Service Desk - Definition of Services and Components (DSC)

Introduction

This document defines the Co-Managed IT Services delivered by Tigunia, LLC, under the relevant Statement of Work and Tigunia's Master Services Agreement ("MSA").

The descriptions, features, and scope of each tier of Tigunia's three-tiered Service Desk offering, *i.e.,* Service Desk Core, Standard, and Service Desk Premium**,** are referenced below. Each tier builds on the features of the previous tier(s). We offer automated IT management and security at the core level to fully manage support and compliance-related services at the premium level. Collecting these services and related efforts are collectively called the "Services."

Objective (Mission Statement)

The Service Desk provides technical support for Client's users, systems, networks, and essential technology operations.

Service Tiers & Definitions

Service Tier	Description	Support Plan
Service Desk Core	Automated, software-driven services that are focused on basic vulnerability scanning, patching, remote access controls, MDR, security tools, and foothold detection.	T&M Support
Service Desk Standard	Full managed service desk offering, covering incidents, requests, endpoint management, and user support in alignment with NIST Cybersecurity Framework 2.0 and ITILv4 service management commitments. The scope includes endpoint management, patching, vulnerability scanning to CIS benchmark standards, IT procurement services, infrastructure co-management, shared documentation platforms.	T1 and T2 Support Included

Service Desk Premium	Includes all Standard features with additional compliance evidence gathering (on request), Just-in-Time (JIT) password management via PIM for service technicians, and password management for end-users. Excludes configuration or engineering services.	T1 and T2 Support Included + Security Incident user support and Compliance evidence collection.

We describe below \the three tiers of the Service Desk, each with distinct levels of support and performance. Each tier delivers the services of the prior tiers plus additional services.

Service Desk Core

Service Desk Core is the basic Tigunia Service Desk tier. Service Desk Core Clients are provided with the tooling and configurations for Remote Monitoring and Management, Remote Desktop, and Endpoint Protection. All Service Desk Core services are invoiced on a time and materials basis and include the following benefits:

Managed Endpoint Agents

- Tigunia will provide the required management agents for each user endpoint.
- Defined agents in this service:
    - **Endpoint Management**: Centralizes management and performance monitoring of all endpoints.
    - **Remote Access**: Facilitates secure remote connections and desktop access.
    - **Configuration Management** Tracks configuration changes and ensures compliance through auditing. Asset Management monitors the inventory and lifecycle of hardware and software assets.
    - **Mobile Device Management ("MDM")** manages device enrollment and supports remote wipe capabilities. The Scripting Agent executes automated scripts for system management and remediation tasks.
    - **Software Distribution**: Automates software deployment and tracks installations.
    - **Service Desk Integration**: Creates automated tickets from alerts that include asset details.
    - **Vulnerability Scanning** identifies known vulnerabilities and provides remediation recommendations. **Patch Management** Automates patch deployment and offers compliance reporting.
    - **Endpoint Security**: Provides antivirus protection and real-time threat detection.

- **Managed Detection and Response ("MDR")** provides continuous monitoring and threat response capabilities. Incident Response Isolates infected endpoints and executes predefined remediation actions.
- **Ransomware Canary**: Deploys honeypots to detect potential ransomware attacks.
- **Foothold Detection Agent**: Monitors for signs of unauthorized access or footholds by attackers.

Automated Vulnerability Scanning

- **Service Description**: Automated vulnerability scanning of endpoints and network devices using software solutions.
- **Standards**: Vulnerability detection follows CIS benchmarks for compliance and security posture improvement.
- **Frequency**: Weekly scanning with automated reporting.

Automated Patching

- **Service Description**: Automated patch management for OS and critical applications.
- **Coverage**: Patch management follows critical security updates that are aligned with industry standards.
- **Monitoring**: Ongoing patch status monitoring and alerting.

