7 Scope of Service

7.1 Scope and Basis of the Requirement

The scope of services for this contract covers the provision of a new Managed Network Service for Authority locations, which at the time of tender publication is c143 existing managed sites, c50 additional new sites, and c9000 users.

7.2 In Scope

- Design of all aspects of the solution in collaboration and consultation with the Authority
- The collaborative development of an implementation schedule, to ensure existing sites are implemented on the Provider's service by October 2026
- Development of technical security policies and mechanisms across the wired and wireless networks, adhering to and reflecting relevant Authority policies and industry best practice
- Submission of high-level designs (HLD) and low-level designs (LLD) for approval by the Authority
- A new Managed Network Service to include:
    - A security first framework
    - Zero Trust access for users and devices
    - Consistent application access
    - Simplicity of design
    - Visibility across the entire security stack
    - Enhanced management information for the Authority
    - Support for technologies such as multiple cloud environments (Azure and Oracle Cloud), SaaS and Cloud applications, secure connectivity across Authority sites, Microsoft Teams communications including Voice over Internet Protocol (VoIP), Microsoft Office 365, Internet of Things (IoT) and legacy devices at sites
    - Secured Web/Internet access
- Fully managed service to include:
    - Service delivery based upon Information Technology Infrastructure Library (ITIL) principles and practices
    - Clear financial management of the contract with accurate, consistent and frequent reporting
- Single Point of Contact Service desk (desk-to-desk)
    - Security management
    - Request Management (e.g. catalogue, minor and complex)
    - Incident Management
    - Problem Management
    - Operational Change Management

  - Business Continuity
  - Disaster Recovery
  - Release Management
  - Service Delivery and Service Level Management
  - Availability, Capacity and Performance Management
  - Continuous Service Improvement
  - Invoicing and Cost Management
  - In-Life provisioning and project services
  - Service continuity management
  - On-site break/fix service and replacement
  - Storage and management of any hot standby and spare hardware
- Active asset lifecycle management, including Configuration Management Database (CMDB) tracking, appropriate refresh and disposal
- Maintenance of a compliant and fully vendor supported network throughout the life of the contract, through regular patching, management and refresh cycle
- Implementation of a connection agnostic WAN "underlay network" with secured internet egress
- Implementation of an Overlay network to enable secured access to the Authority's Azure environment
- Implementation of Secure Remote Access solution
- Wireless data network
  - Initial Wi-Fi refresh at contract start, due to end-of-life of existing equipment in October 2026
  - In line with manufacturer guidance and to maintain a compliant network, an expected Wi-Fi refresh during the initial contract term
- Wired data network
  - Deploy new LAN edge as part of implementation and, in line with manufacturer guidance and to maintain a compliant network, an expected LAN refresh during the initial contract term
- Proof of concept activity (lab or on premise as appropriate)
- Build and test of the network solution
  - Including submission of legal documentation such as wayleaves and permit to work
- End to end acceptance testing, including any software required on Authority managed devices to meet security requirements
- Integration with legacy systems and solutions
- Deployment activity including
  - Installation
  - Configuration
  - Testing

- User migration activity
- Training and knowledge transfer
- Recycling and waste management of all packaging and materials associated with implementation and refresh
- Maintaining and updating BAU documentation
- Holistic, centralised, management approach to include asset management, patching, reporting, BAU engineering support, Provider led service reviews
- Open and customisable network monitoring, administration and management systems to provide the Authority with insight
- Professional Services for the delivery of all of the above
- Call off for additional items for the duration of the contract through formal change control process, supported by a catalogue of services

7.3 Service Duration

The initial term shall be contracted for a period of seven (7) years, commencing on the contract completion date.

The service can be extended for a further forty-eight (48) months of any duration and multiples thereof, at the discretion of the Authority.

An additional period, called the Transition Assistance Period (TAP), of up to twenty-four (24) months, shall be included within the contract terms for any transition arrangements from the Provider to a new supplier. The TAP shall apply at the end of the initial contract term or end of any extension term up to the maximum period. Please refer to subsequent sections on exit transition.

7.4 Technology Acquisition

Providers are advised that the Authority intends to purchase any technology (Hardware, Software, Licences) required for delivery of the new managed service in the lifetime of the contract (implementation and refresh).

The Authority is not expecting the Provider to recover the cost of such purchases through the contract. This approach will enable the Authority to better manage its financial position and provide transparency. These assets will be managed by the Provider through this Managed Network Service.

It is the Authority's approach to align the purchasing to operate 'just in time' in the implementation phase, ordering on a quarterly basis.

7.5 Out of scope

- Azure Landing Zones for servers and networks
- Management of the Authority's Azure, Amazon Web Services (AWS) or other cloud environments
- End user mobile related services, e.g. airtime contracts, handset provision

7.6 Potential Future Scope

- The Authority's Azure based firewalls (Palo Alto)
  - Global Protect Remote Access VPN
  - Azure zone security
- External Connectivity Services (Public Sector Network (PSN), Health & Social Care Network (HSCN), and other Virtual Private Network (VPN) connections the Authority has
- Voice services, e.g. Session Internet Protocol (SIP) Trunks
- "Co-Working Spaces" may be created as part of the Estates Transformation Programme, which will require internet connectivity for tenants of those spaces
- Low Power Wide Area Networking technologies

7.7 Accessibility

The Provider will ensure that its full proposed service, including any proposed third-party software, shall be accessible to all, meeting the Web Content Accessibility 2.2 Guidelines (WCAG 2.2 AA standard) as a baseline and ensure compliance with relevant regulations, for example The Public Sector Bodies Accessibility Regulations 2018. A continuous improvement approach to accessibility shall be applied by the Provider throughout the duration of the contract and an annual statement of compliance to current acceptable Accessibility standards shall be provided to the Authority for review from contract commencement.

The Provider shall ensure that any changes to any aspect of the proposed service, including upgrades will not have a negative impact on accessibility at any time. The Provider accepts that accessibility standards will change over the duration of the contract and through the continuous improvement approach and working with the Authority they shall be expected to always meet these. The Provider shall execute any remedial work required to achieve compliance at their own expense.

If the planned service, as delivered, and any upgrades delivered subsequently under the same contract, are found to be non-compliant against the WCAG 2.2 AA accessibility standard, the Provider will put right any issues, at their cost, before the service or the upgrade is deployed. The service will continue to be compliant with future releases of WCAG as these become available.

8 Service Transition (Implementation) Requirements

8.1 General Requirements

The Provider must offer a comprehensive set of implementation services addressing the full scope of the project.

The Provider must work with the Authority to develop, provide and execute a comprehensive and consultative implementation plan. The plan must ensure a smooth and seamless transition from the incumbent MSP to the Provider without compromising the quality and continuity of the Authority's services, while mitigating against excessive duplicate operating costs. Further detail on when the plan must be provided is within section 8.20. In developing their response, Providers must review the list of sites in Appendix XXXX for current operational hours, determine the most appropriate method of transition and ensure any assumptions are clearly stated.

It is expected that the Provider shall deliver a structured approach to site acceptance, cut over and terminations that streamlines operational processes and contributes to overall cost efficiency.

The expected outcomes for the Authority are:

- Develop and execute a detailed Transition Plan in consultation with the Authority and the incumbent MSP, covering all aspects of the transition, such as governance, roles and responsibilities, communication, staff transfer, knowledge transfer, asset transfer, service delivery, quality assurance, risk management, contingency planning, and financial
- Align the Transition Plan with the Authority's business priorities, operational needs, and contractual obligations, and ensure minimal disruption and impact to the Authority's services and users during the transition period
- Provide dedicated resources, expertise, and tools to support the transition activities, and coordinate with the Authority and the incumbent MSP to facilitate (as appropriate) the transfer of information, assets, and services
- Adhere to the agreed transition timelines, milestones, and deliverables, and report on the progress and status of the transition regularly to the Authority
- Identify and mitigate any risks or issues that arise during the transition and escalate them to the Authority as appropriate
- Ensure that the transition is completed within the agreed budget and scope and achieve the required service levels and quality standards from day one of the new contract

8.2 Scope

The Provider's implementation activities must include the following:

a. Installation, commission and testing of the services including all security and network services proposed as part of the service

b. Integration with existing security and network services & equipment

c. Carry out pre-installation surveys to confirm location of all existing and future equipment (Telco and Provider). Providers are advised that audits of IT equipment spaces at the c50 new sites have been undertaken, and this information will be made available, without liability, to Providers invited to tender

d. Migration and transition period plan

e. Full migration strategy and impact assessment

f. Completion of a System Acceptance Testing (SAT) for sign-off by the Authority.

g. Support of and participation in User Acceptance Testing

h. Wayleaves / permits to work pre-requisites

i. Access and security

j. Background checks of all engineers

k. For each site:

    a. Site survey for each site

        i. Including equipment locations, floor plans, existing services, potential issues

        ii. Audits of APs, switches, utilisation

- Post install Wi-Fi surveys

8.3 Interface to the Authority

The proposed implementation of the project will be managed overall by an Authority Project Manager.

