



Disaster Recovery Plan (Public)

Published 2021

Contents

Statement of Intent	3
Policy Statement	4
Objectives	4
Activation of Emergency Response.....	4
Disaster Recovery Team.....	5
Financial Assessment	5
Legal Assessment	5
DRP Exercising.....	5
Appendix A – Disaster Recovery Plan Templates.....	6
Client application access and distribution	6
ClickOnce.....	6
Server-side Components.....	7
Dragon Medical Server.....	7
Nuance Management Centre.....	8
Intermediary Components.....	9
Databases.....	9
File Storage.....	10
Load Balancing and Application Gateways	10
IP Address Management.....	11
Domain Resources	11
SSL/TLS Certificates	12

Statement of Intent

This plan may be used to identify the assessed risks and recovery procedures involved with the following solutions:

- Dragon Professional Anywhere Cloud
- Dragon Legal Anywhere Cloud
- Dragon Medical Direct Cloud
- Dragon Anywhere Mobile

Individual components included in this plan cover:

- Client application access and distribution including
 - ClickOnce
- Server-side components including
 - Dragon Medical Server
 - Nuance Management Centre
- Intermediary components including
 - Databases
 - File storage
 - Load Balancing and Application Gateways
 - IP Address Management
 - Domain Resources
 - SSL/TLS Certificates

Procedures Included in this plan cover:

- Risk Assessment per component
- Preventative measures
- Notification measures
- Disaster Recovery measures

In the event of an actual emergency situation, modifications to this document may be made to ensure physical safety of people, systems, and data.

Please note this document is a shortened version of ORdigiNAL's official recovery procedure, where the information contained within this document has been deemed suitable for the public domain. You may assume that ORdigiNALs full recovery plan details more extensive information pertaining to the necessary roles and methods used to implement specific recoveries of any component listed and others not listed.

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 that 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 own respective roles.
- The disaster recovery plan is to be kept up to date to take into account changing circumstances.

Objectives

The principal objective of the disaster recovery program is to develop, test and document a well-structured and easily understood plan which will help the company recover as quickly and effectively as possible from an unforeseen disaster or emergency which interrupts information systems and business operations. Additional objectives include the following:

- The need to ensure that all employees fully understand their duties in implementing such a plan
- The need to ensure that operational policies are adhered to within all planned activities
- The need to ensure that proposed contingency arrangements are cost-effective
- The need to consider implications on other company sites
- Disaster recovery capabilities as applicable to key customers, vendors and others

Activation of Emergency Response

When an incident occurs the Emergency Response Team (ERT) must be activated. The ERT will then decide the extent to which the DRP must be invoked. All employees must be issued a Quick Reference card containing ERT contact details to be used in the event of a disaster. Responsibilities of the ERT are to:

- Respond immediately to a potential disaster
- Assess the extent of the disaster and its impact on the business, data centre, etc.
- Decide which elements of the DR Plan should be activated
- Establish and manage disaster recovery team to maintain vital services and return to normal operation
- Ensure employees are notified and allocate responsibilities and activities as required.

Disaster Recovery Team

The team will be contacted and assembled by the ERT. The team's responsibilities include:

- Establish facilities for an emergency level of service within 4 business hours
- Restore key services within 8 business hours of the incident
- Recover to business as usual within 8 to 48 hours after the incident
- Coordinate activities with disaster recovery team, first responders, etc.
- Report to the emergency response team

Financial Assessment

The emergency response team shall prepare an initial assessment of the impact of the incident on the financial affairs of the company. The assessment should include:

- Loss of financial documents
- Loss of revenue
- Theft of tangible / intangible assets etc.
- Loss of reputation

Legal Assessment

The company legal department and ERT will jointly review the aftermath of the incident and decide whether there may be legal actions resulting from the event; in particular, the possibility of claims by or against the company for regulatory violations, etc

DRP Exercising

Disaster recovery plan exercises are an essential part of the plan development process. In a DRP exercise no one passes or fails; everyone who participates learns from exercises – what needs to be improved, and how the improvements can be implemented. Plan exercising ensures that emergency teams are familiar with their assignments and, more importantly, are confident in their capabilities.

Successful DR plans launch into action smoothly and effectively when they are needed. This will only happen if everyone with a role to play in the plan has rehearsed the role one or more times. Simulating the circumstances within which it has to work and seeing what happens should also validate the plan.