Remote Access Controls

- **Features**: Secure remote access management for devices and users.
- **Access Tools**: Managed through centralized remote access software.
- **MFA Integration**: Multi-factor authentication ("MFA") is enforced for all remote access points.

Managed Detection and Response ("MDR")

- **Service Description**: Continuous monitoring and threat detection using MDR tools.
- **Proactive Alerts**: Automated alerts for security threats, anomalies, or unusual network activity.
- **Foothold Detection**: Detection of unauthorized presence in the system, with immediate isolation measures.

Support Services and Related Labor

- This tier does not include any support effort labor for the end system, network, or Client applications. All support at this tier is invoiced on a Time and Materials ("T&M") basis. Assistance with issues regarding the service application itself can be performed based on requests submitted to noc@tigunia.com.

- The Service Desk provides frontline support for users in an organization and support for complex technical issues. The Service Desk handles problems and inquiries related to hardware, software, networks, and other IT services. Tigunia's Service Desk helps to provide smooth operations and minimize downtime by resolving issues promptly and efficiently.
- The Service Desk provides nationwide business-hour support for all supported systems from Monday through Friday, 7:00 a.m. to 7:00 p.m. CST (excluding holidays).
- Emergency support is available twenty-four hours a day, seven days a week.

Reporting

- Tigunia provides detailed reporting that provides insights into the performance, efficiency, and effectiveness of Client's IT environment. This effort helps Clients understand how their IT resources are utilized, identify areas for improvement, and make informed decisions about future investments and strategies. Reporting includes Case metrics, Security, Trend Analysis, and IT recommendations.
- This Service tier only includes reporting directly related to each applicable service agent.

Exclusions

- This tier's cost does not include hands-on troubleshooting or user support. It focuses on automated, software-driven tasks.
- This service does not include proactive labor to manage Client endpoints and is provided strictly as a best-efforts T&M engagement.
- Human interaction for incident resolution is not included unless escalated by Client request.

Service Desk Standard

Service Desk Standard customers pay a flat monthly fee per supported workstation, including all required agents and the regular business hours of Tier 1 and Tier 2 Service Desk. Service Desk Standard includes all the benefits of the Endpoint Core services referenced above but with a predictable recurring rate per supported workstation. Additionally, the Service Desk Standard consists of the following benefits:

Full Managed Service Desk

- **Scope**: IT support for incidents, requests, and general user assistance.
- **Channels**: Available via phone, email, and self-service portal.
- **Incident Management**: Aligned with ITILv4 Incident Management and prioritization based on criticality and impact.

Endpoint Management

- **Features**: You can fully manage endpoint devices, including desktops, laptops, and mobile devices. This includes onboarding and offboarding endpoint devices.
- **Monitoring**: Continuous monitoring for device health, performance, and compliance.
- **Patch Management**: Hands-on patching and vulnerability remediation performed by service desk agents.
- **Advanced Endpoint Agents:** In addition to the tooling provided by Endpoint Core,
    - Service Desk Standard includes Managed Detection and Response ("MDR") for Office
    - 365, Extended Detection and Response ("XDR"), DNS security, and OS and Application vulnerability management.

Problem Management

- **Proactive Issue Resolution**: Root cause analysis for recurring issues to prevent future incidents.
- **Managed Alert Response:** Using the NOC capabilities, Service Desk Standard endpoints are monitored 24/7 for system-generated alerts, with automatic remediation and experienced technical resources for addressing more complex issues.

User Management

- **Password Management**: Support for password resets and security policy enforcement.
- **Account Provisioning**: Support for user onboarding/offboarding in systems.

Governance

- **Service Manager:** Tigunia's Service Desk Standard includes a dedicated Service Manager so customers get the most from Tigunia's services. This effort includes managing issues, trend analysis, identifying underlying issues, and regular Client update meetings.
- **Microsoft 365 Backup: The** Service Desk Standard includes Microsoft 365 backups that go well beyond the basics included by Microsoft. This effort provides more granular backup and recovery options, which protect against data loss from accidental deletion, ransomware attacks, or service outages.
- **Reports**: Monthly service reports on incidents, performance, and uptime metrics.

