MERAKI SERVICE DEFINITION

Version: 7.1
Date: 14 October 2022

redcentric

AGILE • AVAILABLE • ASSURED

1 Service Overview

Introduction

Meraki’s range of connectivity and security devices are proving to be very popular due to the market leading traffic visibility and diagnostic capabilities, also the scalability and ease of management using the cloud-based management portal. Redcentric’s Meraki Service provides the design, deployment and ongoing support of Meraki’s connectivity and security devices to deliver a multitude of network solutions including traditional and software-defined wide-area networks (SD-WAN) and distributed and complex wired and wireless local area networks (LANs).

2 Service Description

2.1 Introduction

Meraki's cloud managed networking devices enable customers with even modest IT support departments to provide a first-class service to their end-users. Redcentric provides design and integration consultancy to ensure the most appropriate Meraki devices are selected and integrated with other services to meet specific Customer needs. Redcentric pre-configures the cloud management platform ready for device deployment. Redcentric engineers deploy and connect the Meraki devices at Customer locations and provide end-to-end testing. Redcentric monitors the Meraki network devices and works with the Customer's IT department to identify and replace any unit that develops a fault. Further Redcentric provides a level of configuration support should the Customer require it.

2.2 Related Products

Redcentric offers an extensive portfolio of services designed to meet the requirements of companies of all sizes. Customers can focus on their core business applications when the Meraki Service is taken in conjunction with other services from Redcentric's connectivity, infrastructure and unified communications portfolios. Section 2.20 details a complimentary service which, as well as providing detailed insight into the userbase, addresses the compliance obligations associated with offering a public Wi-Fi service.

2.3 Solution Design

Redcentric consultants work with the Customer to establish and document specific design objectives and requirements. The consultants then use this as the basis to produce a high-level design. The design work should include all aspects including for example Security, WAN, LAN & RF coverage where applicable.

2.4 Supported Appliance Types

Redcentric supports Meraki's current range of security, LAN switching and wireless access point devices.

Meraki MR

The Meraki MR series is the world's first enterprise-grade range of cloud-managed WLAN access points. Designed for demanding enterprise environments, the current range of MR devices deliver lower-cost Wi-Fi 5 and ultimate-performance Wi-Fi 6 capability. The latter supporting high user density using MU-MIMO, special re-use and the latest modulation technologies to deliver the throughput and reliable coverage required by demanding business applications.

The MR series comes equipped with industry-leading features that make them ideal for demanding enterprise deployments:

- 802.11ac and 802.11ax technologies with multiple spatial streams, built for voice and video
- Integrated enterprise security and guest access
- Dedicated radio for security and RF optimization with integrated spectrum analysis
- Integrated intrusion detection and prevention system (WIDS/WIPS)
- Self-learning application-aware traffic analytics engine
- Flexible group policy engine for creating and applying application- aware policies by network, device-type, and end-user

Meraki MS

The Cisco Meraki MS wired switch series brings the benefits of the cloud management to networks of all sizes: simplified management, reduced complexity, network wide visibility and control, with lower operational cost for campus and branch LAN deployments. Cisco Meraki access switching is available in both Layer 2 and powerful Layer 3 models. Mission-critical features like Layer 7 application visibility, network topology visualisation, virtual stacking, QoS for business-critical applications, 802.1X access control, and more — are present in all models.

Meraki MX

Built on Cisco Meraki's award-winning cloud-managed architecture, the MX is Cisco's 100% cloud-managed Unified Threat Management appliance. MX appliances self-provision, automatically pulling policies and configuration settings from the cloud. Powerful remote management tools provide network-wide visibility and control and enable administration without the need for on-site networking expertise.

Cisco Meraki MX Security Appliances are ideal for organizations with large numbers of distributed sites. Since the MX is 100% cloud managed, installation and remote management is simple. The MX has a comprehensive suite of network services, eliminating the need for multiple appliances. These services include Layer 7 application firewall, content filtering, web search filtering, intrusion prevention, web caching, Intelligent WAN with multiple uplinks.

