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

Table of Contents

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

1. Overview

Remote access to our corporate network is essential to maintain business requirement fulfillment, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. This Remote access policy is a document which outlines and defines acceptable methods of remotely connecting to the internal network.

2. Purpose

The purpose of this policy is to define standards for connecting to AETL's network from any host. These standards are designed to minimize the potential exposure to AETL from damages which may result from unauthorized use of AETL resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical AETL internal systems, etc.

3. Scope

This policy applies to all AETL employees, contractors, vendors and agents with an AETL-owned or personally owned computer or workstation used to connect to the AETL network. This policy applies to remote access connections used to do work on behalf of AETL, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, MPLS, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

4. Policy

3.1 General

1. It is the responsibility of AETL employees, contractors, vendors and agents with remote access privileges to AETL's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to AETL.
2. General access to the Internet for recreational use by immediate household members through the AETL Network on personal computers is permitted to limited use. The AETL employee is responsible to ensure the family member does not violate any AETL policies, does not perform illegal activities, and does not use the access for outside business interests. The AETL employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of AETL's network:

    a. *Networking & telecommunication Policy*
    b. *Acceptable Use Policy*

4. For additional information regarding AETL's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., discuss with IT Head.

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong password. For information on creating a strong password see the Password Policy.
2. AETL employees, vendors and contractors can access AETL applications and network thru FortiGate VPN solution which has 2 factor authentication the OTP verification is sent on email or mobile configured on FortiGate VPN.
3. At no time should any AE employee provide their login or email password to anyone, not even family members.
4. AETL employees, vendors and contractors with remote access privileges must ensure that their AETL-owned or personal computer or workstation, which is remotely connected to AETL's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
5. AETL employees and contractors with remote access privileges to AETL's corporate network must not use non-AETL email accounts (i.e., Gmail, Hotmail, Yahoo, AOL), or other external resources to conduct AETL business, thereby ensuring that official business is never confused with personal business.
6. Routers for dedicated ISP lines configured for access to the AETL network must meet minimum authentication requirements.
7. Non-standard hardware configurations must be approved by IT Team. IT Team must approve security configurations for access to hardware.
8. All hosts that are connected to AETL internal networks via remote access technologies must use the most up to date anti-virus software.
9. Organizations or individuals who wish to implement non-standard Remote Access solutions to the AETL production network must obtain prior approval from IT Team.

5. 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.

6. Enforcement

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

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

7. 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

8. ISMS Steering Committee Members

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

9. AETL IT Helpdesk Contact Details

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