1. ROSSENDALE ICT SUPPORT SPECIFICATION

Rossendale requires the following:

- Data Centre on site visits located in Wakefield, Northampton and Derby.
- Cisco Firewall Real Time Monitoring, full Management & configuration including patch, firmware and version upgrades
- Cisco VPN Real Time Monitoring, management & configuration including patch, firmware and version upgrades
- Cisco Real Time Monitoring for Switch / Router / Nexus / Network Device Configuration including patch, firmware and version upgrades
- Cisco UCS Real Time Monitoring, configuration including patch, firmware and version upgrades
- VMWare Real Time Monitoring and configuration including patch, firmware and version upgrades
- Windows Server Real Time Monitoring & support for all versions
- Terminal Servers Real Time Monitoring & support for all versions
- Cisco Umbrella Support
- Office 365 support
- SharePoint support
- Exchange on line support
- Webroot Antivirus, Anti Malware Monthly Platform Reviews
- Cisco Any Connect VPN support and rule base configuration reviews
- Service Device Management
- Maintaining Network Documentation

1.1 VM / Cisco Firewall / Cisco Switch / Cisco UCS / Cisco Nexus Monitoring

Vendor will monitor all VM's for availability, performance and alert any issues to Rossendale ICT team.

Monitoring service includes but it not limited to

- Availability
- Vulnerability / CVSS Score prioritisation
- Dashboard
- Automated Alerting and resolution

The Vendor will provide all the software and deployment services to implement the VM / Firewall / Switch / UCS / Nexus monitoring service Firewall Management / VPN

The Vendor will monitor all Cisco firewalls for availability and performance and alert any issues to the Vendor Service Desk and Rossendale ICT Support team via the dashboard, email and / or SMS.

Firewalls will be patched to the latest recommended firmware levels twice a year (unless a serious security vulnerability is discovered sooner). The Rossendale ICT Support team will be consulted prior to firmware patches being implemented to firewalls and any other appliances.

All Firewall configurations will be backed up to a central repository every month. The backing up of firewalls and devices fall in to the following 3 categories:

- **Change management backups**

  When a device configuration is changed, the running configuration before the change is made is secured, then once the change is complete the updated configuration is secured.

- **Project backups**

  As part of a project, when a device configuration is changed, the running configuration before the change is made is secured, then once the change is complete the updated configuration is secured.

- **Automated / monthly backups**

  Where a device has the ability to run an automated schedule (such as switches) then this is configuring to run a monthly backup. If the device does not have such functionality (Firewalls), this is undertaken manually.

Vendor will provide remote support as required and changes when requested.

1.2. Managed Security Solutions

Vendor will administer, manage, monitor and provide remote support, these include Cisco Umbrella, Cisco AnyConnect Office 365 products and Mimecast. Configurations and policies will be documented and kept up to date.

1.3. Network Device Management

Vendor will monitor the local area network devices for availability and performance and alert any issues to the Vendor Service Desk and Rossendale ICT Support team.

Network devices will be patched to the latest recommended firmware levels once a year (unless a serious security vulnerability is discovered sooner). Rossendale ICT Support team will be consulted prior to firmware patches being applied to firewalls and any other appliances covered under the Managed Services Agreement.

Network device configurations will be backed up to a central repository every month and retained for twelve months.

Automated backups will be checked by the Vendor Service Desk.

Manual backups will be undertaken by the Vendor Service Desk.

Vendor will provide remote support as required and changes when requested.

1.4. Service Device Management

Vendor will monitor the local area network service devices for availability and performance and alert any issues to the Vendor Service Desk and Rossendale ICT Team utilising the Vendor's chosen monitoring service.

Service devices will include but not limited to Cisco, VMWare and Netscaler.

Cisco devices will be patched to the latest recommended firmware levels once a year (unless a serious security vulnerability is discovered sooner). The Rossendale ICT Team will be consulted prior to firmware patches being applied to firewalls and any other appliances covered under the Managed Service Agreement.

