Kyocera Protect Service Description

Prepared by KYOCERA Document Solutions

Contents

1 Service Overview

This document is provided to define the products and services to be delivered to [Company] within the Kyocera Protect delivery.

Kyocera protect is provisioned based on two service elements:

1. SaaS Backup Solution
2. Service Management

2 SaaS Backup

The following defines the selected levels of service to be provided by Kyocera to support the SaaS Backup requirements identified by [Company].

2.1 Backup Solution Overview

Backup tasks are applied to [Company] tenancy domain to capture data retained within the tenancy for all licensed consumers. Backup licenses are subsequently aligned to the user volume of consumption within the tenancy.

Heading	Description
Services Covered	Office 365's Exchange Online, Calendar, Contacts, all OneDrive file types, OneNote data in Sharepoint and OneDrive Document libraries, Sharepoint Sites, Custom Site Collections, Team Sites
Automated Backup	Automated daily point-in-time backups begin after initial ingest
Backup Frequency	3X Daily at 8 hour intervals
On-Demand Backup	Able to initiate anytime on service level; will not interrupt regularly scheduled backups
Automatic New User Detection	Able to add all current users and back up new users automatically (Nightly job detects status of services in Office 365 environment)
Automated Archive	Nightly job detects status of services in Office 365 environment, then archives those services that are archived in Office 365
Office 365 Licenses Supported	E1, E3, E5, Exchange Only 1 and 2, Sharepoint only 1 and 2, Business Essentials, Business Premium, EDU, GOV, NPO
Storage Locations	Stored in private cloud, with options for storage located in US, EMEA, AUS, CAN; built-in redundancy; geo-replicated within geographical region; ZFS file storage; SOC 2 Type II audited; built-in encryption
Restore Function	To original user or alternative user in original file format
Restore Granularity	File level, folder level with nested hierarchy intact
Export Format	MBOX for Mail, .ical for Calendar, VCF for Contacts, Original MS format for OneDrive
Search	Search across multiple users; metadata search
Administrative Roles	Super Admin; unlimited General Admins
Audit Logging	Available within the Administrative UI
Data Retention	Configurable; set to 1 year by default

2.2 Security Overview

The Cloud to Cloud Backup Solution has completed a SOC 2 Type II audit against the AICPA Service Organization Control Trust Services Principles, Criteria, and Illustrations for Security, Availability and Confidentiality. The audit firm concluded that controls were suitably designed and operating effectively to provide reasonable assurance that control objectives would be achieved. SaaS Protection data is also stored in leading co-location facilities compliant with HIPAA.

2.2.1 Encryption

When it comes to encryption, Kyocera Protect deploys the highest level of security for customer data. At rest, data is encrypted using industry standard 256-bit (AES-256) encryption. All data written for the user is encrypted prior to storage. In transit, Kyocera Protect employs TLS 1.2 encryption.

2.2.2 OAuth Token

When setting up [Company] using Kyocera Protect, the authorization of the backup is captured through the app's UI and uses Oauth tokens, so there is no need to store sensitive user credentials in backup database. The app's connection with Office 365 will not be lost with admin password changes, as the Oauth token will maintain the authorization with Kyocera Protect.

2.3 Retention Policy

Standard retention policies apply within the SaaS Backup solution.

Retention determines how and/or for how long data backups for a SaaS Protection Service Subscription are retained in the Cloud backup data repository.

Following the successful completion of an initial full backup, all subsequent backups are "snapshots" of a point in time and capture only changes made since the previous backup. Following the full backup, backup snapshots are retained in accordance with the pre-set schedule in accordance with [Company] SaaS Protection Service Plan, described below, and will be retained for each active Service Subscription for which payment is current.

If a Service Subscription terminates, Kyocera reserves the right to securely delete, after 60 days, the backed-up data retained in the Cloud backup data repository associated with your Service Subscription. It is [Company]'s responsibility, on or before this period, at [Company] expense, to export a copy of the data if you would like a copy of the backed up data in the Cloud data repository associated with your Service Subscription for a SaaS Protection Product.