The Authority Project Manager is the single point of contact for all Provider activities during implementation.

8.4 Supplier Responsibilities

The Provider is responsible for the design, supply, installation, and configuration and commissioning of all hardware, software and services to deliver the services.

This responsibility includes integration works relating to existing systems and services.

8.5 Procedures

The Provider must agree all installation and commissioning procedures, configuration schedules and timescales with the Authority’s Project Manager in advance of any work being undertaken.

8.6 Documentation

The Provider must provide full and up to date project documentation covering all aspects of the services and its configuration before, during and on completion of the implementation.

Documentation, including though not limited to the following:

- Project Initiation Document
- High level design
- Low level design
- System Acceptance Testing plan
- User Acceptance testing plan
- Project plan
- Transition / Migration plan
- Exit plan
- Disaster Recovery and Business Continuity plan (including DR test plan)

8.7 Transition (Implementation) Activities

The Provider must liaise with the Authority through its Implementation Project Manager to identify the sites in the transition plan, prepare the communications, liaise with any technical functions and obtain approval from the Authority before bringing a site online in the new environment.

The Provider must prepare the core network services, test and have signed off all design and configuration before any pilot testing can take place. It is anticipated that up to 8 sites will be included within the Pilot phase: 4 existing and 4 new.

Please refer to the implementation scope in section 8.2 for activities required.

8.8 Coordination of Provider Activities

8.9 Implementation Project Manager

The Provider must provide an accredited 'Implementation Project Manager' to work with the Authority's Project Manager.

The 'Implementation Project Manager' must take a leading and proactive role on behalf of the Provider and any sub-Providers and will be an integral member of the Authority's project team.

8.10 Primary Interface

The 'Implementation Project Manager' must be the primary interface for all matters relating to the implementation between the Provider and the Authority (via the Authority Project Manager).

The 'Transition Project Manager' must be responsible for all of the Provider's activities on site including those of its Technical Architect, Lead engineers and sub-Providers.

8.11 Third Party Liaison

The 'Implementation Project Manager' in partnership with the Authority, must liaise, as required, with third parties involved in the project, for example the Authority's facilities management provider.

8.12 Continuity

The ‘Implementation Project Manager’ must remain in post for the duration of the service transition.

However, the Authority reserves the right to request a change of ‘Implementation Project Manager’ if performance is deemed to be unsatisfactory.

8.13 Implementation Project Meetings

Applicable Provider representatives must attend all implementation project meetings reasonably requested by the Authority. These to include:

- Stakeholder Consultation
- Design Meetings
- Implementation planning meetings
- Project progress and review meetings
- Project closure and review meetings

The ‘Implementation Project Manager’ and other applicable representatives must represent the Provider and all its sub-Providers at these meetings.

The ‘Implementation Project Manager’ must attend project meetings (or conference calls) to discuss progress and resolve any issues arising.

It is anticipated that on-site project meetings will be held at least fortnightly during the implementation period with other meetings (or conference calls) to discuss individual aspects of the project held as and when required and at the discretion of the Authority.

8.14 Dates

The ‘Implementation Project Manager’ must proactively advise the Authority’s Project Manager of all confirmed / anticipated activity dates so that the master Programme of Work held can be updated.

8.15 Actions Log

The ‘Implementation Project Manager’ must proactively advise the Authority’s Project Manager of all completed actions so that an accurate Actions Log can be maintained.

8.16 Risk Log

The ‘Implementation Project Manager’ must proactively advise the Authority’s Project Manager of all identified risks so that an accurate Risk Log can be maintained.

8.17 Issue Log

The ‘Implementation Project Manager’ must proactively advise the Authority’s Project Manager of all identified issues so that an accurate Issues Log can be maintained.

8.18 Organisation Chart

Following contract commencement and no later than 6 weeks from this date, the ‘Implementation Project Manager’ must submit an organisation chart showing the position of ‘Implementation Project Manager’ within the organisation and the relationship to Technical Architect, Lead engineers, and sub-Providers.

8.19 Design

Prior to starting work on site, the Provider is responsible for preparing High Level and Low-Level design documents for approval by the Authority. These shall be developed in conjunction with applicable Authority stakeholders representing operational and technical functions.

The ‘High Level Design’ must be an overview of the entire service solution including integration between solution elements and with applicable Authority systems.

The ‘Low Level Design’ must be a detailed technical document that confirms exactly how the services will be architected and configured at day 1 on a per site basis.

8.20 PID and Project Plan

Within four (4) weeks of contract completion, the Provider must prepare a Project Initiation Document (PID) and submit to the Authority. As a minimum, the PID shall confirm the project scope, resources, methodologies and deliverables. The Authority will review this within six (6) weeks from contract completion, with the intent to agree and approve this within eight (8) weeks from contract completion.

The Provider shall be responsible for preparing a Project Plan that shows a phased transition of existing sites and new sites to the new service and align to the timetable in section **Error! Reference source not found.** of this document. Development of the plan will require consultation and input from the Authority and the incumbent MSP, which will be coordinated by the Authority’s project manager. The Provider must ensure that name and designated personnel are available to facilitate agreement of the plan, which must be submitted within six (6) weeks of contract completion with the intent to approve no later than eight (8) weeks from contract completion. The ‘Project Plan’ shall include all implementation activities and confirm dates down to week level and will be used as the project baseline.

8.21 Risk Management

All existing services are classed as a business-critical application for the Authority.

Providers must develop their service transition plan and approach so that the risk of service disruption is minimised.

8.22 Installation Work

8.23 Security

All installation work shall be carried out with a focus on security.

In particular:

- The Provider must always comply with the Authority's security policies, standards and procedures
- All default passwords must be changed before any item of equipment is connected to the network and passwords shall be managed in accordance with Authority policies, NCSC guidelines and accepted best practice
- Any requirement for remote access during the implementation period must be documented and submitted in advance for authorisation (in writing) by the Authority's Project Manager
- The Provider must report any defect in physical security to the Authority as soon as possible following the discovery

8.24 Health & Safety Policy

The Provider must comply with the Authority's Health & Safety policy (see Appendix XXXX) when working on site.

The Provider must supply details of all staff who will be carrying out on-site activities and confirm they are appropriately checked via DBS and other relevant checks as required, and to allow for the management of Authority security pass allocation.

8.25 Site Rules

8.26 Asbestos Register

The Provider will conduct site surveys including accessing and reviewing the asbestos register at each site, to ensure they have fully understood the health and safety aspects each site.

8.27 Providers on Site Rules

The Provider must comply with Authority site rules when working on site.

The rules will be tabled and discussed at the project mobilisation phase.

8.28 Site Access

The Provider must note that the transition of service must be undertaken with minimal disruption to the operation of a site.

Accordingly, all access to site must be pre-arranged and pre-agreed with the Authority's Project Manager. There may be instances where access to site may need to be out of hours dependent upon the site and service.

It is strongly recommended that the Provider uses a dedicated team for site transition for continuity of knowledge, consistency of approach and ease of building access. There may be a requirement to attend a site induction session prior to working on site, Providers shall note that some sites have limited operating hours

The Provider will be required to work according to the detailed project plan agreed with the Authority's Project Manager.

8.29 Health and Safety Operations

The Provider must take on the necessary roles in relation to Construction Design & Management (CDM) Regulations as required by law.

CDM roles apply to works in delivering circuits and any additional data points. Installation works that do not involve construction will require risk assessment and method statements (RAMS) as a minimum if they replace brackets for APs, routers or install switches onto walls etc.

RAMS would refer to as a minimum, Asbestos registers, Authority specific H&S policies, site specific H&S requirements.

