Policy Domain	**Logical Access Control 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.	Logical Access Control 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	Logical Access Control Policy	Creation Date	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

Table of Contents

Policy Domain	Logical Access Control Policy	Creation Date	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

1. Objective

Objective of this policy is to cover user access to IT systems at various levels like operating system, database, server shared data folders and applications.

2. Scope

This policy applies to all employees, contractors, consultants, temporaries, and other workers providing services or working at AETL, including all personnel affiliated with third parties. This policy applies to all systems that are owned or leased by AETL.

3. Purpose

The purpose of this policy is to establish the requirements for controlling access to AETL information or information systems that it is responsible for, including computing and physical resources. Computer systems, networks and allied hardware and other peripherals are an integral part of our operations.

4. Ownership

The IT Head is the owner of this policy and System Administrator is responsible for maintaining it.

5. Policy Norms

5.1 Access Control - Operating System Level

5.1.1 For each user, access to the system must be protected by a password in line with the password policy of AETL.

5.1.2 The number of unsuccessful login attempts shall be restricted to max five wherever functionality available.

5.1.3 Accounts, which are not used continuously used for over a period of 90 days, shall be disabled.

5.1.4 Users shall log off from the workstation if he is to be away for an extended period.

5.1.5 Only one operating system may be installed on desktops/laptops, unless otherwise there is a specific need for project or test environment.

5.1.6 BIOS password shall be enabled for the computer systems for protecting unauthorized modifications to the hardware configuration.

5.1.7 Autorun functionality should be disabled on all workstations.

5.1.8 Users shall be granted access to files, data and other resources as per the access rights approved by his HOD's or Management.

5.1.9 The user-ID and password should be authenticated as a whole. Authentication failure should provide an error message to the user that does not indicate whether the user ID is correct (e.g. "incorrect login" and "incorrect password").

5.1.10 The user shall be prompted by the system for change of the user password after the lapse of specified period (90 days).

5.1.11 Users created for audit/maintenance purpose shall be disabled immediately after the work is over.

5.1.12 When a user is left the organization or terminates employment, his account shall be disabled or deleted.

5.2 Access Control – Server shared data folders

5.2.1 Any shared folder data access request should come from End user or Department Head to helpdesk support portal or at the time of joining formalities and approved by their HOD.

5.2.2 Any shared folder data access modification request should come from End user or Department Head to helpdesk support portal and approved by their HOD.

5.3 Access Control - Application Level

5.3.1 Application shall provide for unique user IDs and passwords for all users.

5.3.2 Application shall prompt for change of user password after lapse of specified period.

5.3.3 Application shall ensure secrecy and security of the user passwords and the access rights granted to users.

5.3.4 The access privileges granted in the application shall be in accordance with the roles/duties assigned.

5.3.5 Allocation of the suspended, disabled user ID to new users shall be avoided.

5.3.6 User IDs of the transferred, retired, suspended or dismissed employees shall not be active in the systems.

5.3.7 The user ID of employees on long leave, training/ onsite deputation etc. shall be suspended / disabled.

5.4 Access Control - Database Level

5.4.1 All users connecting to database shall authenticate themselves.

5.4.2 Database shall provide for unique user IDs and passwords for all users.

5.4.3 Application shall ensure secrecy and security of the user passwords and the access rights granted to users.

5.5 User Identification

5.5.1 User Identification code

All users shall be granted access to the computing resources through a unique identification code (User-ID).

5.5.2 User Credentials

User credentials shall consist of a user-ID and password that is unique to an individual. The IT shall be maintaining the records for all users.

5.6 Creation of User IDs

5.6.1 Creation of new Users

New users at operating systems, applications, and database and network levels shall be created based on formal request from End User / HR & authorizations by the HR / HOD / Management.

5.6.2 Use of Common User IDs

Common user IDs shall be created based on request with explanation for end user usage.

Common user IDs shall maintain ownership.

5.7 Control of User IDs

5.7.1 Disabling users inactive accounts

User accounts that have been inactive for more than 90 days shall be disabled. Systems Administrator shall re-enable them only on the request of the specific user and where required, with the approval of the respective department head or Management.

5.7.2 Disabling default User IDs

Default user IDs shipped with all software shall be disabled or if any default user need to be active then password should maintain as per password policy and kept with IT Head only.

5.7.3 Deactivation of User IDs

If the wrong password is entered five times, the user-ID shall be automatically deactivated and only the Administrator shall carry out reactivation, after ascertaining genuine request.

5.7.4 User ID expiration dates for non-employees

For contract employees and consultants, an User ID expiration date that coincides with the conclusion of the contracted project shall be created.

5.7.5 System account suspension for failed login attempts

Five successive failures shall result in a user's account being locked; they shall not be able to login until their account is unlocked and the password reset. The user shall contact the IT Dept. for getting the account unlocked. A history of all such failed attempts shall be maintained and reviewed by IT Dept.

5.7.6 Inactivity time out

The terminals shall be deactivated after 15 minutes of inactivity. Additionally, screen saver passwords shall be encouraged.

5.8 Notifying IT department of User job/function changes

The immediate supervisor / HOD of the user shall notify IT of changes in the user's job function in order to ensure that access privileges are appropriately maintained.

5.9 User Transfer / Exit or Termination Controls

5.9.1 Notification to IT upon user Transfer / Exit or Termination

The HR shall immediately notify the IT upon the resignation, termination or transfer of employees. The No Due Form, requiring clearance from all the departments when an employee is transferred or retires/resigns his job, shall also include clearance from the IT Department.

5.9.2 Revocation of user credentials

The Systems Administrator shall revoke all the user-ids upon termination or resignation of employee and revoke or modify access upon transfer of responsibilities.

5.9.3 HOD / Immediate Supervisor coordination with IT

For situations where users with access to highly sensitive information are terminated, the employee's HOD or immediate supervisor is responsible for directly coordinating with the IT to remove the user's access rights.

5.9.4 User clearance requirements

All PCs, ID cards, software, data, documents, manuals etc. of left / terminated personnel shall be returned to the employee's HOD or immediate supervisor or the HR dept.

6. Monitoring & Control

It is the responsibility of the IT Head to monitor and review that his team is adhering to the defined Policy Norms.
In case it is found by IT Head or by internal audit team that the employee is not adhering to the terms defined under the policy, the same shall be highlighted to the Management for required action.

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	RA	-

R	Responsible
A	Accountable
C	Consulted
I	Informed

9. Risk for Non-Compliance

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

- Unauthorized data access.
- Information leakage, violation of IPR
- Change of Network and systems settings.
- Misuse of Servers & other IT Infrastructure.
- Information disclosure

10. ISMS Steering Committee Members

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

11. AETL IT Helpdesk Contact Details

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