The Service device configurations will be backed up to a central repository every month and retained for twelve months.

- Automated backups will be checked by the Vendor Service

  Desk. Manual backups will be undertaken by the Vendor

  Service Desk.

- Vendor will provide remote support as required and changes

  when requested.

1.5. Maintaining Network Documentation

The Vendor will take responsibility for maintaining and keeping up-to-date network documentation for devices managed by Vendor. This includes network diagrams and the configuration spreadsheet. Any changes or additions to the network, made by Vendor, will be recorded and the appropriate diagrams and documentation updated.

The documentation will be hosted on the Vendor SharePoint and version controlled; the Rossendale ICT Team will be provided with secure access.

1.6. SharePoint Support

The Vendor will assist with administration, management, monitoring and provide support and guidance to the Rossendale ICT Team across all aspects of our SharePoint environment.

1.7. IT Support Team Advice and Guidance

The Vendor will provide advice and guidance to the Rossendale ICT Team across all aspects of IT infrastructure, operating systems, applications, Microsoft 365, SQL Server, Terminal Services, Active Directory, Microsoft KMS, all certificates internal and external and associated processes and procedures.

1.8. Bi-Annual Wellbeing and Configuration Reviews

The Vendor will provide bi-annual well-being checks to include configuration reviews for all connected network devices, including but not limited to;

- UCS
- VMware
- V-Centre

1.9. Private Tenant Network Support & Management

Vendor will monitor the Futures Park private tenants network devices for availability and performance and alert any issues to the Vendor Service Desk and Rossendale ICT Team utilising the Vendor's chosen monitoring service. The tenant device is Cisco Meraki MX69 / 75.

1.10. Civica Automated Process Support

Vendor will monitor, update alert any issues to the Vendor Service Desk and Rossendale ICT Team for the automated Civica file and management processes for all of the Civica Financials applications including but not limited to Civica UX, SQL Server, Web, Icon hosted, Webstaff2, ATP and internet payments.

2. HOURS OF SERVICE

2.1. Weekday Cover

The Vendor Service Desk will be available to RBC ICT Team during the following hours:

Monday	**-**	**08:30 - 17:30**
Tuesday	**-**	**08:30 - 17:30**
Wednesday	**-**	**08:30 - 17:30**
Thursday	**-**	**08:30 - 17:30**
Friday	**-**	**08:30 - 17:30**

All Public holidays are excluded from Support

2.2. Restrictions to Service Desk Hours of Service

2.2.1. Planned Down-time

Occasionally there may be changes required which will affect the service availability. Where possible, the Vendor will undertake these planned changes outside of business hours. However, where service outages may be required during business hours, then Vendor will provide as much notice as is possible and seek prior agreement with Rossendale ICT team.

Should there be an increased risk to service by not undertaking the activity at short notice, then Vendor reserves the right to provide notification of change without prior agreement. These circumstances are expected to be exceptional.

2.2.2. Unplanned / Emergency Down-time

In the event that the service must be withdrawn from users at short notice, for whatever reason, at the request of Vendor or Rossendale ICT team, Vendor will inform the Rossendale ICT team as soon as possible (and, if possible, before withdrawing the service).

Where possible, Vendor will inform all signed on-users by means of an on-screen message and bring the system to an orderly close. The Vendor will keep the Rossendale ICT team informed regarding the likely time of the resumption of service.

In the event of a critical hardware failure, relevant recovery procedures shall apply and Vendor will keep Rossendale ICT team informed of progress.

3. INCIDENT MANAGEMENT

In the event of a service issue, it is the responsibility Rossendale ICT Team to log the problem with the Vendor Service Desk. All calls are logged on an on-line system, which is used as the basis of regular statistical reporting. Unless the issue has been detected by the monitoring service provided by the Vendor.

