Backup and Disaster Recovery Services - Service Level Agreement (SLA)

Introduction

This Service Level Agreement ("SLA") by Tigunia, LLC ("Tigunia") applies to all clients, collectively referred to as the "Client." It governs the provision of fully managed Backup and Disaster Recovery ("BCDR") services as outlined below.

This document sets forth Tigunia's commitments, including service availability, performance metrics, support responsibilities, and the procedures for addressing service disruptions and downtime.

Purpose

This SLA aims to establish a clear framework for delivering and managing Backup and Disaster Recovery Services. Tigunia agrees to meet the service levels referenced herein so that Client receives reliable and consistent service. This SLA specifies the expectations for service availability, uptime, response times, and support of the services and defines the remedies available to Client in the event of service failures. This agreement supports Client's operational needs and is intended to foster a transparent and accountable relationship between Tigunia and Client. Each objective stated herein will be defined as a Service Level Objective ("SLO") with explicitly defined targets.

To avoid doubt, this SLA applies solely to the availability and performance of the "Recovery Service" and its use. It does not cover protected systems, such as any private computing environment, ERP, BI, or SQL data.

Service Level

This SLA defines two distinct service levels: **Core** and **Standard.** Below, we outline the scope, Recovery Point Objective ("RPO"), Recovery Time Objective ("RTO"), data retention policies, and responsibilities at each level.

This SLA clarifies Client's responsibilities for managing Business Continuity Planning (BCP) and addresses key aspects such as fail-back time, data retention, service credits, service changes, testing responsibilities, and reporting requirements.

Core Level – Co-Managed Backup and DR

The **Core** service level provides a co-managed disaster recovery solution, where Client maintains primary responsibility for managing their backup operations. In contrast, Tigunia provides tools, monitoring, and support for disaster recovery. Specific responsibilities include:

- **Client Responsibilities**:
  - Managing and verifying the scheduling and execution of backups.
  - Ensuring backups are configured and running according to their recovery needs.
  - Initiating recovery requests via Tier 1 phone support with written confirmation.
  - Maintaining their business continuity plan ("BCP") to address operational recovery beyond technical backup and recovery.

- **Tigunia Responsibilities**:
  - Provide tools and support for monitoring and verifying backup statuses.
  - Availability of backup service:

Uptime Percentage	Maximum downtime allowed (monthly)
99.9% to 99% (0.1% to 1% downtime)	44 minutes to 7 hours 15 minutes
Less than 99% (more than 1% downtime)	7 hours 15 minutes or greater

  - Assisting with virtual machine ("VM") data restoration efforts based on Client-managed backups, subject to the following standard targets:

Recovery Scope	Objective
RPO	1 hour
RTO	4 hours

  - Offering backup consistency for file or asset recovery assistance with the following targets:

Recovery Scope	Recovery Time Objective
Secondary-Region file-only	4 hours
In-Region File-only	3 hours

Standard Level – Fully Managed Backup and Disaster Recovery (BCDR)

The **Standard** service level offers a fully managed disaster recovery solution where Tigunia assumes full responsibility for managing backups, disaster recovery, and restoration efforts. The scope of services includes:

- **Client Responsibilities**:
  - Establishing and maintaining their own BCP to address operational recovery, personnel, and process concerns beyond the technical recovery efforts provided by Tigunia.
  - Engagement with solutions to validate that targets and solution aspects align with business needs.

- **Tigunia Responsibilities**:
  - Protected virtual machine ("VM") data is subject to the following standard targets:

Recovery Scope	Objective
RPO	1 hour

  - Managing backup scheduling, monitoring, and execution for single and multi-instance VM recovery to comply with the agreed-upon targets after an applicable Tier-1 recovery request:

Recovery Scope	Recovery Time Objective
In-Region Single VM	1 hour
In-Region File-only	1 hour
In-Region Full vDC	3 hours

  - Complete Virtual Data Center ("vDC") recovery to secondary region agreed targets after an applicable Tier-1 recovery request:

Recovery Scope	Recovery Time Objective
Secondary Region Full vDC	4 hours

  - Timely restoration of individual files or assets within a 2-hour objective following a Tier-1 recovery request.