Cloud services deliver seamless firmware and security signature updates, automatically establish site-to-site VPN tunnels, and provide 24x7 network monitoring. Moreover, the MX's intuitive browser-based management interface removes the need for expensive and time-consuming training.

The MX platform has an extensive suite of security features including IPS, content filtering, web search filtering, anti-virus / anti-phishing, geo-IP based firewalling and IPsec VPN connectivity, while providing the performance required for modern, bandwidth-intensive networks.

Layer 7 fingerprinting technology lets administrators identify unwanted content and applications and prevent recreational apps like BitTorrent from wasting precious bandwidth.

The platform delivers superior intrusion prevention coverage, a key requirement for PCI 3.0 compliance. The MX also uses the Webroot BrightCloud® URL categorization database for CIPA / IWF compliant content- filtering, Kaspersky Safestream II® engine for anti-virus / anti-phishing, and MaxMind for geo-IP based security rules.

Best of all, these industry-leading Layer 7 security engines and signatures are always kept up to date via the cloud, simplifying network security management and providing peace of mind to IT administrators.

Meraki vMX

vMX virtual appliances can extend a Customer's software defined wide area network (SD-WAN) to include their 3rd-party hyperscale cloud environments. Redcentric supports Meraki vMX virtual appliances deployed by the Customer within the Customer's 3rd-party hyperscale cloud environment subscription.

2.5 Hardware Ownership and licensing

All Meraki products require licensing to operate. Meraki's licensing combines ongoing software upgrades with centralised systems management and hardware support. Meraki operates two license models: co-termination and per-device. When co-termination licensing is implemented and additional devices are added to the Customer's inventory during the license period, the license expiration date for all devices is adjusted such that the existing and new devices expire together. When per-device licensing is implemented and additional devices are added to the Customer's inventory during the license period, the license expiration date of existing devices does not change – commonly resulting in device licenses expiring at different times.

Redcentric offers two options, 1) an overlay service where the Customer owns the hardware and is responsible for the purchase of licenses and 2) where Redcentric supplies the hardware and licensing as part of the service. When the customer wishes to own the Meraki hardware, they are also responsible for the purchase of ongoing operation licences. As a Meraki re-seller, Redcentric is well-placed to supply hardware and licensing on a sale basis.

If the Customer wishes to own the Meraki hardware, it is the Customer's responsibility to buy, renew and/or extend licenses when required to keep the environment operational. If there is an infringement or when licenses lapse, the Meraki cloud management platform will ultimately stop devices passing traffic. Please consult Meraki's website for up-to-date details of this critically important aspect.

2.6 LAN Cabling

The Redcentric Meraki service does not include any structured cabling checks, cable work or patching between the Customer's existing wired switch infrastructure and the location of each Meraki device. Redcentric will undertake a general or detailed survey of existing structured cabling on request and provide a report on its suitability. Redcentric can arrange for cabling to be upgraded, repaired, corrected, extended, tidied, re-patched, labelled and replaced as required to ensure a Customer's entire LAN is fit for purpose. This work is chargeable and priced on application.

2.7 Site Surveys

Customers can select optional site surveys which generally results in a design more likely to meet specific requirements. This is particularly applicable when aged LAN wiring exists and when Meraki Access Points are to be deployed and wireless coverage is critical.

2.8 Power and Space

The Customer is required to provide space in a suitable environment at each site for the various pieces of equipment required to deliver the service. In addition, the Customer is required to provide sufficient suitable 13A mains power points within 1m of the various pieces of CPE. Note that in some cases, LAN switches can provide power to Access Points using power-over-Ethernet.

2.9 Deployment

Redcentric generally undertakes physical installation, configuration, commissioning, and testing of the Meraki Access Points, switches and security devices which form part of the agreed design. Project management and engineering charges apply to cover this work.

Where vMX software appliances are required as part of a design, the Customer is required to undertake deployment in their subscription within 3rd-party hyperscale cloud environments.

