Disaster Recovery & Business Continuity Plan

IMPLEMENTED IN THE EVENT OF A DISASTER TO ENSURE BUSINESS CONTINUITY

TABLE OF CONTENTS

POLICY STATEMENT

VTSL management has approved the following policy statement:

- The company shall develop a comprehensive IT disaster recovery plan.
- A formal risk assessment shall be undertaken to determine the requirements for the disaster recovery plan.
- The disaster recovery plan should cover all essential and critical infrastructure elements, systems and networks, in accordance with key business activities.
- The disaster recovery plan should be periodically tested in a simulated environment to ensure it can be implemented in emergency situations and that the management and staff understand how it is to be executed.
- All staff must be made aware of the disaster recovery plan and their respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

STATEMENT OF INTENT

The purpose of this plan is to establish high level procedures to recover in the event of a disaster situation within VTSL.

The objectives of this plan are to maximise the effectiveness of contingency operations through a plan that consists of the following stages:

- Notification/Activation stages to detect and assess damage and to activate the plan
- Recovery stage to restore temporary services
- Reconstitutions stage to restore services to normal operational capabilities

The plan identifies the activities, resources and procedures required to maintain service during prolonged interruptions to normal operations.

The plan assigns responsibilities to designated VTSL personnel and coordinates external points of contact or specialist contractors to restore service.

More detailed recovery plans for individual systems are documented separately and may be implemented depending on the nature of the incident.

This document outlines our recommended procedures and may be modified during an emergency situation to protect people, property, systems and data.

OBJECTIVES

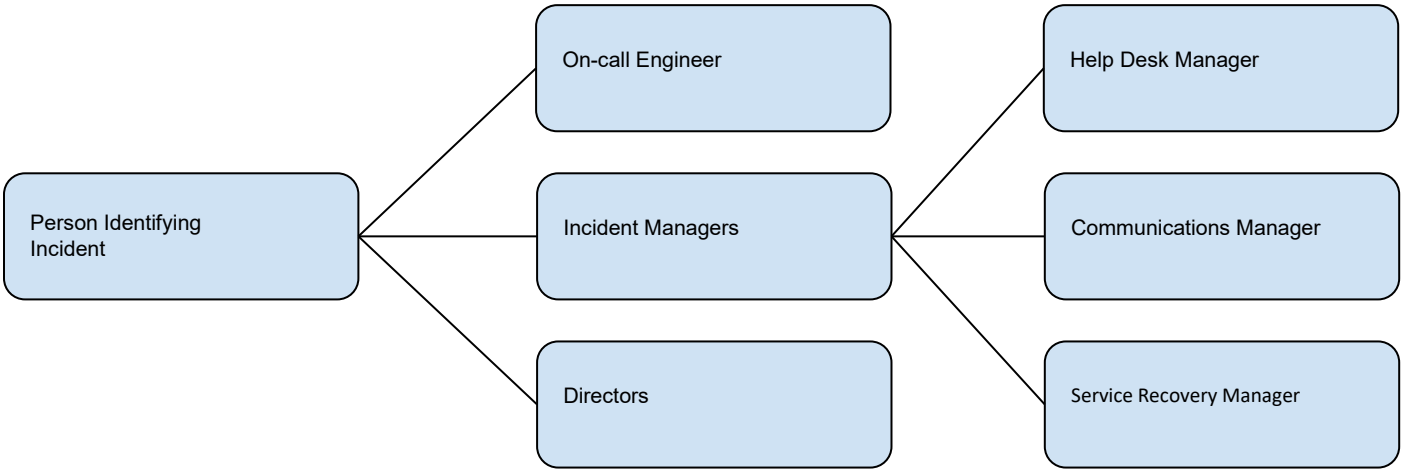
- Establish a structured plan that can be easily understood to help VTSL recover quickly and effectively from an unforeseen incident or emergency which interrupts normal business operations.
- Ensure that everyone understands their role in the DR plan
- Ensure that the plan can be tested (partially if necessary) on a regular basis
- Ensure that contingency arrangements are practical and cost effective
- Ensure that the impact on customers is minimised and that effective support is in place for 3rd parties
- Establish a framework for testing various DR scenarios

