Example Performance Work Statement (PWS)

For Managed IT SErvices

# How to use this document

If your organization is subject to strict procurement rules, requiring Request for Proposal (RFP) or other formal procurement methods, purchasing complex Information Technology services can pose a challenge. In order to effectively engage with your procurement team to solicit these services you must be able to formally describe the services.

This document provides example content which could be used in the creation of such a formal procurement.

Please confer with your own procurement team to make sure you are compliant with all requirements, procurement rules and laws before using the contents of this document.

# Disclaimer

This document is not, and is not intended to, constitute legal advice; instead, all information, content and materials in this document are for general informational purposes only. Information in this document may not constitute the most up-to-date information. The content in this document is provided “as is;” with no representations or warranties whatsoever about the suitability of this content for any purpose or that the content is error-free.

# License

Copyright 2023 Vicinity Group, LLC

Permission is hereby granted, free of charge, to any person obtaining a copy of this document and associated documentation files (the “Document”), to deal in the Document without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Document, and to permit persons to whom the Document is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Document.

Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this Document without specific prior written permission.

THE DOCUMENT IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE DOCUMENT OR THE USE OR OTHER DEALINGS IN THE DOCUMENT.

**[Agency/Department Name]**

**Information Technology Support Services**

**Performance Work Statement (PWS)**

1. **Background/Overview**

[Provide background information on the Agency or Department (“Organization”), including its history, mission, vision, and organizational structure.]

[Provide background information on how technology systems support the execution of the Agency or Department mission.]

1. **Scope**
	1. **Statement of Objectives**

The purpose of this award is to obtain Information Technology (IT) services supporting the Organization to include:

**Endpoint Management** - Provide for the proper management, monitoring, inventory, maintenance, and upkeep of endpoint devices operated by the Organization, including but not limited to laptop and desktop computers, mobile devices, tablets, printers, and video conferencing equipment.

**Server & Application Management** - Provide for the proper management, monitoring, inventory, maintenance, and upkeep of server systems operated by the Organization, including but not limited to servers (on-premise and cloud), hypervisors (on-premise and cloud), and server hosted applications & databases.

**Network Management** - Provide for the proper management, monitoring, inventory, maintenance, and upkeep of network and communications systems operated by the Organization, including but not limited to switches, routers, firewalls, telephone systems (including VoIP), wide area network connectivity, wireless (WiFi) access points, and wireless controllers.

**Remote Assistance & Support** - Provide remote technical support via telephone, email and interactive chat for government employees, contractors, partners, and other authorized individuals (“End Users”) in the day-to-day use of technology systems and assets deployed by the Organization.

**In Person Assistance & Support** - Provide in person technical support for government employees, contractors, partners, and other authorized individuals (“End Users”) in the day-to-day use of technology systems and assets deployed by the Organization.

* 1. **Service Requirements**

The following scope items provide guidance on the minimum level of performance required under this award, but the Contractor is required to at all times execute reasonable and prudent judgement in delivering services. The Organization relies upon the professional judgement, guidance and capabilities of the Contractor in protecting the confidentiality, integrity and availability of all in scope government owned technology systems and assets. To this end, Contractor shall at all times utilize commercially reasonable industry best practices. Further, Contractor shall maintain all technology systems in keeping with federal law, regulation and policy including, but not limited to:

* + the Federal Information Security Modernization Act of 2014 (FISMA 2014);
	+ all current and future emergency and binding operational directives issued by the Cybersecurity & Infrastructure Security Agency (CISA).

**Endpoint Management**

The following activities represent the minimum acceptable levels of performance for Endpoint Management under this Award:

|  |  |  |
| --- | --- | --- |
| **Activity** | **Objective** | **Outcome** |
| Endpoint device inventory | To maintain an accurate and up to date inventory of all endpoint devices in use by the organization. | Inventory is up to date |
| Endpoint device health | To monitor and proactively initiate repairs to endpoint devices showing signs of defect or improper operation. | Endpoint devices are monitored proactively for defects. |
| Endpoint device lifecycle | To monitor and proactively recommend replacement of endpoint devices nearing the end of their service lifetime. | Deployed endpoint devices are within their established service lifetimes.Endpoint devices are not subject to failure due to use beyond their service lifetime. |
| Endpoint security | To monitor and protect the confidentiality, integrity and availability of data and applications stored on endpoint devices. | Endpoint anti-malware protection software is in place and up to date.Endpoint operating systems are up to date with all vendor provided security patches and updates.Endpoint operating systems are within their service lifetime (i.e. no unsupported operating systems in use.) |
| Endpoint management | To maintain all endpoint devices in compliance with established operating policies of the Organization. | Endpoint devices are managed by tools to enforce Organizational policies.Sufficient policies have been deployed to adequately protect the confidentiality, integrity and availability of the Organization’s technology systems. |
| Endpoint application deployment | To sanction and deploy only approved software on to endpoint devices. | Endpoint devices are deployed with only sanctioned applications and software.Unsanctioned software installations are detected and blocked or removed.Standardized application deployments are documented including application whitelists. |

