DISASTER RECOVERY PROCEDURES

1. Overview

Disaster recovery and business continuity are important functions for Qumu. Both the management team and support & services leaders have oversight of this and ensure that DR/ BCP plans are regularly reviewed and tested annually. A governance structure is in place to ensure that policies and procedures are up to date. All appropriate team members are made aware of policies and procedures and any updates relating to these policies. This document outlines the disaster recovery procedures for the systems and data relating to the Qumu Cloud Platform in two scenarios (partial outage in a datacenter, loss of a datacenter). Unless otherwise defined below, all capitalised terms shall have the meaning attributed to them in the Agreement for the Provision of the Qumu Cloud Platform available at **www.qumu.com/legal.**

2. Purpose

This document is designed to ensure appropriate disaster recovery procedures are in place to protect Software and Client Data in the Qumu Cloud Platform in order to limit data loss and to facilitate the recovery of Client Data in the event of a service failure or disaster.

3. Scope

These procedures apply to all equipment and data owned and operated by Qumu and the services provided to Qumu by any 3rd party hosting providers.

4. Disaster Recovery Scenarios

4.1. Qumu has worked closely with its third-party hosting provider to ensure that a set of disaster recovery scenarios and responses have been clearly defined and documented.

4.2. The Qumu Cloud Platform is maintained on servers that are hosted by its 3rd party hosting partner with over 40 data centers in 15 countries and growing. Each datacenter includes stringent security measures such as entry gates, 24x7 guard, CCTV and restricted access control.

4.3. All systems used for the Qumu Cloud hosted platform are monitored both by Qumu Cloud Services and by our datacenter provider. All outages and incidents are reported immediately to Qumu and are tracked, addressed in a timely manner.

4.4. In addition, Qumu has a documented data Backup Policy that ensures the following parts of the Cloud Platform are backed up: server and application infrastructure, any relevant databases, media assets, and Qumu application code.

4.5. The following disaster recovery procedures describe how the Qumu Cloud Platform is recovered in the event of a disaster. Roles and responsibilities are clearly defined.

Scenario 1: Major – Outage in the Primary Datacenter

In this scenario, there is a partial outage in the primary datacenter. A partial outage is the loss of all nodes of an application component in a highly available (HA) configuration.

Task	Team
Notify Clients of the issue and provide timely subsequent updates	Qumu Support
Devise a plan to restore affected application component in the same datacentre, within the identified RTO and RPO	Qumu Cloud Services, 3rd party hosting provider
Restore application component	Qumu Cloud Services, 3rd party hosting provider
Notify Client of issue resolution and application availability.	Qumu Support

Expected Impact	
Affected area	Qumu Support
Recovery Time Objective (“RTO”)	4 hours
Recovery Point Objective (“RPO”)	4 hours

Scenario 2: Critical – Total Loss of Datacenter

In this scenario there is a complete loss of the primary datacentre due to a catastrophic event.

Task	Team
Notify Clients of the issue and provide timely subsequent updates	Qumu Support
Devise a plan to restore application infrastructure in alternate geographically-separated datacenter, within the same continental region (APAC, EMEA, NA), within the identified RTO and RPO	Qumu Cloud Services, 3rd party hosting provider
Restore application	Qumu Cloud Services, 3rd party hosting provider
Notify Client of application availability	Qumu Support

Expected Impact	
Affected area	Application Infrastructure
Recovery Time Objective (“RTO”)	1 week
Recovery Point Objective (“RPO”)	4 hours