KEY CONTACT INFORMATION

FOR INTERNAL USE ONLY

Contact	Role	Phone	Mobile	email
Julia Gaifulina	Help Desk Manager	0207 0000000	0207 0000000	xxx@vtsl.net
Domas Poliakas	Service Recovery Manager	0207 0000000	0207 0000000	xxx@vtsl.net
Malik Ahmed	Service Recovery Manager	0207 0000000	0207 0000000	xxx@vtsl.net
Nicola White	Communication Manager	0207 0000000	0207 0000000	xxx@vtsl.net
David Walton	Incident Manager	0207 0000000	0207 0000000	xxx@vtsl.net
Robert Walton	Incident Manager	0207 0000000	0207 0000000	xxx@vtsl.net

COMMUNICATION SUMMARY



ALTERNATIVE CONTACTS

In the event of a designated Team leader not being available or contactable, responsibility for that area will be assumed by one of the other team leaders as required, or delegated to a senior member of that team.

DR PLAN SCOPE

For the purpose of this plan, a disaster is defined as loss or damage to all or part of the data centre, infrastructure or offices which would have a high business impact on VTSLs ability to provide services to customers.

Elements of DR may be invoked if an event raises risk exposure levels significantly before any actual loss of service. This will ensure that the appropriate levels of management are engaged and that the necessary resources are available to help mitigate risks. (E.g. warning of flood, power interruption etc.).

All VTSL sites are included in this scope, namely

- 4 and 5 Nichols Walk
- Interxion Data Centre
- Equinix Data Centre

Sites not under the direct control of VTSL may suffer an outage or disaster that could affect services. These sites have been included in the risk assessments and the risks mitigated where possible by having alternate locations (e.g. dual POPs for internet breakout, multi-homed internet transit and diverse fibre connections).

ASSETS INCLUDED

This plan is primarily concerned with restoring the operation of core VTSL services and does not include individual DR plans for customers and their equipment (collocated servers, WAN links etc.). Due to the nature of services supplied, restoration of VTSL systems on the same site will also cover customer equipment. Part of the management of a DR scenario involves liaison with customers.

TRIGGER EVENTS

Events at any VTSL site that would trigger one or more elements of DR or business continuity:

- Loss or degraded Connectivity across customer base
- Loss of Telephone Service
- Failure of core network equipment
- Loss of building access
- Failure of Data Centre Power, Cooling, or other disruption that affects VTSL services in a particular DC

INCIDENT MANAGEMENT RESPONSIBILITIES

Incident Managers have been appointed to contain the situation in which the BC/DR Plans are to be deployed. Several incident Managers have been identified to ensure support availability in the event that a singular individual cannot be contacted. Their remit is to minimize the impact on service, establish communications with other key personnel and to minimise the time in which normal operations can be resumed.

In the event of loss of service outside of normal business hours, these are the two individuals who would be the first to be notified. If a situation arose where neither appointed Incident Managers were able to attend the facility, then responsibility would be passed to the individual who appears in order of seniority on the corporate hierarchy chart.

The Incident Manager will:

- Assess the scope of the incident and root cause where possible
- Establish a line of communication to all DR Team Managers
- Inform Directors of the incident and provide regular updates of the situation (via the DR Team Coordinate all staff activities relating to the incident

DIFFERENCES BETWEEN DISASTER RECOVERY AND BUSINESS CONTINUITY

Business continuity encompasses all the necessary processes and procedures required to minimise interruption to the normal operation of the business. Disaster Recovery refers more specifically to the steps required to restore normal business functions following an incident.

DR TEAM RESPONSIBILITIES

The DR Teams have specific areas of responsibility in a DR scenario to handle communications, system recovery etc. Not all teams will be needed for all scenarios. The appropriate DR teams will be contacted by the Incident Manager as soon as possible following an incident.

Each individual team manager is responsible for mobilising as many team members as is necessary / possible to deal with the situation. Team members may work remotely from home or from another VTSL site during the incident depending on the situation. Some staff may be required onsite to aid recovery.

