# Network Operations Center (NOC) - Service Level Agreement (SLA)

## Introduction

This Service Level Agreement ("SLA") outlines the performance standards, response times, and support expectations for the Network Operations Center ("NOC") services provided by Tigunia to Client. **To avoid doubt, this SLA applies solely to the availability and performance of the NOC service, not the availability or performance of systems or assets monitored by the NOC.** This document and related services are subject to the NOC Definitions of Service and Components ("DSC") and Tigunia's Master Services Agreement ("MSA"). See https://www.tigunia.com/legal-notices/. This SLA governs all SOWs for this service.

## Purpose of this Document

This SLA document establishes the agreed-upon service levels between Tigunia and Client.

This SLA describes which services are included, how they are delivered, and how the reporting of such delivery must be performed. Each objective stated herein will be defined as a Service Level Objective ("SLO") with explicitly defined targets. Any service effort established in the DSC is only rendered on a best-efforts basis if that service does not relate to an established SLO.

## Responsibility and Formal Organization

Tigunia defines the following roles for an incident:

- **Incident Response Team ("IRT" ): The IRT coordinates** the response to security incidents, including investigation, mitigation, and communication. Its highest responsibility in any security incident is immediate containment and triage. This team consists of a Tigunia staff member who is part of the Network Operations Center ("NOC"), Security Operations Center ("SOC"), Service Delivery Team, First Response, Service Desk, or Triage Support teams, respectively.
- **Tigunia Security Team:** Detailed response, eradication, and recovery efforts, with validation from the SOC team post-eradication.
- **VP of Information Technology ("VPIT"):** The VPIT oversees the IRT and Security Team groups so that appropriate actions are taken to address the incident.
- **Tigunia Non-Security Employees or Team Members:** Report incidents, comply with Tigunia policies, and verify Client processes.
- **Legal and Compliance Team:** Responsible for disclosures that comply with legal and regulatory requirements.

- **Communications Team:** Managed internal and external communications related to the incident. Typically, a Tigunia executive or applicable Client account lead.
- **Client Security Contact or Team:** Coordinate incidents involving Client data.
- **Client Representatives:** Engage in disclosure and response processes as needed.

## Services Delivered by NOC

### Operating System ("OS") Patching

NOC includes the patching of the following operation systems:

- **Microsoft Windows:** All versions that have not reached End of Life ("EOL") and End of Support ("EOS").
- **Apple's macOS:** All versions for which Apple actively maintains patches and security updates. Apple does not publicly disclose its support policy, and the period may change from version to version of the operating system.
- **Linux (limited distribution):** Support will be determined per distribution due to the varying distributions and configurations available. Patch management and monitoring will be provided where the distribution supports the installation of the agent software and supporting libraries.

### Endpoint Vulnerability Scanning and Patching Compliance

- The NOC service includes **endpoint operating system vulnerability scanning** and reporting on compliance with Client-defined patching schedules.
- Vulnerability scans will be conducted as part of the NOC Standard and Premium services, and regular reports will be provided.
- **Patching compliance** will be monitored and reported according to Client-defined targets. Still, Tigunia will only be responsible for compliance beyond the reporting and monitoring efforts if explicitly defined in a separate SOW.
- All efforts will be made during an approved maintenance window to apply available patch releases to remediate applicable vulnerabilities.
- NOC vulnerability services are distinct from SOC vulnerability services and are limited to OS vulnerabilities identified by the local vulnerability scanning agent.

Application patching and updating can be performed to a limited degree under the NOC Premium services; however, results are never guaranteed. This service does not include development, engineering design, or redesign efforts. Any software upgrades that would require developer or engineer engagement, such as Microsoft Dynamics ERP Wave Releases or similar software testing against deployed extensions, are outside the scope of this service.

## Alert Management and Response

Alert Management and Response services are provided 24x7x365. NOC will provide comprehensive monitoring and remediation services for servers, network devices, applications, and workstations.

Each monitor created for the service has a corresponding Standard Operating Procedure ("SOP") that outlines Tigunia's responsibilities and response actions. Tigunia can scope any application system or environment upon Client's request, and a new monitor can be established with corresponding SOPs.

