Information Security Management System
Patch Management Policy & Procedure

Document no. JMBGRP/ISMS/Pol-PM

Version no. v1.2

Document details

Classification	Internal	
Released date	28.08.2018	
Description	The policy document is to manage the various patches.	
Custodian	Corporate IT dept.	
Approved by	Manish Jaiswal (Group CTO)	
Owner	Corporate IT Dept.	

Distribution list

Name
To all locations of JMB group.

Version History

Version no.	**Version date**	**Approved by**	**Comments**	**Signature**
v1.0	28.08.2018	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	10.01.2019	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	08.02.2020	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.0	11.02.2021	Manish Jaiswal (Group CTO)	Reviewed & no changes	
v1.1	25.03.2022	Manish Jaiswal (Group CTO)	Logo changes done in this policy	
v1.2	18.08.2023	Manish Jaiswal (Group CTO)	Document reviewed. Modification done to “References”	
v1.3	16.10.2024	Manish Jaiswal (Group CTO)	Document reviewed. Modifications done in Section: “3,4,7,8”	

Contents

Purpose

Patch management is about mitigating risk to the confidentiality of JMBGRP's data and the integrity of JMBGRP systems. Patch management can be the most effective tool used to protect against vulnerabilities and the least expensive to maintain if implemented effectively. The objective is to describe how to establish a routine patch-management procedure and to make it a part of standard operations.

Scope

This policy is applicable to all IT assets that belong to JMBGRP the hardware and software resources owned and/or operated by JMBGRP. Any Application / software not mentioned in the above scope and non-Windows OS are out of the scope of patch management process: The Application owner will be responsible for Patch management lifecycle and compliance for out-of-scope patches. The respective owners/administrator of the out-of-scope application and non-window OS shall ensure that relevant patches are deployed.

Policy Statement

- IT Infrastructure (Workstation & Server Operating Systems, Applications, Databases, Storage & Network devices etc.) shall be patched in accordance with the patching procedure listed in this document.
- Any system version upgrades/patch deployments shall be done considering compatibility to JMBGRP environment. A thorough impact analysis shall be done considering version/patch stability, possible issues etc.
- Business and technical impact of implementing, or not implementing, a particular patch shall be assessed. Patches to be tested on test environment prior to Production deployment.
- Operating Systems, Applications, Databases, Networking Devices and Storage devices shall be deployed with N-1 of OEM's recent version provided it offers stability to JMBGRP IT environment, any exceptions with version/patch upgrades to be documented.
- An exception process must be implemented in the event that a patch cannot be deployed or if no patch is available for an identified vulnerability. This process must include a risk assessment and proposed mitigating controls.

Procedure

The Security In-charge shall subscribe to security related forums in order to receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities. The patch management procedure for JMBGRP is mentioned below:

- The OEM releases the security patches to close the security vulnerabilities.
- Security In-charge will check and approve the security patches applicable to JMBGRP environment based on the above-mentioned scope.

- daysIT Infrastructure Team should download the approved security patches into the Patch repository.
- Patch management notifications are issued to business users and application owners at least 3 days in advance of the scheduled implementation date.
- Security In-charge should create monthly baseline of the approved security patches in the patch management software in case any such software is being used. This baseline will get applied to test environment which is subset of production environment for at least 3 working days. Test environment shall be subset of the production environment that should include system from all critical engagement, environment and projects.
- The reboot activity will be scheduled to ensure security patches are effectively installed on the target systems.
- If the patch compliance report of test environment is above 90 % and there are no reported issues, the same can be released for the deployment in the production environment.
- If patch testing level is less than 90% then patches will be re-deployed on the missing test systems or a special approval has to be taken from Security In-charge.
- The respective Patch Management administrator shall check the test systems for any error, system malfunctioning, performance or connectivity issues, if any.
- During deployment of security patches, if any issue is reported or notified, the same shall be escalated to Security In-charge. Patch deployment process shall halt until issue is resolved.
- If the issue is not resolved within 8 hours, it should be escalated Vendor/partner.
- Re testing shall be performed on the test environment, after corrective actions taken to resolve the issues.
- Restart should be scheduled for all systems once in a month for effective deployment of the patches. For servers, sysadmin shall coordinate with application owner for downtime.
- Monthly patch compliance report shall be generated and reviewed periodically.

Enforcement:

- This policy and procedure is applicable for all the employees of the company who have access to and use the information assets and IT assets as listed in the Information Asset Classification sheet which have been created for all the departments. Any violation shall be dealt in accordance with the disciplinary action process as laid down in the Code of Conduct.
- Management's interpretation of the clauses in this procedure shall be final and binding. Management reserves the rights to alter or amend any clause in this document at any time as per its discretion.

Metrics

- The metrics shall be measured by the Incident Management team.
- The periodicity of reporting shall be monthly.
- Following are the metrics to be monitored as under:
    - Number of security patches to be tested and deployed.
    - Number of security patches not deployed.
    - Number of patches deployed as per patch deployment schedule.
    - Number of patches not deployed as per patch deployment schedule.

Exceptions

- Exceptions shall not be universal but shall be agreed on a case-by-case basis, upon official

request made by the information owner. These may arise, for example, because of local circumstances, conditions or legal reasons existing at any point of time.

- Exceptions to this Security Policy and Procedures shall be allowed at the time of implementation of this policy and procedures or at the time of making any updation to this document or after implementation on an ad-hoc basis as per business or a specific and a peculiar manifestation of circumstances which shall be of temporary or permanent in nature.
- All exception requests shall be submitted by respective HOD/Business Security In-charge. These shall be submitted through an Exception Form and sign-off on the same shall be maintained by the requester.
- The Security In-charge shall review all exceptions, as the case may be, every year for validity and continuity.

Disclaimer

- JMBGRP reserves all rights and is the exclusive owner of all intellectual property rights over this Acceptable usage Policy and Procedures document. This document shall not, either in part or in full, be reproduced, published, copied, displayed, distributed, transferred, stored into any media (such as hard disks, USB Drives, Pen Drives, Memory Cards, CDS, DVD's), and/or captured or transmitted through by any means (such as electronic, digital, mechanical, photocopying, recordings, video and film or photographs and otherwise) by any person without prior consent from the Apex Committee. The Acceptable usage policy and procedure document is meant to be published on the intranet of JMBGRP and/or any other forum as decided by the management of JMBGRP. Anything not specifically stated in this

Acceptable usage policy and procedure document shall not be considered as implied in any manner.

- For any clarifications related to this Acceptable usage policy and procedure document with respect to its interpretation, applicability and implementation, please raise a request on Ticketing Tool.

References:

- Control Objectives: A.8.8, A.8.19