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

Table of Contents

1. **Overview**.....3
2. **Purpose**.....3
3. **Scope**.....3
4. **Policy Statement**.....3
5. **Email ID Lifecycle Management**.....4
6. **Email Etiquette**.....6
7. **Email Security**.....8
8. **Disclaimer**.....9
9. **Policy Review**.....9
10. **Enforcement**.....9
11. **Roles & Responsibility Matrix (RACI)**.....10
12. **Roles and Responsibilities**.....10
13. **Risk for Non-Compliance**.....10
14. **ISMS Steering Committee Members**.....10
15. **AETL IT Helpdesk Contact Details**.....10

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

1. Overview

Communication over email is important means for transferring information from one part to another in any business. Messages can be transferred quickly and conveniently across internal/external network via the public Internet. However, there are risks associated with conducting business via email. Email is not inherently secure, particularly outside internal network. Messages can be intercepted, stored, read, modified and forwarded to anyone.

The objective of this policy is to define acceptable usage of email services provided by AETL.

2. Purpose

The E-mail system shall be used for business purposes only. However, the personal use of the E-mail systems is allowed to a reasonable extent (only after getting approval from the business as well as the information security team) as long as that does not damage the information and/ or reputation of AETL.

The purpose of an email security guideline is to define how AETL is going to protect itself from the risks originated while using various emails.

All messages generated by the E-mail System are the property of AETL.

3. Scope

The scope of email policy is to all employees of AETL using email services for communication. The emails can be accessed through the Microsoft outlook client or webmail or Gmail Web access on AETL owned devices or Employees owned devices. Employees can access the corporate email on office provided phone or tablets after configuring it thru IT helpdesk.

4. Policy Statement

Electronic mail service shall be provided to all employees of AETL for conducting their daily operation which is for business purpose. Usage of email for personal use is personal use is acceptable as long as it does not hamper AETL functioning and interest. AETL reserves the right to monitor the email communication details of all its users and submit it to law enforcement agencies, if demanded.

AETL considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Below are the important points related to Email policy:

- All AETL employees shall be provided with an e-mail address for use while in service with AETL, only after HR initiates the process of email account creation.
- All e-mails created, sent, or received using AETL facility, are the property of the AETL.

- IT Team (ISMS Steering Committee) reserves the right to disclose all communications, including text and images, to law enforcement agencies or other third parties without prior consent of either the sender or the receiver. User emails can be monitored without prior notification if AETL deems this necessary.
- Every user shall remain accountable for mails sent by him / her. Important E-mails need to be suitably archived for later references.
- All Email logs of Inbound/Outbound will be periodic audited as per the policy and in case any discrepancy found, strict disciplinary action initiated subjected to the criticality of the confidential data.
- All incoming emails shall be checked for virus and spam infection and blocked if it is virus or spam infected. All internal and external malicious attachment type shall be blocked at email gateway level. All outgoing mails are checked at desktop level for virus or spam.
- Email service shall be configured in such manner that only authorized individual should send email to internal email group or distribution lists.
- All outgoing emails shall be restricted to send email size upto 25MB only.
- Automatically Suspend email accounts if not logged in for 15 days from email account creation date.
- On resignation of employee, IT Administrator shall disable / delete email account upon confirmation from HR. Email forwarding to a designated employee will allowed on approval from respective Department Head or Management.
- All PST or OST files will be downloaded and backed up by IT.
- In case of employee leaves the organization, the business email configured on their personal mobile devices will be removed.
- Company reserves the rights to lock and wipe the company data of any of the mobile devices issued to the employee in case of absconding employee.

5. Email ID Lifecycle Management

The lifecycle of the Email ID shall be governed as User ID Management procedure with a special mention around special ID, as described below:

5.1 Individual Email ID

These Email IDs are owned and operated by individual user and is designated on personal name. The naming convention should be first name separated by last name. Example: firstname.lastname@advanacedenzymes.com. Request for creation of such email ID is to be placed by HR during joining process.

Individual Email ID's to be disabled or deleted on the last working day of the user by IT Help desk and IT Team respectively.