Redcentric's commercial offer is based on the premise that site access will be available between 9am and 5pm Monday – Friday and on-site work will be undertaken during this time unless specifically agreed in writing.

2.10 Detection of Rogue Access Points and Other Security Alerts

Meraki's cloud managed wireless access points (APs) come equipped with Air Marshal, a built-in wireless intrusion detection and prevention system (WIDS/WIPS) for threat detection and attack remediation. APs configured in Air Marshal mode will scan their environment in real-time and take pre-emptive action based on intuitive user-defined preferences. Air Marshal triggers alarms and can be configured to automatically contain suspect and known rogue APs. Intuitive cloud-based management with flexible remediation policies makes Air Marshal ideal for security-conscious distributed networks.

The Customer is solely responsible for monitoring, investigating and eliminating rogue access points and investigating other security alerts.

2.11 Monitoring for Device Failure and Service Issues

Redcentric systems poll the cloud management platform approximately every 5 minutes to confirm that each Meraki device is available. This is in line with industry standard network management best practices. If a device does not respond to several successive polls, an automatic alert is forwarded to the Redcentric network fault management system.

Section 2.23 details two service options. When the Customer selects the Managed option, the system also monitors for sustained delay and packet-loss on WAN links and automatically raises alerts accordingly.

Alerts result in the automatic generation of an incident which is placed in the technical support queue. Technical support engineers investigate these incidents 24 hours a day, 365 days a year.

Customers can become aware of problems in the short window before the polling procedures verify a problem and issue an alert. Redcentric provides additional means for Customers to raise faults, i.e., via telephone, email and the web portal.

Redcentric classifies problems according to severity. This allows the prioritisation of resource on issues that have the most impact on Customers' businesses. Further details of the classifications can be found in Redcentric's Customer Welcome Pack which is available on request.

Redcentric is committed to continually improving and expanding its services, and in order to facilitate these improvements, it is necessary to carry out essential work from time to time. In accordance with Information Technology Infrastructure Library (ITIL) service management standards, these activities are carefully scheduled through the use of an internal change control process; this gives Customers maximum visibility of any given change and thereby ensures that planning and implementation is carried out to minimise the effect on Customers using Redcentric services.

Maintenance windows and procedures for communicating emergency outages are detailed in the Customer Welcome Pack.

2.12 Hardware Support

If Redcentric support desk staff, in conjunction with the Customer and Meraki support staff, determine that a piece of Meraki equipment has developed a fault, Redcentric will work with Meraki to have a replacement unit shipped. Meraki usually aim to despatch hardware replacements within 24 hours of accepting a valid RMA request. Customers wishing to minimise down-time resulting from hardware failure are advised to buy spare devices and store them at their location(s) for immediate replacement or incorporate spare active devices into the design – i.e., high-availability design. To minimise expense, the Customer is required to perform the straightforward operation of swapping faulty units under instruction from Redcentric staff if required. The Customer is also required to return faulty units. Enhanced support options including on-site engineering assistance are available to meet specific Customer requirements and must be agreed in writing by both parties prior to finalising a Service Agreement.

2.13 Access to Report Information

The Meraki cloud-based management platform provides extensive information on all aspects of the environment. The Customer will be able to access this information directly through the portal and configure and modify reports as required. Therefore, Redcentric does not create or modify or issue reports etc. but will happily assist the Customer if required.

2.14 Portal Access

The Customer's administrative staff will have full read access on the Meraki portal as well as write access so that they can make changes to certain aspects of the Meraki platform as detailed below.

Redcentric Staff will have unrestricted access to the Meraki portal to provide support to the Customer.

There are two basic types of Dashboard administrators: Organization and Network.

Organization administrators have complete access to their organization and all its networks. This type of account is equivalent to a root or domain admin, so it is important to carefully maintain who has this level of control. Please see below for best practices regarding these accounts.

Network administrators have access to individual networks and their devices. These users can have complete or limited control over their network configuration, but do not have access to organization-level information (licensing, device inventory, etc).