Appendix A – Disaster Recovery Plan Templates

Client application access and distribution

ClickOnce

- Assessed Risks
 - DDoS
 - Availability Uptime
 - Application Link Availability
 - Failover
 - Compute
 - Storage
- Preventative Measures Implemented
 - Web Application Firewall / Gateway
 - Gateway distributed to 3 datacentres
 - Multiple Compute Resources
 - Compute Resource Monitoring and automatic scaling
 - Automatic Compute Failover
 - Storage Backup Procedure
 - Automatic Alert for downtime
 - Known and reliable global link provider used (WeTransfer)
 - Other transfer methods available if required
 - Download kept to a small package for ease of transfer
 - Application Installation is not reliant on global link provider and can be provided by any other means
 - Non-sensitive data access given to IT staff for data recovery access if required.
- Notification Measures
 - Downtime Alert for
 - dragonprofessionalanywhere.ordiginal.com
 - dragonlegalanywhere.ordiginal.com
 - dragonmedicaldirect.ordiginal.com
 - Alert ORdigiNAL Cloud Administrators/Architects
 - Alert ORdigiNAL Support Manager
 - Alert any other ORdigiNAL key personnel
- Disaster Recovery measures
 - Designated Cloud Administrator to initiate recovery plan
 - Recovery Options Include:
 - Automatic failover
 - Manual compute recovery via disk snapshots
 - Storage recovery via
 - Backups
 - Manual intervention

- An Incident report and recovery assessment to be completed by designated Cloud Administrator, and Helpdesk to be notified to facilitate end-user support

Server-side Components

Dragon Medical Server

- Assessed Risks
 - DDoS
 - Availability Uptime
 - Failover
 - Compute
 - Storage
 - Updates
 - Resource Utilisation
- Preventative Measures Implemented
 - Web Application Firewall / Gateway
 - Gateway distributed to 3 datacentres
 - Multiple Compute Resources
 - Primary Compute
 - Datacentre 1
 - Secondary Compute
 - Datacentre 2
 - Automatic Compute Failover
 - Compute Resource Monitoring and automatic scaling
 - Storage Backup Procedure
 - Automatic Alert for downtime
 - Automatic update schedule
 - Primary Update Schedule
 - Secondary Update Schedule
- Notification Measures
 - Downtime Alert for
 - sas-uk.ordiginal.com
 - sas-au.ordiginal.com
 - sas-eu.ordiginal.com
 - sas-eu1.ordiginal.com
 - Alert ORdigiNAL Cloud Administrators/Architects
 - Alert ORdigiNAL Support Manager
 - Alert any other ORdigiNAL key personnel
- Disaster Recovery measures
 - Designated Cloud Administrator to initiate recovery plan
 - Recovery Options Include:
 - Automatic failover

- Manual compute recovery via disk snapshots
- Storage recovery via
 - Backups
 - Manual intervention
- An Incident report and recovery assessment to be completed by designated Cloud Administrator, and Helpdesk to be notified to facilitate end-user support

Nuance Management Centre

- Assessed Risks
 - DDoS
 - Availability Uptime
 - Failover
 - Compute
 - Storage
 - Updates
 - Resource Utilisation
- Preventative Measures Implemented
 - Web Application Firewall / Gateway
 - Multiple Compute Resources
 - Primary Compute
 - Datacentre 1
 - Secondary Compute
 - Datacentre 2
 - Automatic Compute Failover
 - Storage Backup Procedure
 - Automatic Alert for downtime
 - Automatic update schedule
 - Primary Update Schedule
 - Secondary Update Schedule
- Notification Measures
 - Downtime Alert for
 - nms-uk.ordiginal.com
 - nms-au.ordiginal.com
 - nms-eu.ordiginal.com
 - nms-eu1.ordiginal.com
 - Alert ORDigiNAL Cloud Administrators/Architects
 - Alert ORDigiNAL Support Manager
 - Alert any other ORDigiNAL key personnel
- Disaster Recovery measures
 - Designated Cloud Administrator to initiate recovery plan
 - Recovery Options Include:
 - Automatic failover
 - Manual compute recovery via disk snapshots
 - Storage recovery via

- Backups
- Manual intervention
- An Incident report and recovery assessment to be completed by designated Cloud Administrator, and Helpdesk to be notified to facilitate end-user support

Intermediary Components

Databases

- Assessed Risks
 - DDoS
 - Availability Uptime
 - Failover
 - Compute
 - Storage
 - Updates
 - Resource Utilisation
 - SQL Injection
- Preventative Measures Implemented
 - No Public access
 - Whitelisted VNet only
 - Private-Link communication measures
 - Automatic Compute Failover
 - Storage Backup Procedure
 - Automatic Alert for downtime
 - Daily security assessments
 - PaaS service mitigating update requirements
 - Database resource monitoring and automatic scaling
- Notification Measures
 - Resource Utilisation Alert
 - Alert ORDigiNAL Cloud Administrators/Architects
 - Alert ORDigiNAL Support Manager
 - Alert any other ORDigiNAL key personnel
- Disaster Recovery measures
 - Designated Cloud Administrator to initiate recovery plan
 - Recovery Options Include:
 - Automatic failover
 - Manual compute recovery via disk snapshots
 - Storage recovery via
 - Backups
 - Manual intervention
- An Incident report and recovery assessment to be completed by designated Cloud Administrator, and Helpdesk to be notified to facilitate end-user support