5.2 Group Email ID/Distribution List

Group email IDs (or Distribution List) are those email IDs which are mapped to multiple email IDs and are used to send email using one email ID to multiple recipient. Naming convention should ensure that the email ID reveals the names in self explanatory fashion. Example of group Email ID: tco@advancedenzymes.com Following controls are envisaged for the governance of group email ID:

- Ensure the group email ID creation request is raised and owned by the designated department head.
- Group email ID shall be treated as per User ID Management Procedure to ensure that group email ID and mis utilization of such group ID is tracked and owned by the same.
- The rights of sending emails using group email IDs shall be restricted to only designated personnel, as per approval.

5.3 Generic Mailbox/Email ID

Generic email IDs are those IDs, which are generic in nature and may be used by multiple users simultaneously. Naming convention should ensure that the email ID reveals the names in self explanatory fashion. Example of Generic Email ID: hrconnect@advancedenzymes.com Following controls are envisaged for the governance of shared e-mail ID:

- Ensure the shared email ID creation request is raised and owned by the designated department head.
- Generic ID should be treated as an exception, since track ability is an issue during misuse.
- Such email ID must be also owned by designated authority with specification of list of users authorized to receive email using the same and separate list of users sending email using the same.
- Generally, it is promoted to use group email ID or shared email box for the purpose.
- Such IDs should ideally be implemented with 9 characters strong password.
- As far as possible sending email outside AETL should be discouraged using this ID.

5.4 Generic/Non-interactive Email ID

Non-interactive email IDs are the one used by tools, which are used for the purpose of sending user notification without human intervention using relay system. Example of non-interactive email ID: donotreply@advancedenzymes.com Following controls are envisaged for the governance of non-interactive email IDs:

- The generic/non-interactive email IDs should be configured or named to be identified as AETL group email ID.
- All the generic/non-interactive email IDs, used in AETL network for notification to end users, using relay system, should be only allowed to relay using AETL email infrastructure only after the same is created, compliant to User ID management system. These non-interactive email IDs are to be owned by the respective department heads.
- Such email IDs should not be able to send notification, unless has business justification outside AETL group domain.

- Generally, it is promoted to use group email ID or shared email box for the purpose.
- Such IDs should ideally be implemented with 9 characters strong password.
- As far as possible sending email outside AETL should be discouraged.
- There shall be no receiving rights of email on such ID unless approved by appropriate levels in information security team.

5.5 Disclaimer

Legal approved email disclaimer should be used for all outbound emails from AETL.

6. Email Etiquette

The section email etiquette describes the common etiquette and diligence a user must use while using AETL email infrastructure.

6.0 Email Font

Employees are encouraged to use **Calibri** size **11** as the email font.

6.1 Out of Office

It is imperative for an employee to understand that the information so posted in Out of Office does not provide unnecessary information, which can be exploited to gain personal or official information.

Out of office reply marked with dates of total absence, reasons of absence, telephone numbers can be used as exploitable information by hackers using social engineering techniques for gaining unauthorized access.

It is recommended to use the following line for the purpose of Out of Office posting:

"Dear sender,

Thanks for your email.

I have no/limited access to email hence your reply will be delayed.

Regards,
Name
Designation"

6.2 Email Signature

The signature should have only information relevant to showcasing the following:

Name
Designation
Company Name
Complete Office Address
Telephone/& Mobile No.
Email address and Company website
Use of **images** is considered inappropriate and unprofessional signature. Avoid using the same.

6.3 Construct of Email (Do's)

- Write well-structured mails. Always include a short and descriptive subject heading.
- AETL email style is informal. Keep the sentences short and to the point.
- Start your e-mail with 'Hi', 'Hello' or 'Dear', and the name of the person.
- End the message with "Warm Regards' or 'Best Regards'.
- Use spell checker before you send out an email.
- Compress attachments wherever possible.
- Do not send unnecessary attachments.
- Do not send "Reply All" mails on trailing mails when it not necessary.
- If you forward mails, state clearly what action you expect the recipient to do.
- Only mark emails as important / priority if they really are important / priority.
- Delete any email message that you do not need to have a copy of, and set your email client to automatically empty your 'deleted items' on closing.
- Periodically purge messages, no longer needed for business purposes, from your personal electronic message storage areas.
- Look at the email address completely, not just the sender and email body. What you see in the e-mail body can be forged, the sender's address or return address can be forged and the e-mail header can also be manipulated to disguise its true origin. Unless the e-mail is digitally signed you can't be sure it wasn't forged or 'spoofed'.
- Watch for email senders that use suspicious or misleading domain names.
- Never reveal information, such as passwords, to anyone contacting you.