COMMUNICATIONS MANAGER

- Establish communication with Incident Manager to obtain information regarding MSO (Major Service Outage)
- Staff Updates
    - Alert Staff of MSO explaining the nature of the issue.
    - Provide a 2 - 3 sentence statement that can be used to communicate with customers
- System Updates
    - Updating of live status page on VTSL Website
    - MSO auto-attendant activated for VTSL inbound phone numbers
- Customer Updates
    - Email sent from Hubspot to Customer List
    - Email sent from Hubspot to Irish Customer List
- Repeat every 30-60 minutes or as directed by the incident manager with Updates

CONSIDERATIONS

Where possible, senior technical staff should be left to restore services as quickly as possible without dealing directly with customer issues.

Customers should be directed to a central information source (https://www.vtsl.net/live-status-update) to obtain updates from a consistent, reliable source.

Communications team members must ensure that they give a consistent view on events and avoid speculation or unauthorised comments.

CUSTOMER COMMUNICATION CHANNELS

VTSL has several methods of communicating directly with customers. In a DR scenario, one or more of these channels may be temporarily unavailable and alternatives should be used.

The preferred line of communication is via https://www.vtsl.net/live-status-update

Contact Type	Hosting Location	Phone Number	
General Number	VTSL	0207 078 3200	
Technical Support	Gamma	0333 405 0000	

The main office number is 0207 078 3200 which is operational during day time. This is hosted in VTSL network so we can make changes to it as and when required.

The 0333 405 0000 number is routed the same way as 0207 078 3200, however this is hosted within Gamma network rather than VTSL. This ensures that if there is a major problem with VTSL network, customers can still call 0333 405 0000 number as this number does not rely on VTSL network. We can make changes to the routing for 0333 405 0000 to point to anywhere, in cases of a major problem with VTSL network.

HELP DESK MANAGER

- Ensure that all communications channels are working
- Team Leader to create and share Google Document to help with the identification of the issue and collaboration of response
- Team Leader to communicate to team the messaging to be given to customers
- Remind team to 1) empathise, 2) apologise, and to take careful notes of everyone the speak to so that they can follow up

Help Desk team members must ensure that they give a consistent view on events and avoid speculation or unauthorised comments.

SERVICE RECOVERY MANAGER

- Re-establish connectivity and deal with re-routing of traffic. Liaison with network providers on faults
- Re-establish telephony services and liaise with Telco providers on faults
- Recovery of VTSL systems (Google Apps, Salesforce, BOSS etc.) and restoration of data from backups

ASSUMPTIONS

When developing the Disaster Recovery Plan the following assumptions have been made

- The plan has procedural effectiveness 24 hours a day 365 days a year
- That the deployment of the plan may be required outside of normal business hours
- That the Integrity of the service has been compromised to such an extent that VTSL are unable to meet their contractual obligations
- Normal redundancy / resilience precautions have failed to maintain services
- Two Incident Managers, holding senior roles within the company will manage the incident DR Teams will manage particular communication and technical roles.
- All further staff will have knowledge of the location of the Disaster Recovery Plan and the back-up copy to deputise or manage in the event of the two appointed Incident Managers being unable to coordinate activities through absence, injury or death
- Backups of the application software and data are intact and available
- Service and maintenance agreements with hardware and software suppliers are up to date and both active and passive incident containment machinery are operative
- The incident only affects one physical location (5NW, Interxion DC or Equinix DC)

RISK ANALYSIS

A number of risk assessments are performed as part of our ISO9001 and ISO27001 management systems. These detail risks that may include incidents that would lead to a full or partial invocation of the DR plan, and other more minor risks that may only affect some elements of service. This DR plan is part of the ISO9001 and ISO27001 management systems. Risk Assessments are stored in Google Docs.

To reduce the probability of a malicious attack upon VTSL's Core Network and to limit the impact on the operational capabilities of the organization through negligence or an act of god the following active precautions have been taken.

- Our Network topology and diverse data centres will allow re-routing of network traffic in the event of a site loss
- Core network equipment and servers are distributed / replicated between sites
- Network connectivity equipment is situated at Interxion and Equinix are served by physically diverse fibre connections
- VTSL's data center buildings are protected by a perimeter security fence and other security measures
- The premises are protected by numerous CCTV cameras with continuous digital recording
- The buildings are manned 24/7 by staff or security. Security firms have adequate backup personnel available
- Entry to the data centres is controlled through electronic swipe cards
- The buildings are protected by a fire alarm
- The data centres are protected by a redundant uninterruptible power supply unit (UPS) and a N+1 diesel generator bank
- Backup hardware is tested by the Technical Manager on a monthly basis.
- The network infrastructure (both physical and logical) has sufficient protection from attack

DATA CENTRES AND OFFICE FACILITIES

Interxion & Equinix Data Centres have sufficient free rack space to accommodate VTSL systems and hardware. General Internet transit is available from both sites, via diverse POPs.

