SERVICE LEVEL AGREEMENT

1. OVERVIEW

Tricent Security Group A/S (Tricent) is delivering a data sharing compliance solution that allows Google Workspace and Microsoft 365 users and admins to view and act on file shares to align with data compliance demands and help prevent data leakage.

The solutions will be named Tricent for Google Workspace or Tricent for Microsoft 365 for the purposes of this document.

This document details the scope of the Tricent for Google Workspace and Tricent for Microsoft 365 service delivery related to the data access, operational specifics, and general support of the tool in relation to the respective responsibilities of Tricent and the customer parties.

The document is considered accurate at the time of writing but its content may evolve over time as requirements and usage of the Tricent for Google Workspace and Tricent for Microsoft 365 software solution changes.

2. SYSTEM DESIGN

The Tricent for Google Workspace and Tricent for Microsoft 365 software solutions consist of 5 high-level components interacting to provide the system functionality:

Authentication layer

The users and admins wanting to access the Tricent for Google Workspace and Tricent for Microsoft 365 software solution will authenticate via SSO (Single Sign-On) via the Oauth2 protocol granting the solutions access and data permissions in the Tricent for Google Workspace and Tricent for Microsoft 365 solution based on their existing session access in Google Workspace or Microsoft 365 platforms.

User Interaction layer

Once a user is authenticated via SSO in the Tricent for Google Workspace and Tricent for Microsoft 365 solutions they will be presented with a web frontend granting them access to viewing and managing their file sharing. Admins will have access to manage settings and files domain-wide as well as see actions taken by users and/or the automated scheduler (see below).

Automated scheduler

The Tricent for Google Workspace and Tricent for Microsoft 365 software solutions each contain a scheduler system that is responsible for notifying users when they are required to review their file sharing. The scheduler is also able to act on users' file sharings and clean these up if the user has not acted within a predefined configurable time limit.

Email layer

The Tricent for Google Workspace and Tricent for Microsoft 365 solution uses email as its primary end-user communication format when sending out file-sharing review call-to-action messages. The emails are routed via an external email service provider (ESP) to the end-users mailbox. Emails are tracked in the ESP’s backend to ensure debugging traceability and audit trails are always available no matter what the reason is. The call to action emails contain no sensitive information and all links that lead back to the application are authenticated to ensure proper authorizations and

identifications are in place when accessing the company's data.

Logging backend

The Tricent for Google Workspace and Tricent for Microsoft 365 software solutions carry out the main part of its functionality via upstream calls to Google's and Microsoft APIs. All user and admin access and API actions are logged in the data backend and kept for the duration of the service.

3. DATA ACCESS

The Tricent for Google Workspace and Tricent for Microsoft 365 solutions will process user and authentication data from the customer's Google Workspace or Microsoft 365 using Google's or Microsoft's API backends as part of its service delivery.

The data involved in this process are retrieved over an encrypted HTTPS connection to Google's and Microsoft API backends and stored encrypted on disk in the Tricent for Google Workspace infrastructure in GCP or Tricent for Microsoft 365 infrastructure in Azure for the duration of the data lifecycle.

The data involved in the Tricent for Google Workspace or Tricent for Microsoft 365 software transactions are as follows:

1. User email address
2. User full name
3. Drive filename
4. Drive file share data permission list
5. Shared or Team Drive names
6. Teams Channel names
7. Domain names
8. Sharing message
9. Document ID

Regular end-user accounts will have access to their own Drive data and Shared / Team Drives and Teams Channels for which they are designated as Content Manager/Owner. Admin accounts will have access to domain-wide settings and configuration data in order to perform their administrative duties as well as data overviews over Teams and Shared Drives.

A technical service account needed for the automated schedulers functions will have domain-wide delegated data access to the customer's Google Workspace and Microsoft 365 tenants via the respective Google and Microsoft API backends.
All actions carried out by users, admins, and the automated scheduler in the Tricent for Google Workspace and Tricent for Microsoft 365 software solution are logged and kept for the duration of the service lifetime.

Tricent monitors security events continuously on the Tricent for Google Workspace and Tricent for Microsoft 365 platforms. The security monitor ensures the integrity of the Tricent for Google Workspace and Tricent for Microsoft 365 platforms - this happens via a dedicated service account without the need for human intervention or customer data access.

In special security and software patching scenarios Tricent uses full administrative access for a defined period of time to the platforms and as such also customer data - all access and actions are logged.

In debugging and troubleshooting scenarios Tricent needs full application access to the platforms and may also see customer data as part of the investigation and debugging process.

Full administrative application access and as such also customer data access may also be needed to remedy error conditions that may arise in the Tricent for Google Workspace and Tricent for Microsoft 365 production environment.

In Tricent for Google Workspace and Tricent for Microsoft 365 software deployment scenarios Tricent will also need administrative application access and may as part of this process also see customer data.