Custom SOPs can be adapted to Client's specific operational or compliance requirements. However, they must be defined in advance and mutually agreed upon during onboarding or through an explicit written statement of work.

## Alert Classification

The information below outlines the classification of alerts and the system that generated the alert, and it is based on the potential impact on Client. This policy mirrors Tigunia's Incident Classification using a 5 Priority level system:

| Severity | Alert Examples | Response Example |
|---|---|---|
| P1 Critical | Infrastructure, systems, or business critical applications are down. | Review monitoring and reach out to infrastructure team or vendor. Investigate services, configs, and underlying hardware. |
| P2 Major | Non-critical business applications down. Redundancies are in effect. | Investigate service, configs, and the service tier. Engage with client for status updates or to work with on-site teams if applicable. |
| P3 Intermediate | Warnings indicating issues with system or application performance | Review cause, and either: Notify Client of impact or make changes on client's behalf |
| P4 General | Minor performance warnings, e.g., hard drive capacity warnings or memory leaks | Review cause, and either: Notify Client of impact or make changes on client's behalf. |
| P5 Informational | Informational events, or scheduled notifications, e.g., uptime notifications or monitor based status reporting. | Notate status for reporting, schedule reboots, take action as needed. |

## Alert SLO - Initial Response Levels

The NOC will respond within the timeframes below based on the classification below and the type of alert.

| Priority Level | Alert Acknowledgement | Response Interval / Escalation | SLO |
|---|---|---|---|
| P1 Critical | Within 15 Minutes | 30 Minutes | 96% |
| P2 Major | Within 30 Minutes | 1 Hour | 96% |
| P3 Intermediate | Within 1.5 Hours | 4 Hours | 96% |
| P4 General | Within 6 Hours | 24 Hours | 96% |
| P5 Informational | Within 1 Day | 7 Days | 96% |

## Alert SLO - Resolution Time

The Services outlined herein do not include Service Level Objectives ("SLOs") for resolution efforts. This exclusion is based on the following considerations:

1. **Incident Complexity**: The nature of incidents managed by the NOC may involve factors beyond our control, such as third-party vendor performance, client-side configurations, and external dependencies. The NOC cannot commit to resolution timelines for issues influenced by these external factors.
2. **Scope of Responsibility**: NOC services primarily focus on monitoring, alerting, and performing initial triage. While we work to provide rapid responses, full resolution may require further action from Client's IT teams or third-party service providers, which is outside the NOC's direct responsibility.
3. **Emphasis on Response Times**: While resolution times are not guaranteed, the NOC commits to adhering to defined response SLOs to prompt incident acknowledgment and action. Response times are measured and tracked according to the SOP for each established monitor.
4. **Customization of Client SOPs**: By establishing custom monitors, incident response procedures, including troubleshooting steps, are tailored to each Client's environment. These custom monitors have Standard Operating Procedures ("SOPs") with target objectives, but these targets are internally tracked and can vary significantly based on the specific setup. For this reason, resolution timelines cannot be standardized or measured for this SLA.
5. **Flexible Service Targets**: The NOC targets scaling time objectives as outlined in our SOPs, based on the complexity and type of monitor established for each Client. However, given the broad flexibility of the services offered, these targets are internal and cannot be guaranteed or measured within the context of this SLA.

## NOC Service Level Agreement

A specific list of use cases and the standard assigned priority levels will be agreed upon and issued to Client before onboarding.

Based on the performance levels provided below, a Client may receive a service credit that can be used against future purchases. However, such credits will only be applied to charges for NOC services.

**Alert Acknowledgement and Responses**

| **SLO Adherence %** | **Service Credit** |
|---|---|
| 96% and Above | 0 |
| >=95% and <96% | 5% |

| | |
|---|---|
| >=92% and <95% | 10% |
| >=90% and <92% | 15% |
| <90% | 20% |

SLA credit for Acknowledgment and Responses are tracked together per alert.  This SLA is calculated across all alert cases for the billing period.

### SLA Adherence Calculation

Service adherence to the agreed-upon Service Level Agreements ("SLAs") will be calculated monthly to create transparency and measure our performance.  The calculation reflects the percentage of support incidents handled within the specified SLA response and resolution times across all incidents for a given period.

