Q222 iQuda Patch Policy

1. Purpose

This Patch Policy document outlines the policy and process that iQuda Ltd (iQuda) follows with respect to patch/update management, both internally at iQuda and for clients for whom iQuda has IT management responsibility.

2. Audience

This policy has been developed for internal and external viewing. The policy will be made available to all staff working at iQuda, and to all clients and prospective clients we support. Copies may be made available on the company website (www.iquda.co.uk).

3. Definitions

Patch/Update	A patch or update is a software update comprised code inserted (or patched) into the code of an executable program. Typically, a patch is installed into an existing software program. Patches are often temporary fixes between full releases of a software package. Patches may do any of the following: • Fix a software bug • Install new drivers • Address new security vulnerabilities • Address software stability issues • Upgrade the software
Remote Monitoring and Management (RMM Tool)	A Remote Monitoring and Management (RMM) tool is deployed through an "agent" (a small software footprint), which is installed on client systems, workstations, servers, mobile devices etc. It's these agents that send back to the deploying party (in this case iQuda) information about client machines. This information includes machine status, machine health and more. Therefore, by deploying RMM tools, the deployer can gather insight into client networks. We are thus able to monitor machines remotely, maintain them and keep them up-to-date and even get the machines to stay ahead of issues and resolve them remotely. An RMM also allows iQuda to detect, manage, monitor, test and deploy security patches.
Unpatched Workstations	An unpatched device is a device for which patches are available but have not been applied. This can occur for any number of reasons but may occur in the following circumstances: • The device is no longer illegible to receive updates from the vendor.

	• The device has not been switched on and can therefore not apply relevant patches. • The device is malfunctioning. • Patches are incompatible with the device.
Asset	An information asset is any data, device, or other component of the environment that supports information-related activities. Information assets are divided into two categories: • - IT Assets • - Non-IT Assets IT Assets include Information systems (e.g. servers), applications, and network devices that store, process, or transmit information, and enable iQuda or it's clients to conduct its IT operations. Non-IT Asset are assets which are key for the storage, processing and transmission of information (such as data centres, server rooms, Office locations, hard copies of documents, etc.).
Threat	Any circumstance or event with the potential to adversely impact an IT asset through unauthorized access, destruction, disclosure and/or modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit an asset vulnerability.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by an attacker or lead to any other undesirable event compromising the security of an IT asset.
Technical Team	The Technical Team at iQuda are responsible for proactive IT management and maintenance both within the company and for customers whose IT systems are managed by iQuda.
Best-Effort Basis	Best effort basis is an agreement that something will be attempted without any guarantee provided that it will succeed. The term implies use of an improvised approach and extraordinary efforts in the context of challenging conditions or constraints.

4. Overview

Security is highly important to the integrity of iQuda's IT infrastructure and that of our clients. In order to protect the confidentiality, availability and integrity of these systems, it is company policy to apply vendor released security updates ('patches') on a regular basis. Patches are necessary to protect systems, applications and data from malicious attacks, threats and malfunction. This policy defines our committed and approach to patch management.

5. Scope

This policy applies to all IT equipment (hardware & software) used within iQuda or managed by iQuda on behalf of our clients. All persons employed by iQuda (whether permanent, temporary, voluntary or contractual) who are involved in maintaining, configuring or managing these systems, will be required to adhere to this policy.

IT equipment covered by this policy may include, but is not limited to:

- Computers – including servers, desktops PCs, laptops, notebooks, netbooks etc.
- Portable devices – including mobile phones, tablets, iPads etc.
- Applications – including operating systems, Microsoft Office packages, email systems, customer relationship management systems, security applications etc. whether cloud or locally based.
- Networking equipment – including firewalls, routers, modems, switches etc.
- Phone systems – including VoIP telephony systems, PABX equipment etc.
- Cloud based systems and applications.
- Peripheral devices – including mouse/keyboard, webcams, projectors, monitors, external hard drives, SAN devices etc.
- Printers, scanners, copiers etc.

