Information Security

Patch Management Procedure

Version: 1.0

This version issued: 21/06/20

Date approved: 21/06/20

Date for review: 21/6/21

Owner: Matt Francis, Chief Information Officer

A. Procedure

1. Audience

1.1 All employees performing roles of system or application administrators managing Procreation UK Limited ICT services and systems. This procedure also applies to contractors, vendors and others managing Procreation UK Limited ICT services and systems.

2. Executive Summary

2.1 Procreation UK Limited is committed to and is responsible for ensuring the confidentiality, integrity, and availability of the data and information stored on its systems.

2.2 The IT Staff at Procreation UK Limited have an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, worms, and software bugs which could adversely affect the security of a system or the data entrusted on the system. Effective implementation of this procedure will limit the exposure and effect of common malware threats and vulnerability exploitation to the systems within this scope.

3. Scope

3.1 This procedure covers all computers, servers, systems, applications, and network infrastructure owned and maintained by Procreation UK Limited and it's approved suppliers, and the administrators of all such systems and networks.

3.2 This procedure is primarily aimed at system administrators and technical staff, including IT Services' staff who are responsible for the ongoing maintenance of ICT services and systems. The scope also extends to anyone else who is similarly undertaking activities governed by this procedure.

4. Patch Management Procedures

4.1 All Procreation UK Limited owned and maintained computers, computer systems, computer networks and electronic communications devices must be updated with the latest but stable patches released by the respective vendors.

(a) A System Owner or team must be identified for the overall security management of each system or device.

(b) Those responsible for each system, device and application must monitor relevant sources of information which may alert them to a need to act in relation to new security vulnerabilities.

(c) Patches must be obtained from a known, trusted source.

(d) The integrity of patches must be verified through such means as comparisons of cryptographic hashes to ensure the patch obtained is the correct, unaltered patch.

(e) Patches must be tested and assessed before implementation in a production environment to ensure that there is no negative impact as a result.

(f) A backup of the production systems must be taken before applying any patch.

(g) An audit trail of all changes must be created and documented. The System Owner must verify that the patches have been installed successfully after production deployment.

(h) Production patches must be deployed regularly as per the SLA defined below.

(i) System owners outside of IT Services that manage the security of their own systems are required to use patches in accordance with this procedure.

(j) A Request for Change (RFC) must be raised for all patch deployments including emergency updates, critical and operational updates.

(k) Refer Information Security Operations Management Procedure for guidelines to be followed for Change Management Process

4.2 SLA with Priority

(a) Patches must be deployed as per below mentioned category classification and SLAs from the time of the patch being released.

Device Type	Potential Business Impact	Critical	High	Medium	Low	Compliance	
						Target	Acceptable Level
Internet Facing		2 hrs	4 hrs	8 hrs	24 hrs	100%	98%
Non-Internet Facing		4 hrs	8 hrs	24 hrs	3 days	100%	98%
Laptops / Desktops		8 hrs	24 hrs	24 hrs	7 days	100%	98%
Network Devices		Within 5 days			7 days	100%	98%

4.3 Category Definitions to be considered for Patch Deployment

Rating	Red Hati, Microsoftii & Adobeiii Rating	Typical CVSS Scoreiv	Description
Critical	Critical	10	A vulnerability whose exploitation could allow code execution or complete system compromise without user interaction. These scenarios include self-propagating malware or unavoidable common use scenarios where code execution occurs *without* warnings or prompts. This could include browsing to a web page or opening an email or no action at all.
High	Important	7.0 – 9.9	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources. This includes common use scenarios where a system is compromised *with* warnings or prompts, regardless their provenance, quality, or usability. Sequences of user actions that do not generate prompts or warnings are also covered.
Medium	Moderate	4.0 – 6.9	Impact of the vulnerability is mitigated to a significant degree by factors such as authentication requirements or applicability only to non-default configurations. The vulnerability is normally difficult to exploit.
Low	Low	< 4.0	This classification applies to all other issues that have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences

4.4 Error handling and Exception Handling

(a) Error handling:
The System Owner or team is responsible for identifying and rectifying failed patch deployments. Compliance with approved patches must be verified at least on a weekly basis.

Note: Exceptional cases may be considered including, but not limited to, where the impact of applying a patch (downtime etc.) is higher than the impact of not applying the patch, e.g. taking down a system running a compute. In such cases appropriate compensating controls must still be implemented until such time as the patch can be applied.

4.5 Patch Enforcement

(a) Implementation and enforcement of this procedure is the responsibility of System Owners. Procreation UK Limited or it's clients may conduct random external and internal vulnerability assessments to ensure compliance with this procedure without notice. Any system found in violation of this procedure shall require corrective action.

4.6 Monitoring and Reporting

(a) All System Owner and teams responsible for the administration of systems defined within the scope above are required to constantly monitor the outcome of each patching cycle. Reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk.

5. Roles and Responsibilities

Role	Responsibilities
System Owner	The System is responsible for the overall security management of each system or device that is assigned to them.
IT Security	Responsible for the following: ○ routinely performing compliance checks with the patch management procedure; ○ providing guidance in issues of security and patch management; ○ ensuring that if something is not secure, it is included on the ICT agenda driving and documenting the status.

About this Document

Approval Authority	Chief Information Officer
Subject Matter Expert	Graham Potter
Contact Details	graham@procreation.tv
Review Date	June 2021

Further information

i Red Hat Issue Severity Classification - https://access.redhat.com/security/updates/classification

ii Microsoft Severity Ratings - https://technet.microsoft.com/en-us/security/gg309177.aspx

iii Adobe Severity Ratings - https://helpx.adobe.com/security/severity-ratings.html

iv CVSS Scoring - https://nvd.nist.gov/cvss.cfm