Patching Policy

1. **Introduction**

1.1 Computer systems that connect to the INA Prime Solutions network, including application, operating system and network infrastructure, must be protected from malicious code, ransomware, and hacking attacks which could exploit security vulnerabilities. To meet this requirement, critical security patches must be installed universally across applicable infrastructure when they become available.

2. **Policy statement**

2.1. The purpose of this document is to outline a INA patching strategy incorporating maintenance windows, and allowing for regular testing of backup procedures. IT Department staff would be the main users of this document, and are required to ensure desktops, servers, and applications are regularly backed up, patched, and kept up-to-date.

3. **Roles and Responsibilities**

3.1. The following roles and responsibilities apply in relation to this Policy where appropriate:

3.1.1. **Vice President - Technology & Operations**

- To review and approve the policy on a periodic basis

3.1.2. **IT General Manager**

- To ensure the Policy is reviewed and approved by the VP - Technology & Operations
- To adhere to the standards defined in this policy
- To consult as appropriate with members of the Management Teams
- To liaise with the VP - Technology & Operations on information received in relation to potential breaches of the policy
- To ensure the appropriate standards and procedures are in place to support the policy
- To define and implement standards and procedures which enforce the policy
- To oversee, in conjunction with Data Owners, compliance with the policy and supporting standards and procedures.

3.1.3. **Staff**

- To adhere to the practices contained in this document
- To report suspected breaches of this policy to their manager

4. **Scope**

4.1. This Patching Policy covers the deployment of security updates to operating systems installed on INA procured desktops and portable devices, network infrastructure, and application software.

4.2. This policy applies to, but is not limited to all staff, contractual workers and third-party suppliers.

4. **Supporting Standards & Procedures**

4.1. The Policy should be read in conjunction with the following INA Prime Solutions policies and Users should ensure compliance with these policies in addition to this policy:

- Data Protection Policy
- Data Retention Policy
- IT Operations and Network Security Policy
- Acceptable Use Policy

5. **Operating System Patching - (Microsoft)**

5.1. **Patch Sourcing**

5.1.1. Microsoft releases security patches on the second, and occasionally the fourth Tuesday of each month. Critical patches and updates will be approved and made available via the centrally provided patching service within ten working days of Microsoft release. Other patches and updates will be made available via the centrally provided patching service within thirty working days of Microsoft release.

5.1.2. If problems are discovered with the patches during the initial ten day period, the patch will not be released. Should adverse conditions be met subsequent to deploying a patch into a production environment, patch roll-back will be initiated.

5.1.3. Any member of staff who discovers a problem with a patch during testing is required to alert the IT Department by emailing details to it@inaprime.com

5.2. **Accelerated Patch Release**

5.2.1. When an exploit to a vulnerability is published prior to the deployment of a patch, an assessment will be carried out by the IT Department to determine whether a reduced testing period and/or early deployment is considered necessary.

5.2.2. Where the risk of system compromise is considered to be greater than the deployment of a new patch and/or service pack, a decision will be taken to release early.

5.3. **Service Pack Testing, Deployment and Compliance Reporting**

5.3.1. The IT Department will release service packs through the centrally provided update service. Service packs are to be released to test environments prior to deployment, although the testing of them will vary depending upon their complexity. Should issues be identified during the test phase, roll-back will be initiated on the affected systems.

5.3.2. The IT Department will use an automated mechanism for reporting service pack compliance of machines that are connected to the INA Domain. INA IT Department support staff who utilize the reporting facility are responsible for confirming the service pack compliance of their systems, and for taking prompt remedial action where systems are found to be not fully up to date.

5.4. **Desktops**

5.4.1. All Windows-based desktop computers and portable devices that are attached to the INA network must be fully patched and up to date.

5.5. **Servers**

5.5.1. Servers running Windows Server Operating systems are to have security patches applied within ten working days of the patch release. Deployment must be implemented on all INA servers. Reboot schedules are to be chosen by the IT General Manager rather than being fully automated.

5.5.2. An email is to be sent to it@inaprime.com reporting any issues that need to be raised concerning the deployment of server patches.

6. Operating System Patching - (Non-Microsoft Operating Systems)

6.1. Patch Sourcing

6.1.1. All INA IT staff with a responsibility for the maintenance of desktop machines and servers that run operating systems other than Windows, are required to subscribe to the appropriate security mailing services of their respective technology providers, so that they are kept up to date with details of vulnerabilities, exploits and patches associated with their particular platform.

