Policy Domain	Data Center Physical Security 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.	Data Center Physical Security 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	Data Center Physical Security Policy	Creation Date	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

Table of Contents

Policy Domain	Data Center Physical Security Policy	Creation Date	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

1. Policy

This policy is developed to support the AETL IT Policies, government regulations and audit compliance. This policy provides support for managing physical and environmental security controls to prevent unauthorized physical access, damage, and interruption to AETL information assets controlled within a data center environment.

2. Purpose

The data center physical control guideline is designed to provide procedures and support to prevent, detect, suppress fire, water damage, and loss or disruption of operational capabilities due to electrical power fluctuations or failures or unauthorized personal.

3. Scope

This policy is intended to address physical controls for AETL data centers. This policy is intended to implement Information Security Policy and associated standards related to physical control for AETL data centers.

4. Procedure

The AETL applications are hosted in in-house Data Center that feature 24x7 onsite guards, CCTV, access restricted entry point, early warning fire detection systems and CO2 fire extinguishers, redundant power supply, N+1 UPS and generator power.

A. Data Center Physical Control

AETL Data Centers are Limited Access Areas based on Physical Security Standard. AETL IT has implemented an access control list that includes the name and access granted for data centers. A copy of the access list is being maintained.

B. Data Center Operational Guideline:

1. Data center rooms are kept clean and free of dust. Upon completion of any work in the room, staff performing the work ensures that they have left the area as clean as it was before their work begins.
2. All rack enclosures are kept neat and free of manuals, diskettes, cables, etc.

3. AETL Data Centers should have processes and facilities in place to prevent, detect, suppress fire, and loss or disruption of operational capabilities due to electrical power fluctuations or failures.
4. Inside Data Center Controls
   a) No food or drink is allowed within the Data Center.
   b) No hazardous materials are allowed within the Data Center.
   c) Do not power any electrical or mechanical device without IT authorization.
   d) All packing material should be removed from computer equipment/components outside the data center before being moved into the Data Center.
   e) No cleaning supply is allowed within the Data Center without prior approval. This includes water.
   f) No cutting of any material (pipes, floor tiles etc.) should be performed inside the Data Center unless special arrangements are made in advance.
   g) Boxes, tapes, CDs and other material should not be stored inside the Data Center racks.
   h) Do not lift floor tiles without prior knowledge, consent, and oversight of the IT person.
   i) Communicate all problems to IT team.
   j) In the event of an emergency notify to IT team immediately.
   k) Do not touch a Power Distribution Unit within the Data Center.
   l) Air conditioning equipment shall be managed in presence of IT team.
   m) Communications cabinets can be opened only by authorized personnel.

C. Data Center Access Authorization

All requests for access to the AETL Data Center need to be approved by the IT Head. Access is restricted to specific individuals with job functions related to operating mission critical equipment in the Data Center. The IT Head or designee must approve all changes to physical controls, such as, locks and alarm.

The following role shall have access to AETL data center.

a) IT Head
b) IT Team Members
c) Management

D. Data Center Access Requirements

Data Centers shall be equipped with digital access controls. Individuals who do not have access require authorization from IT Head or IT administrator. Such persons are required to be signed and fill the visitor register.

Virtual Access - Devices with virtual access to Data Center Assets, such as remote consoles, should be secured with unique passwords and only access with secured Virtual Private Network (VPN) connections.

E. Access Limited to Authorized Personnel Only

Physical access to the Data Center spaces should be restricted to those with operational need to enter those spaces. Access is non-transferable. Administrators should not be permitted to share their keys, access cards and should not bring any guests (children, siblings, spouses, colleagues or friends) into the Data Center at any time.

F. Visitor Access

Anyone who does not have unrestricted or restricted authorization is considered a visitor. All visitors to the Data Center will need to adhere to facility guidelines and other best practices as detailed below:

1. All exceptions will need to have prior approval by the IT Head.
2. All visitors to Data Center Spaces will be accompanied at all times by an individual with unrestricted access and need to be entered into the visitor register.
3. Visitors will need to be signed in when entering the AETL Data Center on visitor register the time and purpose of their visit and will need to sign out when leaving.

G. Maintenance and Cleaning of Data Center

The following service shall be maintained and monitored on regular basis.

1. Temperature
   a) Maintain the data center room temperature between 20^0 - 26^0.
   b) The following temperature monitoring tools are installed in the data center.
      i. Temperature meter.
      ii. AC controller.
      iii. Hooter for high temperature.
   c) For maintenance and fault repairing of AC, Vendor can perform the work in data center in presence of designated IT staff and same shall be recorded in Visitor register.
   d) Preventive maintenance for above shall be carried out on quarterly basis and records for the same to be maintained.
   e) Maintain the data center room humidity between 40% - 60%.
   f) The following humidity monitoring tools shall be installed in the data center.
      a. Humidity meter.

2. Fire Safety & Prevention
   The following fire monitoring equipment shall be installed in data center
   a) Smoke detector shall be installed in data center.
   b) "C" class fire extinguisher.
   c) For maintenance and fault repairing of fire monitoring devices, Vendor can perform the work in data center in presence of designated IT staff and same shall be record in Visitor register.
   d) Preventive maintenance for above shall be carried out on monthly basis and records for the same to be maintain.

3. Cleaning of the Data Center room.
   Dusting of the room shall be done on weekly basis in the presence of designated IT staff.

4. CCTV Monitoring
   a) CCTV camera to be installed to monitor the employee/visitor or unauthorized movement.
   b) Recording of CCTV footage to be kept for at least 1 month.
   c) Preventive maintenance for above shall be carried out on once in year basis and records for the same to be maintain.

5. Incidents reporting procedure
   IT support for data centers shall be available 9*5 at all the data centers location. In case of any unexpected breakdown of data center environmental system or supporting system failed the responsible IT staff will take appropriate action in consult with IT Head.

Policy Domain	Data Center Physical Security Policy	Creation Date	10th Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

5. 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

6. Risk for Non-Compliance

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

- Unauthorized access of data center,
- System down and avoidable interruptions,
- Security failures,
- Loss of unavailability of important data

Compliance with this policy initiates the following key controls:

- Only authorized access is provided to Data Center
- Unwanted access is stopped, increasing the security of the IT systems

7. Disciplinary Actions

Violation of this policy may result in disciplinary action which may include termination for employees and temporaries.

8. 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.

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**

* List of users having access to the Data Centers at TCO, WRC and NTRC locations.

Access Control List			
SR#	**User Name**	**Dept**	**Access Control System**
1	Mukund Kabra	Management	Spectra Door Access Control System
2	B. P. Rauka	Management	
3	Maruti Divekar	IT	
4	Jitendra Patil	IT	
5	Santosh Mali	IT	