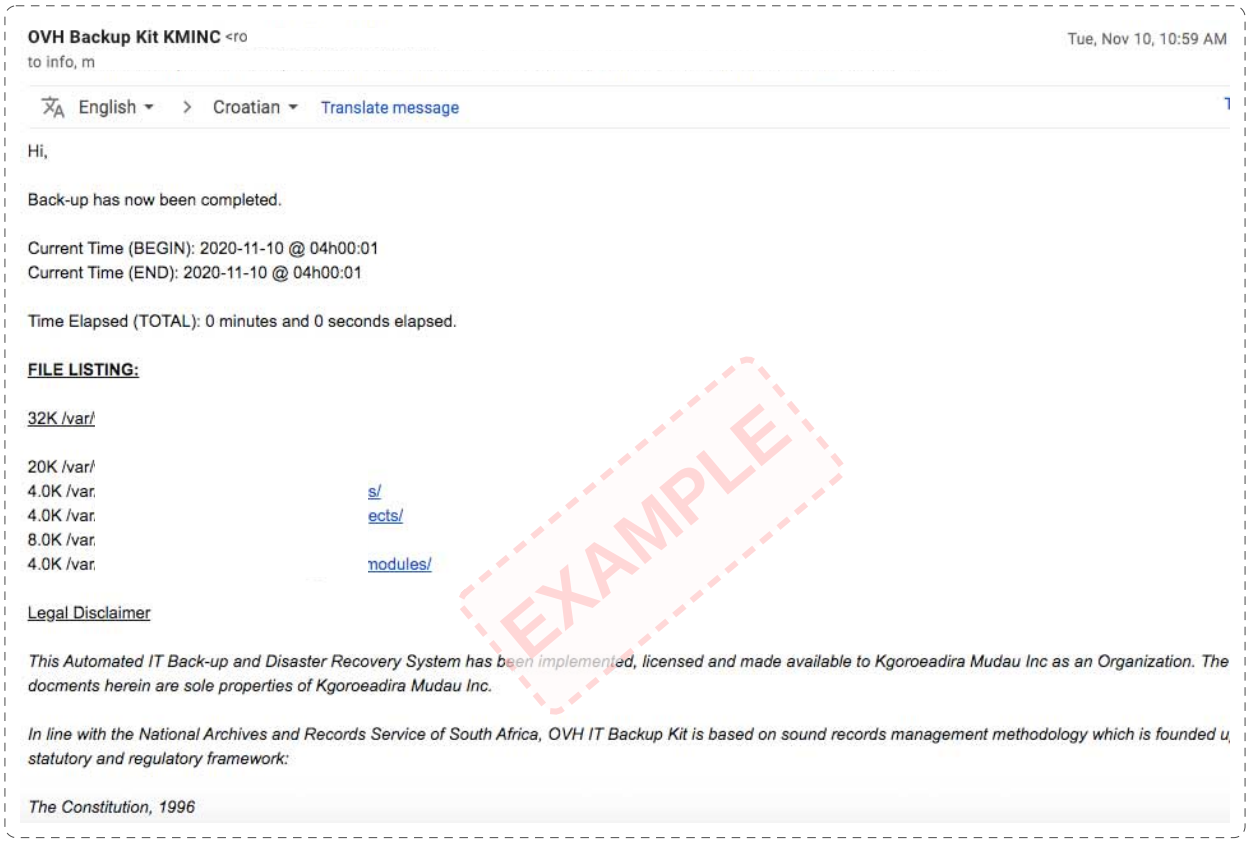


(Image from Internet Solutions Data Centre)

References

Reference #1:	
Title:	**OVH Backup Kit:**
Description:	*Auto Data Backup and Disaster Recovery Solution*
Author:	*Eric M. Mulovhedzi*
Type:	Shell Script
License:	*Comercial*
Programing Language:	*Shell Script (OS: Linux)*
URL:	*www.ovhbackupkit.co.za*
Year:	*2015*
Reference #2:	
Title:	**OVH Server Basement:**
Description:	*Virtual Hosts configuration utility tool for auto-managing webservers such as Apache.*
Author:	*Eric M. Mulovhedzi*
Type:	Application
License:	*Open Source: GNU General Public License, version 2 (GNU GPL v2)*
Programing Language:	*C++ (OS: Linux)*
URL:	*www.ovhserverbasement.co.za*
Year:	*2014*

Annexure A: Example of our Daily Automated Back-up Email Notification



OVH Backup Kit KMINC <ro
to info, m

Tue, Nov 10, 10:59 AM

English ▾ > Croatian ▾ Translate message

Hi,

Back-up has now been completed.

Current Time (BEGIN): 2020-11-10 @ 04h00:01
Current Time (END): 2020-11-10 @ 04h00:01

Time Elapsed (TOTAL): 0 minutes and 0 seconds elapsed.

FILE LISTING:

32K /var/

20K /var/
4.0K /var. s/
4.0K /var. ects/
8.0K /var.
4.0K /var. nodules/

Legal Disclaimer

This Automated IT Back-up and Disaster Recovery System has been implemented, licensed and made available to Kgoroeadira Mudau Inc as an Organization. The docments herein are sole properties of Kgoroeadira Mudau Inc.