6.2. Apple Devices and Desktops

6.2.1. All Apple desktops that are attached to the INA network must be fully patched and up to date. Portable devices, including devices that are not connected to the INA network for lengthy periods of time must be fully patched up to date prior to connecting to the INA network.

6.2.2. Updates are downloaded and approved to a central Apple server that is running the Apple Software update server role. All managed Mac OS devices connected to the INA network will acquire updates from this server. Critical updates are tested and released within ten working days of release from Apple. The IT General Manager is responsible for implementing policies to apply patches and updates.

6.3. Linux and Unix Based Operating Systems

6.3.1. The IT Department will ensure automated updates are applied to Linux Systems.

6.3.2. All INA IT staff operating Linux and Unix based systems are responsible for the delivery of patches and updates in a timely manner. In addition, the effectiveness of the patch deployment must be demonstrable.

6.4. VMWare and other virtual environments

6.4.1. The IT Department will regularly monitor for critical VMWare and other virtual environment updates . Updating VMWare will not cause service disruption, once all servers hosted on the VMWare environment are capable of VMotion. Each VMWare server will be patched in succession on a monthly basis. Where hosted servers are not capable of VMotion, the VMWare server hosting these servers will be patched during a maintenance window.

7. **Network Infrastructure including Switches, Firewalls and Application Domain Controllers**

7.1. The IT Department subscribes to appropriate security alert emailing lists and proactively monitors appropriate websites for notification of any vulnerabilities affecting network infrastructure.

7.2. Where vulnerabilities are found to apply to network infrastructure, advice will be sought from the relevant third party supplier to determine whether it is feasible to use a work-around solution rather than apply a patch immediately. Where possible the application of patches will be deferred until the next available scheduled maintenance window. However, where deferment is not advisable, a risk assessment will be carried out by the IT Department and remedial action will be taken.

8. **Application Tier Patching**

8.1. **Microsoft Applications**

8.1.1. Critical patches and updates will be approved and made available within ten working days of Microsoft release. Other patches and updates will be made available within thirty working days of Microsoft release.

8.1.2. Microsoft Update is available to patch all other Microsoft Products. Patch management schedules must fulfill delivery in a timely manner so that deployment is completed in conjunction with the centralized roll-out. The IT Department is responsible for implementing policies to apply patches and updates.

8.2. **Other Applications (e.g. Google, Chrome, Adobe, etc.)**

8.2.1. IT staff that are responsible for the maintenance of applications running on desktops and servers must ensure these applications are patched and up-to-date. IT staff are required to subscribe to the appropriate security mailing services for their respective technology providers, so that they are kept up to date with details of vulnerabilities, exploits and patches associated with their particular platform.

8.2.2. Where vulnerabilities are found in these applications, advice should be sought from the relevant third party supplier, where applicable, to determine whether it is feasible to use a work-around solution rather than apply a patch immediately. Where possible the application of patches will be deferred until the next available scheduled maintenance window. However, where deferment is not advisable, a risk assessment will be carried out by the IT Department and remedial action will be taken.

9. **Exception Process**

9.1. In circumstances where compliance with some or all of this policy is not practically achievable in the immediate term, an exception must be documented and approved. This will require detailing the nature of the exception, and any steps that can be taken to mitigate the resulting risk.

10. **Monitoring**

10.1. Systems must be monitored to ensure that the patches have been applied. The IT Department will use an automated mechanism for reporting the patching compliance of desktops and servers that are attached to the INA Domain. IT staff who participate in the reporting mechanism are responsible for confirming the patch compliance of their systems and taking prompt remedial action where systems are found to be not fully up to date.

11. **Backup Processes**

11.1. The IT Department is responsible for ensuring a robust backup and recovery environment for INA Prime Solutions Enterprise Systems and Business Applications.

12. **Violation of Policy**

12.1. When the perceived risk warrants such action, devices that are not kept fully up to date with patches and service packs may have their network access blocked to ensure the INA network is protected against potential threats.

12.2. Devices that are blocked from the network will only be reconnected when it can be demonstrated that they have been brought up to date, and are secure.

Review and update of this document will take place when changes require revising the **Patching Policy**. Such modifications may relate to changes in roles and responsibilities, release of new legislation or the identification of a new policy area, in consultation with appropriate members and their approval on all revisions to this Patching Policy. When approved a new version of the policy will be issued and all affected departments will be informed of the changes.