Title: Security Patch Management

Effective Date: 11/10; Rev.: 07/12

POLICY: Security patching of computer systems attached to the IHS network will follow a defined process that includes, but is not limited to, risk assessment, testing, scheduling, installing, and verifying, regardless of the platform or criticality of the patch.

SCOPE: IHS system wide. All IHS and affiliate facilities including, but not limited to, hospitals, ambulatory surgery centers, home care programs, physician practices, all IHS and affiliate departments, and covered group health plans.

BACKGROUND: The purpose of this policy is to ensure that IHS computer systems are patched in a way that ensures a consistently configured environment that is secure against known vulnerabilities in operating systems (i.e. Windows), database systems (i.e. SQL), and other systems software (i.e. Internet Information Server).

Due to the varying requirements of application security patching, application patching is not included in this policy.

Due to the complexity and lowered risk of exposure, security patching of low-level components of computers and servers, (i.e. BIOS and Device Drivers) are not included in this policy.

PROCEDURES:

1. Definitions.

1.1 Security Patch Management: Process that involves acquiring, assessing, testing, installing, and verifying Security Patches (or “fixes”) for IHS computer systems.

1.2 Vulnerability: A weakness in the operating system or system software that could be exploited for any number of reasons, including, but not limited to, executing malicious code, tampering with data, or hindering network activity.
1.3 **Security Patch:** A fix to a program that eliminates a Vulnerability that can be exploited by malicious hackers.

1.4 **IHS Computer Systems:** Mainframes, mini and microcomputers/personal computers (PCs), laptops, servers, networks, routers, bridges, hubs, and various peripheral equipment (e.g. printers and modems) and the software (i.e. operating system) installed on these systems that are owned, leased or maintained by IHS.

1.5 **System Administrator:** A person who manages and maintains an IHS Computer System. This includes, but is not limited to, server administrators, network administrators, database administrators, and Biomed administrators.

2. **Monitoring.**

2.1 System Administrators are responsible for monitoring vendor notifications and/or websites, security mailing lists, and other public websites for the availability of new Security Patch releases as they apply to their system. If automated patch management solutions will be used to monitor for patch releases, the solution must be able to provide information regarding available patches, criticality of patches, and systems affected.

3. **Review and Evaluation.**

3.1 System Administrators are responsible for reviewing each available patch relevant to their system (including reading and understanding applicable release notes), evaluating each patch, and categorizing the criticality of each patch according to the following:

   3.1.1 Emergency – Targets an imminent threat to IHS systems and/or network.

   3.1.2 Critical – Targets a known security Vulnerability that affects IHS systems and/or network.

   3.1.3 Non-Security – A standard patch release update that applies to IHS Computer Systems, but is not intended to fix a security flaw.

   3.1.4 Not Applicable – No IHS systems affected.

3.2 The criticality of patches, as defined in section 3.1 in this policy, that are applied to the production environment should be documented in the associated Change Control.
3.3 It is the responsibility of the affiliate System Administrator to review patches and their applicability to FDA-regulated devices (i.e. Biomed devices, etc.) and alert the Information Technology Department when it is appropriate to install the patches.

3.4 IHS is dependent on application vendors to ensure their products are compatible with the new Security Patches being released. In the event that a patch fails testing or is not acceptable by an application vendor, System Administrators must implement mitigating controls to reduce the risk of the patch not being applied to the IHS environment. The System Administrator is also responsible for documenting the patch exception on the Patch Exception Form located on the Intranet in accordance with 4.4.2 of this policy.

3.4.1 It is the responsibility of the analyst(s) who supports an application to alert the server administrator(s) if a patch cannot be applied to the servers/workstations on which their supported application resides.

4. Testing and Installation.

4.1 If the System Administrator and/or Information Protection categorizes a patch as an Emergency that will fix an imminent threat to IHS systems, then the testing/install schedule for the specific patch may be expedited. The Manager of Information Protection and the manager of the affected IHS system will determine/approve the expedited testing and install schedule.

4.2 All Emergency and Critical Security Patches must be acquired for testing on IHS Computer Systems within 10 business days of the patch release date.

4.3 It is recommended, but not required by this policy, that non-Security Patches be acquired for testing at least quarterly and a determination made as to whether or not the patch will be installed in the production environment.

4.4 All Security Patches will be tested for 2 weeks before being installed in the production environment, excepting Emergency patches if an expedited testing schedule is approved per paragraph 4.1 of this policy. Testing must include validation that the patch was successfully applied and did not cause adverse effects.

4.4.1 If during testing, it is determined that a Security Patch will adversely impact the production environment, the patch will not be pushed to production and other steps to mitigate the Vulnerability must be investigated.
4.4.2 If a Security Patch is not applied to the production environment, the exception must be documented with the following information and submitted to Information Protection for approval via the Patch Exception Form found on the Intranet:

- System(s) Affected
- Name and/or Number of Patch
- Criticality of Patch
- Release date of Patch
- Patch testing date(s)
- Reason Patch was not applied to production
- Mitigating controls applied in place of patch
- IT Manager who approved Patch Exception

Information Protection will store the patch exceptions in the Exceptions Database located in the Audit & Compliance shared directory.

4.5 All Security Patch installations in the production environment must follow the change control process.

4.6 Non-Security Patches should be installed during regularly scheduled system maintenance to reduce impact to end users. Emergency and Critical Security Patches may be installed outside of regularly scheduled system maintenance only if it is deemed necessary by the Manager of Information Protection and the manager of the affected IHS system.

4.8 Newly installed devices must be patched to the latest patch level according to the specific documented patch management procedures as defined by the System Administrator(s).

5. Verification and Auditing.

5.1 Following the release of all Security Patches to the production environment, the System Administrator(s) is responsible for verifying the patch was installed on all affected systems, and that there are no adverse effects to production systems. System Administrator(s) are responsible for ensuring that patches are installed by manual methods if automated pushes fail on their respective computer systems.

5.2 If adverse effects exist after Security Patch installation, it is the responsibility of the System Administrator to document and implement the roll-back process as defined in the Change Control documentation for the patch. Documentation of the patch roll-back process and the affected system must
also be provided to Information Protection for audit purposes via the Patch Exception Form found on the Intranet.

5.3 Information Protection will conduct quarterly audits on random samplings of IHS computers to ensure Security Patch levels and documentation of patch exceptions are in compliance with this policy.

6. **User Responsibility.**

6.1 At the close of business each day, users should close all applications and logoff of Windows, leaving the PC powered on to receive security and/or software updates overnight. If PCs are taken off the network or shut down overnight, the updates will be installed on the PC the next time the device is attached to the network and powered on.

6.2 Users must not interfere or disrupt the Security Patch installation process on their computers.

7. **Violations.**

7.1 Violations of this policy may result in disciplinary actions at the department level, immediate revocation of system access, and/or termination of employment or business contract.


/s/ William B. Leaver

William B. Leaver
IHS President