The following roles would apply:

- CDM Client: Essex County Council
- Principal Designer: The Provider
- Principal Provider: The Provider
- CDM Designers: Telcos Vendors / 3rd Party suppliers as required to fulfil the contract from the Principal Designer
- CDM Providers: Telcos, Civils, required to install new circuits, replace existing ones

The Provider must produce necessary RAMS which will need to be reviewed and approved by Authority Health and Safety representatives prior to undertaking work on site. Turnaround for such documents will be given approval within 5 working days, subject to no amendments required.

The Provider must make due allowance for this requirement.

8.30 Acceptance Testing

For the new managed network service, it is expected there will be Core System Acceptance Testing (CSAT) relating to the core service elements which are agnostic of site, Site Acceptance Testing (SAT) and User Acceptance Testing (UAT). SAT essentially confirms the site is Ready for Service and after UAT, the site can be Brought into Service.

The Provider shall be responsible for developing acceptance testing documentation and ensuring that this is agreed with the Authority's Project Manager. Acceptance testing criteria for each element of the contract will be agreed with the Provider at the appropriate time (typically within a project framework). Acceptance testing will generally correspond with a project and financial milestone.

The Provider is responsible for testing and proving the functionality of the infrastructure equipment and the deployed configuration to the Authority.

A core element of the testing must be to prove the resilience of the service. Providers must carry out tests that demonstrate that the system will continue to provide full service in the following scenarios:

- Core Resilience Failure Testing
- Connectivity Testing
- Connectivity speed and performance (including QoS metrics)
- Application access tests (in conjunction with the Authority service owners)
- Voice and video tests
- Backbone link failure
- Local equipment failure

8.31 Procedure

Following the completion of the Provider's installation procedures, which must include Provider tests, the service (hardware and software) shall be declared provisionally 'Ready for Service' (RFS).

8.32 Configuration Testing

The Provider is responsible for testing and proving the functionality of the infrastructure equipment and the deployed service to the Authority.

The results of the Provider's tests must be tabulated and included within the documentation to be provided to the Authority upon commissioning of the new service.

The purpose of these tests will be to verify the configuration against the pre-installation expectations and to verify the configuration within the live network.

8.33 Preparation of Test Plans

The Provider must prepare the Configuration and Acceptance test plans where the Authority will, where appropriate, contribute to application specific test plans. Test plans will be prepared in conjunction with the Authority's Project Manager.

The Authority reserves the right to negotiate changes to the test plans as the installation progresses, to reflect changes in the requirement or configuration.

8.34 Attendance

The Provider must provide appropriate on-site resources during the Acceptance Testing activities to ensure they are successfully completed.

The cost for participating in the Acceptance Testing must be included within the installation charges.

8.35 Re-Test Attendance

The Provider must provide relevant on-site resources, at no additional cost to the Authority, during any re-testing activities that are required due to issues with the supplied equipment or services.

8.36 Out of Hours Working

The Provider shall assume the following:

- All non-service affecting installation works shall take place during normal working hours. i.e. during the following times on a normal working day, Monday – Friday, 9am – 5pm. Providers must note that some sites have limited operating hours.
- All service affecting integration works involving the legacy systems and any other significant work that will / may result in any service loss must take place out of normal working hours, taking account of business operational requirements to minimise operational impact. Specific times will be agreed between the Authority and the Provider to minimise impact upon operational services.

8.37 Knowledge Transfer

The Provider must work closely with Authority resources during the implementation activities to facilitate knowledge transfer as sites and services move from Transition to BAU. This must include:

- Solution Management and Monitoring Processes
- Service Escalation and management processes
- Moves, Adds and Changes (MAC) processes
- Updates to the CMDB and adherence to Authority IT Service Management (ITSM) processes
- Support processes and integration with the Authority's service desk
- Solution architecture
- Functionality
- Back-up processes

Overall, these form the basis of an over-arching Operational Delivery Process Document (OPD) which the Provider will provide to the Authority.

8.38 Transfer of Service

Where defined in the migration plan, it will be the responsibility of the Provider to install all the equipment and connect the LAN, ensuring full service end-to-end operation. The Provider must therefore be responsible for interconnecting the new infrastructure equipment with the Authority's existing LAN & WAN cabling and 'Network Services' infrastructure. These works must be undertaken at a time agreed with the Authority and this may be outside normal working hours.

9 Managed Service Requirements

9.1 Overview

The Authority is seeking a suitable Provider to partner with the Authority to provide a new Managed Network Service for the in-scope items.

The Provider must provide, refresh (when needed) and maintain, with full manufacturer backed support, the necessary hardware, software, licenses, and security certificates for the Managed Network Service, including the edge devices (WAN, LAN & Wi-Fi), core network (centralised infrastructure), and central management platform.

The Provider must ensure the Managed Network Service interoperates with the Authority's existing cloud environments (Azure and Oracle) and potential future environments (such as AWS, Google Cloud Platform, etc.) and ensure seamless connectivity and performance across different cloud providers and UK regions.

The Provider must provide proactive and reactive support and maintenance for the Managed Network Service, including incident management, problem management, change management, configuration management, capacity management and service continuity management, and adhere to the Authority's policies and procedures for service delivery and governance, see Appendix XXXX for details.

The Provider must demonstrate innovation and continuous improvement in the Managed Network Service and provide recommendations and best practices for optimising the service efficiency and effectiveness.

The Provider must provide an overall Managed Network Service proposal that meets the Authority's outcomes in:

- **Management**
  - Overall coordination and oversight of the Managed Network Service
  - Ability to respond to the level of change that happens across the Authority
- **Monitoring and Measurement**
  - Continuous surveillance of IT systems and the quantitative assessment of service performance
- **Maintenance**
  - Encompassing regular upkeep, updates, and preventive care of IT infrastructure, software, and systems
- **Managed Service Desk**
  - Single point of contact for all IT-related issues and requests

9.2 Management: Account and Service

Management refers to the overall coordination and oversight of IT services. Key activities include:

- Strategic IT planning and alignment with business objectives
- Service Management in alignment with ITIL © V4

- Change Management
- Incident and Problem Management
- Asset, Configuration and Resource management and allocation
- Knowledge Management
- Governance and compliance activities and cyber security position
- Continuous service improvement initiatives
- Vendor and contract management
- Financial administration and management of the contract
- Risk management and mitigation strategies

9.3 Nominated Individual(s)

The Provider must nominate a named individual(s) to be the Authority point of contact. The named individual will act as a single point of contact for the legal, commercial and operational aspects of the contract.

9.4 Authority

The named individual(s) must have the authority to submit firm quotations on behalf of the Provider.

9.5 Right to Audit

The Authority reserves the right to investigate and audit the Provider's compliance with the required security requirements and standards detailed in this document, against the delivery of the Managed Network Service, and throughout the life of the contract.

The Provider must cooperate fully with any such investigation or audit and provide the Authority with access to its premises, systems, data, personnel and documentation as requested. The Provider must also notify the Authority of any security breaches, incidents or vulnerabilities that affect or could affect the delivery of the services. The Authority may share the results of any investigation or audit with third parties for legal or security purposes.

9.6 Configuration Management

The Provider must maintain a current and accurate CMDB and make it readily available to the Authority through an agreed information sharing mechanism and as a minimum, this shall include:

- All hardware components
- Criticality / Operational Classification
- Logical diagrams
- Data flow diagrams (including list of logical connections to other applications)
- Software information, including version
- Maintain IP management addresses and associated VLANS/VRFs/etc.
- Log configurations maintained in line with good business practises

- End of Service/Support date
- Mapping of services and locations
- Wireless surveys / Heatmaps / Coverage

9.7 Configuration Management Integration

The Provider must maintain a CMDB for the managed network service and integrate it with the Authority’s own system.

Common item, service and system descriptors will be agreed before implementation to ensure that updates to the CMDB is reflected universally in the respective systems.

Any changes made to the CMDB will be audited and be inspected in real-time either directly or through integration.