**Server & Application Management**

The following activities represent the minimum acceptable levels of performance for Server & Application Management under this Award:

|  |  |  |
| --- | --- | --- |
| **Activity** | **Objective** | **Outcome** |
| Server and application inventory | To maintain an accurate and up to date inventory of all servers and applications in use by the organization. | Inventory is up to date |
| Server health | To monitor and proactively initiate repairs to server systems showing signs of defect or improper operation. | Server hardware is monitored for failure including high temperature and disk failure.Server operating system is monitored for network connectivity via ICMP, SNMP, WMI or other approved monitoring.Automated alerts are generated when a server system is offline outside of scheduled maintenance hours. |
| Server and application lifecycle | To monitor and proactively recommend upgrades or replacement of servers and applications nearing the end of their service lifetime. | Deployed servers are running on hardware that is either eligible for or under active hardware warranty from the OEM. |
| Server security | To monitor and protect the confidentiality, integrity and availability of data and applications stored on server systems. | Server anti-malware protection software is in place and up to date.Server operating systems are up to date with all vendor provided security patches and updates.Server operating systems are within their service lifetime (i.e. no unsupported operating systems in use.)Applications and database systems are up to date with all vendor provided security patches and updates.Application and database systems are within their service lifetime (i.e. no unsupported applications or databases in use.) |
| Server management | To maintain all server systems in compliance with established operating policies of the Organization. | Server systems are configured according to established configuration baselines and exceptions have been documented.Configuration management software had been deployed to detect deviations from approved configurations for server systems. |
| Cloud services management | To maintain all services operated through a third-party cloud provider in compliance with established operating policies of the Organization. | Cloud services are documented and administrative credentials are protected with two-factor authentication. |

**Network Management**

The following activities represent the minimum acceptable levels of performance for Network Application Management under this Award:

|  |  |  |
| --- | --- | --- |
| **Activity** | **Objective** | **Outcome** |
| Network inventory | To maintain an accurate and up to date inventory of all network and communications systems in use by the organization. | Inventory is up to date |
| Network health | To monitor and proactively initiate repairs to network and communications systems showing signs of defect or improper operation. | Network device hardware is monitored for failure conditions including environmental issues.Automated alerts are generated when a network device is offline outside of scheduled maintenance hours. |
| Network lifecycle | To monitor and proactively recommend upgrades or replacement of network devices nearing the end of their service lifetime. | Deployed network devices are running on hardware that is either eligible for or under active hardware warranty from the OEM.Any OEM announced “end of life”, “end of support” or similar date has not passed for deployed network devices.  |
| Network security | To monitor and protect the confidentiality, integrity and availability of data and applications transmitted over the network and communications systems of the Organization. | Network firewalls and other protective measures are deployed and configured in keeping with industry best practices.Network devices are up to date with all vendor provided security patches and updates.Network device firmware is within its service lifetime (i.e. no unsupported or superseded firmware in use.) |
| Network performance monitoring | To monitor the performance and transmission characteristics of the network are meeting the objectives of the Organization. | The network is monitored for conditions including loss of connectivity, saturation, transmission errors and other indicators of poor performance.Automated alerts are generated when a network performance is outside of established baselines for performance. |

**Remote Assistance & Support**

The following activities represent the minimum acceptable levels of performance for Remote Assistance & Support under this Award:

|  |  |  |
| --- | --- | --- |
| **Activity** | **Objective** | **Outcome** |
| Help Desk | To respond to and attempt to resolve end user support requests via telephone, email and web chat. | Help Desk is available during normal business hours (8am – 5pm Monday through Friday excluding federal holidays)Help Desk personnel are based in the United States. |
| Service Request Escalation | To escalate support requests which cannot be resolved by the Help Desk to qualified support technicians for further troubleshooting and repair to resolve the support request. | Unresolved service requests are escalated within the same business day. |

**In Person Assistance & Support**

The following activities represent the minimum acceptable levels of performance for Remote Assistance & Support under this Award:

|  |  |  |
| --- | --- | --- |
| **Activity** | **Objective** | **Outcome** |
| Dispatched Assistance | To dispatch a qualified support technician to the office or location of an End Users to resolve a service request which cannot be resolved remotely. | Qualified technician is dispatched on the next business day. |

* 1. **Qualifications**

The Contractor shall be sufficiently skilled, staffed and responsible in the delivery of services as to meet the needs of the Organization. To this end, the Contractor shall submit evidence of their past performance, current proficiency, licensure and certification as follows:

* + [Include any specific licenses, professional certifications or other requirements here];
	+ experience supporting endpoints devices for government or professional business organizations;
	+ experience supporting server systems for government or professional business organizations;
	+ experience supporting network and communication systems for government or professional business organizations;
	+ experience delivering remote assistance & support for government or professional business organizations; and
	+ experience delivering in person assistance & support for government or professional business organizations.