File Storage

- Assessed Risks
 - Data Loss
 - Data Corruption
 - Data Protection
- Preventative Measures Implemented
 - No Public access
 - Whitelisted VNet only
 - Private-Link communication measures
 - Storage Backup Procedure
 - Storage Encryption
 - Automatic Alert for downtime
 - Automatic Alert and scaling for resource availability
 - Daily security assessments
 - PaaS service mitigating update requirements
- Notification Measures
 - Data resource limit reached
 - Data breach
 - Alert ORdigiNAL Cloud Administrators/Architects
 - Alert ORdigiNAL Support Manager
 - Alert any other ORdigiNAL key personnel
- Disaster Recovery measures
 - Designated Cloud Administrator to initiate recovery plan
 - Recovery Options Include:
 - Storage recovery via
 - Backups
 - Manual intervention
- An Incident report and recovery assessment to be completed by designated Cloud Administrator, and Helpdesk to be notified to facilitate end-user support

Load Balancing and Application Gateways

- Assessed Risks
 - DDos
 - Availability
 - Failover
 - Security
- Preventative Measures Implemented
 - WAF
 - Path rules
 - SSL Encryption
 - Multi-Datacentre spread

- Automatic Alert for NMS Pool downtime
 - Automatic Alert for DMS Pool and downtime
 - Automatic Alert and scaling for resource availability
 - Daily security assessments
 - PaaS service mitigating update requirements
- Notification Measures
 - Activity and resource alerts
 - Alert ORDigiNAL Cloud Administrators/Architects
 - Alert ORDigiNAL Support Manager
 - Alert any other ORDigiNAL key personnel
- Disaster Recovery measures
 - Designated Cloud Administrator to initiate recovery plan
 - Recovery Options Include:
 - Gateway recovery via
 - Automatic Failover to other Datacentres
 - Manual Intervention via Gateway templates

An Incident report and recovery assessment to be completed by designated Cloud Administrator, and Helpdesk to be notified to facilitate end-user support

IP Address Management

- Assessed Risks
 - IP Duplication
- Preventative Measures Implemented
 - IP Record
 - IP Policy
- Notification Measures
 - Not required
 - Policy blocks IP Duplication
- Disaster Recovery measures
 - Designated Cloud Administrator to initiate recovery plan
 - Recovery Options Include:
 - Re-designate IP affected IP address(s)

An Incident report and recovery assessment to be completed by designated Cloud Administrator, and Helpdesk to be notified to facilitate end-user support

Domain Resources

- Assessed Risks
 - Domain Unavailable
 - Domain Server Uptime

- Domain Updates and Security
 - Domain Policy Failures
- Preventative Measures Implemented
 - PaaS Domain Service
 - Automatic Domain Failover
 - Automatic Domain Updates
 - No public access
 - Domain outage mitigation via software features
- Notification Measures
 - PaaS notification
 - Alert ORDigiNAL Cloud Administrators/Architects
 - Alert ORDigiNAL Support Manager
 - Alert any other ORDigiNAL key personnel
- Disaster Recovery measures
 - Designated Cloud Administrator to initiate recovery plan
 - Recovery Options Include:
 - PaaS provider support
 - Manual Domain access and policy management

An Incident report and recovery assessment to be completed by designated Cloud Administrator, and Helpdesk to be notified to facilitate end-user support

SSL/TLS Certificates

- Assessed Risks
 - Certificate Expiration
 - Unauthorized Certificate Access
- Preventative Measures Implemented
 - Renewal plan
 - Certificate vault encryption
 - Certificate access restricted to key ORDigiNAL personnel
- Notification Measures
 - Renewal plan notification
 - Alert ORDigiNAL Cloud Administrators/Architects
 - Alert ORDigiNAL Support Manager
 - Alert any other ORDigiNAL key personnel
- Disaster Recovery measures
 - Designated Cloud Administrator to initiate recovery plan
 - Recovery Options Include:
 - Certificate provider support

An Incident report and recovery assessment to be completed by designated Cloud Administrator, and Helpdesk to be notified to facilitate end-user support