[LOGO]

**NETWORK OPERATIONS CENTER**

**SUPPORT**

RFP Released: [DATE]

Questions Due: [DATE]

Response Due: [TIME\_DATE]

All RFP-related Questions and final RFP submissions should be submitted to:[EMAIL]

**[TABLE OF CONTENTS]**

**Support Contract Requirements**

The respondent receiving the RFP award will serve as the primary Network Operations Center on a continuous basis 7 days per week, 24 hours per day and every day of each year. In general, those authorized to contact the NOC will be limited to [ENTITY] staff, operational representatives of [ENTITY].

**Service Desk**

The service desk component describes the coordination center for the NOC services. The service desk function must provide the following capabilities:

* Perform **event and incident management** functions, including:   
  + Monitoring of the [ENTITY] technology environment and all associated service endpoints.
  + Generate alerts when any component of the [ENTITY] Technology Environment exceeds defined operational parameters.
  + Provide first-tier incident response, including creation, assignment and tracking of incident response tickets as appropriate based on generated alerts or other notifications from [ENTITY] staff.
  + Provide granular and targeted notification of outage events or other service impacts to affected users and [ENTITY] staff.
  + Provide online accessible and real-time status updates for ongoing incidents with appropriate informational view for [ENTITY] staff.
  + Close incident response tickets upon service restoration, including timely notification as appropriate to affected parties.
  + Manage major incident communications according to a set playbook and as requested. For major incidents, participate in post-incident root cause analysis and process improvement determinations conducted by [ENTITY].
  + Provide daily status report of incident management status to operational management staff at [ENTITY].
  + Develop and provide regular human-reviewed summary of incident management activities to operational management staff at [ENTITY].
  + Escalate unresolved issues to appropriate [ENTITY] on-call staff.
* Perform **service request fulfillment functions**, including:   
  + Working with [ENTITY] staff to define specific service request templates for [ENTITY] Technology Environment services.
  + Creation and tracking of service request tickets as appropriate based on requests from [ENTITY] staff.
  + Fulfillment of service requests or referral of service request tickets to appropriate [ENTITY] functions.
  + Closure of service request tickets upon completion, with timely notification to the original requestor.
  + Daily status reporting of request fulfillment status to operational management staff at [ENTITY].
  + Regular summary reporting of service request fulfillment activities to operational management staff at [ENTITY].
* Perform **inventory control and change management** functions, including:  
  + Participation in the [ENTITY] change management process to determine maintenance windows, planned outages, or other service-impacting activities.
  + Creation and tracking of change control tickets.
  + Issue granular and targeted notification of maintenance windows and planned outages to [ENTITY] staff and affected users within the [ENTITY] membership.
  + Close change control tickets upon completion, with timely notification to affected parties.
  + Daily status reporting of inventory and change management status to operational management staff at [ENTITY].
  + Regular summary reporting of inventory and change management activities, including human review, to operational management staff at [ENTITY].
  + Tracking and communication to [ENTITY] of any inventory records for replaced parts.
  + Management and tracking of physical access to technology environment colocation facilities in coordination with the [ENTITY] security office.
* Provide **web-accessible interfaces** to [ENTITY] staff with visibility into current and historical incident management, service requests, and change management activities.
* Additionally:   
  + Service Level Agreements (SLAs) will be jointly developed by the Service Desk and [ENTITY] to monitor system and service performance of the [ENTITY] technology environment and to trigger appropriate alerting or other notifications to [ENTITY]. It is expected that the potential provider, once selected, would come to [ENTITY] with a Standard SLA as a starting point upon which [ENTITY] and the provider would define any customized processes and that the provider would be responsible for making updates, including training for its staff and lifecycle management of SLA documents.
  + The Service Desk must implement a modern and comprehensive service management infrastructure to support and proactively improve processes and procedures. Proposals will need to detail not only the processes and procedures that are used but also how they are managed, continuously improved and communicated with [ENTITY]. For example, in the RFP evaluation process, [ENTITY] will want to understand how the NOC manages its policies and procedures for major ITSM processes like incident, problem, request, change, introduction of new services, etc. [ENTITY] will expect the NOC to have mature processes and communications plans for each process.
  + The Service Desk may also be requested to collaborate with [ENTITY]’s Network Planning & Architecture, Security, and Infrastructure Systems & Software teams to review and improve end-user satisfaction, plan new features and to review and plan process and communications improvements, including:
  + Participation in meetings with [ENTITY] Leads to coordinate service support objectives;
  + Providing a monthly report of NOC statistics on incident management, service request, and change control activities. Such reports should include
    - human-reviewed analysis of trends or emerging issues that should be tracked and acted upon, if any;
  + Complete timely Reason for Outage reports on major incidents or problems, and describe plans for future response improvements and other mitigation strategies; and
  + Conducting a quarterly review session including periodic discussions on process improvement or other relevant issues.
* Respondent will provide information on how its software can be linked to [ENTITY]'s systems-of-record regarding customer, and third party vendors. [ENTITY]requires the respondent to state whether their systems have the capability, via API's or other methods to:
  + accept data from [ENTITY]'s system-of-record,
  + the capability to run the system-of-record for various types of information (customers, contacts, etc.) that can be pushed into [ENTITY]'s systems or,
  + if the respondent’s normal practice is some mixture of both of the above.