Most Dashboard administrators will fall into one of the two above categories, the information below details the options and limitations associated with different admin types.

Organization Permission Types

Read-only: User able to access most aspects of network and organization-wide settings, but unable to make any changes.

Full: User has full administrative access to all networks and organization-wide settings. This is the highest level of access available.

Network Permission Types

Guest ambassador: User only able to see the list of Meraki authentication users, add users, updated existing users, and authorize/de-authorize users on an SSID or Client VPN. Ambassadors can also remove wireless users if they are an ambassador on all networks.

Presented with user management portal only.

Monitor-only: User only able to view a subset of the Monitor section in Dashboard and no changes can be made.

Read-only: User able to access most aspects of a network, including the Configure section, but no changes can be made.

Full: User has access to view all aspects of a network and make any changes to it.

2.15 Meraki Portal Training

The Cisco Meraki portal has been developed over time to be both highly functional and intuitive. Meraki have an extensive range of self-paced, easy to access training videos available on YouTube® covering a wide range of functions to assist network administrators. Further, classroom training courses are available which underpin a formal certification programme if required. Portal training is therefore not provided as part of the Meraki Service.

2.16 Wireless LAN Performance Assurances

Due to the nature of wireless networks where environmental conditions change constantly and it is not possible to control user density, any issues relating to RF interference and bandwidth congestion are beyond Redcentric's control. (E.g., coverage, throughput, bandwidth availability etc.).

Redcentric will on-request undertake on-site investigation and site-surveys to identify issues, which may for example result in a recommendation to install additional access points. Investigation and remediation work is chargeable.

2.17 Meraki Protection, Privacy & Security

Cisco Meraki is committed to data protection, privacy, and security and has designed its cloud architecture specifically in a way that enables customers to securely protect their data. European customers can confidently deploy scalable, secure Meraki networks that comply with applicable data protection regulations across the European Economic Area (EEA).

The Meraki EU Cloud

The Meraki cloud architecture leverages a globally distributed public cloud architecture that provides built–in reliability, security, and redundancy. To meet the needs of European customers, Meraki created the EU Cloud, a separate part of the Meraki cloud architecture designed to meet the needs of European customers and regulations. Hosted on data centres located exclusively in the EEA, the Meraki EU Cloud provides reliability and business redundancy offered by a distributed architecture while ensuring that no personal data leaves the EEA.

Additionally, the EU Cloud's out–of–band architecture ensures only management information, and not network traffic, passes through EU Cloud datacentres. The EU Cloud architecture enables customers
to satisfy their legal obligations and simultaneously realize all the advantages cloud management offers, including centralized visibility and control, unified management of wireless and wired networks, and reduced operational expense.

The Meraki EU Cloud is built on a PCI DSS Level 1 certified system architecture and operates with a 99.99% Service Level. Additionally, Meraki EU Cloud data centres are certified with one or more of the following: ISO 9001:2008, ISO 27001:2008 & PCI DSS

Meraki and the EU Cloud are compliant with the following applicable European data protection regulatory frameworks and local laws: EU Directive 95/46/EC, German Federal Data Protection Act & Article 29 Working Party Opinion of July 1, 2012

2.18 Evolving Requirements

Redcentric is committed to delivering solutions that meet Customers' evolving needs. Consequently, when possible, Redcentric is happy to accommodate changes to the service as required during the contract period. Any changes to the service requiring design work, additional coverage, or support for new features, VLANs or WLANs etc. may incur design, hardware, software, licensing, implementation, support and/or other charges.

2.19 Public Wi-Fi Access and Communications Data

Where applicable, wired and/or wireless access to the Internet is provided to end users by the Customer, and not by Redcentric (Redcentric will provide such services to the Customer separately if ordered). The Meraki Service must be branded accordingly in communications to end-users.

The Customer will be responsible for all user management in relation to the Services, including (1) (unless otherwise agreed in writing) user authentication and (2) maintaining and supplying to government agencies etc. any records relating to the use of the Service as required by law from time to time.