Internet connectivity at both is independent.

Key network components are distributed between Interxion & Equinix where possible, providing extra resilience in VTSL's core infrastructure. Core network equipment is split between sites and servers are virtualized and distributed. Full High Availability (HA) is being implemented for VTSL systems. Backups are made across the WAN to each alternative site.

The VTSL office is non-critical to the business as all users are able to work remotely if they cannot get to the office for any reason. But in any case, we have three redundant internet connections in the office as well as capability of running over 4G connections.

DATA BACKUP PROCESS

All core network device configurations, VM images, databases and other business data are backed up on a regular basis. This information is transferred offsite to ensure physical diversity of data. The frequency of backups and retention depends on the nature of the information. This data includes hardware information, network documentation and network diagrams along with all configuration scripts for network devices appertaining to both customer networks (where appropriate) and to Node4 score network.

These backups are verified as part of the daily checks performed by the tech support engineers. Backup tapes, where used, are stored in a fire safe

Core network servers in both data centres are imaged regularly and the snapshots are backed up as part of this process.

Customer data may also be backed up and stored off site as part of a full or partially managed DR Service

STAGES OF BUSINESS CONTINUITY AND DISASTER RECOVERY

At all stages of the DR process, people should follow the advice of the expert in each affected area and not take unnecessary risks to attempt to restore service or save property or other assets.

1: NOTIFICATION / ACTIVATION STAGE

This stage includes those actions required by the Incident Manager to assess the situation and launch the Disaster Recovery Plan (or parts of it).

The Incident Manager will assess the scope of the incident. Consideration will be given to the impact the situation has on the effectiveness to maintain the continuity of services. This impact assessment will be based upon:

- Cause
- Who is affected?
- When services began to be disrupted
- Exact impact on customers
- What we are doing to solve the problem
- Expected resolution time
- Whether this is a VTSL only issue, or larger network issue
- Whether further interruptions to service are likely (and if it is better to delay restoration of service to avoid intermittent faults)

2: RECOVERY STAGE

The Incident Manager will delegate responsibility to the team of DR Managers to assess system issues in more detail and begin the restoration of services.

The recovery stage may involve purchasing of equipment to restore service. This should go through preferred suppliers and the normal purchasing process where possible. Insurance or warranty replacements should be used wherever these are available. Comms-care may not cover physical damage, only failure of components.

During the recovery stage, certain elements of the operation may be compromised, and risks must be reassessed on a rolling basis.

COMMUNICATIONS

Depending on the nature of the incident, normal communication routes may be disrupted. One of the priorities of the recovery stage is to re-establish both internal and external communications as quickly as possible. This will be the responsibility of the Communications Manager, but may involve technical support. The internal calling tree at the top of this document should be used to contact the relative staff members who will assist with the DR process. Staff members not directly involved in the DR process should be contacted and informed of the situation and given direction.

3: RECONSTRUCTION STAGE

The purpose of the Reconstruction Stage is to return the operation to that state prior to the incident occurring

4: DEBRIEF & AFTERMATH

Once the Incident Manager has declared that normal service has been restored he will:

- Debrief all department heads and address the following:
    - Problem clients that need attention
    - More information about the technical issue and the fix
    - Operational issues if there were any
    - Communications problems if there were any
- Produce full technical explanation of what happened to be put on file; Technical Lead to assist.
- Speak to Accounts regarding the details and timeline of a refund if applicable to this MSO.
- Write a statement to be emailed to the customer base the following day. Draft and send to Communications Lead. If refunds will be issued make sure to include this information.
- Ensure department heads brief their staff on the exact language to use with customers, including “Expected Questions” and answers. Communications Lead to write up in an internal email that can be used for reference.
- Update Technical CAPA log

CHANGE HISTORY

Issue	Issue Date	Additions/Alterations	Initials
1.0	14/01/2020		DW