**Break/Fix Engineering**

As part of the proposal, it is expected that the Service Desk will coordinate and deliver a Break/Fix Engineering component that will:

* Provide supporting engineers trained to troubleshoot and repair problems with the deployed components and configurations of the [ENTITY] network and/or compute platforms.
* Monitor the deployed components and configurations of [ENTITY]’s technology environment, detect routine operational failures.
* Undertake appropriate restorative actions in response to operational failures to return functionality to originally deployed and configured levels and communicate such actions to [ENTITY].
* Where unable to repair an impaired or down service within a set service level expectation, make an escalation to [ENTITY] staff to assist in repair.
* When escalation staff are needed to assist in break/fix repairs, participate in documentation, training and other activities to assure the NOC can repair identified recurring issues independently during future incidents.
* Examples of expected break/fix support include:
  + Monitoring alerts, system logs, and system telemetry, and recognizing indicators of a deviation from expected state required to identify failed hardware and associated service impacts.
  + Diagnosing failed components within an SLA.
  + Diagnosing circuit failures, or other physical impairments to the network and coordinating with the associated vendors within an SLA to open and track tickets for the outage or service degradation.
* Engaging remote smart hands assistance for problem identification where necessary.
* Engaging in a portion of the Return Merchandise Authorization (RMA) process.
* Writing and/or executing replacement Methods of Procedures (MoPs) to direct remote hands in failed part replacement, and managing the execution of MoPs to successful conclusion.
* Documenting failure resolution and communication of failure and remedy details to [ENTITY] staff.
* Engaging escalated support when necessary, from [ENTITY] technical resources in a timely manner, when established break/fix procedures cannot identify and/or remedy the issue.
* Engaging with third-party suppliers including maintenance contract providers, fiber providers, circuit providers, colocation providers, and other [ENTITY] contractors as needed to completely resolve identified issues.
* Working with [ENTITY] operational management staffing to continuously improve documentation and processes to better prevent the occurrence of and break/fix support for future failures and related incidents.

[ENTITY] would provide initial documentation and training for any [ENTITY]-specific systems. The NOC would be required to write run books and provide staff training based on this information.

**Tooling and Software Systems**

The capabilities, reliability, security and usability of the tooling and software systems that support the NOC and break-fix engineering are a critical part of the services [ENTITY] will evaluate. Respondents should be prepared to document support in the following areas related to their operational tooling and related software systems:

* The provider must have adequate systems and software to support a modern operational regime that combines ticketing, monitoring, alerting, SLA tracking, customer contact information and configuration management information necessary to provide service desk and operational break/fix engineering support for the [ENTITY] technology environment. Ideally, the provider would offer a configuration management system that is sophisticated enough to allow the NOC to support all aspects of the environment from the customer demarcation point through to the configurations of the systems.
* [ENTITY] requires that the tooling and software systems are operated in a high availability configuration that assures necessary operational support systems are always available and secure. The NOC will be responsible for providing a secure and controlled environment to operate these systems and will need to describe how they propose interconnecting these systems to the [ENTITY] technology environment.
* The ideal provider would have predictive analysis tools that analyze service delivery trends across the ITSM processes and effort levels and assists both in informing areas for potential process improvement and in system hardening. [ENTITY] will seek the respondent’s insights into existing practices and emerging activities in this area.
* The provider must detail its approach to each system it would use to support [ENTITY] in terms of their approach for custom development, or vendor tools.

**NOC Interconnect and Supporting Infrastructure**

Respondents should be prepared to document support in the following areas related to interconnect and supporting infrastructure security and resiliency:

* The NOC will be responsible for providing secure, resilient, independent and dedicated connectivity to the [ENTITY] technology environment.
* The NOC will also be responsible for providing appropriate, secure, resilient access to operational software and systems functions from the general Internet and via the dedicated connection to [ENTITY] in order to allow [ENTITY] staff and membership to interact with those systems and services, e.g., to report issues, track incidents, submit service requests, etc.
* Operational tooling and software systems (see above) should be implemented using best practices for high availability and disaster recovery, i.e. as multiple geographically distributed instances, maintained with a regular backup rotation, with documented processes in place to handle common scenarios like Distributed Denial of Service (DDoS) attacks, ransomware threats, and other commonly-recognized security issues. [ENTITY] will expect to review the respondent’s business continuity and disaster recovery plans as they are relevant to services covered under this RFP.
* The NOC will be responsible for coordinating with [ENTITY] staff in performing regular backup verification tests, including annual failover/disaster recovery drills as required to confirm process and implementation support for those scenarios.

**Security of NOC and [ENTITY] Operational Environment**

* The NOC and [ENTITY] Network Security will collaborate to produce security plans designed to protect both the [ENTITY] environment and the operational support systems. For example, plans should address vulnerability management processes that reduce the time to patch, anomaly detection such as Crowdstrike, protections against ransomware, and implementation of a zero-trust architecture.
* All NOC systems used to support [ENTITY] environment and services will include a dedicated instance for [ENTITY]. Access controls must be in place to prevent staff without an [ENTITY] relationship from access or viewing data on these systems.
* [ENTITY] requires that providers have and share a security and continuity of business plan for the operational support systems it provides to [ENTITY]. These plans must include at minimum the ability to sustain operations during attacks and other emergencies that could impact the systems or the facilities they reside in.
* [ENTITY] will require the provider to detail its plans for major incidents, attacks and events that could affect the systems or facilities used by the provider. At minimum, we would expect to see evidence that the provider has clear plans for DDoS, ransomware, catastrophic destruction or access restriction at one of its data centers and related contemporary scenarios.
* [ENTITY] requires immediate notification of any security breach/event/incident that jeopardizes the confidentiality, integrity, availability, or control of the operational support systems used to support [ENTITY] or possibly exposes our data to unauthorized individuals.
* In support of continuous security monitoring, the NOC will provide [ENTITY] Network Security with continuous and unfettered direct access and system logging feeds for all systems and devices used to support the [ENTITY] networks and services.
* The NOC will follow [ENTITY] security policies such as, security incident management (covering suspected or active attacks, or intrusions against the [ENTITY] technology environment or operational support systems).
* Because threats are constantly evolving, the NOC and [ENTITY] Network Security will perform annual security risk assessments of support systems, processes, and personnel. The exact scope of each security assessment will be determined by [ENTITY] Network Security. Recommended improvements identified by the security risk assessment will be developed jointly by the NOC and [ENTITY] Network Security. Ultimately it will be [ENTITY] leadership that decides the resolution of identified risks (e.g., accepted or mitigated).
* The NOC staff working with [ENTITY] will complete at least the same annual security awareness training as that of [ENTITY] Network Services staff in addition to any annual training provided by the NOC itself.

