**Technical Requirements**

Provision requirement for purchase, pre-stage configuration, installation, and support of MAG International Global Cisco Meraki Network.

**Countries and Locations**

We operate in 32 countries globally and have 79 locations within these countries which house MAG international employees. We have around 6,000 employees globally in all operational capacities however, we have circa 1,500 active technology users.

**Our Specifications and Assessments**

We have 3 different site sizes – Large (>50 users), Medium (>10 users but <50 users) and Small (<10 users). Our technical and product requirements should fit the criteria for these sites. We have one location that would be classified as Large which is our Headquarters in Manchester, UK which houses up to 120 users, we have 15 locations that would be classed as Medium sized sites and rest would be Small.

We would require our global network to be cloud enabled and cloud managed from our HQ in Manchester, UK. We need to be able to manage and monitor our global network across a distributed network infrastructure through the Cisco Meraki dashboard.

It is imperative that we can monitor our global WAN, access and IoT technologies in one place with end-to-end visibility. Through this single pane of glass, we need to be able to monitor and manage the overall health of our network and locations proactively solving any issues before they become business critical.

As we are a global humanitarian organisation, its vital that we can deploy new countries networks quickly through simple configurations staying aligned to corporate standards required by our donors and our audit compliances.

We should have the technical capability to push out network and security updates, firmware upgrades out of hours and have a scalable, secure, and seamless Network platform.

**Business Continuity & Assurance**

We would require a service support contract and would be open to pricing for different options up to 24x7x365 support contract. Assurance elements we would look for in our service contract would include and not be limited to

* Significantly reducing service restoration time to minimise operational losses – from days and weeks to hours and minutes
* Never missing an operational change – continuous protection of critical operational data, ensuring the latest recovery point is always available
* Design authority governance – ongoing configuration compliance and drift checking
* Proving the Disaster Recovery process with the Business’ IT team – by providing biannual testing and tabletop exercising (a key ongoing component of this Cloud BC/DR service offering)
* Built-in preventative service outage intelligence - mitigating risk against future downtime through continuous real-time service intelligence to provide additional risk removal
* Increasing control level – removing a barrier to achieve better cyber insurance coverage and help with minimizing insurance costs.
* Providing 24/7 access – Disaster Recovery expertise available for full restoration support

**Business Risk Mitigation**

We need a service that provides MAG International with a service that recovers critical operational data in minutes, resulting in significant risk and impact reduction, which will mitigate:

|  |  |
| --- | --- |
| * **Operational disruption / risk** | * **Potential bankruptcy** |
| * **Brand and reputational damage** | * **Contractual breaches** |
| * **Employee wellbeing** | * **Environment Security** |
| * **Regulatory / Compliance issues and penalties** |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| **Technical Questions (10% weighting of total)** | | |
|  | Question | Answer & Fully/Partial/Non-Compliant |
| 1 | The entire wireless system must be cloud managed and not require any controllers or additional appliances for management, configuration. |  |
| **2** | The solution must not have a single point of failure – all Access Points should run autonomously in the event of a disconnect from the Cloud Management Platform or internet. |  |
| **3** | Data Centres utilised by the solution must have at least a 99.99% SLA, be SSAE16 Certified, and have penetration tests run daily. |  |
| **4** | The solution must offer a “single-pane-of-glass” management platform for managing access points, switches, security appliances and mobile device management. |  |
| **5** | Licensing for the solution should include ALL current and ALL future features. |  |
| **6** | Licensing for the solution shall include next business day hardware replacement and 24x7 support. |  |
| **7** | The solution must provide in depth Layer 7 analytics with respect to client traffic. |  |
| **8** | The solution must alert administrators if the status of hardware changes, or if a change is made to the system. Additionally, all system changes must be logged and tracked by user and values changed. |  |
| **9** | The management application must support two factor authentication. |  |
| **10** | The solution must be WiFi6 certified. |  |
| **11** | The solution must allow for 1-click mass upgrades for all Access Points simultaneously, regardless of model. Additionally, the solution must notify Network Administrators when a new feature or firmware version is available. |  |
| **12** | The wireless system must support a stateful application-layer firewall that can identify, classify, and prioritise applications using layer 7 intelligence. Applications should be able to be traffic shaped as well to ensure that recreational applications (like BitTorrent, Pandora, Spotify, etc.) do not consume all of the available bandwidth |  |
| **13** | The wireless system must support the ability to fingerprint client device types (i.e. iPad, Android, iPhone, Windows, etc) and apply security settings to those devices, without the need for additional appliances or licenses. For example: iPads on the BBC SSID may have access to only the web and are rate limited to 512 kbps, and no peer to peer traffic is allowed. |  |
| **14** | Gateway services to allow Airplay, Printing, iTunes and other Bonjour-based services to flow seamlessly across the wireless network. |  |
| **15** | The wireless access points must have a dedicated radio designed to identify interference sources on the 2.4 and 5 GHz spectrum, provide real-time spectrum analysis on those spectrums, as well as identify any interfering access points across all channels in those spectrums. |  |
| **16** | The wireless system must support integration with Google Maps, with the ability to upload a custom floorplan and overlay it on the map. |  |
| **17** | The wireless system must support the ability to easily replicate and clone configurations across multiple different sites using a single click. Ideally, a config could be changed once and then replicated across multiple sites. |  |
| **18** | The wireless system must support the ability to take a packet capture directly from the management interface. This packet capture should be able to filter based on client, IP address, MAC address and other filters. |  |
| **19** | The wireless system must support the ability to provide deep application visibility into all of the applications that are used on the wireless network, including hostname visibility to view the individual URLs of all of the applications. This information should be exportable and downloadable on a per network and per SSID basis. |  |
| **20** | The wireless system should have the ability to identify information from probe requests of mobile devices and have a way to export the probe request information using an XML. |  |
| **21** | The wireless system should have built in guest access and not require any additional appliances or licenses for guest users. |  |
| **22** | The wireless system must have a way to open cases with support and monitor their status directly from the management console. |  |
| **23** | The wireless system must support the ability to send summary reports to certain administrators on a daily, weekly and monthly basis. These summary reports should show information like top users, top applications, bandwidth consumed per day, etc. |  |
| **24** | An Option for Access Points with integrated BLE (Bluetooth Low Energy) Beacons must be included in the response. |  |
| **25** | The solution must allow Access Points to be upgraded to newer hardware without the need to repurchase valid, unexpired licenses. |  |
| **26** | All Access Points must include full time Auto RF and WIPS while simultaneously serving clients. |  |
| **27** | Access Points must have the ability to run local layer 2, layer 3, and layer 7 firewall rules. |  |
| **28** | Access Points must support at least 15 SSIDs simultaneously |  |
| **29** | Access Points must have the ability to identify themselves by flashing their LED status light on command. |  |
| **30** | Access Points must have a local landing page for client troubleshooting, which must include device information for both the AP and Client, as well as signal strength and nearby interference sources. |  |
| **31** | Access Points must automatically transition to repeaters in the event of a loss of network connectivity. |  |
| **32** | Access Points must include Location Analytic information to track visitor frequency, duration of stay, and number of daily visitors. |  |
| **33** | Access Points must natively integrate with a Mobile Device Management application for automatic onboarding and provisioning. |  |
| **34** | The new infrastructure must have the potential to extend the platform across switching and security, maintaining a single management platform. |  |
| **35** | The management application must allow for multiple sites, and multiple levels of administrative roles, including “read-only”, “monitor-only” and Guest Admin (for creating guest Wireless Access) |  |
| **36** | The management solution must include a free Mobile App for basic management and reporting, which must run on the latest iOS and Android platforms. |  |
| **37** | 100% device configuration done via dashboard/GUI |  |

**System Testing/Acceptance**

User Acceptance Testing must be conducted and verified by post installation survey to confirm the coverage, signal strength and speed of the installed solution. It is our understanding that the industry-standard tool for this is Ekahau, please can you confirm whether you use this solution and any certifications that you hold for this type of works. If you do not use Ekahau, please provide details on the solution used.

**Professional Development – Staff Training**

We would require appropriate Cisco Meraki training for 4 staff at HQ to be built into tender response.

Full administration training to be provided onsite by trained and accredited personnel/trainers to IT staff.