Exclusions

- **Backup and Recovery**: Automate data backups and offer restoration options with version control.
- **User Activity Monitoring**: Log user activities and alerts for suspicious behavior.
- **File Integrity Monitoring**: Detects changes and alerts for unauthorized file modifications.
- **Data Loss Prevention (DLP)**: Enforce policies to prevent data loss and track violations.

- **Customization:** Custom configuration and advanced engineering of security solutions must be handled via a separate services statement of work.
- **Compliance:** Evidence gathering is not included.

Service Desk Premium

Tigunia's highest level of Service Desk offering, Service Desk Premium, includes all of the benefits of the two previous tiers and extends the focus on security. This service includes:

Mature IT Operational Considerations

- **NIST 2.0 Governance:** Monthly oversight and review of managed systems with rapid vulnerability scan reporting to align security efforts and governance.
- **Security Event Coordination:** Review security incidents through automated workflows with SOC integration and escalation.
- **Tier 3 Technical Support:** Advanced technical support for complex coordination and handling of security events and system remediations.

Security Considerations

- **Security Services Alignment:** Continuous alignment with industry security frameworks such as CIS Benchmarks, ISO, or other relevant IT compliance standards.
- **SOC Services Integration:** We integrate directly with Tigunia's 24/7 SOC for advanced threat detection and response and collaborate with third-party SOC services to provide comprehensive threat monitoring.
- **XDR (Extended Detection and Response) Collaboration:** Unified visibility and real-time response capabilities across all endpoints through XDR platforms that improve threat detection and incident response.

Governance, Risk, Compliance, and Regulation

- **Governance, Risk, and Compliance ("GRC") Evidence Gathering**: Support gathering compliance control evidence for Client audits, regulatory requirements, and vendor requests.
- **Orchestrated Compliance and Security Operations:** Advanced coordination and execution of compliance-related tasks and security incident responses to create proper alignment with operational governance standards.

Advanced Support for cloud-native Modern Work

- **M365 Security Alerting**: Proactive and custom monitoring of Microsoft 365 environments, including alerts for potential threats and compliance issues.

- **Fortress Monitoring ("FoMo") for M365**: Enhanced alerting and reporting features for security visibility and engagement with Client's Microsoft 365 environments.
- **Custom Reporting and Telemetry**: Tailored security and performance reporting incorporating detailed endpoint telemetry for insights into system health and risk assessment.

Premium Endpoint

- **Advanced Endpoint Management**: Comprehensive endpoint security management includes patching, vulnerability scanning, and threat hunting.
- **Endpoint Encryption Support**: Full endpoint encryption management and monitoring to safeguard sensitive data.

Advanced Security Management

- **Security Posture Audits**: Regular monthly audits that use rapid scans to assess and maintain the security posture of credentials, identity management, and associated services.
- **Named Support Users Only**: Ensures that support access and actions are limited to predefined, authorized users to enhance security.
- **Privileged Identity Management ("PIM")**: Managed identity and access controls using Just-In-Time ("JIT") administration for privileged accounts.
- **Just-In-Time Password Administration**: Automated password management workflows for privileged access create secure, time-limited access for sensitive systems.

Attestation Support

- **Attestation Reporting and Evidence Gathering:** While Tigunia does not provide attestation services, this tier of support includes providing the applicable security and compliance evidence as part of the service based on Client-defined frameworks (*e.g.,* SOC 2, HIPAA, PCI-DSS, CMMC) according to the related statement of work. We also perform on-demand, ad-hoc evidence gathering for audits at the request of Clients, attestation officers, or third-party vendors.
- **Scope of Support:** Collect logs, security control data, and compliance reports for regulatory or audit requirements. Submit requested evidence to third-party vendors or auditors.
- **Process:** Collaborate with Client's compliance officer to identify necessary evidence. Compile and deliver evidence based on predefined audit requirements and frameworks.