2.3.1 Infinite Cloud Retention

With the Infinite Cloud Retention service plan backup snapshots are retained for an indefinite period of time for as long as the Infinite Cloud Retention Service Plan Service Subscription is current. Automatic consolidation of backup snapshots is applied on a rolling basis as shown below.

The following schedule for consolidating backup snapshots are applied within the data repository

Pruning of Incremental Backups	Period
Intra Dailies	30 Days
Dailies	90 Days
Weeklies	365 Days

2.4 Recovery Point Objectives (RPO)

Recovery point objectives refer to [Company] loss tolerance: the amount of data that can be lost before significant harm to the business occurs. The objective is expressed as a time measurement from the loss event to the most recent preceding backup.

If backup is completed in regularly scheduled 24-hour increments, then in the worst-case scenario you will lose 24 hours' worth of data. Kyocera Protect backup is completed every 8 hours by default. Additional backup period options are available to meet requirements of RPO.

- ➢ Standard Applied RPO – 8 Hours

2.5 Recovery Time Objective (RTO)

RTO refers to how much time an application can be down without [Company] suffering significant damage to the business. Generally certain applications can be down for days without significant consequences. Whereas some high priority applications can only be down for a limited time period without incurring employee irritation, customer anger and lost business.

RTO is not simply the duration of time between loss and recovery. The objective also accounts for the steps IT must take to restore the application and its data. If IT has invested in failover services for high priority applications, then they can safely express RTO in seconds. (IT must still restore the on-premises environment. But since the application is processing in the cloud, IT can take the time it needs.)

Microsoft 365 and Google G-Suite operate a 99.9% uptime SLA, which allows for up to 8 hours 45 minutes and 56 seconds offline time per annum. Kyocera Protect SLA is only applied while the service is available to facilitate a recovery of data.

Data recovery requests are actioned during Kyocera Core Hours, Monday to Friday 08:30 to 17:30 excluding bank holidays, requests made outside of these working hours are actioned the next working day. Alternative options are available for service provision, however these require dedicated commercial considerations, where a requirement is identified to provide service outside of Core Hours on a contracted basis notification should be given to the Account Manager.

Applied RTO's are as follows for completion of recovery from the time the request is received or the start of the next working day.

- **Tier-1:** Mission-critical applications 2 Hours
- **Tier-2:** Business-critical applications 4 hours
- **Tier-3:** Non-critical applications 8 Hours
- **Tier**-4: Individual file recovery 24 Hours

3 Service Management

Kyocera Protect is provided to [Company] as a fully managed implemented backup solution. This includes Kyocera Management functions within the service, which are available in three formats depending on the individual requirements of [Company].

Bundle 1	Bundle 2	Bundle 3
• License Management • Reporting • T&M Restore Support	• License Management • Reporting • Security • Restore Test 1 per Month • Retention Catalogue • 5 Restores per Month	• License Management • Reporting • Security • Restore Tests 3 per Month • Retention Catalogue • Unlimited restores per Month

[Company] have identified a preference for service provisioning of Kyocera Protect utilising the chosen Bundle. This scheduled service provision is flexible and can be amended on request to meet the business requirements of [Company].

3.1 License Management

The licensing applied to Kyocera Protect is aligned to the volume of users consuming the service on a per user per month basis. The service provides Automatic New User Detection service to ensure all user data is captured within the backup service provided.

Licensing is applied as new users are identified and [Company] are informed of any license changes through the service reporting process. Where [Company] identify changes in applied end user licensing, such as leavers, it is the responsibility of [Company] to notify Kyocera of these changes in writing, so backup licensing is aligned.

3.2 Reporting

Reporting of the services is provided by the account management team on an agreed and scheduled basis. The baseline of reporting is a service health and verification report provided by Kyocera Monitoring Platform; additional elements of the report are dependent on the service bundle provided.

3.2.1 Bundle 1

Bundle 1 reporting includes service health and verification. This includes the following components.