9.8 Continual Service Improvement (CSI)

The Provider must apply the process of identifying and implementing improvements to the service, quality and efficiency throughout the service lifecycle. The Provider must provide the following requirements:

- Establish a register to record and track improvement opportunities and initiatives, aligned with the Authority’s objectives and priorities and with regard to:
    - Services used by the Authority
    - Products used by the Authority
    - New Services and Products that may be of potential interest to the Authority
- Conduct regular service reviews and audits to assess the performance, satisfaction, risks, and issues of the service delivery and identify areas for improvement.
- Implement improvement actions and monitor their outcomes and benefits, using agreed metrics and indicators.
- Report on the progress and results of CSI activities, highlighting any achievements, challenges, or recommendations.
- Collaborate with the Authority and other stakeholders to share best practices, lessons learned, and feedback for CSI.
- Improvement of the technical and functional services and solutions provided
- Improvement of the maintenance and support service provided

9.9 Monthly Performance Reviews

The nominated individual(s) will lead monthly meetings with the Authority to review performance for the preceding period, this must include as a minimum, but not be limited to, service level performance (KPIs), incidents during the period, change activity, capacity planning, financial position, security considerations/awareness, continuous improvement opportunities, project progress (where applicable). risks, cashable and non-cashable benefits, Social Value and Carbon reduction commitments.

The meetings will be on-site at the Authority, unless by agreement to vary e.g. to a Teams meeting, and held within 10 working days of the end of the previous period. No less than 3 working days before the meeting, the Authority shall be provided with the relevant performance information and reporting. The meetings shall be minuted by the Provider and the record of the meeting shall be issued within 5 working days of the meeting.

9.10 Quarterly and Bi-Annual Performance Reviews

The nominated individual(s) will lead quarterly and bi-annual meetings with the Authority and attended by Senior representatives of the Authority and the Provider. Quarterly relationships meetings will consider 6 monthly forward planning/roadmap and escalation and summary of operational matters arising from monthly meetings

Bi-Annual meetings will align with the strategic goals of both the Authority and the Provider to develop a joint strategic plan.

9.11 Escalation Procedures

The Provider must have a formal escalation procedure that will allow the Authority to escalate issues if it is not satisfied with any aspect of the performance of the service including Provider personnel.

9.12 Sub-Contracting

The Provider must detail any aspect of the services that is not directly supplied by the Provider and is sub-contracted to a third party.

9.13 Working with Others

The Provider must work and co-operate with others involved in the support of the Authority's IT infrastructure, such as, but not limited to, the Facilities Management supplier.

During the transition phase, this cooperation will involve liaising with the incumbent MSP to facilitate the migration of services.

9.14 End of Contract – Exit Plan

The Provider must plan and execute a smooth and seamless transition of the contract at the end of the contract term or extensions, in consultation with the Authority, covering all aspects of the service, resources, risks, costs, and quality.

The outcomes for exit transition are:

- Develop and execute a detailed Exit Plan in consultation with the Authority, covering all aspects of the transition, such as governance, roles and responsibilities, communication, staff transfer, knowledge transfer, asset transfer, service delivery, quality assurance, risk management, and contingency planning
- Align the Exit Plan with the Authority's business priorities, operational needs, and contractual obligations, and ensure minimal disruption and impact to the Authority's services and users during the exit period
- Identify sufficient resources, expertise, and tools to support the transition activities to facilitate the transfer of information, assets, and services
- Identify any risks that are identified throughout the contract that arise during an exit and escalate them to the Authority

The Exit Plan must be provided by "Readiness to Deploy" and be updated and reviewed with the Authority throughout the contract term. This will be annually, as a minimum, and following any material change to the managed network service.

9.15 Documentation and Diagrams

The Provider must, in an agreed shared area owned by the Authority, provide detailed and editable documentation (in Microsoft Office document formats) of the service design, configuration, and integration throughout the contract term, including any changes that take place which will be updated within two (2) weeks of any change.

The Provider must also provide all documentation to the Authority on request. The documentation will also form part of the current state information for the transition pack.

9.16 Asset Management

The Provider must maintain, within the CMDB, an asset register of all physical and digital artifacts provided as part of the Managed Network Service. The asset register must comprise hardware details, software versions, licenses etc. and be provided to the Authority as part of the Provider's regular performance reporting.

9.17 Service Requests

The Provider must be able to work with the Authority to support changes to the Service through Service Requests. Service Requests comprise of:

- **Standard request**: Defined non-chargeable requests for service which form part of a Standard Operating Procedure (SOP), for example, a firewall rule change, providing new members of Authority staff with access to tooling
- **Minor Project**: A project that does not require multiple resource skill sets to complete the impact assessment and can be delivered within 10 Working Days or less. It may also include Catalogue items and rate card resources (excluding Impact Assessment) at no extra cost to the Authority
- **Complex Project**: A project that requires multiple resource skill sets to complete the Impact Assessment and over 10 or more days of resources to deliver
- **Technical Collaboration**: A collaborative request to aide in the development and delivery of the service. Resources on the rate card or seeking Subject matter expertise.

For Minor, Complex and Technical collaboration requests, a technical Impact Assessment may be required. This must detail, as a minimum: purpose, scope, risks, dependencies, mitigation, testing, roll back, outcome.

The nominated individual(s) will be responsible for supporting the Service Requests within agreed service level timelines. All time is specified in working days unless otherwise stated.

The Provider must ensure it is possible for the Authority to track real-time progress of Service Requests from inception through to closure.

The Provider must be ready to support Service Requests from the Readiness to Deploy milestone.

9.18 Service Catalogue

During the mobilisation period, the Provider must develop a service catalogue that can be used to for future orders during the contract period, e.g. user licences, commodity items, additional access points, etc. This catalogue shall be reviewed annually to demonstrate value for money is being obtained for the Authority.

9.19 Monitoring and Measurement

9.20 Comprehensive Monitoring and Measurement Platform

The Provider must deploy a comprehensive and continuous monitoring, administration and measurement platform that monitors, administers and measures all aspects of the Managed Network Service.

The monthly monitoring periods shall be reflective of the calendar month. Rolling periods will not be accepted.

9.21 Real-time Monitoring

The Provider must monitor and measure all aspects of the new Managed Network Service collecting applicable data that must be presented to both the Authority and Provider network support staff as a real-time dashboard.

The real-time view must display the status of all network and security components in a manner which represents both the geographic and topographic characteristics of the network and allows IT support staff to drill down to more granular detail.

In addition, the location and expected levels of service for incidents and performance issues must be easily identifiable by location and, where applicable, signal strength and coverage can be accessed by the Authority's service desk to initially triage incidents.

9.22 Alerting and Notification

Ongoing alerting and notification thresholds must be continuously reviewed and updated/created to best reflect and maintain the network, the Provider must alert the Authority of those thresholds that have been breached.

The Provider must promptly and effectively notify the Authority in relation to significant and/or major incidents both within and outside of working hours. The notification process will include the Authority's SOC for Cyber related incidents.

9.23 Tracking and Analysing KPI and SLAs

The Provider must be responsible for tracking and analysing the key performance indicators (KPIs) and service level agreements (SLAs) of the Managed Network Service as per the performance management schedules defined in Appendix XXXX.

The Provider must provide access to the tools or portal that enable the Authority to view the insight and performance data of the Managed Network Service. The Provider must ensure that the tools or portal are user-friendly, meet the Authority's accessibility standards, secure (with Authority Single Sign-On (SSO) authentication) and reliable.

The Provider must also provide training and support to Authority staff on how to use the tools or portal effectively, this shall be undertaken prior to the new managed service 'going live', and whenever there is a significant change to the tools or portal. Future Authority employees must be able to refer to the Provider's detailed documentation for training.

9.24 Generating Reports and Insights for Continuous Improvement

The Provider must generate reports and insights to assist in identifying service improvements of the Managed Network Service, that will help support the Authority's strategic aims.

- Service availability and uptime reports
- Service utilisation and capacity reports
- Service quality and customer satisfaction reports
- Statistics per Site, e.g. Wi-Fi utilisation
- Service security and compliance reports

Additional reports and insights can be derived from the list in section 9.25.

9.25 Performance Monitoring Reports

The Provider must prepare monthly performance reports in the first week following the end of the previous period. The reports must include, as a minimum, the following:

- Availability (Actual versus Target)
- Utilisation - bandwidth and application
- List of faults, resolutions and resolution times (target versus actual)
- Proposed changes and outcomes (Change management)
- Unresolved issues and faults
- General observations
- Recommendations
- Patch Management including asset lifecycle management
- Versioning, including reviews of software baselines
- Any failures including remediation plans
- Finance Review (see 9.26 for further details)
- Action/Issues/Problem/Risk tracking

An automated weekly summary highlight report must also be issued by the Provider, including such items as; Top 5 circuit utilisation, Top 5 Site with Errors/Issue, Top 5 Trending Alerts, Top 5 SLA Breaches for the Week.