Custom Reporting

- **Audit Trail Reporting**: Custom reports generated for compliance audits, detailed security logs, access events, patch records, and evidence documentation.

- **Report Frequency:** Custom reports are provided according to audit schedules or at the Client's request.
- **Detailed Logs:** Aggregate security and access logs, patch management history, and relevant compliance data for comprehensive reporting.

Exclusions for Compliance Services

- **No Configuration or Engineering**: The scope does not include engineering or reconfiguring systems to meet specific compliance standards. Security control configuration and remediation efforts are handled separately via professional services or a statement of work.
- **Backup and Recovery**: Automated data backups and restoration options with version control.
- **User Activity Monitoring**: Log user activities and alerts for suspicious behavior.
- **File Integrity Monitoring**: Detects changes and alerts for unauthorized file modifications.
- **Data Loss Prevention ("DLP")**: Enforce policies to prevent data loss and track violations.
- **Customization:** Custom configuration or advanced engineering of security solutions must be handled via a separate statement of work.

General Exclusions for All Tiers

- **Compliance Attestation:** Although Tigunia partners with certification, attestation, and other regulating or governing bodies, Tigunia does not provide direct attestation or certification efforts.
- **Framework Engineering**: None of the service desk tiers include configuration or engineering of security solutions to meet compliance frameworks. Engineering services can be provided separately under a statement of work.
- **Business Continuity and Disaster Recovery (BCDR)**: The design and management of BCDR solutions are not included.
- **Advanced Infrastructure Engineering**: Infrastructure design and network architecture adjustments must be handled via a statement of work.

IT Procurement Services (Available in All Tiers)

- **Procurement Lifecycle Management**: Hardware and software purchasing, including vendor selection, quotes, and delivery coordination.
- **Asset Management**: Integrating procured assets into asset management systems with lifecycle tracking.
- **Vendor Management**: Direct engagement with third-party vendors to present procurement timelines and SLAs.

Co-Management of Infrastructure (Available in Standard & Premium Tiers)

- **Shared Responsibility Model**:
  - **Client Responsibilities include Overseeing** critical applications, custom configurations, and BCP/DR solutions. Provider Responsibilities include Managing infrastructure elements (*e.g.,* virtual servers, firewalls, and switches).
- **Documentation**: Shared access to infrastructure documentation for Client and service provider collaboration.
- **Monitoring & Alerts**: Real-time infrastructure health monitoring, with incident tickets generated for performance or security issues.

Shared Documentation Platform (Available in Standard & Premium Tiers)

- **Client Support Portal:** Tigunia's Client portal provides customers with a centralized platform for creating and reviewing cases and access to all Tigunia-provided reporting—the portal's user-friendly interface streamlines access to Tigunia services.
- **Collaboration**: Shared platform for documentation management (*e.g.,* IT Glue Asset Management and Related Credential Management as applicable) that allows Clients and service providers to access and manage shared documents securely.
- **Version Control**: Full audit trails of changes to infrastructure and service documentation.
- **Security**: Documentation access is governed by role-based access control ("RBAC").

Continuous Improvement

- **Feedback Collection**: Regular surveys and Client feedback sessions to assess service quality.
- **Review Cycles**: Quarterly service reviews for Standard and Premium tiers to address performance, compliance, and potential improvements.

Scope of Service

The scope of this service is expressly limited to the locations, endpoints, systems, and infrastructure explicitly defined in the corresponding Statement of Work ("SOW"). Any services, support, or activities outside these specified areas are considered out of scope and will not be included in the particular or selected service offering. Modifications or extensions to the scope must be formally agreed upon and documented in an updated SOW or separate engagement agreement.

SLAs for Each Service Tier

All services herein are provided with the commitments in the corresponding “Tigunia Platform Services Support Service Level Agreement (SLA)” without warranty or guarantee.