6. General

All systems and software shall be protected from known and emerging vulnerabilities by regularly installing vendor released security patches. iQuda shall implement patch management procedures that allow the organization to accurately identify, assess, test and deploy patches to its assets and those of its clients.

Critical security patches will be applied as soon as possible after they are released, and within a maximum of 30 days from their initial release.

Any systems that are no longer eligible to receive security patches will be recommended for replacement and supported on a best-effort basis. This means that iQuda cannot guarantee they will function properly or securely.

Any exception to this policy will be documented by iQuda and reported to the relevant customer if applicable, for review, endorsement or rejection.

7. Patch Policy

7.1. Unpatched workstations

Where a workstation is unpatched, iQuda will use an automated Remote Management and Monitoring (RMM) scripting tool to notify the customer that the workstation in question must be powered on at the end of the day in order for necessary patches to install. The RMM script will immediately set the workstation to remain active and not enter sleep mode, and will schedule installation of relevant patches, and an automatic reboot of the workstation to commence at 20H00.

7.2. Roles and Responsibilities

The technical team at iQuda will manage all patching at iQuda or at the sites we manage (client sites).

The technical teams' responsibilities will include:

- Patch monitoring and identification.

- Patch assessment, authentication, review, pre-installation testing and security verification.
- Patch deployment.
- Patch management for all ICT infrastructure on the network, operating systems, software and associated components that are covered by the managed services agreement (client sites) or owned and operated by iQuda.
- Patch management for on-site applications that include an update facility and that are covered by the managed services agreement (client sites) or owned and operated by iQuda.
- Reporting compliance with the patch policy and guidance on security issues/general patch status.
- Identifying workarounds where patches cannot be applied or will not install.

The technical teams' responsibilities will not include:

- Patch management on any devices or applications at the client's site which are not covered under the scope of the managed services agreement.

The Data Protection Officer will be responsible for the development, maintenance and enforcement of this policy.

All staff at iQuda, whether permanent, temporary or locum will be responsible for adhering to this policy.

7.3. Client Responsibilities

When their IT systems are managed by iQuda, our clients still retain certain responsibilities. These include:

- Ensuring machines are not disconnected from the network for extended periods – if a machine is disconnected, iQuda will be unable to manage the machine remotely. Therefore, critical security patches will not be applied to the machine.
- Notifying iQuda if machines are retired or due to be retired.
- Issuing internal communications regarding patch schedules and ensuring that machines the client wishes to be patched are available for patching.
- To discourage patching exemptions from becoming 'the norm'. without an oraganised and controlled patch application frequency, IT system security and consistency will rapidly diminish.
- To strongly avoid and discourage the use of any and all systems which are no longer eligible to receive patches. iQuda cannot guarantee the performance, security, reliability or consistency of these systems, therefore they will only be supported on a 'best-effort' basis.

8. Patch Schedule

iQuda Patch Schedule – Internal and Client-Side			
	Servers 8 x 5	**Workstations**	**Laptops**
Detection	19H00 daily	Every 2 hours, daily	Every 2 hours, daily
Pre-Download	23H00 daily	01H00 daily	01H00 daily
Installation	1:00 daily	Every 2 hours, daily	Every 2 hours, daily
Reboot	4:00 each Thursday	Prompts daily, only if reboot required	Prompts daily if only reboot required

9. Emergency Patches

iQuda recognises that there are instances were emergency patches must be applied to prevent a seriously untoward security event from impacting iQuda or its clients. In this event, an emergency patching procedure will be carried out with high priority. The emergency patch procedure will adhere to the patch policy and patch policy process.

10. Patch Policy Process

iQuda will follow this patch policy process to manage patches and ensure they are deployed in a safe and timely manner. This process will be followed throughout the patch management lifecycle, and includes procedures to identify, assess, test, deploy, report on, and monitor patches on an ongoing basis. The process includes continual improvement actions to ensure that the process is routinely improved.