9.26 Billing

The Provider must deliver and operate a clear, insightful and transparent invoicing and billing platform encompassing all the service categories which shall be developed and updated as required. For example, on quotes, invoices and billing platform, WAN links/lines shall show technical specifications and list a site name, full address including street name and postcode.

The Billing platform must be capable of incorporating the Authority's codes/site id so that charges can be attributed to the appropriate party.

The Authority requires the ability to understand the granular detail behind the high-level numbers. It is expected that this will form part of the Finance Review.

The Provider must supply a portal providing access to the invoicing and billing platform.

The Provider must allow access to their billing specialists (via email, phone & meetings) to answer questions about the Authority's invoices and payments.

The Provider must provide the Authority with detailed billing information to support and evidence hardware for capitalisation along with any other documentation required to support the Authority's financial regulations and any other information to support statutory requirements.

The invoicing and Billing platform must be able to export information in a standard format (i.e. it must be compatible with Microsoft Office interchange formats, csv, XML and future standards – to support integration with the Authority's finance system).

Billing must be provided in a timely manner, no later than 2 months after completion of chargeable service requests.

9.27 Maintenance

9.28 Planned Outages

The Provider must ensure that any changes to the network configuration, hardware, software, or firmware are done in accordance with the Authority's change management policy and procedures (see Appendix XXXX) and in collaboration with the Authority's Supplier and Service Assurance (SSA) team.

The following requirements for change management shall apply:

- The Provider's nominated individual(s) must attend the Authority's Change Advisory Board (CAB) meetings for all changes that may affect or impact on the operation of the Managed Network Service
- Detailed Request for Change (RFC) must be proposed for each change, including the impact assessment, risk analysis, rollback plan, testing plan, and approval status
- The Authority currently host a twice-weekly CAB and the Provider must ensure at least 1 week notice is provided to allow assessment of RFCs and communication, to have taken place
- Written approval must be obtained from the Authority before implementing any change that may affect the availability, performance, security, or functionality of the network services
- Where a change is determined to be non-service impacting and/or low-risk or an emergency, the change shall, by agreement, be made within business hours. All

other changes must be undertaken outside of core business hours unless otherwise agreed

- Notification of completion and post implementation reporting must be provided to the Authority including the results of the testing and verification, within one working day after the change
- Documentation must be updated with changes to the network inventory, configuration, and topology diagrams to reflect the change within 2 weeks

9.29 Scheduled Updates and Patches

All updates and patches to the Managed Network Service and any associated system the Provider is to be responsible for, that has a potential service impact to Authority systems and services, must follow the steps outlined in the Planned Outages section.

9.30 Hardware Support

The Provider must maintain manufacturer support for hardware on all in scope equipment of the Managed Network Service.

- Reduced risk of hardware failure and service disruption
- Guaranteed availability of spare parts and replacement devices
- Access to technical expertise and troubleshooting from the manufacturer
- Compliance with Authority obligations, such as, but not limited to, ISO27001, PSN and HSCN standards and NCSC Cyber Essentials and any further iterations or new legislation, for example the forthcoming Cyber Security and Resilience Bill

9.31 Software Support

The Provider must maintain manufacturer support for software on all in scope equipment of the Managed Network Service.

- To ensure compatibility and interoperability with other devices and systems in the network
- To benefit from the latest features and enhancements that improve performance, security, and functionality
- To ensure that updates for potential future vulnerabilities are being received/provided by the manufacturer
- To comply with the manufacturer's warranty and service level agreements
- To reduce the risk of downtime, data loss, or breaches due to outdated or unsupported software
- To leverage the manufacturer's expertise and technical support for troubleshooting and resolving issues
- Compliance with Authority obligations, such as PSN and HSCN standards and NCSC Cyber Essentials and any further iterations or new legislation, for example the forthcoming Cyber Security and Resilience Bill

9.32 Preventative Maintenance

To ensure the optimal performance and security of the hardware and software, the Provider must perform regular preventative maintenance activities, such as updating the software, applying patches, scanning for malware, and testing the functionality.

- The Provider must schedule the preventative maintenance in advance, and this must be agreed via the Authority's change management process. The activity shall aim to minimise the risk of disruption or inconvenience
- The Provider must document the preventative maintenance procedures and provide a report of the results and any recommendations for improvement
- The Provider must comply with the manufacturer's guidelines and best practices for preventative maintenance

9.33 Repair and Replacement of Faulty Equipment

Through proactive monitoring, the Provider must identify hardware that needs to be repaired or replaced. The Provider shall follow the requirements below:

- The Provider must notify the Authority of the issue and the proposed solution as soon as possible, in the monthly review meetings or sooner if the issue has urgency
- The fully supported equipment must be repaired by the Provider or repaired or replaced under vendor Return Merchandise Authorisation (RMA) within the costs of the Managed Network Service
- Replacement equipment must be provided in advance of removing the faulty equipment with either spares from the Provider or direct from the vendor
- Replacement equipment must have the same manufacturer hardware and software support and maintenance until at least the end of the Managed Network Service contract (this includes any extension period), unless the Authority agrees to a different option
- The Provider must obtain Authority approval through change management process before proceeding with the repair or replacement
- The Provider must use the same or equivalent hardware as the original one, unless the Authority agrees to a different option
- The Provider must complete the repair or replacement within the designated SLA parameters
- The Provider must test the repaired or replaced hardware and ensure that it meets the specifications and standards of the original one

9.34 Managed Service Desk

9.35 Service Desk

The Provider must provide the Authority and its staff with direct access to a Service Desk 24 hours per day, seven days per week and 365(6) days per year. The Provider must provide a single Managed Service Desk for all elements of the service.

The Provider must maintain an ITSM platform for the managed network service and integrate it with the Authority's own system for ticket alignment/synchronisation. This will enable the Authority to track incidents and project requests.

Common item, service and system descriptors must be agreed before implementation to ensure that updates to one ITSM are reflected in the respective systems.

Any changes made to the ITSM will be audited and be inspected in real-time either directly or through integration.

9.36 Service Desk Portal

The Provider must provide the Authority with direct access to an online Service Desk 24 hours per day, seven days per week and 365 days per year.

Phone access to the service desk will be provided and all service desk calls for support will be in English.

9.37 Named Contacts

The Provider must only accept support calls from an agreed list of Authority employees to be defined, stored, and maintained in the Provider's ITSM, to ensure approved contacts are easily known.

9.38 Service Level Agreement

A Service Level Agreement has been proposed in Appendix XXXX for review and acceptance by the Provider.

The Provider must be proactive in the delivery of its services to the Authority's with proactive notifications of major issues and incidents out of hours.

9.39 On-site Accommodation

Accommodation will be made available at County Hall, should the Provider wish to utilise it in the delivery of their proposed Service.

9.40 Expected Service Level Outcomes

The Authority requires that the new Managed Network Service is supported by a comprehensive support package owned and managed by the Provider.

The Provider must be proactive in supporting the Managed Network Service by taking ownership of critical support elements outlined below and encompassed within this specification:

- Implement continuous Monitoring
- Adhere to Key Performance Indicators
- Set up Alerting and Integration with 3rd party systems
- Implement Real-time Dashboards
- Conduct Regular Reporting
- Use Synthetic Monitoring
- Implement Log Analysis
- Conduct Root Cause Analysis
- Set up Service Level Objective Tracking
- Implement Capacity Planning
- Conduct Performance Testing
- Conduct Application Performance Monitoring
- Monitor External Dependencies
- Implement User Experience Monitoring
- Lead on network related Major Incidents (MI) with a Major Incident Manager role

9.41 Fault Reporting Service

The Provider must operate a standards-based monitoring and alerting service that is able to receive fault and incident reports and assistance requests on a 24/7 basis.

Fault, incident and assistance requests shall be responded to on the basis of the Hours of Cover.

Out Of Hours service outages shall be restored by the start of the next business day.

9.42 Major Incidents

The Provider must respond to Major Incidents as they arise and provide timely and effective solutions to close the vulnerability and restore the service as soon as possible.

