Policy Domain	**Patch Management Policy**	**Creation Date**	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

Document Control			
Prepared By **Vineet Kumar Chawla** **(Sr. Consultant IT)**	**Reviewed By** **Maruti Divekar** **(IT Head)**	**Checked By** **B P Rauka** **(CFO)**	**Approved By** **Mukund Kabra** **(Director)**

Document Modification History

SR #	Document	Version No.	Reviewed On	Checked On	Approved On	Effective Date	Authorized Signatory
1.	Patch Management Policy	1.0	05TH Mar 21	10th Mar 21	10th Mar 21	11th Mar 21	
2.							
3.							

Document Control

- This document is subject to version control and shall be managed by IT Head. Any request for amending this document shall be approved by Director. The IT Head shall review this document at least once in a year and/or when there is a significant change in technology adopted, business objectives, identified threats, legal environment, social climate and business processes.

- The document is available on Helpdesk Portal under Announcement and Server shared folder under AETL Policies and provided with HR Joining Kit, in non-editable pdf format and all the employees are expected to read and adhere to it. The approved and signed copies are available with IT Team, which can be used for audit purpose only. IT Team is responsible for maintaining updated copy of this document and its effective communication within Advanced Enzymes (AETL).

Policy Domain	Patch Management Policy	Creation Date	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

Table of Contents

Policy Domain	**Patch Management Policy**	**Creation Date**	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

1. Overview

The Information Resources infrastructure at AETL is expanding and continuously becoming more complex. There are more people dependent upon the network, more client machines, upgraded and expanded administrative systems, and more application programs. As the interdependency between Information Resources infrastructure grows, the need for a strong patch management process is essential.

Managing these patches is a critical part of providing a robust and valuable Information Resources infrastructure.

2. Purpose

The purpose of the Patch Management Policy is to manage patch in a rational and predictable manner so that IT department can plan patch accordingly. Patch implementations require serious forethought, careful monitoring, and follow-up evaluation to reduce negative impact to the user community and to increase the value of Information Resources.

This policy defines the guidelines to keep track of all patches implemented in the network and to keep track of all changes made to these objects.

3. Scope

This policy applies to all infrastructure servers and network devices that form a part of AETL's IT landscape. It is imperative that everyone adheres to this policy so that IT Department can efficiently manage IT assets and maintain the integrity of user accounts created in Windows, Linux and applications.

4. Entry & Exit Criteria

Entry Criteria:

- Whenever any Patch update is required on any information system.

Exit Criteria:

- When the change has been done and the systems are running in desired condition by IT team

Policy Domain	Patch Management Policy	Creation Date	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

5. Policy

AETL's IT infrastructure including applications must be properly patched with the latest appropriate updates and patches from the OEM's in order to reduce system vulnerability and to enhance application functionality. The purpose of this policy is to establish standard procedures for the identification of vulnerabilities, potential areas of functionality enhancements as well as the safe and timely installation of patches. It's the only way to stay organized and to keep track of which patches have been deployed and why.

All patch update requests must be submitted in accordance with patch management procedures so that the IT Head has time to review the request, determine and review potential failures, and make the decision to allow or delay the request.
IT Head may deny a scheduled or unscheduled change for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available.

The "***Patch Management Process***" shall include the following: -

- Assessment of the potential impact, including security impact of the change(s) on critical systems and network devices;
- Identification of the patch authorizers;
- Procedure for testing including security-testing of the patch updates;
- Rollback procedure for aborting and recovering from failed patch updates.
- All changes on the critical systems shall be tested prior to implementing them on the production systems.

IT Head will govern change meetings at defined frequency and review scheduled all the changes being presented. The IT Head will provide final approval/rejection to the change basis its review and impact analysis. Below is the list of documents that the IT Head requires to review any change being presented:

- Plan of action
- Roll back plan
- Test cases
- Release document (In case, of a release)

a. all patches must be downloaded from the relevant system vendor or trusted sources. Each patch's source must be authenticated, and the integrity of the patch verified. All patches must be submitted to an anti-virus scan upon download.
b. New servers and desktops must be fully patched before coming online in order to limit the introduction of risk.
c. New software's must be fully patched when installed on AETL resources to limit the introduction of risk.

d. All patches must be tested prior to full implementation since patches may have unforeseen side effects.

6. Patch Management Process

6.1 Patch Sources

This policy applies to all software, servers, desktops, laptop computers operated by AETL.

The following list provide the scope of IT infrastructure where patch management policy is applicable within Company along with formal patch sources.

Products / Configurations	OEM	Patch Sources
Server OS	Windows Server	OEM
Server OS	Linux Server	OEM
Laptop / Desktop OS	Windows	OEM
SAP	SAP S/4HANA Application	OEM
Database	SAP HANA	OEM
Database	SQL Server	OEM
Office Applications	MsOffice	OEM
Antivirus	Seqrite Endpoint Protection	OEM
Firewall	Fortinet	OEM
Network Switches	Dlink, Dell	OEM

6.2 Patching Priorities

The following Patch Priority Matrix represents all systems and applications at AETL, their relative priority for patching, and timeframes within which patches must be applied.

