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

Table of Contents

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

1. Overview

AETL's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to AETL's established culture of openness, trust and integrity. AETL is committed to protecting AETL's employees, partners and the company from illegal activities or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of AETL. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every AETL employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

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 equipment's that are owned or leased by AETL.

3. Purpose

The purpose of this policy is to outline the acceptable use of computer assets including (Hardware, Software and Applications) at AETL. These rules are in place to protect the employee and AETL both. Inappropriate use could expose AETL to many risks including virus attacks, compromise of network systems / services, and legal / compliance issues.

4. Ownership

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

5. Policy

This policy defines DO's which is acceptable and Don'ts which are unacceptable as per the AETL policy.

DO's

5.0.1 While AETL's network administration desires to provide a reasonable level of privacy, the Users should be aware that the data they create on the corporate systems remains the property of AETL. Because

of the need to protect AETL's network, management cannot guarantee the confidentiality of information stored on any network device belonging to AETL.

5.0.2 Employees are responsible for exercising good judgment regarding the reasonableness of personal use and if there is any uncertainty, employees should consult their supervisor or manager.

5.0.3 Ethical use of resources by all employees. A culture encouraging participants to disallow misuse or abuse of any IT resources by self or peers.

5.0.4 Postings by employees from AETL email address to newsgroups should contain a disclaimer stating that "The opinions expressed are strictly their own and not necessarily those of AETL", unless posting is in the course of business duties.

5.0.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, Malware, spy ware, or Trojan horse code.

5.0.6 When employees receive unwanted and unsolicited email (also known as SPAM), they must refrain from responding directly to the sender. Instead, they should forward the message to the system administrator who will take steps to prevent further transmissions.

5.0.7 Employees must treat electronic mail messages and files as "Confidential" information. Electronic mail must be handled as a "Confidential" and direct communication between a sender and a recipient.

5.0.8 AETL electronic mail system is to be used only for business purposes. All messages sent by electronic mail are AETL records. AETL reserves the right to access and disclose all messages sent over its electronic mail system, for any purpose.

5.0.9 Keep all credential secure and do not share. Passwords shall be minimum 8 characters long and should contain alphanumeric characters with special characters.

5.0.10 Authorized users are responsible for the security of their credential. User level passwords should be changed every 30 days. Password should not be written down, except for lodging with departmental security staff or secure safekeeping, where appropriate. Password should be changed whenever there is any indication of possible system or password compromise.

5.0.11 Ensure the system used by an employee is protected by approved virus-scanning software with a current virus database.

5.0.12 Employees should only connect office issued equipment, while not on AETL premises, to the Internet by AETL pre-defined service providers.

5.0.13 System should be secured with a password-protected screensaver with the automatic activation feature set at 3 minutes or less, or by logging-off when the computer/laptop is left unattended.

5.0.14 Because information contained on portable computers is especially vulnerable, special care should be exercised to protect information from being gleaned by others in a public place. Using Notebook in public places (conferences, training rooms etc.) calls for additional physical security, usage of Laptop Locks is advised.

5.0.15 Laptop/note book have a continuous threat of theft as they are easily visible. Keep in close custody. There have been incidents related to laptop thefts inside the car. Avoid getting tricked by incidents that drive your attention around the car when someone can open your door and pick up your laptop in a fraction of seconds.

5.0.16 Smart phones used for downloading office emails. They should be physically secured and an individual is responsible for protection.

5.0.17 In case of loss of Laptop/ Notebook/ smart phone report immediately to the IT infrastructure team so that the email configuration can be changed to avoid unauthorized access to your emails. An FIR should be lodged with the nearest police station and copy of FIR be sent to IT department at corporate office.

5.0.18 Users are responsible for physical protection of cryptographic keys. So, ensure that they are kept in a secure manner and the opportunity of physical theft is minimal.

5.0.19 Interaction with any external entity (strategic partner, vendor, customers) requires careful consideration both in terms of information exchanges and verbal communication. Members of staff should ensure that the communication with any external service provider is being conducted with due consideration and based on “need to know”.

5.0.20 It is the responsibility of AETL personnel to ensure that visitors accompanying them inside office premises follow the visitor declaration with respect to assets such as Notebook, USB drives, other electronic media devices such as CD, DVD etc.

5.0.21 Employees must position their computer screens such that no unauthorized person can look over their shoulder and see the sensitive information displayed.

5.0.22 Equipment’s should not be moved or displaced to other locations without authorizations.

5.0.23 During non-working hours all employees must lock-up all media (USB sticks, CD’s, Floppy’s, Paper, etc.). Unless information is in active use by authorized personnel, desks must be absolutely clear and clean during non-working hours.