3.1. Service Requests

All service requests will be logged via the Vendor Service Desk. Service requests can be logged by one of the following methods:

- Phone
- Email
- Web - Web access to the Vendor Service Desk online system

3.2. Priority Levels & Response Times

The following priority levels are required:

Priority	Definition	Response Time
Urgent (P1)	**Business critical, affects multiple people significantly or critical functions significantly**	**15 minutes**
High (P1)	**Affects a small group of people significantly or critical functions are impaired**	**1 hour**
Medium (P2)	**Affects multiple people, but work can still be performed**	**4 hours**
Low (P3)	**Affects a small number of people or functions, but work can still be performed**	**NBD**
Service request (P3)	**Low impact, long term work**	**5-10 days**

Response Time is defined as the amount of time elapsed after receiving notification of the incident until work is started. The time is counted when the Service Desk is open. In the event of a service issue, users will log the problem with the Vendor Service Desk.

3.3. Call Targets

With reference to the priority levels, the Vendor Service Desk will respond according to the following targets:

Priority	Target
Urgent	**95%**
High	**90%**
Medium	**80%**
Low	**75%**
Service request	**75%**

3.4. Escalation process

Escalation involves the notification of support call issues to a higher level of authority.

Please detail the Vendor escalation process including job roles, contact numbers, and the associated escalation points where invoked. Also, include any methodologies adopted for example ITIL.

4. MONITORING SERVICE

4.1. Network and Device Monitoring

Please detail how the vendor monitoring service works. In particular does the Network and Device Monitoring service require an onsite agent to monitor the status and availability of critical devices on an organisations network?

4.2. Inventory

The Vendor monitoring service is required to be able to connect to any network connected devices and retrieve basic device inventory data (make, model and serial number) which is then stored in the inventory database.

4.3. Availability

Availability monitoring is required to ensure that a device is still connected to the network. Availability data needs to be recorded so that it can be used to provide historical analysis and real-time alerting.

4.4. Automated Alerting

Automated alerting is required to either send an email or SMS alert message to a nominated user (or group) when a device state changes, for example when a network switch becomes unresponsive, or disk capacity on a monitored server goes below a defined threshold.

4.5. Monitoring Dashboard

A web enabled monitoring dashboard is required so that Rossendale ICT Team can see an overview of the status of all the monitored devices, check historical data and respond to alerts.

5. VENDOR SUPPORT

The Vendor will support the following:

5.1. Hardware

- All RBC Networking equipment
- Cisco UCS and Blades
- Cisco switches at all connected sites
- Cisco Any Connect VPN / Firewall
- All Voice gateways
- Cisco Routers
- Cisco Nexus
- Cisco Firewalls
- Meraki Wi-Fi devices
- Meraki Firewalls
- Cisco Telephony

5.2. Software

- All VMWare
- VMWare vCenter
- VMWare vSphere
- Windows Operating Systems for all VM's any outdated software best endeavours
- SQL Server all versions
- Active Directory / Entra AD
- Azure current RBC services
- Terminal Services all versions
- Webroot AV
- Cisco Umbrella
- Cisco Any Connect
- Cisco AMP for Mac / Windows devices
- Mimecast
- Office 365
- Teams
- Exchange on line
- Teams
- One Drive
- SharePoint Cloud
- All Certificates whether internal or external including CA Authority
- Application Software to provide functionality updates, software patches, term licenses, etc
- Maintenance of System Software such as Operating System, Systems Management,

6. APPENDIX A: ICT SCHEDULE

The following table lists the supported hardware for Rossendale.

Category	Description	Totals
Users	IT Users up to	1000
Sites	Main offices	4
WAN Circuits	Internet, WAN, VPN, LES, MPLS	4
Firewalls	ASA Firewall or Context, Meraki Firewall	2
Core Servers	Virtual servers delivered in Cisco UCS up to 8 blades up to 100 VM's	100
Network Devices	Core / Distribution Switch, Router, Basic L2 access switch, Cisco UCS, Nexus, Cisco Meraki	50
Service Devices	Cisco ISE, Netscaler	4