

Table of Contents

1. Purpose	3
2. Scope	3
3. Roles and Responsibilities.....	3
DevOps/Development Team	4
4. Compliance Table.....	4
5. Review	4
6. Patch Management Process	4
6.1 Patch Identification and Monitoring	4
6.2 Patch Evaluation and Risk Assessment.....	4
6.3 Patch Testing.....	4
6.4 Patch Approval	5
6.5 Patch Deployment	5
6.6 Monitoring and Verification	5
6.7 Emergency Patch Management.....	5
7. Patch Rollback and Recovery.....	5
8. Compliance and Reporting	6
9. Exceptions.....	6

DOCUMENT CONTROL

VERSION CONTROL

Document Control ID	EFR-Patch Management Policy-036
Issued Date	
Effective Date	
Owner	Information Security & Compliance Department

REVISION TABLE

Date	Version	Brief Description	Author
11/11/2024	1.0	Draft- Patch Management Process	Ms. Ratisha Kukreja
03/12/2024	1.0	Final-Patch Management Process	Ms. Ratisha Kukreja

RELEASE AUTHORIZATION

Task	Author	Title	Date
Prepared By	Ms. Ratisha Kukreja	Consultant	

REVIEWER AUTHORIZATION

Task	Author	Title	Date
Reviewed By	Mr. Antony Arul Selvaraj	Consultant	

APPROVAL AUTHORIZATION

Name	Title	Signature	Date

Important Note: This document is intended solely for the use of the individual or entity to whom it is transmitted to, and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

1. Purpose

The purpose of this Patch Management Policy is to establish the guidelines and procedures for the timely identification, testing, approval, deployment, and monitoring of patches for the company's IT infrastructure, systems, applications, and network devices. This policy aims to reduce security vulnerabilities, maintain compliance with regulatory requirements, and ensure the continuous operation and integrity of the company's technology environment.

2. Scope

This policy applies to all software, hardware, and network devices used within the company, including but not limited to:

- Operating systems (servers, workstations, mobile devices)
- Software applications (both internal and third-party)
- Network devices (routers, switches, firewalls)
- Virtual environments.

It is applicable to all employees, contractors, vendors, and third-party service providers who are involved in the management or operation of the company's IT systems.

3. Roles and Responsibilities

IT Department

- Patch Identification: Continuously monitor for new patches, updates, and security advisories related to all company software and hardware.
- Testing and Validation: Test patches in a controlled environment to ensure they do not negatively impact systems or applications.
- Approval: Review patches for relevance and compliance and approve patches for deployment based on severity and impact.
- Deployment: Deploy patches across the IT infrastructure according to the schedule defined in this policy.
- Monitoring and Reporting: Continuously monitor systems to ensure patches are applied successfully and generate periodic reports for internal audits and compliance purposes.

Employees

- Follow IT security protocols and report any system irregularities that could indicate a missing or failed match.

Information Security Risk Management Team

- Defines patch management policies, procedures, and best practices.
- Identifies vulnerabilities and assesses their impact.
- Collaborates with other teams to prioritize patches based on risk assessment.
- Monitors compliance with patching policies and standards.

DevOps/Development Team

- Collaborates with the operations team to ensure applications are patched appropriately.
- Develops automated deployment pipelines for patching infrastructure as code (IaC).
- Tests application compatibility with patches and updates code as necessary.
- Implements infrastructure changes to support patching requirements.

4. Compliance Table

Policy/Procedure Name	ISO 27001:2022 Control	UAE IA Policy/Procedure Name	UAE IA Control	Requirements
Patch Management Policy	A.12.6.1	Technical Vulnerability	T7.7.1	NIST SP800-144 Guidelines.

5. Review

The Policy, with its supporting guidelines and procedures, shall be reviewed by the Information Security team, every year from the date of the last update/review to ensure completeness, effectiveness, and usability.

6. Patch Management Process

6.1 Patch Identification and Monitoring

- The IT department is responsible for regularly monitoring software vendors, security bulletins, and patch management services for updates and patches.
- All critical patches (e.g., those addressing security vulnerabilities) must be identified and evaluated within 24 hours of release.
- Non-critical patches should be reviewed within 5 business days.

6.2 Patch Evaluation and Risk Assessment

- **Critical Patches:** Should be deployed within 6 hours of release, with high priority given to those addressing critical vulnerabilities or security risks.
- **Non-Critical Patches:** Should be reviewed and deployed within 5 business days, or as per operational requirements.
- A risk assessment must be conducted for each patch to evaluate potential impact on the company's systems, security posture, and business operations.

6.3 Patch Testing

Patches must be tested in a staging environment that mimics the production environment. Testing should verify that:

- The patch resolves the intended issue (e.g., security vulnerability, bug fix).
- The patch does not negatively affect system functionality, performance, or other applications.

- Rollback procedures are available in case of failure.

Patches must be tested within 5 business days of identification, depending on severity.

6.4 Patch Approval

- The IT Department, in collaboration with system owners, will review test results and approve patches for deployment based on severity, risk assessment, and successful testing outcomes.
- For critical patches, approvals may be expedited, but they should still undergo a minimal level of testing.

6.5 Patch Deployment

- **Critical Patches:** Must be deployed within 6 hours of approval, especially for security patches that address known vulnerabilities.
- **Non-Critical Patches:** Should be deployed during regular maintenance windows (e.g., weekly or monthly), with deployment completed within 5 business days.
- **Automated Deployment Tools:** The IT department will utilize automated patch management tools to ensure that patches are applied consistently across all systems and devices.
- **Notification:** End users should be notified of upcoming patches or system downtime when required.

6.6 Monitoring and Verification

- After patches are deployed, the IT department will monitor systems to ensure successful implementation.
- A verification report should be generated to confirm that all systems have been patched according to the deployment schedule.
- Any patch deployment failures should be addressed immediately, and a plan should be put in place to remediate issues.

6.7 Emergency Patch Management

- In case of critical vulnerabilities that require immediate attention, the IT department can deploy patches outside the regular schedule, provided the patch is tested and does not disrupt business operations.
- Emergency patches should be applied within 24 hours of release if they address high-risk vulnerabilities (e.g., zero-day exploits).

7. Patch Rollback and Recovery

- A rollback plan must be developed in advance for each patch. If a patch causes issues, the IT department should have a clear process for reverting to the previous stable version of the software or system.
- Rollback testing should be part of the patch evaluation process.
- **Backup and Recovery:** Before applying patches, full system backups should be taken to ensure data can be restored in case of failure.

8. Compliance and Reporting

- Regular patch management audits will be conducted to ensure compliance with this policy and verify that all systems are up to date.
- **Audit Logs:** Patch deployment activities must be logged, including patch identification, testing, approval, deployment, and any issues encountered. These logs should be kept for a minimum of one year for compliance purposes.
- **Patch Status Reports:** The IT department will provide periodic patch status reports to senior management, including the percentage of systems that are up to date and any systems that are at risk due to unpatched vulnerabilities.

9. Exceptions

- Any exceptions to this policy must be documented and approved by the IT department and relevant system owners.
- Exceptions will only be granted if there is a valid business reason and proper risk mitigation strategies are put in place.

--End of Document--