5.0.24 No use of USB sticks, CD ROM’s from sources outside of AETL offices.

5.0.25 Media may not be removed from the department without written authorization.

5.0.26 Shredders should be used for destruction of paper containing critical information.

5.0.27 Sensitive or confidential information when printed should be cleared from the printers immediately.

5.0.28 All the print given by the user shall be protected and can be printed only when credentials entered at printing machine.

5.0.29 Printers are to be used for documents that are relevant to the day-to-day conduct of business at AETL. AETL printers should not be used to print large personal documents.

5.0.30 Installation of personal printers is generally exempted at AETL due to the cost of maintaining and supporting many dispersed machines. In certain circumstances, however, where confidentiality, remote location, the need to print a large number of low volume print jobs, or other unusual situation is an issue, personal printers may be allowed once approved on a case to case basis by AETL IT.

5.0.31 Make efforts to limit paper usage by taking advantage of duplex printing (i.e. double-sided printing).

5.0.32 Many printers do not support certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper. If you need to use any of the paper types, consult with IT Help Desk.

5.0.33 Color printing is typically not required by general business users. Given this selective need, as well as the high cost per page to print color copies, the number of color-capable printers available has been minimized. You are strongly encouraged to avoid printing in color when monochrome (black) will do.

5.0.34 Report any malfunction of any printing device to IT Helpdesk as soon as possible. Enforcement Any employee who is found to have violated this policy may be subject to disciplinary action.

5.0.35 Ensure that paper documents/files, other assets are kept in lock and key, when no longer in use;

5.0.36 All employees shall lock their screen (Pressing Windows + L or Control-ALT-DEL) when no longer working in their PC/ notebook;

5.0.37 While using social media such as (but not limited) twitter/ Facebook /linked-In avoid disclosing information that reflects organization's performance in anyway. Avoid using any language comment that can damage the image and reputation of the organization.

5.1.0 Don'ts

5.1.1 Employees must not employ scanned versions of hand-rendered signatures to give the impression that the sender signed an electronic mail message or other electronic communications.

5.1.2 Sending of large number of emails to any outside address is prohibited unless written permission from the Information Technology Manager has first been obtained.

5.1.3 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which AETL or the end user does not have an active license is strictly prohibited. Employees should not save games, jokes, mp3s or any such information for entertainment purposes.

5.1.4 Using AETL computing asset to actively engage in procuring or transmitting material that is in violation of business code of conduct sexual harassment or hostile workplace laws in the user's local jurisdiction.

5.1.5 Making fraudulent offers of products, items, or services originating from any AETL account.

5.1.6 Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

5.1.7 Port scanning or security scanning is expressly prohibited unless prior notification to AETL is made.

5.1.8 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet

5.1.9 Employees are prohibited from using AETL electronic communication system for charitable endeavors, private business activities or amusement/ entertainment purposes.

5.1.10 Employees should not share folders on their workstations.

5.1.11 Employees are forbidden to use any messenger/chat applications such as (but not limited to) like MSN Messenger, Yahoo messenger, WhatsApp, ICQ etc.

5.1.12 Photography, video recording and audio equipment's should not be allowed inside critical sites without approval.

5.1.13 Do not print multiple copies of the same document – the printer is not a copier and typically costs more per page to use. If you need multiple copies, print one good copy on the printer and use the photocopier to make additional copies.

5.1.14 Avoid printing large files, as this puts a drain on network resources and interferes with the ability of others to use the printer. Please report any planned print jobs in excess of 100 pages to the IT department so that the most appropriate printer can be selected, and other users can be notified.

5.1.15 Avoid printing e-mail messages. This is wasteful. Instead, use the folders and archiving functionality in your e-mail application to organize and view your messages.

5.1.16 Strictly prohibited to all employees for installing / Introduction of any malicious programs into the systems / network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5.1.17 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

5.1.18 Effecting security breaches or disruptions of network communication; Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

5.1.19 Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

5.1.20 Providing information, data, code, document to any external parties / agencies or consultants, without proper authorization / approval or assigned as part of Job.

5.1.21 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

5.1.22 Use of unsolicited email originating from within AETL networks of other Internet/Intranet service providers on behalf of, or to advertise, any service hosted by AETL or connected via AETL network.

5.1.23 Employees shall not send any official documents outside of AETL offices without permission of their immediate superior either by electronic medium or otherwise.

5.1.24 Configuring external email service provider id/accounts in AETL's email account and using such email a/c for sending / receiving email.

5.1.25 Employees shall not engage in any blogging on social websites like Twitter, Facebook, Linkedin etc. from outside office network that may harm or tarnish the image, reputation and/or goodwill of AETL and/or any of its employees.