6.4 Construct of Email (Don'ts)

- Do not write emails in capitals.
- Do not subscribe to a newsletter or news group without prior permission from your supervisor.
- Do not use the electronic mail resources for personal monetary gain or for commercial purposes that are not directly related to AETL business.
- Do not send copies of documents /software in violation of copyright laws.
- Do not capture /intercept and / or open electronic mail not meant for you, except as required in order for authorized employees to diagnose and correct delivery problems.
- Do not use electronic mail to harass or intimidate others or to interfere with the ability of others to Conduct AETL business.

- Do not use electronic mail systems for any purpose restricted or prohibited by law or regulations.
- Do not forward mails (dot forward) to Public e-mail service providers (Hotmail, Yahoo, etc)
- Do not indulge in "spoofing". i.e., constructing an electronic mail communication such that it appears to be from someone else.
- Do not indulge in "Snooping", i.e., obtaining access to the files or electronic mail of others.
- Do not attempt unauthorized access to electronic mail or breaching the security measures on any electronic mail system.
- Do not send mail addressed to all employees without consulting Technical Department.
- Do not make or post indecent remarks, proposals or materials.
- Do not reveal or publicize confidential or proprietary information which includes, but is not limited to: financial information, new business and product ideas, marketing strategies and plans, databases and the information contained therein, customer lists, technical product information, computer/network access codes and business relationships.
- Do not use official email systems for charitable endeavors, private business activities, and amusement / entertainment purposes unless expressly approved by AETL.
- Never create either the appearance or the reality of inappropriate use of e-mail system.
- Do not forward MP3, Irrelevant JPEG or other image files.
- Do not send mass greeting cards.
- Do not forward e-mail to multiple addresses unless it serves genuine business purposes. Do not use official email to send confidential/sensitive information, particularly over the Internet, unless it is first encrypted by an encryption system approved by Information Security.

7. Email Security

7.1 Limits

- IMAP will be disabled by default for any new email user being created; user needs to get this approved by Head of the department or Management for this facility.
- Shared Mailboxes will be given only for generic IDs based on request and approved by Head of the department or Management.
- Outside office email access will be disabled by default for any new email user being created; user needs to get this approved by Head of the department or Management for this facility.

7.2 Bulk Emails

- User is not allowed to send out Bulk Email via Corporate Email System
- If Bulk Email is required, proper business justification / CFO approval is required
- Right to mark email to the group ID needs to be approved by designated authorities.

7.3 Internal Email Security

AETL uses Seqrite Endpoint security and spam filters. Seqrite delivers inbound and outbound messaging security, with effective and accurate antimalware, antispam, content filtering and email encryption services from a global cloud platform. It is designed to provide 100% protection against known and unknown email viruses. Seqrite Endpoint Email Security helps protect AETL from email-borne viruses, malware, spam, phishing and targeted attacks.

The following security options, at a high level are configured:

- Attachment for most common kind shall be scanned.
- All email found with malware are deleted.
- Content filter for Profanity, Racial Discrimination, Sexual Discrimination and Hoaxes are configured.
- Email attachments containing movie, music like .mpg, .mov, .avi, .mp3, .wav, .aiff etc. are blocked.

7.4 External Email Security

AETL uses built in Email Security provided by Google Workspace cloud for gateway level email security. The following security options, at a high level are configured.

- Positively identified spam/malware contained emails are dropped.
- All suspected emails with spam are being quarantined or moved to spam folder.

8. Disclaimer

AETL reserves absolute right to alter or abolish the access rights of users based on threat landscape of email usage.
Such discretion may be exercised any time whenever there is a risk of security breach.

9. 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.

10. Enforcement

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

11. 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

12. Roles and Responsibilities

Roles and their specific responsibilities for the defined policy are as under:

- **IT Head**
  - Shall assist in risk assessment and identify security controls,
  - Shall perform document review and version control.

- **IT Administrator**
  - Shall be responsible for maintaining adequate security of email service.
  - Shall create, disable, delete email account.

- **User**
  - Shall use email service judiciously.
  - Ensure security of information contained in e-mail messages.
  - compress files before sending via email.

13. Risk for Non-Compliance

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

- Email Spam, Junk Emails
- Misuse of Email service

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

14. ISMS Steering Committee Members

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

15. AETL IT Helpdesk Contact Details

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