4. SECURITY REQUIREMENTS

The Tricent for Google Workspace and Tricent for Microsoft 365 software solutions use Google's and Microsoft's authentication APIs enabling SSO so that a user with an already logged in Google Workspace or Microsoft 365 session will be logged in directly to their Tricent for Google Workspace or Tricent for Microsoft 365 dashboard without further authentication prompts.

This requires that the Tricent for Google Workspace and Tricent for Microsoft 365 software solution requests, processes and stores an Oauth2 session ticket in the Tricent for Google Workspace and Tricent for Microsoft 365 infrastructure.

For its scheduled clean-up processes the Tricent for Google Workspace and Tricent for Microsoft 365 software solution needs domain-wide delegation to the customer's Google Workspace environment in order to take actions on individual users' files without manual end-user or admin intervention.

This requires that the Tricent for Google Workspace and Tricent for Microsoft 365 software solution stores and uses a token with a client certificate for a GCP or Azure service account that is granted domain-wide access to the customer data which is accessed via Google's or Microsoft's APIs.

All access and actions on behalf of both users, admins, and the automated scheduler is logged and kept for the duration of the Tricent for Google Workspace and Tricent for Microsoft 365 service lifetime.

5. OPERATIONAL IMPLEMENTATION AND ONBOARDING

The infrastructure components including any operating systems, web servers, cache layers, databases and application engines needed to deliver the Tricent for Google Workspace or Tricent for Microsoft 365 solutions are hosted in Google Cloud Platform (GCP) and Microsoft Azure platform (Azure) respectively.

The settings requirements and installation procedures for onboarding the Tricent for Google Workspace or Tricent for Microsoft 365 solutions into the customer's Google Workspace or Microsoft 365 tenants are documented in Tricent's Support Portal and delivered to the customer as part of the onboarding process.

6. SUPPORT SCOPE

The Tricent for Google Workspace and Tricent for Microsoft 365 solution is delivered in a managed portal solution hosted and supported by Tricent running in Google Cloud Platform (GCP) and Microsoft Azure (Azure) respectively.

To support end-users and admins Tricent may need administrative access to the Tricent for Google Workspace and Tricent

for Microsoft 365 software solution in specific scenarios in order to troubleshoot users' interaction with the system.

All administrative access and actions in the Tricent for Google Workspace and Tricent for Microsoft 365 software solution on both frontend and backend is logged and kept for the duration of the service lifetime.

7. DATA RECOVERY

The full Tricent for Google Workspace and Tricent for Microsoft 365 software solution, corresponding application data, databases, and log data is backed up daily to offline storage in GCP and Azure and the restore capability is maintained for the duration of the Tricent for Google Workspace and Tricent for Microsoft 365 software service lifetime.

In situations caused by human errors, the Tricent for Google Workspace and Tricent for Microsoft 365 software solutions are by design able to roll back actions performed by users, admins, and the automated scheduler.

In case Tricent for Google Workspace and Tricent for Microsoft 365 software system malfunction causes customer data inaccessibility this is considered a special scenario and recovery times fall under the SLA tied to the Tricent for Google Workspace and Tricent for Microsoft 365 software as a service agreement between the customer and Tricent (see below).

8. SERVICE UPTIME

The Tricent for Google Workspace and Tricent for Microsoft 365 software will have a target uptime of 99.9% (excluding announced maintenance service windows usually scheduled during business off-hours)

In scenarios where intermediate vendors such as Google Cloud Platform, Microsoft Azure, customer ISP, etc. are the primary cause of a service interruption, Tricent's SLA commitment begins when any intermediate vendors have resolved their service interruption.

9. SERVICE LEVELS

The Tricent for Google Workspace and Tricent for Microsoft 365 software solution is expected to align to the following service levels:

Severity Level	Response Time	Resolution Time
Severity Level 1 (P1)	Within 4 hours	Within 12 hours
Severity Level 2 (P2)	Within 8 hours	Within 1 day
Severity Level 3 (P3)	Within 24 hours	Within 3 days
Severity Level 4 (P4)	Within 2 business days	Except for new feature suggestions, not later than the next release

10. INCIDENT MANAGEMENT

For all customer support scenarios where Tricent requires access to the Tricent for Google Workspace or Tricent for Microsoft 365 software solutions, a service request and/or incident is required in Tricent's service management system indicating:

1. The problem that requires the access (deployment, patching, support, debugging).
2. The work expected to be carried out.
3. The timeframe of the work expected to be carried out.
4. The customer contact raising the request for service.
5. The Tricent technician responsible for carrying out the work.

If additional personnel such as Google or Microsoft personnel or developers need involvement and access in a support case this will be logged in the service ticket.
All access and actions carried out for the Tricent for Google Workspace or Tricent for Microsoft 365 software solution are logged and kept for the duration of the service lifetime.