5.1.26 Employees shall not attribute personal statements, opinions or beliefs to AETL when engaged in blogging on social websites like Twitter, Facebook, LinkedIn etc. from outside office network. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee should not, expressly or implicitly, represent themselves as an employee or representative of AETL. Employees assume any and all risk associated with blogging.

5.1.27 Handling and disclosure of copyrighted, AETL's trademarks, logos and any other intellectual property shall not be used in connection with any blogging activity

5.1.28 Revealing or publicizing proprietary or confidential information representing personal opinions as those of the company

5.1.29 Downloading any software or electronic files without reasonable virus protection measures in place

5.1.30 Use or possess Internet scanning or security vulnerability assessment tools, without the permission of the Network Administrator.

5.1.31 Use the company logos or the company materials in any web page or Internet posting unless the company management has approved it, in advance,

5.1.32 Attempt to connect telnet or port scan of any remote systems on the Internet.

5.1.33 Use of internet for Chatting, Blogging, and accessing social media groups / network on AETL's systems using data card or external network is prohibited.

6. Weakness & Incident Reporting

A security weakness / incident may be a result of compromise to Confidentiality, Integrity, and availability, non-repudiation and/or Legal or Contractual Non-conformity. The impact of any security incident may result in serious consequences to the business and therefore an adherence to this policy is to avoid any such serious incident. Each employee is expected to participate in the conduct of ISMS. The following guidelines are defined:

a) Employees must promptly report all information security alerts, warnings, suspected vulnerabilities, weaknesses, and the like to the Information Security Manger using the incident reporting Form/Procedure.
b) Users are prohibited from utilizing AETL systems to forward such information to other users, whether the other users are internal or external to AETL.
c) Users should not be found exploiting any identified weakness.

Areas that can be reported are as follows (not exhaustive):

Any event or weakness that can jeopardize the confidentiality, integrity and/ availability' of information assets is worthy of reporting. This can include physical controls, technology controls, personnel behaviors related to information assets, and procedural controls.

An example of each of these is give below:

Physical controls can cover all aspects of physical security such as weak doors, access control systems, entry and exit areas, and associated processes.

Technical controls can cover strengths and weakness such as password complexity (less than 6), lack of antivirus, email attachments, accidental or deliberate mass mails etc;

Personnel controls such as unauthorized access attempts, violation of company policy, violation of internet usage policy etc.

Administrative controls such as asset not identified, document classification, no documentation, no change and access definition etc.

Note that an employee can report his/her head of department/reporting manager. Alternatively, one can also approach the IT by email at it.helpdesk@advancedenzymes.com or maruti@advancedenzymes.com.

Consequence Management/Disciplinary action Procedure (DAP)

Disciplinary action is an action towards the non-compliance to the stated objective in this policy. Any act deliberate or accidental, wherein the motive of the end-user is found to be malicious, shall lead to disciplinary action.

In case of clarifications on any areas of the ISMS, please contact to IT Head or write to him at maruti@advancedenzymes.com

7. Intellectual Property/Ownership

AETL owns all hosted infrastructure including information stored, processed, and transmitted in the company offices. No employee can claim the content or intellectual property of the assets/hosted infrastructure as their own.

8. Right to Audit

All company owned infrastructure is owned by AETL, and AETL has the right to audit any part of the infrastructure at any point of time, without giving any notice to the employee. This is to ensure that in case of a security event, the organization would need evidence to demonstrate compliance, and if necessary bring the culprit to the court of law, the culprit can be insider or outsider to the organization.

9. Governing Policy/Procedures

Information Security Policy - All employees should review the apex information Security management systems Policy and adhere to it.

10. 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.

Definitions

Term	Definitions
Information	Information is defined as anything having business value. Examples of information are customer information (such as Name, contact details, phone number etc.), financial performance, operational or communication information.
Information Asset	Information *assets* may be categorized into two categories: information *containing* assets, and information *supporting* assets. An example of information containing assets can be a business application which hosts the customer contact details, an example of information supporting assets can be personnel, paper, network infrastructure, external service providers and so on.
Security	Protection against loss of Confidentiality, Integrity, privacy, availability of an information asset.
Security Incident	An event resulting in organizational loss.
Threat	A disaster events. Threat materialization depends on the presence of vulnerabilities – either known or unknown vulnerabilities.
Vulnerability	An inherent weakness of loophole. Vulnerability may arise due to a design flaw, an implementation flow, or simply an absence of a control to prevent or detect any security incident.
Security Incident procedure	Procedure of reporting information security suspected vulnerabilities and events.

11. Enforcement

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

12. 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

13. ISMS Steering Committee Members

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

14. AETL IT Helpdesk Contact Details

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