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

Table of Contents

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

1. Overview

The purpose of the Physical access control policy is to: establish the rules for granting, control, monitoring, and removal of physical access to office premises; to identify sensitive areas within the organization; and. to define and restrict access to the same.

2. Objective

To prevent unauthorized access, damage and interference to business premises & information. To prevent loss, damage or compromise of assets and interruption to business activities. To prevent compromise or theft of information and information processing facilities.

3. Applicability

This policy applies to the physical premises at Corporate office, Branch Offices, Plants, Warehouse of Advanced Enzymes.

4. Policy Norms

Physical Access:

- Security Personnel shall guard the building entry point to AETL Premises.
- Visitors and Vendors shall make an entry in the Visitor's register. During their presence inside AE premises, they shall always be escorted, and their movements monitored.
- Personal laptops are not allowed for use in AE data center premises.
- CCTV Cameras have been deployed in critical areas and all the movements shall be monitored and recorded.
- Critical areas like Server Room have limited authorized access.
- Card Access will be configured to allowed employees in data center room.
- Vendors entering data center room are escorted by authorized IT team member. The entry of vendor is recorded in the register kept in server room.

Safety Equipment:

Appropriate safety equipment is to be installed, such as heat and smoke detectors, fire alarms, fire extinguishing equipment and fire escapes. Safety equipment is to be checked regularly in accordance with manufacturers' instructions. Employees are to be properly trained in the use of safety equipment. Combustible computer supplies such as stationery, other than immediate operational needs, should not to be stored within server room.

Ensuring Suitable Environmental Conditions:
Suitable environment control procedures shall be in place for smooth and reliable working of Information processing facilities. The environmental dangers that threaten the computer premises and the means by which they may be lessened or eliminated shall be aptly identified and implemented. Countermeasures or contingency procedures are to be defined for environmental hazards such as fire, smoke, water, dust, vibration, electrical supply interference.

Issues to be considered by the Admin for implementing the above procedure:
- Serious fire damage could make it impossible to continue business operations.
- Flooding can cause severe disruption to business in any form.
- Failure of air conditioning equipment can unsettle business operations and potentially result in halting of business output.
- Smoking, eating and drinking is prohibited in computer equipment areas.
- Suitable Insurance Policy coverage for IT equipment's.

Power Supplies:
Equipment shall be protected from power failures and other electrical disturbances. A suitable electrical supply shall be provided that conforms to the equipment manufacturer's specifications. Various options shall be considered to achieve continuity of power supply:
- Un-interruptible power supplies with n+n configuration
- Back-up generator

UPS equipment shall be regularly checked to ensure its adequate capacity and shall be tested with the manufacturer's recommendations. UPS shall support orderly close down or continuous running is recommended for equipment supporting critical business operations. There shall be SLA that ensures the maximum uptime with the supplier/contractor for maintaining of UPS.

Cabling security:
Administration Division shall develop and implement the procedure for protection of power and telecommunication cabling. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception and damage. The following is an example of the security standards relating to cabling:
Issues to be considered for implementing the above procedure:
- Power and telecommunications lines to the information processing facilities shall be underground, where possible or subject to adequate alternate protection.
- Network cabling shall be protected from unauthorized interception or damage.
- Power cables shall be segregated from communication cables to prevent interference.
- For sensitive or critical systems further controls to consider:
- Installation of armored conduit and locked rooms or boxes at inspection and termination points.
- Use of alternate routings or transmission media.

Network cabling is to be protected from unauthorized interception and communications loss or damage by:

- Use of conduits;
- Avoiding routes through public areas;
- Installation of locked rooms or boxes at inspection and termination points
- Implementation of secondary transmission media and/or routings.

Equipment maintenance & Security:

IT Administrator is responsible for developing the procedure for equipment maintenance. IT Equipment's shall be correctly maintained to ensure its continued availability and integrity.

Issues to be considered for implementing the above procedure:

- Equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications.
- Manufacturers' instructions regarding the protection of equipment, such as its protection against exposure to strong electromagnetic fields, is to be observed at all times.
- Only authorized maintenance personnel shall carry out repairs and service equipment.
- Records shall be kept of all suspected or actual faults and all preventive and corrective maintenance.
- Appropriate controls shall be taken when sending equipment off premises for maintenance. All requirements imposed by insurance policies shall be complied with.

IT equipment should be sited or protected to reduce the risks from environmental hazards and to minimize the opportunity for unauthorized access.

Critical equipment should be protected from power failures or other electrical anomalies.

Environmental Conditioning:

Appropriate air conditioners are to be installed to maintain temperature and humidity for the Server Room.

- Temperature for the server room be continuously monitored and temperature should be maintained within the set limits.
- Humidity in the server room should be maintained within set parameters.
- Regular checks are to be recorded and routine preventive maintenance schedule has to be executed.
- Supply air should be dust free and filtered before reaching the server room.

5. Monitoring & Control

It is the responsibility of the IT team to monitor and review that all employees are adhering to the defined Policy Norms.

In case it is found by IT team 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 HOD for required action.

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

6. 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.

7. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

8. Roles & Responsibility Matrix (RACI)

Role / Activity	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. ISMS Steering Committee Members

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

10. AETL IT Helpdesk Contact Details

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