The Provider must, as part of the Authority's Major Incident management process immediately alert the Authority through an agreed contact process. These alerts can be, but not limited to, early warnings, potential threats and actual incidents.

The Provider will need to be part of the Authority's resolver team, in the event of a Major Incident where the root cause is not determined.

The Provider must communicate with the Authority and other relevant stakeholders throughout the resolution process and provide a root cause analysis and a report of the incident after it is resolved.

10 Overarching Security Requirements

The Provider must, wherever possible, ensure security is non-intrusive from a user's perspective. It must be easy to authenticate on to the service to access applications seamlessly and securely without compromising the network security or performance.

10.1 Security Standards

The Provider must comply with relevant security standards and best practices throughout the duration of the contract, from the outset of the contract this must include ISO/IEC 27001, Cyber Essentials Plus, and NCSC Cloud Security Principles.

The Provider must ensure that any systems and services it utilises as part of its solution shall conform to relevant security standards such as, but not limited to, NCSC, NIST, CIS, and ISO27001.

The Provider must provide proof of certifications upon renewal, be that annually or as required by the standard.

Where standards evolve, update or are replaced, the Service must ensure compliance with the new equivalent standard. Providers must advise the Authority of any potential impact of doing so and timescales for achieving compliance. Such activities shall be treated as a Provider initiated Change Control.

On an annual basis as part of a service review meeting, there will be a formal review of required security standards between the Provider and Authority to determine if any changes are needed.

10.2 Security Operations

The Provider's proposed Managed Network Service must:

- Operate a bi-directional relationship with the Authority's existing SOC, which includes third-party organisations, and to support the investigation and remediation of cyber alerts from either party
- Operate a policy management platform that can apply consistent and granular network policies and access rules for users and devices to cloud applications, based on their identity, role, location, and device type
- Have a unified platform that can integrate with the Authority's existing SOC and ITSM tools, as well as provide visibility and analytics for the network traffic and security events.

10.3 Security and Compliance

The Provider will ensure the Managed Network Service conforms to recognised best practice and provide sufficient control, visibility and other capabilities as necessary to support the Authority in achieving compliance with standards and frameworks including, but not limited to: ISO27001, PCI-DSS, Cyber Assessment Framework (CAF) and Cyber Essentials Plus.

10.4 Data Sovereignty and Jurisdiction

The Authority must understand where data is transmitted, processed and stored. Cloud security and networking offered by the Provider must choose hosting regions aligned with UK data sovereignty requirements.

10.5 Integration and Interoperability

The Provider must ensure that the Managed Network Service seamlessly and securely connects to the Authority's SOC and other nominated third-party applications and systems as required.

10.6 Change Management

The Provider must ensure that security is integrated into every aspect of the change management process, to protect the confidentiality, integrity, and availability of the Managed Network Service and the Authority's data and systems. The Provider must:

- Provide a detailed change management plan that outlines the roles and responsibilities, procedures, timelines, cost and communication channels for any changes to the Managed Network Service
- Conduct regular reviews and audits of the change management process to ensure its effectiveness and compliance with the Authority's policies and regulations
- Follow the Security by Design principles and demonstrate the change has been reviewed so that it does not impact on the security of the solution by maintaining compliance with the relevant security standards including Cyber Essentials Plus, ISO 27001, NIST, and PCI-DSS when implementing any changes to the Managed Network Service
- In accordance with NCSC best practice guidance at the time, the Provider will ensure that the service receives patches/updates within 14 days of release, this shall apply to any classed as Critical or High Risk by the vendor, or vulnerabilities with a CVSS v3 base score of 7 or above (based on NCSC guidance at the time of writing this document)
- Conduct risk assessments and security testing before, during, and after any changes to the Managed Network Service, to identify and mitigate any potential threats or vulnerabilities
- Implement appropriate security controls and measures, such as encryption, authentication, authorisation, logging, monitoring, and backup, to prevent unauthorised access, modification, or loss of data and services
- Provide clear and timely security updates and alerts to the Managed Network Service users and administrators and advise them on the actions to be taken in case of any security incidents or breaches

10.7 Governance and Policy Frameworks

The Provider must align access controls, data retention policies, and usage guidelines in line with the Authority's security and operational requirements.

Relevant governance and policy frameworks that the Provider must adhere to include:

- Information Security Policy, which defines the roles and responsibilities of information security management, the principles and objectives of information security, and the standards and procedures for information security
- Data Protection Policy, which sets out the legal obligations and best practices for processing personal data in compliance with the Data Protection Act 2018 and the General Data Protection Regulation (GDPR)
- Acceptable Use Policy, which specifies the rules and guidelines for using the Authority's IT resources, including the Managed Network Service, in a responsible and ethical manner
- Business Continuity Policy, which outlines the framework and arrangements for ensuring the continuity of critical business functions and services in the event of a disruption or disaster
- Disaster Recovery Policy, which defines the roles and responsibilities for ensuring the restoration of IT systems and data in the event of a major incident or failure that affects the normal operation of the Authority. The policy also establishes the minimum standards and procedures for disaster recovery planning, testing, and reporting

10.8 Security Monitoring Performance Requirements

The Provider must ensure the managed network service provides the following:

- Collection of logs from various sources, such as firewalls, servers, applications, and devices and that can be fed into the Authority's SIEM to align incidents
- Configuring alerts and notifications for potential security incidents, anomalies, or breaches based on predefined rules and thresholds
- Reporting and documenting any security incidents or issues and conducting root cause analysis and lessons learned to prevent recurrence and improve security posture

10.9 Comprehensive Security Assessments

The Provider must conduct security assessments as follows:

- Provider must conduct a comprehensive security assessment of <u>its own</u> IT infrastructure and systems, covering all aspects of physical, technical, and administrative security controls, at least annually or after any significant changes or updates
- Provider must use a NCSC CHECK accredited third-party provider to conduct the comprehensive security assessment, in addition to its own internal assessment
- Provider must conduct an annual review of the managed network, including firewall rules, and undertake vulnerability and penetration testing, along with attestations for standards including PCI-DSS, supporting the Authority with PSN compliance, and other standards that may apply through the duration of the contract

- Provider must use a NCSC CHECK accredited third-party provider to conduct the annual reviews and will present the documented and unredacted results for review by relevant Authority stakeholders
- Provider must implement the recommendations and remediation actions from the comprehensive security assessment report within two (2) months of receipt and monitor and report on the progress and effectiveness of the implementation
- Provider must maintain an up-to-date security risk register and action plan based on the findings and recommendations of the comprehensive security assessment, and review and update it regularly to reflect any changes in the threat landscape, business needs, or regulatory requirements

11 Core Network (Centralised Infrastructure)

11.1 Core Network Requirements

The Authority requires a flexible and core network solution that can support the delivery of cloud-based services from multiple providers for staff and users working on-site or remotely.

The solution must provide consistent network policies and access rules for all users, regardless of their physical location or device type.

The Provider shall provide components for secure connectivity that work together to provide a comprehensive approach to network security and performance optimisation, suitable for modern, distributed organisations with diverse IT environments. Components include, but not limited to:

- Wide Area Network optimisation to improve network performance, application access and performance and management across geographically dispersed locations
- Cloud Security Gateway to act as an intermediary between users/devices and cloud applications, enforcing security policies and monitoring usage
- Identity-Based Access Control to require explicit verification and authorisation for users and devices to access resources, regardless of their location
- Web Traffic Security to filter malicious content from user-initiated internet traffic and enforces web access policies
- Cloud-Based Network Security that provides firewall capabilities and other security features delivered from the cloud
- A system that monitors network traffic for suspicious activity such as intrusion and takes action to prevent potential threats
- Domain Name System (DNS) Protection that guards against DNS-based threats and malicious activities
- Distributed Denial-of-Service (DDoS) Protection that detects and mitigates large-scale attacks that aim to overwhelm and disrupt the network availability or performance
- A Unified Management Platform for controlling and administering all security and networking components.

11.2 Core Network Performance

11.3 Resilience and Availability

The Core Network must be resilient and available to all users irrespective of individual site issues. The solution must be resilient to single point of failure issues and available 24/7/365 at the Service Level detailed in Appendix XXXX.

11.4 Business Continuity and Disaster Recovery

The Solution must offer seamless high availability for all core elements to ensure continued network operation in the event of any single core component loss.

The Core and overall solution must be able to mitigate issues through a gradual degradation of service to maintain continuity of the business.