- Maintain consistent snapshots of production systems, stored on immutable storage, with encryption in transit and at rest, and replication to a secure secondary region.
- Coordinate with Client on fail-back to the production environment following disaster recovery. The fail-back time objective ("FBTO") is 12 hours, depending on the environment and storage volume.

Exclusions for Both Levels

These services do NOT include labor or engineering efforts in the target systems for application troubleshooting, development, or other related efforts. At Tigunia's discretion, the services may provide complimentary validation services by the NOC team for clients with or without NOC services, where the Tigunia NOC would validate the availability and operability of client-end applications within the recovered system. These referenced services are offered without warranty or guarantee and are rendered on a best-efforts basis only.

Service Considerations

Data Retention

Backup data will be retained for 13 months unless otherwise specified in writing by Client and agreed upon by Tigunia. Custom retention periods may incur additional costs. Following the retention period, data will be automatically deleted unless alternative arrangements are made.

Production Environment Fail-Back Time ("FBTO")

After a disaster recovery, Tigunia will work with Client to restore the production environment. The fail-back time objective (FBTO) is typically 12 hours, subject to the complexity of the environment and coordination with Client.

Service Changes

Changes to the DR service must be requested in writing by Client and agreed upon by Tigunia. Changes to custom DR targets, backup schedules, or data retention policies may result in additional charges and impact service availability.

Minor updates by Tigunia, such as system patching or configuration updates, will be communicated in writing at least 14 days in advance unless urgent changes are required for security or operational reasons.

Testing and Liability

Annual or mutually agreed DR testing will be performed in coordination with Client. Client is responsible for providing accurate data, system access, and third-party coordination for testing. Tigunia is not liable for DR process failures due to inaccurate information, third-party systems, or environmental factors beyond its control. Tigunia is not liable for the performance of the recovery services if Client refuses or fails to participate in testing.

Reporting

Upon request, Tigunia will provide Client with reports that include the following:

- **Backup Success Rates:** Percentage breakdown of successful and failed backups.
- **SLO Performance:** Performance metrics comparing Restore Point Actuals ("RPA") and Restore Time Actuals ("RTA") to RPO/RTO with agreed-upon objectives.
- **Restore Requests:** The number of restore requests and corresponding restore times, including compliance with the 3-hour file/asset restore objective.
- **Incident Reporting:** Details on incidents related to DR operations, corrective actions taken, and steps to prevent future incidents.

Restore Requests

Client may request both Test Restore and Actual Restore operations under the terms of this SLA.

Test Restore Requests

Client may request up to two test restores per quarter or four test restores annually without incurring additional charges. Test restores include verifying the recovery of data, files, or virtual machines to comply with Client's RPO and RTO. Tigunia may determine the type and quantity of data, files, and virtual machines subject to testing to validate the recovery services.

Test restore operations do not constitute all-encompassing disaster recovery testing or business continuity planning ("BCP") simulations. If an all-encompassing simulated DR or BCP test is required, we will schedule that as a separate services engagement.

Actual Restore Requests

Actual restore requests for live environments (non-testing purposes) are not limited but are subject to reasonable use as outlined in the service contract. All restore requests must be initiated via a Tier-1 phone support request with written confirmation.

Service Credits

Service Credits for Remediation

Service Credits are Client's sole and exclusive remedy for any performance or availability issues and any service referenced under Tigunia's Master Services Agreement and this SLA. You may not unilaterally offset Client's Applicable Monthly Service Fees for performance or availability issues.

Limitation of Service Credits

Service Credits apply only to fees paid for the Recovery Service for which a Service Level has not been met. In cases where Service Levels apply to individual or multiple Recovery Services, Service Credits apply only to fees paid for the affected Recovery Service, as applicable. The Service Credits awarded in any billing month for a particular Recovery Service will remain within Client's monthly service fees for that Recovery Service in the billing month, as applicable.

If you purchased Services as part of a suite or other single offer, the Applicable Monthly Service Fees and Service Credit for each Service will be pro-rated.

If Client purchased a Service from another partner reseller, Client could receive a service credit directly from that partner.

Requesting Service Credits

Clients must request service credits within thirty (30) days of the end of the affected month. Requests must be made in writing and include detailed documentation of the downtime.

