QUMU

Backup Policy

1. Overview

This document defines the Backup policy for systems and data relating to Qumu Cloud. These include but are not limited to the software components and customer data that comprise Qumu Cloud. Parts of the application that are expected to be backed up include server and application infrastructure, databases, media assets, and Qumu application code.

2. Purpose

This policy describes the strategy used by Qumu Cloud Services to protect software and customer data in Qumu Cloud to ensure that it can be recovered in the event of an equipment failure, accidental or intentional destruction of data, or disaster.

3. Scope

This policy applies to all data, media assets, application configurations, and databases operated by Qumu Cloud Services and 3rd party hosting provider services used by Qumu Cloud Services.

4. Definitions

"**Qumu Cloud**" – A software application operated and maintained by Qumu on behalf of customers subscribed by contract to Qumu Cloud.

"**Backup**" - block level replication and retention of files and data to offsite mass-storage media.

"**Archive**" - The saving of old and/or unused files onto offsite mass-storage media for the purpose of either releasing onsite storage space or for specific compliance-related data retention requirements.

"**Restore**" - The process of bringing back application data from offsite backup and making it available for real time processing.

"**Recovery Time Objective ("RTO")**" – the duration of time within which a service is targeted to be restored to full functionality following a major or critial disruption of the service. The RTO is 4 hours for a major distruption and 1 week for a critical distruption.

"**Recovery Point Objective ("RPO")**" – The maximum time period for which loss of data associated with a service can be tolerated. The RPO for Qumu Cloud solutions is 4 hours.

5. Approach

Incremental snapshots of file systems and databases as applicable.

6. Storage

All data backups are transferred to secure ISO27001-certified offsite datacenters geographically separated from the primary datacenter, but within the same geographical region in compliance with EU Model Clauses.

If data is removed from the application, this will be reflected in subsequent snapshots. Incremental snapshots will be retained for 30 days, after which the oldest snapshot will be destroyed. Maximum period of time deleted data will exist within the backup infrastructure is 30 days.

7. Sanitation of Media Devices

In the event that a piece of equipment needs to be relocated or retired, its Hard Disk Drives will be removed from the equipment and all data is erased using Department of Defense (DoD) 5220.22- m standards.

In the event that a Hard Disk Drive needs to be relocated for any reason, all data is erased using Department of Defense (DoD) 5220.22-m standards.

In the event a disk fails and cannot be securely erased, or where a Hard Disk Drive has reached the end of its useful life, it will be destoroyed, certification of destruction of the drive can be provided to the customer upon request.

8. Recovery from Backup

The ability to restore data from backups shall be tested at least once a year.