In the event of a disaster and the service requires restoration due to data loss or compromise, the Provider must have a robust Disaster Recovery Plan and have sufficient back-up and recovery capabilities.

11.5 Scalability and Flexibility

The Core must be flexible and scalable to support the users of the solution and based on the user and application experience.

Individual sites have specific requirements for the number of users they support, applications used and public users however, the Core must be sized appropriately to meet the demands of the service and support scaling down as well as up. Consider the following for the core network:

- Be designed to support high availability and redundancy for critical services and applications
- Be able to dynamically adjust the bandwidth allocation and routing based on the traffic load, priority and quality of service requirements
- Be able to integrate with multiple WAN technologies and providers, such as broadband, cellular, satellite, dark fibre, and other relevant connectivity technology available today or in the future
- Be able to support secure and seamless connectivity for remote users and devices, irrespective of the underlying technology
- Be able to provide visibility and analytics for network usage, trends and issues
- Be able to automate and orchestrate the configuration, provisioning and troubleshooting of the network components and services

12 WAN Service Requirements

The new WAN Service must operate separate underlay and overlays, following software defined principles. The WAN Service must support all in-scope Authority sites and their operations.

As the Authority has moved its data centre operations to IaaS, delivering applications and services via cloud landing zones and SaaS, the new network must be designed with security at the heart and be cloud centric with no reliance on any Authority location.

WAN circuit bandwidth allocated to each site must be based on user and application experience.

The Provider must demonstrate that the new service can deliver appropriate bandwidth consistently to all sites or, where currently not available, Providers must detail any plans for migration of sites towards a higher speed delivery.

Key factors for the new service include security, flexibility, performance, availability, resilience, scalability, and support services.

12.1 WAN Underlay Requirements

12.2 Connectivity

The Provider must deliver business grade universal connectivity with SLAs based on individual site requirements and be agnostic to any connectivity medium.

The connectivity bandwidth requirements must be linked to user and application experience.

12.3 Delivery

The Provider must provide a managed service for the delivery of WAN underlay, access circuits, that meets the Authority's needs for quality, reliability, scalability, and flexibility. The Provider must list out change management activities in provision of the connectivity, e.g. any Excess Construction Charges, etc.

12.4 Protocol Support

The underlay network must support end-to-end encryption protocols, such as IPsec or TLS, and allow permissible end-point devices to establish secure tunnels across different networks.

12.5 Monitoring and Performance

The Provider must utilise appropriate tools to monitor performance and experience of each site's connection.

Being proactive in the management of the underlay, the Provider must suggest improvements and enhancements and identify any issues or anomalies at regular reporting periods.

12.6 Flexibility and Scalability

The Authority's estate constantly evolves as services are developed added or removed. The Provider's solution must be flexible to add and remove sites as required and be manageable through standard operating procedures defined within the Operational Delivery Process Document (OPD).

Sites must be scalable to deliver the required bandwidth and performance based on the user and application experience. Each site shall have a baseline for the number of users and applications that are supported and, have flexibility and scalability to meet the demands of the service.

12.7 WAN Overlay Requirements

The Provider must utilise a scalable Overlay Service for the WAN that enables the Authority to securely connect its end user devices, sites and applications over the top of any WAN Underlay or home internet connection.

12.8 Overlay Connectivity

The Provider must provide 'universal connectivity' enabling devices and users to connect to the Authority's network from any Authority premises or remote location.

Sites' WAN edge equipment must be sized to meet the user and application experience required.

The user experience for Remote Users must be indistinct from on-site users.

12.9 Security

The Provider must provide end-to-end encryption of the overlay traffic using current industry-standard protocols and algorithms, including, but not limited to, IPSec, AES, and SHA and consideration of emerging future encryption standards such as CRYSTALS-Kyber (FIPS 203). Through the duration of the Contract, the Provider must ensure that the baseline adjusts to new and retiring standards.

In addition, the Provider must provide:

- Secure authentication and authorisation of the overlay devices using certificates, tokens, or other methods to prevent unauthorised access or tampering
- Advanced threat detection and prevention capabilities, such as antivirus, firewall, IDS/IPS, sandboxing, etc., to protect the overlay network from cyber attacks
- Visibility and reporting of the security events and incidents on the overlay network, such as alerts, logs, audits, etc.

12.10 Management

The Provider must ensure the overlay devices are configured and operated in a coordinated and efficient manner, as well as track the health and performance of the network. The devices must also enable easy and remote provisioning and management.

The Provider must enable a read-only view for the Authority to view policies, rules, and settings for the overlay service in a centralised and user-friendly interface, such as QoS profiles, firewall rules, security parameters, application priorities, etc.

12.11 Cloud Integration

The Provider must provide secure and seamless connectivity between the overlay and public cloud services, such as Microsoft Azure (where Authority applications are hosted), Amazon Web Services, Oracle Cloud and Google Cloud Platform.

The Provider must propose the best combination of hardware and software solutions that can meet the requirements for the WAN overlay service, as well as the cost and timeline for the deployment and maintenance of the infrastructure.

12.12 Monitoring and Performance

The Provider must provide comprehensive monitoring and analytics in line with the overall monitoring, management and measurement platform to monitor and troubleshoot the overlay service in real time, as well as generate reports on the network performance, usage, and availability.

12.13 Segmentation

The Provider must provide a design for the Managed Network Service that segments logical networks to isolate, secure and prioritise different types of traffic and devices on the WAN. The Provider must propose a network virtualisation solution that supports the Authority's requirements for security, scalability, and flexibility.

12.14 Network Performance

The new Managed Network Service must support latency sensitive applications such as real-time voice and video applications, telemetry applications allowing the prioritisation of different types of traffic over the WAN, ensuring that the most critical applications and services receive the highest level of performance and availability.

The Provider must provide a QoS policy that aligns with the business needs and objectives of the Authority, as well as the technical specifications of each site grade.

As a minimum the network must be designed to meet the following criteria:

- Support IEEE 802.1x
- Support emergent technologies
- Capable supporting all security requirements of the Authority
- Capable carrying data voice and video class traffic
- Capable carrying multicast traffic
- Resilience and redundancy provided within the network links and network equipment comprising the WAN

12.15 Application Optimisation for Microsoft Teams

The Provider must optimise the WAN to transport Microsoft Teams traffic from users on the network to Microsoft's network.

12.16 Network Optimisation for Microsoft 365 Applications

The solution must be optimised to transport Microsoft 365 application traffic from users on the networks to Microsoft's network.

12.17 IP Addressing

In conjunction with the Authority and as part of HLD development, the Provider will propose an IP addressing scheme which should not restrict a new infrastructure design or implementation.

Consideration will be given to any re-addressing and any associated disruption this would cause. If any re-addressing is required under a new WAN deployment, then the Provider will be responsible for undertaking any IP addressing changes needed to support the new infrastructure.

Support for geolocation and use of the Authority's public IPv4 address range will be reviewed as part of HLD development.

13 Wi-Fi and LAN Service Requirements

13.1 Wi-Fi Infrastructure

The Provider must consider the Authority's Wi-Fi first approach as part of its digital transformation across its estate.

The existing Wi-Fi solution is coming to the end of its supported life in October 2026 and as such will need to be replaced during the transition.

Appendix XXXX lists the current number of APs and quantities at each site and overall.

As part of the Authority's transformation and estates strategy, it can be expected that there will be changes to the quantities of APs required.

13.2 Connectivity

The Provider must propose a solution that enables users to connect using wireless connectivity and users/devices shall be able to roam between wireless access points within a location with no disruption to service.

The Provider must ensure:

- Sufficient bandwidth is available on the WAN of each site to handle peak user loads and data-intensive applications
- Seamless roaming between access points and sites for uninterrupted connectivity
- Coverage in all required areas
- Integration with Microsoft Teams for location tracking with emergency calling

Providers shall work on the premise of an initial replacement in the same location as an existing AP, though location optimisation may be required as part of a post-installation coverage survey.

The Authority has a small number of locations, such as waste sites and country parks, where external coverage may be required, and potentially the need to link on-site buildings via wireless. The Provider must take this into consideration when developing their solution.

13.3 Standards

In support of inclusion ambitions, the Authority needs to ensure that technical barriers to using the Wi-Fi service are as low as possible, potentially requiring support for devices with older Wi-Fi standards.