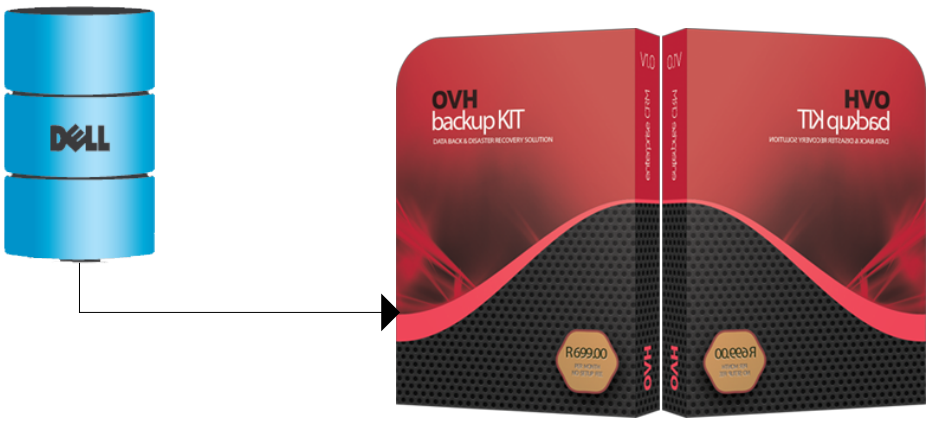
In line with the National Archives and Records Service of South Africa, OVH IT Backup Kit is based on sound records management methodology which is founded u statutory and regulatory framework:

The Constitution, 1996

EXAMPLE

The image above depicts an example of our automated Back-up Email Notification sent automatically, from the cloud electronic system, to your organization's company emails on a daily bases as proof of back-up.

Note that, this email notification must be annexed to the IT Back-up and Disaster Recovery Plan when bidding as a proof of your organization's business continuity.



(www.ovhbackupkit.co.za)

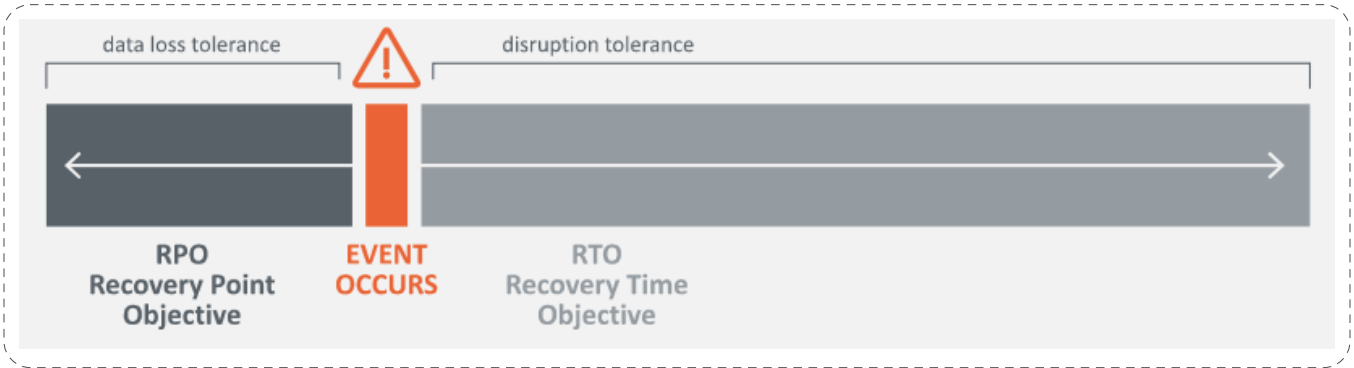
Appendix A: Glossary of Terms, Abbreviations, and Acronyms

Recovery Time Objective (RTO):

The goal for how fast to restore technology services after a disruption (based on the acceptable amount of down time and level of performance). For example, an RTO 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.

Recovery Point Objective (RPO):

The goal for the point at which to restore data or information after a disruption (based on the acceptable amount of data or information loss). For example, an RPO of 6 hours for payroll services means that the payroll data must be backed-up every 6 hours so that no more than 6 hours of data entered into the payroll application is lost af ter a disruption.



Term / Abbreviation	Explanation
Programming	*Also known as Coding, performing the activity of designing and writing a computer program.*
Coding	*Also known as Programming, performing the activity of designing and writing a computer program.*
Developer	*Software Coder or Programmer or the one who performs the activity of coding or programming.*
System Architect	*In systems design, the architects (and engineers) are responsible for: Interfacing with the user(s) and sponsor(s) and all other stakeholders in order to determine their (evolving) needs. Generating the highest level of system requirements, based on the users' needs and other constraints.*
Programming Language	*A vocabulary and set of grammatical rules for instructing a computer or computing device to perform specific tasks.*
RnD	*Research and Development*
Web Service	*A service offered by an electronic device to another electronic device, communicating with each other via the World Wide Web.*
WSDL	*Web Services Description Language*
ReST	*Representational State Transfer, a software architectural style that defines a set of constraints to be used for creating Web services.*
XML	*Extensible Markup Language, defines a set of rules for encoding documents.*
HTML	*Hypertext Markup Language*
CSS	*Cascading Style Sheets, is a style sheet language used for describing the presentation of a document.*
OVH Enterprise Framework	*Base Software Platform, PHP predominantly coded, developed and owned by Spider Black Online.*
OVH Backup Kit	*IT Backup and Disaster Recovery Plan technology developed and owned by Spider Black Online.*
CCBSA	*Coca Cola Beverages South Africa*
CCBA	*Coca Cola Beverages Africa*
GSK	*Glaxo Smith Kline*

Spider Black Online

Head Office:

Unit A1, A2, A3 Halfway Gardens Office Park

Cnr Fred Verseput & Asparagus Road

Halfway House

Midrand

1685, Johannesburg

Gauteng

South Africa

+27.87 791 5984

info@spiderblackonline.co.za