Service Credits Calculation

Recovery Services - Core Level

The following Service Levels and Service Credits apply to Client's use of each Protected Instance within the Core Recovery Service for Foortress Cloud Recovery and from either a Foortress Cloud vDC or on-premises instance:

Uptime Percentage	Maximum downtime allowed (monthly)	Service Credit
99.9% to 99% (0.1% to 1% downtime)	44 minutes to 7 hours 15 minutes	10%

Uptime Percentage	Maximum downtime allowed (monthly)	Service Credit
Less than 99% (more than 1% downtime)	7 hours 15 minutes or greater	25%

Protected Item refers to a collection of data, such as a volume, database, or virtual machine, that has been scheduled for Backup to the Backup Service so that it is identified as a Protected Item in the Protected Items tab in the Recovery Services section of the Management Portal.

Recovery or **Restore** is restoring computer data from the Core Recovery Service to an applicable server or instance.

Deployment Minutes is the total number of minutes during which a Protected Item has been scheduled for Backup to the Recovery Service.

Maximum Available Minutes is the sum of all Deployment Minutes across all Protected Items for a given Instance during an Applicable Period.

Downtime means the total accumulated Deployment Minutes across all Protected Items scheduled for Backup by you in a given Recovery Service subscription during which the Recovery Service is unavailable for the Protected Item. The Recovery Service is considered unavailable for a given Protected Item from the first Failure to Back Up or Restore the Protected Item until the initiation of a successful Backup or Recovery of a Protected Item, provided that retries are continually attempted no less frequently than once every thirty minutes.

Uptime Percentage is calculated using the following formula:

$$\frac{\textit{Maximum Available Minutes-Downtime}}{\textit{Maximum Available Minutes}} \; x \; 100$$

Recovery Services - Standard Level

The Standard Level of Recovery Services includes managing and administrating requests within a limited scope. If these efforts by Tigunia fail to meet the agreed-upon Recovery Service Targets (RPO, RTO, FBTO) for a given Recovery Service, Client may be entitled to service credits. These credits are calculated as follows:

- For each failure to meet a Recovery Service Objective by more than 10%, Client shall receive 10% of the monthly service fee as a credit, up to 100% of the total monthly payment.

Foortress Region to Region Recovery

The following Service Levels and Service Credits apply to Client's use of the Standard Recovery Service for Foortress Cloud-to-Foortress Cloud recovery scenarios.

Service availability for the standard solution is managed by, and the responsibility of, Tigunia.

Recovery Scope	Recovery Time Objective	Service Credit
In-Region Single VM	>1 hour	100%
In-Region File-only	>1 hour	75%
In-Region Full vDC	>3 hour	100%
Secondary Region Full vDC	>4 hour	100%

On-premises to Foortress Region Recovery

The following Service Levels and Service Credits apply to the availability of the service to Client:

Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

The following Service Levels and Service Credits apply to Client's use of each Protected Instance within the Site Recovery Service for the On-Premises-to-Foortress Cloud:

Recovery Scope	Recovery Time Objective	Service Credit
In-Region Single VM	>1 hour	100%
In-Region File-only	>1 hour	75%
In-Region Full vDC	>3 hour	100%
Secondary Region Full vDC	>4 hour	100%

One hour is the Recovery Time Objective for a specific Protected Instance configured for Foortress Cloud-to-Foortress Cloud Service Recovery in each Applicable Period.

Recovery Time Objective ("RTO") means the period from the time Client initiates a Recovery or Tigunia acknowledges the request for recovery of a Protected VM or vDC Instance to the time the Protected Instance is running as a virtual machine in the secondary Foortress Cloud region,

excluding any time associated with any required manual action, network or DNS adjustments, or the execution of Client scripts.

Limitations

Exclusions

This SLA explicitly excludes the following:

- **Backup Maintenance:** The applicable Network Operations Center (NOC) services handle backup maintenance and testing separately.
- **Maintenance Windows:** Backup and recovery operations may require planned maintenance windows affecting production system availability. Such windows will be scheduled in coordination with Client and will not impact service availability metrics.
- **Business Continuity Planning ("BCP"):** This service does not include developing or managing Client's BCP. Client is solely responsible for their BCP, which should cover Client's operational recovery beyond the technical system restoration.
- **Live Failover or Active-Active Availability Services:** The DR service does not provide live failover or active-active availability. Adjustments to DNS, networking configurations, or external service providers may be necessary during a disaster recovery event.