In general, the solution must support the following Wi-Fi standards:

- Wi-Fi 6e / 802.11ax or Wi-Fi 7 / 802.11be (subject to ratification, expected late 2024)
- Backward compatibility with older Wi-Fi standards (802.11a/b/g/n/ac)

The Provider must standardise on access point models, with exceptions made in agreement with the Authority, e.g. for external coverage.

13.4 Security

The solution must provide a secure connection for devices with full client isolation.

The solution must be inherently secure and compliant to the current and relevant NCSC guidelines and include:

- WPA3 encryption 'ready' for the highest level of Wi-Fi security
- Integration with network security infrastructure (firewalls, intrusion detection systems)

13.5 Management

The Provider must use a centralised management system that is not dependent on physical data centres and has automation and orchestration capabilities.

The Provider must provide:

- Real-time monitoring and analytics for network performance and user and application experience
- Automated alerts for network issues or security threats
- Remote troubleshooting and configuration capabilities
- Live coverage 'heatmaps' that can be viewed by the Authority
- Integration with existing IT service management tools

The Provider must ensure there is no single point of failure within the wireless solution comprising of management, monitoring and control.

13.6 Segmentation and Authentication

The Provider must propose a Wi-Fi solution that separates the required personas and IoT devices into different network segments.

The solution must provide:

- Integration with central authentication services for seamless public sector guest access
- Support for various authentication methods (e.g. 802.1X, captive portal, social login)
- Role-based access control to restrict network resources based on user type

13.7 Public Wi-Fi

The Provider must provide a fully supported Public Wi-Fi service to the general public that is independent, operationally, from the Authority.

- The service shall be owned, branded, operated and fully supported by the Provider
- Public Wi-Fi must be made available free of charge to the end user
- The Authority will not support, or service end user requests related to Public Wi-Fi

- The same physical infrastructure could be used to deliver Public Wi-Fi as the new Wi-Fi solution, with bandwidth management to ensure no degradation of service to Authority users at the location
- The Provider should identify and present any opportunities for commercial advantage with the service, for example, advertising on log-in screens/captive portal screens
- Provide detailed statistics of user engagement, usage and issues of Public Wi-Fi as part of the monthly reporting and general managed service review meetings
- Public Wi-Fi will be required to enforce Prevent and other content/acceptable usage policies appropriate for a public service
- The Provider must respond directly to police investigations and requests for information, when instructed

13.8 LAN Infrastructure

In delivering the new Managed Network service, the Provider must implement new LAN equipment as part of transition/implementation activities and, subject to when End of Life/Software Support (EoL/SS) is reached for the equipment, refresh the LAN equipment.

The expected quantities for the requirements are provided in Appendix XXXX.

As part of the Authority's transformation and estates strategy, it is anticipated there will be a change in the future number of LAN switches required.

13.9 Connectivity

The Provider must provide a LAN that has:

- High-speed Ethernet connections (minimum 1 Gbps and potential 2.5 Gbps for Wireless APs at County Hall and Tier 1 locations)
- Support for Power over Ethernet (802.3af/at/bt) to power Wireless Access Points, IP phones, cameras, and other devices
- Redundant network paths and equipment for high availability in high density locations
- Support for multi-gigabit (mGig) and/or link aggregation to increase bandwidth and reliability
- Support for copper or fibre uplinks (OM3 & OM4)
- Support for multicast traffic
- Support for Quality of Service

13.10 Standards

The Provider must provide a new LAN solution that:

- Is compliant with IEEE 802.3 standards for Ethernet, and specifically 802.3az Energy Efficient Ethernet (EEE)
- Supports for IPv4 and IPv6 protocols

- Adheres to TIA/EIA structured cabling standards
- Is compatible with industry-standard network management protocols (SNMP, RMON)

13.11 Security, Segmentation and Authentication

The Provider must ensure the service supports the following security requirements:

- Implementation of 802.1X port-based authentication
- Support for segmentation of network traffic, e.g. VLAN, VRF
- Integration with existing firewalls and intrusion detection/prevention systems
- Ability to implement Access Control Lists (ACLs) at the switch level
- Support for MAC address filtering and port security

13.12 Management

The Provider must provide the following management requirements:

- A centralised network management system with GUI interface and CLI access
- Remote configuration and firmware update capabilities
- RADIUS or TACACS+ support for administrator authentication
- Detailed logging and reporting features
- Integration with Authority IT service management (ITSM) tools
- Support automation and orchestration activities

13.13 Flexibility and Scalability

The Provider must take into account the following for flexibility and scalability:

- Modular switches to allow for easy expansion
- Support for stacking or chassis-based systems for scalability
- Quality of Service (QoS) capabilities to prioritise critical traffic
- Low-latency switching for time-sensitive applications

13.14 Environmental Considerations

In choosing their service components for Wi-Fi and LAN, the Provider must take into account the following environmental requirements:

- Energy-efficient equipment with power management features, for example, scheduled power down/low-power options for times of low usage, such as overnight
- Compliance with environmental standards (e.g. RoHS)
- Support for monitoring and reporting on power consumption to assist the Authority with Net Zero targets

13.15 At Home Service

The Authority operate a number of adult and children care homes, that aim to make the residents feel as if they were in a “home-like” situation.

The Authority is seeking confirmation from the Provider that it is able to provide such a service for internet access, if this was to be taken up.

The overarching required outcomes for this service are:

- Each resident to have their own securely, segmented, private network to which they can easily add/remove devices just by connecting to ‘their’ network
- For this service to be delivered by Wi-Fi primarily
- Support any ‘at home’ device such as IoT, gaming, streaming, computing, etc.
- In an Adult care home setting, residents shall have the ability to choose what level of filtering/protection they require, for example, restricting/allowing adult content, via a simple to use portal
- Time based access – ability to restrict access, for example in a Children’s care home
- Minimal logging of information for adult users, only that which is required to comply with potential police requests
- To be part of the monthly reporting and managed service reviews

The provision of such a service could require separate infrastructure/components to that which might be deployed at a location for general Authority access and users. Providers shall still need to monitor and manage that environment, if that is the case.

13.16 Data Cabling

The Provider must install internal cabling, where additional cabling could be required at a site. This could be during the transition phase and during the life of the contract.

The Authority must, not exclusively, be able to procure within a timely manner to reasonably carry out a requested Non-Standard Service Request (NSSR) for data cabling internally. This could include internal cabling for WAN circuits, uplinks and edge data ports.

The Provider must support occasional incidents related to replacement of damaged cabling or support investigations.

Any data cabling installed must be subject to support and maintenance with a minimum life of 10 years and be a minimum of ISO/IEC 11801 Category 6A for copper and OM4 for fibre.

Data cabling carried out by the Provider to support placement of Service Provider (SP) circuits, shall be the responsibility of the SP.

14 Secure Network Access Service Requirements

Secure Network Access for Authority users currently use Palo Alto's Global Protect solution, configured as an Always-On VPN for end-user devices. The Authority operate virtual Palo Alto firewalls within our Azure environment. Users authenticate using their Azure Entra ID with Multi-Factor Authentication (MFA) enabled to provide user specific access.

Traffic is additionally split between the Azure data centre accessing custom and corporate services, SaaS applications and internet-based applications such as Microsoft 365 and Teams. All remaining web traffic is filtered through the iBoss SWG.

The Secure Network Access service is currently owned, operated and managed by the Authority though, as part of this Managed Network Service, the Authority wants remote network access and traffic filtering to be ubiquitous with consistent levels of access for all staff, to give users a consistent secure network access wherever they connect.

14.1 Remote Connectivity

The Service supplied by the Provider must enable Remote Network Access Users to connect securely and seamlessly to Authority applications and services hosted on cloud landing zones and SaaS platforms, regardless of their physical location or device.

14.2 Remote Security

The Service supplied by the Provider must enable Remote Network Access Users to have the same level of security and performance as on-premise users, with consistent policies and enforcement across the network.

The Service supplied by the Provider must authenticate Remote Network Access Users using multifactor authentication (MFA) and single sign-on (SSO) mechanisms, and their identity and access rights shall be verified through the Provider's solution. Where applicable, the service shall support device certification authentication.

The Service supplied by the Provider shall protect Remote Network Access Users from malware, phishing, ransomware, and other cyber threats by the Provider's cloud-based security services.

.