All contractors (including contractor employees, subcontractors and others with access to technology assets) must have or obtain a Non-Sensitive Public Trust clearance from the U.S. Office of Personnel Management.

* 1. **Period of Performance**

[Indicate the period during which this contract will run, including any required phase in or phase out timelines. Example: “The period of performance shall be for twelve (12) months commencing on January 1, 2023 and two (2) optional renewal periods of twelve (12) months each.”]

* 1. **Place of Performance**

The Contractor shall perform services remotely or on site at one of the office locations of the Organization listed below:

|  |  |  |
| --- | --- | --- |
| **Location** | **Address** | **On Site Point of Contact** |
| [Location Name] | [Street Address 1][Street Address 2][City], [State] [ZIP] | [First Name] [Last Name][Title][Phone Number][Email Address] |

 From time to time, the Contractor may be required to perform services at remote locations.

* 1. **Performance Objectives**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Performance Objective** | **Standard** | **Performance Threshold** | **Method of Surveillance** | **Incentives/Disincentives** |
| Endpoint patch management | All operating system patches applied within 30 days. | No more than 5% deviation (unless prior written deviation by COR) | Monthly Report to COR | Positive/negative pastperformance.Unacceptable performancewill be grounds for revising work products at no cost tothe Organization.Contractor shall remediate unpatched operating systems and systems within 30 days at no additional costto the Organization. |
| Customer Satisfaction Index (CSAT) | Maintain CSAT of 90.0 or greater for each calendar year. | 0% deviation | Quarterly Report to COR | Positive/negative pastperformance.Contractor shall implement a plan of action to improve service delivery within 90 days should performance threshold not be met. |
| Response Time | After initiating a service request, Contractor shall contact the initiator with a first point of contact no later than the following business day. | 10% deviation | Quarterly Report to COR | Positive/negative pastperformance.Contractor shall implement a plan of action to improve service delivery within 90 days should performance threshold not be met. |
|  |  |  |  |  |

* 1. **Reporting**

The Contractor shall submit reports to the Contracting Officer’s Representative (“COR”) as follows:

|  |  |  |
| --- | --- | --- |
| **Report** | **Content** | **Interval** |
| Open Service Requests | A listing of all currently open or unresolved service requests including the name of the person initiating the request. | Weekly |
| Service Exceptions | A listing of all issues requiring the attention or approval of the COR. | Weekly |
| Endpoint Inventory | Inventory data for all endpoint devices and installed applications. | As Requested |
| Server & Application Inventory | Inventory data for all server devices and installed applications. | As Requested |
| Network Inventory | Inventory data for all network and communications devices. | As Requested |
| [Name of the report] | [Specification for the data to be contained in the report] | [Requested Reporting Interval] |

* 1. **Constraints**

[Outline any specific or unusual circumstances surrounding the delivery of services under this contract. Examples may include special access procedures for sites or locations, insurance requirements, disclosures, hazards, or safety procedures.]

1. **Key Personnel**

**Account Manager**

Contractor shall initially designate an Account Manager as a point of escalation and who shall be responsible for and have authority to respond on behalf of the Contractor in any formal requests from the COR or other Organization staff which cannot be resolved through normal service channels.

The Account Manager shall be responsible for:

* + Acting as a point of escalation and providing remedy for issues, problems or complaints that arise during the course of providing services,
	+ Acting as a resource for the COR in seeking clarification or guidance from Contractor about the nature, scope, quantity or other attributes of contracted services, and
	+ Meeting regularly with the COR to verify that all Performance Requirements are being met to the satisfaction of the COR and that necessary improvement plans (if necessary) are executed on in a timely manner.

Key personnel may, with the consent of the contracting parties, be amended from time to time during the course of the contract to add or remove key personnel.

**Attachment A – Inventory of Endpoint Devices**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Serial Number** | **Endpoint Name/Description** | **Make** | **Model** | **Notes** |
|  |  |  |  |  |

**Attachment B – Inventory of Servers & Applications**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Serial Number** | **Server Name** | **Make** | **Model** | **IP Address** | **Critical Applications** |
|  |  |  |  |  |  |

**Attachment C – Inventory of Network & Communications Devices**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Serial Number** | **Device Name** | **Make** | **Model** | **IP Address** | **Notes** |
|  |  |  |  |  |  |

**Attachment D – End User Demographics**

|  |  |  |
| --- | --- | --- |
| **Location** | **Number of End Users** | **Notes** |
| [Location Name][Street Address 1][Street Address 2][City], [State] [ZIP] | [Total number of End Users at this location] | [List VIP’s or other special requirements here] |