This SLA and any applicable Service Levels do not apply to any performance or availability issues resulting from, but not limited to, the following:

- Any issues related to the Application layer can be addressed on a Time and Materials basis upon Client's request.
- Due to factors outside Tigunia's control, *e.g.,* natural disaster, war, terrorism, riots, government action, or a network or device failure external to Tigunia data centers, including at Client's site or between Client's site and Tigunia data center.
- That results from using services, hardware, or software not provided by Tigunia, including, but not limited to, issues resulting from inadequate bandwidth or related to third-party software or services.
- Client's use of a Service caused this after Tigunia advised Client to modify its use of the Service, and if Client did not modify its use as advised.
- During or concerning preview, pre-release, beta, or trial versions of a Service, features, or software as determined by Tigunia or to purchases made using service credits.
- That results from Client's unauthorized action or lack of action when required, or from Client's employees, agents, contractors, vendors, or anyone gaining access to Tigunia's network using Client's passwords or equipment, or otherwise resulting from Client's failure to follow appropriate security practices.

- That result from Client's failure to adhere to any required configurations, use supported platforms, follow any policies for acceptable use, or Client's use of the Service in a manner inconsistent with the features and functionality of the Service, *e.g.,* attempts to perform operations that are not supported or inconsistent with Tigunia's guidance.
- This results from faulty input, instructions, or arguments, *such as* requests to access files that do not exist.
- That resulted from Client's attempts to perform operations that exceeded prescribed quotas or that resulted from Tigunia's throttling of suspected abusive behavior.
- Due to Client's use of Service features outside of associated Support Windows.
- For licenses reserved but not paid for at the time of the Incident.

This Service Level Agreement does not include on-premises or Hosted Virtual Machine Operating Systems and application support.

Tigunia is not responsible or liable for the data stored on protected systems by Client. Client is fully responsible for and the controller of any such data.

Client's Responsibilities

To support the above SLA, for all covered sections, Tigunia will need a minimum of two (2) authorized contacts for any relevant third-party vendor with whom Tigunia must communicate if contracted by Client. These contacts are required for the following purposes:

- Provide access to systems, equipment, and other resources needed to support the configuration.
- Maintain active support agreements with hardware and software vendors and provide Tigunia with appropriate credentials or permissions to interface with the vendor.
- Provide authorization to Tigunia to act on Client's behalf if vendor coordination is required.
- Provide a primary point of contact for escalations and issue resolution.
- Provide a point of contact with the authority to make decisions about change orders, budgets, scopes, resources, and other project-related issues.
- Provide reasonable notice of requirements to allow Tigunia sufficient time to mobilize the appropriate resources.
- Submit a change request for services outside of this SOW in writing. Changes may cause the fee schedule to change and additional charges to be assessed.
- Provide accurate, detailed documentation including but not limited to credentials, backup strategies, network diagrams,
- Troubleshooting: Tigunia requires documentation specific to Active Directory, Email, Files, and Applications at minimum. If sufficient documentation is not provided, which

results in more prolonged and extensive efforts, any affected support cases may require escalation.

Service Level Agreement Review

This Service Level Agreement will be reviewed at least once per year. Contents of this document may be amended as required and updated on Tigunia's website. See https://www.tigunia.com/legal-notices/.

Tigunia reserves the right to remove any unsupported software if it is suspected the software causes a recurring problem on a supported client-owned system/device and upon the authorization of Client's primary contact).

Issues relating to this SLA should be addressed to Tigunia Support at **(866) 562-8911** or **support@tigunia.com**. Unresolved issues will be escalated to the Director of Cloud Infrastructure.

Definitions

Contract and Agreement Terms

- **Service Credit**: A credit issued to Client when Tigunia fails to meet agreed performance objectives (*e.g.,* RPO, RTO). Service credits are the sole remedy for failing to meet SLA performance standards.
- **Statement of Work ("SOW")**: A legally binding document that outlines the scope of work provided by Tigunia for a specific project.
- **Master Services Agreement ("MSA")**: A contract between parties that defines the terms that will govern future transactions or agreements. See https://www.tigunia.com/legal-notices or the applicable MSA.
- **Service Level Agreement ("SLA")**: A contract between a vendor and a Client that specifies what the vendor will furnish, the period in which it will be furnished, and the criteria for measuring vendor success.