**Service Desk and Break/Fix Support SLAs**

[ENTITY] expects the NOC to maintain SLAs for key performance metrics. Submitted proposals must address the items in the list provided below as well as any additional information about standard offerings of the NOC’s standard SLA’s or Service Level Objective (SLO)s. [ENTITY] will work with potential awardees to finalize a set of metrics and performance targets for the eventual contract.

* KPIs and metrics - include the KPI's and other related metrics supported by an SLA.
* Service levels, rankings, and priority - include a description of the services, severity levels of disruptions and target response times.
* Service response - include the service description, SLA target, Performance Metric(s), and method of measurement (e.g., MTTF).
* Exceptions and limitations - list any exceptions to the SLA conditions, scope, and application.
* Responses and responsibilities - define the responsibilities of both the service provider and the customer.
* Service Management - define the service management and support details applicable to the service provider in this section, such as hours of operation for each support service, ( e.g., Service Desk Hours, On-Call hours, etc.).

**Quarterly Reviews**

[ENTITY] requires an in-depth review of activity in the NOC service desk at quarterly intervals throughout the year. The provider would need to agree to providing the following:

* Quarterly, [ENTITY] and the NOC will meet to discuss upcoming activities, milestones, observations from the prior quarter, process improvements or changes, staffing, training and other strategic items.

**Performance Management**

The NOC will be responsible for providing and maintaining an escalation matrix from the shift management to senior executives within the providers’ organization. An executive sponsor should be named as a liaison to [ENTITY] senior management.

The NOC will be expected to manage its performance metrics and to regularly engage with [ENTITY] related to areas of improvement for both the NOC and [ENTITY] in tuning and [ENTITY] continuously improving the services delivered to [ENTITY] customers and the efficiency of activities between [ENTITY] and the NOC.

**Other Requirements and Facilities**

**Onboarding Requirements**

[ENTITY]’s current expectation is that contracts would be in force by [DATE], with the NOC service being in place and ready.

Respondents need to provide and explain the total cost of transition, including any system setup or hardware requirements, including one-time costs, associated with a new agreement.

| **About this RFP Template**  This RFP template is designed for organizations seeking to procure comprehensive NOC support services. It outlines the requirements for a service provider to deliver 24/7/365 NOC support, including:   1. Service Desk functions 2. Break/Fix Engineering 3. Tooling and Software Systems 4. NOC Interconnect and Supporting Infrastructure 5. Security measures 6. Service Level Agreements (SLAs) 7. Performance management and reporting   The template is structured to help organizations clearly communicate their expectations for NOC services, including incident management, service request fulfillment, change management, and operational support. It emphasizes the need for secure, resilient, and efficient operations, as well as continuous improvement and collaboration between the service provider and the organization.  Key features of this template include:   * Detailed descriptions of required capabilities and responsibilities * Emphasis on security and operational resilience * Expectations for reporting, reviews, and performance management * Flexibility for customization based on specific organizational needs   Organizations using this template should review and adjust the requirements to align with their specific technology environment, operational processes, and business needs. The template provides a comprehensive starting point for defining NOC support services and can be tailored to suit various scales of operations and industry-specific requirements. |
| --- |

| **About INOC, an ITsavvy Company**  INOC is an ISO 27001:2022 certified 24×7 NOC and an award-winning global provider of NOC Lifecycle Solutions®, including NOC support, optimization, design, and build services for enterprises, communications service providers, and OEMs. INOC solutions significantly improve the support provided to partners’ and clients’ customers and end users.  INOC assesses internal NOC operations to improve efficiency and shorten response times, and provides best practices consulting to optimize, design, and build NOC operations, frameworks, and procedures. Proactive 24×7 NOC support is provided with several options, including North America, EU, or APAC only or global integrated NOCs. INOC’s 24×7 staff provides a hands-on approach to incident resolution for technology infrastructure support.  INOC is uniquely positioned to meet and exceed the requirements outlined in this RFP template.  Contact us to learn more or submit your RFP:   * <https://www.inoc.com/> * [info@inoc.com](mailto:info@inoc.com) * +1 (877 529-9101 |
| --- |