AETL categorizes patches as High Priority and Low Priority:

High Priority Patches: Server Operating system, SAP, Databases such patches shall be applied in the development server and post testing are migrated to Quality (Test) and then to Production environment.

Low Priority Patches: Desktop, Laptop based Operating systems & standard application like MS Office, Antivirus, Acrobat Reader etc. the patches are applied as per and when the same are released by the OEM and its suitability to the users. For all other location's patches are pushed directly thru own resources.

All computers attached to AETL network must have standard anti-virus system installed. The software must be active, automated to perform virus checks at regular intervals daily with a full disk scan once every week and have its virus definitions files kept up- to date. End users are prohibited de-activate, disable or uninstall antivirus software.

Such patches are reviewed by IT and applied every monthly.

Asset / Configuration	Patch Testing Period	Patch Deployment Method	Post Deployment Testing	Patch Rollback
Windows / Linux Operating System Servers	Critical – 30-45 Days, Non critical – 90 Days	Patches are tested; UAT is performed on a separate test environment before being deployed.	IT Admin team interacts with relevant [*user groups*] to check and verify successful deployments.	In case a faulty patch is identified IT team restores to the previous version – which is always part of the roll out procedure.
Windows / Linux Operating System Desktop / Laptops	Non critical – 90 Days	Patches are tested on a test laptop and desktop before being deployed on other machines. (Testing not mandatory)	The patches are deployed from OEM resources.	In case a faulty patch is identified IT team restores to the previous version – which is always part of the roll out procedure.
Office Applications	Non critical – 90 Days	Patches are tested on a test laptop and desktop before being deployed on other machines. (Testing not mandatory)	The patches are deployed from OEM resources.	In case a faulty patch is identified IT team restores to the previous version – which is always part of the roll out procedure.
SAP	Critical – 30-90 Days, Non-	Patches are tested; UAT is performed on a	Interacts with SAP Consultant team to checks	In case a faulty patch is identified Basis admin team restores to the

	critical – 730 Days	separate test environment before being deployed.	and verify the deployed patches.	previous version – which is always part of the roll out procedure.
HANA Database	Critical – 30-90 days. Non-critical – 730 Days	Patches are tested; UAT is performed on a separate test environment before being deployed.	IT Admin team interacts with relevant [*user groups*] to check and verify successful deployments.	In case a faulty patch is identified Basis admin team restores to the previous version – which is always part of the roll out procedure.
Other hardware	Critical – 30-90 days. Non critical – 365 Days	Patched confirm from OEM before upgrading and install on systems.	IT Admin team interacts with relevant [*user groups*] to check and verify successful deployments.	In case a faulty patch is identified IT team restores to the previous version – which is always part of the roll out procedure.

6.3 Testing procedure

a. For Server OS and various applications/programs, the patches shall be deployed on UAT, tested and then transferred/implement to Production.
b. A back out plan that allows safe restoration of systems to their pre-patch state must be devised prior to any patch rollout in the event that the patch has unforeseen effects.
c. All configuration and inventory documentation must be immediately updated in order to reflect applied patches.
d. The system administrator shall conduct audits by himself and report to Head-IT to ensure that patches have been applied as required and are functioning as expected.

7. Policy Review

The policy will be reviewed on yearly basis or if there is any major change in IT infrastructure to incorporate changes if any.

IT Head will be responsible for reviewing the policy and communicating the changes made therein.

8. Roles & Responsibility Matrix (RACI)

Activity \ Role	IT Head	ISMS Steering Committee	Internal Users	External Users	Exempted
Authoring of this document	RA	RA	-	-	-
Approval of this document	I	CI	-	-	-
Sign-off of this document	CI	CI	-	-	-
Application of this document	RA	RA	RA	-	-

R	Responsible
A	Accountable
C	Consulted
I	Informed

9. Roles and Responsibilities

Below are the specific roles and responsibilities for the defined policy:

- **IT TEAM**
  - Shall determine the complexity of the proposed Patch.
  - shall understand impact of Patch and approve.

- **Patch Implementer**
  - Shall Implement Patch according to standard build instructions.
  - Shall notify any parties to be impacted by the implementation.
  - Shall confirm once the implementation sequence is completed.
  - Shall communicate the result of the implementation to the relevant parties.

10. Risk for Non-Compliance

Risks arising due to non-compliance with this policy include, but not limited to:

- System vulnerability,
- Unauthorized patch updates,
- Data/Configuration integrity loss,

- System crash and avoidable interruptions,
- Security failures,
- Confusion/delay in system configuration,
- Loss of unavailability of important data

Compliance with this policy initiates the following key controls:

- Only authorized patch updates are implemented.
- Patches are implemented as per priority and in a controlled manner.
- All the patches are scheduled to ensure planned results.
- Patch's with high impacts are tested in advance for satisfaction.
- Patch updates are reversed if they are not successful.
- Only OEM approved patches are implemented.
- All the patch updates are adequately documented for audit trail and post implementation review.

11. ISMS Steering Committee Members

1. Mukund Kabra (Director)
2. B. P. Rauka (CFO)
3. Maruti Divekar (IT Head)

12. AETL IT Helpdesk Contact Detail

- Logging an online support request: **http://192.168.2.7:8080**
- Email: **it.helpdesk@advancedenzymes.com**
- Telephone: **022 41703234**