General IT Terms

- **Agent**: Software installed on a system to gather data for remote management, updates, and troubleshooting by Tigunia.
- **Endpoint**: Any device such as a mobile phone, tablet, workstation, or server that interfaces with a user and is managed under this SLA.
- **Incident**: Any event that disrupts or has the potential to disrupt the regular operation of systems and requires action to restore standard service.

- **Managed IT Services**: IT tasks and processes that a third-party organization fulfills.
- **Planned Maintenance Window**: A scheduled time when systems may be temporarily unavailable because of system updates or maintenance and is exempt from performance metrics.

Recovery Objectives

- **Recovery Point Objective ("RPO")**: The maximum allowable data loss measured in time, specifying how far back in time data can be restored before a disaster.
- **Recovery Point Actual ("RPA"):** The actual point in time for which data was recovered during disaster recovery and which reflects the effectiveness of the RPO.
- **Recovery Time Objective ("RTO")**: The maximum allowable time to restore systems and return to operational status following a disaster.
- **Recovery Time Actual ("RTA")**: The actual time it took to restore systems during a disaster recovery event, which measures the effectiveness of the RTO.
- **Data Retention**: The policies and periods for which backup data is retained before it is deleted or archived, as determined by Client's requirements or industry standards.
- **Fail-Back Time Objective ("FBTO")**: The time to restore services from the disaster recovery environment to the original production environment once normal conditions are restored.

Recovery Services Terms

- **Failover**: Transferring control of a protected instance from a primary site to a disaster recovery site in case of failure or simulation. Types include:
  - **On-Premises-to-DR Service Failover**: Transferring control from a non-DR primary site to a DR site.
  - **DR Service-to-DR Service Failover**: Transferring control between DR sites.
- **Failover Minutes**: The total minutes during an Applicable Period when a failover was attempted but not completed for a Protected Instance.
- **Maximum Available Minutes (Failover)**: The total minutes a Protected Instance has been configured for DR Service during an Applicable Period.
- **Downtime**: The accumulated minutes during which the Failover of a Protected Instance is unsuccessful due to the unavailability of the Disaster Recovery Service, provided retries are attempted no less frequently than once every thirty minutes.
- **Uptime Percentage**: When a Protected Instance is available for failover, calculated as the Maximum Available Minutes minus Downtime, divided by the Maximum Available Minutes.
- **Replication**: Copying data from one location to another (typically from a primary site to a secondary site) creates redundancy and disaster recovery capabilities.

- **Immutable Storage**: A form of storage where data cannot be altered or deleted after being written, creating integrity and protection against unauthorized changes or ransomware.

Backup and DR-Specific Terms

- **Backup**: Copy data from a registered server to a Backup Vault to ensure data protection.
- **Backup Agent**: Software installed on a registered server that enables backups or restores of Protected Items.
- **Backup Retention Period**: The time backup data is retained before it is deleted or archived. This period is customizable based on Client requirements.
- **Backup Vault**: A container in which Protected Items are registered for backup purposes.
- **Co-Managed Backup**: A service where Client manages their backup process while Tigunia provides support, tools, and disaster recovery assistance as agreed upon.
- **Fully Managed Backup and DR ("BCDR")**: A service where Tigunia assumes full responsibility for managing backups and disaster recovery processes and creating compliance with RPO and RTO.
- **Protected Instance**: A virtual or physical machine configured for replication to handle disaster recovery. Protected Instances are listed in the Recovery Services section of the Management Portal.
- **Protected Item**: Data such as volumes, databases, or virtual machines are scheduled for backup and listed as Protected Items in the Recovery Services section of the Management Portal.
- **Recovery or Restore**: Retrieving backed-up data from a Backup Vault to a registered server.
- **Failure**: A scenario where either the Backup Agent or the service fails to complete a properly configured backup or recovery due to service unavailability.
- **Deployment Minutes**: The total number of minutes a Protected Item is scheduled for backup.
- **Maximum Available Minutes (Backup)**: The sum of all Deployment Minutes across all Protected Items during an Applicable Period.
- **Downtime (Backup)**: The accumulated Deployment Minutes during which the Backup Service is unavailable for a Protected Item, starting from the first failure to back up or restore.

Change Log

All changes are tracked by Tigunia's managed Governance Risk Compliance ("GRC") platform.