1. Identification of successful backups completed
2. Backup failure notification and rectification report
3. Changes to aligned licensing during the reporting period
4. Requests to complete restores, including requestor details

3.2.2 Bundle 2

Bundle 2 reporting incorporates all the report elements of Bundle 1 but with the addition of the following.

1. Single restore test verification and validation
2. Retention catalogue report

3.2.3 Bundle 3

Bundle 3 reporting incorporates all the report elements of Bundle 1 but with the addition of the following.

1. Multiple test verification and validation
2. Retention catalogue report

3.3 Security

In addition to the security aspects identified in Chapter 2.2, [Comments] will benefit from knowing that as a Managed Service provided by Kyocera, all interaction between the service and our operations centre is governed by our compliance requirements within ISO27001, Cyber Essentials and Cyber Essentials+ accreditations.

This means that all interaction will adhere to security policies relating to access controls and password security.

3.4 Test Restores

Test restores are completed monthly within Bundle 2 and Bundle 3 of the available services.

Every test restore is completed on a random piece of data from within the backup set. Restores are completed to a segregated and sandboxed environment to validate the restore capability of the service, without the potential to disrupt the operation live data stores.

On successful completion of a test restore, the completion details are captured for reporting purposes and the data restored is deleted in accordance with ISO27001 standard governance and best practice.

3.5 Retention Catalogue

The retention period, defined by [Company] is managed by Kyocera through the retention Catalogue to ensure backup data does not grow indefinitely without governance, leading to unsolicited data versions and inefficient data sprawl within the backup repository.

Retained backups are pruned in line with the identified retention policy. An example of this pruning being with a 12-month retention policy, backups are completed for 12 months, as month 13 is completed and added to the Catalogue, Kyocera manage the pruning of Month 1.

With Catalogue Management and data pruning, any backup data is removed in accordance with data deletion policies as defined within ISO27001 best practice.

3.6 Data Restores

Data restores are completed on request by Kyocera Service Centre. All requests for restores are processed during Standard Core Hours as identified above.

A restore request is defined by Kyocera as a single instance request, regardless of data volume within that request. Individual requests must be made for a single data source from a single recovery point.

3.6.1 Single Data Source

A single data source which would constitute a single restore is;

- A named user space
- A mailbox
- A file
- A folder
- A database object
- A service datastore

3.6.2 Single Recovery Point

A single recovery point is required for a restore completion. A request to recovery a Single Data Source from multiple recovery points is identified as multiple recovery requests.

3.6.3 Ad-Hoc Data Restores

Ad-Hoc data restores are completed on a Time and Materials basis for each restore completed. These include all restore actions completed outside of the Agreed Service Levels.

All Ad-Hoc restores will be completed and billed separately on a retrospective basis at a rate of £22.90 per instance request.

3.7.3 Power by Datto, Inc.

4 Document History

Once this document has been approved and signed by the Sponsor and the Project Board, any further changes must be managed by the Change Control process.

Authors

Creator	Date	Comments
KYOCERA	08/09/2020	Initial Document Creation

Contact Details

Method	Details	Method	Details
Telephone	+44 1189 311 500	Fax	N/A
Email	info@duk.kyocea.com	Address	Eldon Court, 75-77 London Road, Reading, Berkshire RG1 5BS

Revision History

Revision date	Version/Revision	Summary of Changes
08/09/2020	0.1	Final

Disclaimer

Whilst every precaution has been taken in the preparation of this document, no responsibility is assumed for errors or omissions nor is any liability assumed for loss or damage resulting from the use of the information it contains, to the extent such error or omission is a result of any information, data or documents provided to KYOCERA by the Customer and relied on by KYOCERA in the preparation of this document.

Kyocera Document Solutions has championed innovative technology since 1934. We enable our customers to turn information into knowledge, excel at learning and surpass others. With professional expertise and a culture of empathetic partnership, we help organisations put knowledge to work to drive change.

KYOCERA Document Solutions (U.K.) Limited
Eldon Court
75-77 London Road
Reading
Berkshire RG1 5BS

Tel: 03330 151 855

Fax: 0118 931 1108

e: info@duk.kyocera.com

www.kyoceradocumentsolutions.co.uk