Q1. Software Estate Definition

Please provide a comprehensive inventory of all software in scope for patch management, including:

• Endpoint applications (standard and non-standard)
Microsoft 365, OpenVPN, Foxit, Cysgliad, Websys, Bitdefender

• Server applications and roles

Hosts DHCP in office, VPN server, Microsoft SQL and print server, Backup manager

• Line-of-business systems

AccountsIQ (Finance Software); Moorepay (HR and Payroll); OnBoard (Governance Management Platform); Press Data Media HQ (Media Database)

• Security tools and agents

Intune, Action 1, Bitdefender and Windows Defender

• Network device firmware/software

Draytek 2962, firmware 4.4.6.1, 2 x Draytek and one HP gigabit switch

• Any bespoke or legacy applications

Websys (CRM)

• Any software hosted externally but managed by HCC

No

Please confirm whether any additional software is expected to be discovered post-award via audit, and how this should be treated commercially. None expected

2. Patch Responsibility Boundaries

Please confirm the expected scope of patching responsibility, specifically:

• Should the MSP be responsible for all software installed on endpoints and servers, regardless of vendor?
Yes

• Are SaaS platforms (e.g. Microsoft 365, AccountsIQ, Moorepay) considered in scope for patching, or is responsibility limited to configuration and security management?

Yes

• Are there any third-party managed systems or environments (e.g. Welsh Government infrastructure) where patching responsibility remains outside MSP control?

Yes EID WG control Wi-Fi (Per attachment shared)

Q3. Patch Frequency & Priority Expectations

Please confirm HCC Group's expectations regarding:

• Frequency of patching (e.g. monthly cycles, weekly updates, emergency patching)

Monthly for most

• Priority handling of critical vulnerabilities (e.g. zero-day CVEs)

Immediate

• Required timelines for deployment of critical vs standard patches If not prescribed, please confirm that suppliers are expected to propose an appropriate patching framework. We expect suppliers to propose appropriate patching framework timelines

Q4. Vulnerability Management Approach

Please confirm:

• Expected response approach to critical or actively exploited CVEs

Remediation as soon as possible

• Whether immediate patching is required, or if risk-based assessment and staged rollout is acceptable

Immediate for critical staged for rest

• Whether HCC Group has a defined risk tolerance or acceptance process for delaying patches where stability concerns exist

Servers are patched within 14 days, but none are internet facing , critical patches on laptops pushed out ASAP

Q5. Backup & Recovery Requirements for Patching Activities

Please confirm:

• Whether verified backups or snapshots are required prior to patching (particularly for servers and critical systems)

Yes for servers

• Any defined backup frequency, retention, and validation requirements

Daily backups of Servers and Microsoft 365 environment, minimum 30 days retention, monthly test restores

• How conflicts should be managed where urgent patching requirements overlap with backup windows or availability constraints

Backup first

Q6. Patch Failure & Rollback Expectations

Please confirm:

• Expected process in the event of a failed or disruptive patch

Remove if installed, if failed check and remediate

• Whether the MSP is responsible for remediation regardless of root cause (including vendor patch issues)

Yes

• Whether a formal rollback strategy (e.g. snapshots, staged deployment) is expected within the service

Yes for Servers

7. Change Control & Deployment Model Purpose: Control automation risk

Q7. Change Management Expectations for Patching

Please confirm:

• Whether all patching activities must follow formal change control procedures This will be for the supplier to manage in line with SLA and own internal control procedures

• Whether a phased/controlled deployment approach (e.g. pilot groups, staged rollout) is required or preferred

As most of the applications are standard MS 365 and no laptops are business critical routine patching suffices, the servers are snapshotted prior to roll out

• Any restrictions on out-of-hours or automated patch deployment

No anytime between 19:00 and 07:00 for servers, devices as they are available to patch

8. Out-of-Scope / Third-Party Dependencies Purpose: Identify where you can't control risk Q8. Third-Party and External System Dependencies

Please confirm:

• Any systems managed by third parties or external providers where patching is not within MSP control

Yes

Moorepay (HR and Payroll), AccountsIQ (accounts software), OnBoard (Governance Platform); Websys (CRM); Media HQ (Media Database)

• Any dependencies on Welsh Government-managed infrastructure where patching responsibility is excluded

No

Q9. Endpoint Data Protection Prior to Patching

Please confirm:

• Whether full device backup is required prior to endpoint patching

No

• Or whether reliance on cloud-based services (e.g. OneDrive/SharePoint) is considered sufficient

Yes One Drive / SharePoint is sufficient.

Users are made aware not to store data on local devices

• Expected recovery approach in case of endpoint failure post-patching

Remote access if possible; if not access to the device when it's in the office

10. Commercial Assumption In the absence of a complete and defined software inventory, bidders request confirmation that:

• Pricing may be based on the assumed standard Microsoft-based estate described, and
Yes

• Any material deviation in software volume, complexity, or patching requirements identified post-award will be subject to review and adjustment

Yes