The adherence percentage will be calculated using the following formula:

$$SLA\ Adherence\ (\%) = \left(\frac{\text{Number } of\ Alerts\ within\ SLA}{Total\ Number\ of\ Alerts}\right)\ x\ 100$$

**Definitions:**

- **Number of Alerts within SLA**: The total number of alert cases resolved (resolution implies response) or responded to within the specified SLA timeframes for that given month.
- **Total Number of Alerts**: All alert cases logged during that month, regardless of their SLA performance.

**Example Calculation:**

If, in a given month, 85 Alerts were resolved (resolution implies response) or responded to within the SLA out of 100 total incidents, the SLA adherence would be calculated as follows:

$$SLA\ Adherence\ (\%) = \left(\frac{85}{100}\right)\ x\ 100\ \ =\ \ 85\%$$

### Exclusions

Acknowledgment and Responses will not be measured if due to the following:

- Connectivity issues between client systems and the NOC.

- Emergency scheduled maintenance.
- Actions caused by client staff or external third parties that interrupt service.
- Events or conditions beyond Tigunia's control.  Such events include, but are not limited to:
    - Acts of government authorities not due to Tigunia's prior lack of conformance with regulations or law.
    - Natural disasters.
    - War, insurrection, riot, terrorism, or similar unlawful actions.
    - Suspension or termination of services provided under this agreement per the Master Services Agreement.

## SLA Metrics for Reporting

**Alert Management and Response**

All alerts are tracked by Tigunia's systems and reported monthly to Client.

**Operating System ("OS") Patching**

Patching reports are available monthly.

**Managed Backups**

The status of managed backups will be provided monthly.  NOC Services will provide reports regarding the adherence to the agreed-upon Recovery Point Objectives and Recovery Time Objectives

**Maintenance Efforts and Reporting**

For NOC Premium, monthly maintenance actions will be carried out by a NOC systems analyst. These include:

- Review and adjustment of monitoring thresholds.
- Performance optimization checks.
- Delivery of a monthly performance report to Client.

Maintenance actions are detailed during Client onboarding or in the Service Definitions document.

## Root Cause Analysis ("RCA")

Tigunia will provide an RCA only when this SLA has been breached. The RCA will focus on identifying the cause of the NOC service degradation, not the root cause of the technical issue on Client's monitored systems. The service does not include RCAs related to Client systems and would require a separate billable engagement or coordination with a third-party vendor (*e.g.,* Microsoft).

If an RCA for Client's system is required, Tigunia can engage with a software vendor or external provider, which will incur additional costs payable by Client.

**Root Cause Analysis (RCA) for Service and Client Incidents**:

- **RCA for NOC Service Delivery Failure:** RCAs will only be provided when a Service Level Agreement (SLA) violation occurs due to a failure in the NOC services provided by Tigunia, such as issues with monitoring, alerting, or response times. In such cases, Tigunia will perform an "After Action Investigation" or "Blameless Postmortem" process and deliver an RCA covering the cause of the NOC service failure and any corrective actions required to prevent a recurrence. This RCA will be provided at no additional cost to Client.
- **RCA for Client's Infrastructure or Application Incidents:** RCAs for incidents affecting Client's infrastructure or applications monitored by this service are not automatically included as part of the NOC services and may not always be possible to provide. The NOC services' scope and available diagnostic information limit the ability to generate an RCA for such incidents. If an RCA is requested for an event in Client's environment (*e.g.,* network devices, servers, or applications), and the incident does not constitute a failure in the NOC services, additional engineering support may be required to determine the needed details. In such cases, the provision of an RCA may involve billable hours on a Time and Materials basis, including any necessary involvement from Vendor Partners or third-party providers, for which Client will also be responsible. Tigunia will inform Client of applicable charges and request written approval before proceeding with any billable work.
- **RCA Limitations:** RCAs for Client's infrastructure or applications are subject to the technical limitations of the NOC's visibility and monitoring capabilities. Tigunia does not guarantee that an RCA can be produced for every incident within Client's environment, mainly where the issue lies outside the scope of the NOC services or requires engagement with third-party vendors.