Please see section 2.20 detailing Redcentric's complementary service intended to reduce administrative burden and mitigate risk associated with offering these services to end users.

2.20 Purple - Guest Access, Location, Presence and Analytics

The Purple cloud-based service delivers a guest Wi-Fi capability that benefits all parties. Users login easily using a variety of methods including social media for fast, effortless access.

The portal pulls together multiple data sources allowing businesses to see real-time footfall, passers-by, conversion and bounce rates, dwell times, return visits and frequency; enabling businesses to truly understand their venues. Businesses can then take action when people are in venue using marketing tools to target users through email, SMS and customisable splash pages.

Using Wi-Fi, Bluetooth and GPS, the system can enable additional location services to pinpoint Customer movement in venues down to a few metres. Businesses can then send hyperlocal marketing messages to people as they move around the venue in real-time.

The system has a restful API, so the data displayed in the Portal can be connected to the Customer's other information systems such as CRM and ERP.

The Purple service has proven integration with Meraki infrastructure.

The Purple service can be configured for content filtering. By using the service, the end-user enters into an agreement with Purple. Consequently, the service is provided to end-users by Purple, and not the Customer. Requests for legal-intercept and Regulation of Investigatory Powers Act (RIPA) enquiries are handled by Purple.

2.21 Co-management

The Customer's administration staff can make changes to the Meraki environment via the cloud-based management portal. This approach benefits both parties as it removes some administration burden from Redcentric, and the Customer is able to implement trivial changes very quickly and provide support to end-users (e.g. Search for failed authentication events). However, these co-managed arrangements can pose problems. If Redcentric determines, at its sole discretion, that changes implemented by the Customer's staff have contributed to an issue which impacts Redcentric's ability to provide the service, Redcentric may charge the Customer for any remediation work.

2.22 Firmware Upgrades

Meraki release firmware upgrades from time-to-time which fix software bugs or deliver new features or functionality. Depending on the level of Management, as detailed in section 2.23, upgrades on the Customer's devices may be scheduled by the Customer or Redcentric staff. When Redcentric staff are responsible for scheduling upgrades, Redcentric will:

- Notify the Customer of the proposed upgrade date/time, giving at least 10 business-days' notice.
- Schedule upgrades Monday-Friday, 4am-7am where additional staff are present to oversee issues relating to upgrades should they occur.
- Accommodate Customer requests for postponed or alternative upgrade slots where possible.

Customers are advised to specify, as part of the order, a test environment which can be used by them to test upgrades prior to roll-out across their entire estate of devices

If the firmware or hardware version of your Meraki appliance is forecast to become End of Support (EoS) / End of Life (EoL) during an initial contract term or a renewal of that contract term, Redcentric will no longer be able to provide security or critical firmware updates for that EoS or EoL Appliance.

In order to continue to receive security and critical updates, a hardware refresh of the specific Meraki Appliance will be required. Any hardware refresh, including the provision of new Meraki Appliance, is outside the scope of this Service and will be chargeable. A new Meraki Appliance would be provided by Redcentric for an additional charge.

2.23 Service & Responsibilities

Two on-going support models are available to meet the needs of Customers requiring different levels of control.

In addition to other responsibilities detailed in this definition, a list of typical tasks is shown in the table below with details of responsibility for the two service options.

Function	Monitored	Managed
Routine low-level changes LAN. e.g. port speed, VLAN allocation etc.	Customer	Redcentric
Routine low-level changes Security. e.g. change to rule-base, content filters etc.	Customer	Redcentric

Function	Monitored	Managed
User database administration	Customer	Redcentric
Schedule firmware updates	Customer	Redcentric
Reaction to failed or degraded links when delivering SD-WAN functionality	Customer	Redcentric

In addition to responsibilities in the table above, Redcentric is responsible for the following regardless of which option is chosen:

- Initial configuration, deployment, and testing of the overall solution
- Periodic polling of devices to detect failure
- Coordinating replacement of faulty hardware
- Templated changes effecting critical elements / whole network - e.g. routing
- Deployment of Customer purchased device licenses on Meraki cloud controller if supplied by Redcentric
- Deployment of device licenses on Meraki cloud controller (License Included option)

In addition to responsibilities in the table above, the Customer is responsible for the following:

- Providing Redcentric with the technical details required for the design. E.g., WLAN IP address ranges, SSID names, VLAN assignments, local DNS servers, DHCP scopes and options etc.
- Provision of suitable power, space, and cabling
- Configuring and accessing reports as required
- Meeting any compliance requirements associated with offering a public Internet service to guests (the Customer may choose to use Redcentric's Guest Management, Analytics and Marketing service to achieve this)
- Monitor and address rogue AP & other security aspects
- Procuring Meraki device operational licenses as required. (Customer owned hardware & License option)
- Deployment of device licences on Meraki cloud controller if not supplied by Redcentric (Customer owned hardware & License option)
- Test upgrades prior to roll-out across their entire estate of devices
- Where applicable, diagnose end-user issues and provide support

2.24 SD-WAN support

Meraki MX and vMX devices can deliver SD-WAN functionality. This allows Customers to build a WAN from a mix of private (e.g., MPLS) and public (i.e., Internet) connections from multiple suppliers using a variety of transport technologies (e.g., Broadband, Ethernet & cellular).

The Meraki devices route the Customer's application traffic according to the policy configured on the Meraki cloud-controller. Traffic can be encrypted over private links as well as public (i.e., Internet) links. Thresholds for delay, jitter and packet-loss can be set 'per application'. The system measures these parameters and routes application traffic accordingly. If desirable, the system can be configured to share application traffic across multiple links. For sites that have a link to the Internet (i.e., a direct Internet access [DIA] circuit), the system can be configured to provide local break-out. This is optimal for traffic destined for public Internet facing applications (e.g., applications hosted in Azure or AWS). Providing local break-out also frees up valuable bandwidth on private links that would otherwise be used to carry the traffic to a central breakout point.

When the Customer chooses to take the Managed Service (see section 2.23), Redcentric monitoring systems poll the devices periodically to identify link failures and sustained link quality issues. Redcentric investigates issues relating to connectivity services it provides. Issues relating to 3rd-party connectivity supplied by the Customer are reported to the Customer - Redcentric does not deal with 3rd-party connectivity suppliers directly.

2.25 License Renewal Notifications

When license renewal approaches, Meraki emails Administrators configured on the Cloud Portal with license reminder notifications – these reminders become more frequent as the license end-date approaches. Commonly both Redcentric and Customer staff are configured on the portal so both parties receive these notifications. Customers that have elected to own the Meraki Hardware, and therefore take responsibility for licensing, should contact their Redcentric account manager to discuss timely purchase of renewal licenses and renewal of the Redcentric overlay service. Where Redcentric retains ownership of the hardware, Redcentric will renew the licensing after the Customer has signed a contract renewal/extension for the Redcentric service.

3 Implementation and Acceptance

3.1 Acceptance Criteria

The Acceptance Criteria listed below apply to the Meraki Service:

- All Meraki devices appear on the cloud management portal
- A sample of wired or wireless devices can connect to the network (after authentication when implemented)
- The Customer can access cloud management administration portal

4 Service Levels and Service Credits

4.1 Service Levels

The Service Level applicable to the Meraki Service is as follows:

Service Level: Availability of each individual Meraki Device **Measurement Period: Month**	
Service Level	Not less than 99.5% Availability.