11. Identification, Assessment & Testing

The Technical Team will use the following process to identify patches:

1. Identify all systems and applications to be patched. iQuda will identify these systems through the use of network detection tool, RMM tools, and
2. Establish list of required patches and updates using RMM tools, manual checks and network scans. Confirm validity, integrity and security of all released patches against site-to-site knowledge, vendor notifications and security reports.
3. Confirm patches have been tested for applicability to destination IT infrastructure via RMM tools. Investigate patches which have failed or bypassed tests and conduct manual testing.
4. Investigate whether any known compatability issues exist, and whether patches are likely to cause disruption.
5. Piroritise patches according to age, importance and severity. iQuda will prioritise patches according to current cyber security and/or vendor security risks, issues and events.
6. Document any and all patches which will not be applied, along with clear reasoning.
7. Schedule patch application, installation and system reboot according to the pre-agreed patch schedule and document on internal and customer site documentation.

12. Acquisition

- Verify the source of all patches to ensure the source is secure, reputable and trustworthy.

- Download from the IT system or application vendor, all patches and updates identified during the identification, assessment & testing phase.
- Conduct antivirus scans on all downloaded patches and updates to verify their security and integrity.
- Ringfence any patches or updates which may pose an information security risk if applied.
- Document the sources, patches identified and results of antivirus scans.

13. Deployment

- Issue communications to relevant parties as required regarding patch deployment. In most cases the deployment phase will be pre-agreed according to the patch schedule.
- Deploy patches according to patch schedule, ensuring that any unscheduled changes are avoided which may interrupt the patch process and have an adverse effect on the systems or applications receiving patches.
- Document the completion of the deployment phase.

14. Post-Patch Investigation & Monitoring

- Confirm that all patches and updates which passed the testing phase are applied.
- Confirm that patching has not resulted in any adverse effects on any systems or applications. These results will be confirmed using RMM tools and manual checks.
- Highlight any and all patch or update application failures and adverse effects.
- In the event of any adverse effects, iQuda will use backups and system roll backs where possible to reverse the system or application to the pre-patched state.
- Investigate and establish the reason for patch failure and resolve where possible before reattempting patch application.
- Rescan the environment to ensure that all available and applicable patches and updates are applied.
- Document the completion of the post-patch investigation and monitoring phase and issue relevant communications to all parties concerned.
- Update all relevant configuration and inventory documentation to reflect patches and updates applied.

15. Reporting

- Issue patch report to all parties concerned stating the success and/or failure of the patching process.

16. Continual Improvement

- Identify any 'lessons learned' and document to ensure continual improvement of the patch policy and process.

17. Exemption Process

iQuda acknowledges that in certain circumstances there will be exemptions to this policy. Systems or applications for which patches or updates are missing or cannot be applied according to the patch

schedule, will be documented, closely monitored and managed to ensure their ongoing security, reliability and consistency. All patches and updates will be applied as soon as possible once the exemption concerned is no longer required. Please note that the majority of exemptions will be granted only where patch application will result in severe interruption. Systems which remain unpatched for long periods of time will be investigated individually and recommended for disconnection from the network.

18. Enforcement

iQuda will enforce and monitor compliance with this policy. The policy will be enforced internally and at all relevant client sites where an appropriate managed services agreement is in place.

Any system found in violation of this policy shall require immediate corrective action. Noncompliance with the policy will be handled in line with iQuda disciplinary procedures.

19. Adjustments

This policy will be amended from time to time at the discretion of iQuda. Clients whose IT systems are managed by iQuda may recommend adjustments by request. All requests should be directed to the Data Protection Officer by email at info@iquda.co.uk or by phone on 01442 251 514.

20. Policy Review

This policy will be reviewed at least annually. Compliance with the policy will be tested regularly through the performance appraisal process, audits, compliance spot checks and routine monitoring.