## Additional Services – As Applicable

The following services are available based on additional agreements or service bundles.

### Maintenance

Servers receiving maintenance are reviewed by hand regularly for issues not detected by automation. The NOC team will validate that the automation is running correctly, review system performance, and perform system scanning. Reporting is provided monthly or quarterly based on the frequency of services that Client receives.

### Managed Detection and Response

Clients can access our Managed Detection and Response ("MDR") platform for any Windows or Mac OS Device enrolled in RMM. MDR provides antivirus, anti-malware, foothold detection for potentially risky software, and ransomware detection. Security incidents follow our SOC SLA and are reported monthly with the NOC Alerts if no SOC Services are offered.

### Security Incidents

- **Under this SLA, Security Incidents** are treated as best-effort responses, following the same incident priority and response schedule outlined above.
- Security incident response protocols, including those related to data security, are outside the scope of this NOC SLA.

### Exclusions

- Additional services referenced above must be purchased and included in this SLA.

- **Compliance Attestation Limitations:** Compliance-related efforts are limited to providing operational evidence when requested, such as logs and reports that are part of the NOC service. This operational service does not include compliance attestation efforts, audits, or formal certifications.

- **Remediation Efforts:** Remediation for incidents detected by monitors is limited to the specific response SOP and does not imply unlimited access to engineering resources. Further remediation or complex troubleshooting will require a separate, billable engagement.

- **Security Incident Response:** The remediation of security incidents is limited to the NOC services outlined herein. The entire incident response and resolution process for security-related events is defined under the separate SOC Service SLA, which applies to data breaches or critical security threats.

## Service Credits

Service Credits are Client's sole and exclusive remedy for any performance or availability issues for any service under the Agreement and this SLA. You may not unilaterally offset Client's monthly service fees for performance or availability issues.

Remediation SLAs are only measured for incidents a monitor generates with a defined Standard Operating Procedure (SOP) response. If no SOP exists for a particular monitor or incident type, response times will not be subject to SLA guarantees.

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

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 reseller, Client could receive a service credit directly from that reseller.

**Requesting Service Credits:** Client must request service credits within five (5) days following the end of the affected month. Requests must be made in writing and include detailed documentation of the downtime.

**Limitation of Service Credits:** Service credits are the sole and exclusive remedy for failure to meet the uptime guarantee. They are limited to the invoice amount for the particular service in question during the calendar month.

## Definitions

### NOC

A Network Operations Center (NOC) is a centralized function that monitors and manages an organization's network infrastructure 24/7/365. NOCs are responsible for monitoring an organization's network so that it is available and performing well and that any issues are resolved quickly.

NOCs are critical components of IT support and are used in industries such as telecommunications, financial services, manufacturing, and energy.

The NOC configures and responds to all system-generated alerts for a Client organization. The NOC follows a standard operating procedure for each alert to resolve, respond to, or escalate it to the appropriate support team.

**RMM**

RMM stands for Remote Monitoring and Management. RMM systems generally allow various levels of access and control, monitoring and response, patch management for endpoints (*e.g.,* the user's computer*),* and network devices running multiple operating systems.

**MDM**

Mobile Device Management (MDM) software helps organizations manage and secure devices connected to a Client's network. It can also protect the network and ensure compliance with policies.

**Service Level Objective (SLO)**

A Service-Level Objective (SLO) is a specific, measurable target that defines the performance or quality metric a service must achieve. SLOs represent key benchmarks, such as uptime, response time, or transaction throughput, and are used to measure whether a service meets the expectations set out in an SLA. SLOs are often internal goals that help monitor performance, but they may only carry penalties or legal consequences for non-compliance if explicitly stated in the agreement.

**Service Level Agreement (SLA)**

A Service Level Agreement is a formal, legally binding contract between the service provider and Client that outlines the agreed-upon performance standards and service levels the provider must meet. SLAs typically include specific SLOs and remedies or penalties in the event of failure to meet those objectives. SLAs govern the expectations regarding service availability, support response times, incident resolution, and other critical service elements, ensuring accountability for the provider.

## Change Log

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