4.2 Exclusions from Availability

In calculating Availability, in addition to the exclusions listed in clause 6.7 of the General Terms the following shall be excluded where it is proven or suspected beyond reasonable doubt:

- Failure of any element not supplied by Redcentric which prevents Redcentric from measuring Availability
- Unavailability due to throughput (load) exceeding initial documented requirements
- Unavailability due to onsite power, cabling or local network issues
- Malicious attempts to disrupt service such as wireless jamming, Denial of Service etc.
- Any impact caused in-whole or in-part by configuration changes made by the Customer
- Suspension of the Service by Meraki due to licensing violation (Customer Supplied option)
- Suspension of the Service by Meraki due to licensing violation caused by the Customer (License Included option)
- Impact caused by Meraki software/firmware upgrade regardless of whether it was evaluated on test equipment prior to roll-out
- Unavailability due to hardware failure when non resilient design is implemented
- Unavailability of vMX software located in 3rd-party cloud environments for any reason other than misconfiguration by Redcentric staff

4.3 Floor Service Level

The Floor Service Level applicable to the Meraki Service in respect of Availability shall be 85% per device in any given Month - i.e., each device has its own Availability Service Level and its own Floor Service Level.

4.4 Service Credits

The Service Credits applicable to the Meraki Service shall be calculated as follows:

For each device where availability is <99.5% in the relevant Month, a Service Credit may be claimed according to the table below. For the avoidance of doubt, for the purposes of paragraph 6.4 of the General Terms, the maximum value of Service Credits in any Month shall be a sum equal to half the Charges which would have been payable in respect of the aggregate of all Meraki Service devices in that Month had Redcentric provided the Meraki Service in accordance with the applicable Service Levels.

In the following table:
"≥" means "greater than or equal to" and < means "less than"
"MS" means the average Charge payable for an Access Point in respect of the Meraki Service for the same Month

Service Availability	Service Credit
≥99.5%	none
≥99.0% but <99.5%	5% of MS
≥96.5% but <99.0%	15% of MS
<96.5%	20% of MS

5 DATA PROCESSING

5.1 Data Processing Scope

- The Redcentric Meraki Service delivers design, deployment and support functions.
- The Redcentric Meraki Service does not involve any storage or backing up of data.
- The Customer must separately enter into an agreement with Meraki, a division of Cisco Systems to use the hardware and cloud-based management portal.

5.2 Data Storage and Encryption

- Redcentric configures equipment to encrypt traffic according to Customer requirements.
- Redcentric does not capture, inspect, analyse, store, or share the Customer's traffic/data under normal circumstances.
- Under certain circumstances, when managing a support ticket, Redcentric may capture, inspect, analyse and/or store a small sample of the Customer's traffic to investigate and diagnose a very specific problem, e.g., to help resolve a problem relating to packet corruption. Such diagnosis would involve the examination of a small sample of packets, and this will only be undertaken at the request of and in conjunction with the Customer.

5.3 Data Processing Decisions

- Redcentric does not make any data processing decisions in relation to the Meraki Service. Any processing of data over Customer systems when using the Meraki Service for transit is instigated, configured, and managed by the Customer.
- Redcentric Support can be asked by the Customer to intervene in the event of an issue with the Meraki Service. In such a case Redcentric may make decisions that affect data processing, but such actions will only be undertaken at the request of and in conjunction with the Customer.

5.4 Sub-Processors

- With the exception of physical deployment, no third parties are involved in delivering the Meraki Service, and there are no sub-processors appointed by Redcentric.
- The Customer must separately enter into an agreement with Meraki, a division of Cisco Systems, to use the hardware and cloud-based management portal (and to avoid doubt, Meraki is not a sub-processor of Redcentric for this purpose).

5.5 Customer Access to Data

- The Customer control its own platforms which use the Meraki Service to carry data, and the Customer therefore has full access to its own data.

5.6 Security Arrangements and Options

- Meraki devices are located at Customer locations/sites. It is the Customer's responsibility to ensure physical security at such locations/sites meets its needs.

HEAD OFFICE

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522
E sayhello@redcentricplc.com
W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED

bsi.

ISO 9001 Quality Management	ISO 14001 Environmental Management	ISO/IEC 20000-1 Information Technology Service Management	ISO 22301 Business Continuity Management	ISO/IEC 27001 Information Security Management
FS 603185	EMS 673062	ITMS 668453	BCMS 603194	IS 603187