

<b>Policy Domain</b>	<b>Information Security Policy</b>	<b>Creation Date</b>	10 <sup>th</sup> Feb 2021
		<b>Classification</b>	Internal
		<b>Version</b>	1.0
		<b>Doc. Owner</b>	IT Head

<b>Document Control</b>			
<b>Prepared By</b> Vineet Kumar Chawla (Sr. Consultant IT)	<b>Reviewed By</b> Maruti Divekar (IT Head)	<b>Checked By</b> B P Rauka (CFO)	<b>Approved By</b> Mukund Kabra (Director)

<b>Document Modification History</b>							
SR #	Document	Version No.	Reviewed On	Checked On	Approved On	Effective Date	Authorized Signatory
1.	Information Security Policy	1.0	05 <sup>TH</sup> Mar 21	10 <sup>th</sup> Mar 21	10 <sup>th</sup> Mar 21	11 <sup>th</sup> 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).

<b>Policy Domain</b>	<b>Information Security Policy</b>	<b>Creation Date</b>	10 <sup>th</sup> Feb 2021
		<b>Classification</b>	Internal
		<b>Version</b>	1.0
		<b>Doc. Owner</b>	IT Head

**Table of Contents**

1. Introduction.....3

2. Scope.....3

3. Policy Statement.....4

4. ISMS Policy.....4

    4.1 Objective.....4

    4.2 Purpose.....5

    4.3 Policy Disclaimer..... 5

5. ISMS Policy Statement..... 6

6. Information Security Awareness.....7

7. Compliance Requirements..... 7

8. Roles & Responsibility Matrix (RACI) .....7

9. Roles and Responsibilities.....8

10. Risk for Non-Compliance.....8

11. References.....8

12. ISMS Steering Committee Members.....9

13. AETL IT Helpdesk Contact Details.....9

Policy Domain	Information Security Policy	Creation Date	10 <sup>th</sup> Feb 2021
		Classification	Internal
		Version	1.0
		Doc. Owner	IT Head

## 1. Introduction

Technology is an enabler of business processes at AETL. With forever increasing usage of technology, to manage data, comes also the need to ensure that the data is protected from misuse, theft, etc. Information security has, therefore, assumed great importance for the success of an organization, as the intentional or unintentional misuse of information, information assets, and information processing facility may result into financial loss, business discontinuity, loss of goodwill, dissatisfaction of internal stakeholders, lawsuits and non-compliance with the regulatory provisions etc. Therefore, constant vigilance along with an extensive and properly implemented Information Security Management System (hereinafter referred in the document as ISMS) framework is deemed mandatory requirement for the organization's effective service delivery and continued contribution to economic growth.

This security policy deals with the following domains of security:

- People;
- Process; and
- Technology.

There are three main sources from which security requirements are derived:

- One source is derived from assessing risks to our organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated, and potential impact is estimated.
- Another source is the legal, statutory, regulatory, and contractual requirements that our organization, contractors, and service providers have to satisfy, and also socio-cultural environment.
- A further source is the particular set of principles, objectives and business requirements for information processing that our organization has developed to support its operations.

ISMS policy is to implement the best practices to protect the **Confidentiality, Integrity, Availability** of information assets.

## 2. Scope

This policy applies to all AETL employees. It is the responsibility of all operating units to ensure that these policies are clearly communicated, understood and followed.

This polices also apply to contractors, and vendors/suppliers providing service to AETL that bring them into contact with AETL's Information assets in any form. The AETL employee who contracts for these services is responsible to provide the contractor/vendor/supplier with a copy of these policies before any access is given.

<b>Policy Domain</b>	<b>Information Security Policy</b>	<b>Creation Date</b>	10 <sup>th</sup> Feb 2021
		<b>Classification</b>	Internal
		<b>Version</b>	1.0
		<b>Doc. Owner</b>	IT Head

### 3. Policy Statement

This policy applies to all AETL employees. It is the responsibility of all operating units to ensure that these policies are clearly communicated, understood and followed.

AETL's information systems, and the information held by these systems, are fundamental to their operations and future success. AETL aims at providing a secure environment to ensure confidentiality, availability and integrity of information and it's processing pertaining to our clients and ourselves.

All employees and associates of AETL and related operations are responsible for promoting and exercising good security practices as stipulated in this information security policy so that information assets are properly protected, and business is securely done. Responsibility for security rests with all of us. We at AETL are committed to provide better IT Services to our clients through:

- Adherence to laid down security policies and guidelines
- Ensuring information security
- Complying with laws & regulations
- Continuous enhancement in Information Security Posture
- Availability of services under stated contingencies
- Periodic Security awareness

### 4. ISMS Policy

#### 4.1 Objective

Information is an important business asset of significant value to AETL and is protected from threats that could potentially disrupt business continuity. This policy has been written to provide a mechanism to establish procedures to protect against security threats and minimize the impact of security incidents.

The purpose of this policy is to protect the company's information assets from all threats, whether internal or external, deliberate or accidental.

The policy scope covers physical security and encompasses all forms of Information Security such as data stored on computers, transmitted across networks, printed or written on paper, stored external devices and CD's or spoken in conversation or over the telephone or any other; which may endanger the information due to unauthorized disclosure.

All employees of AETL are responsible for implementing the Policy within their business areas. It is the responsibility of each employee to adhere to the policy. Disciplinary process will be applicable in those instances where any employee fails to abide by this security policy.

Information Security Policy of AETL is intended to achieve, but not limited to the following:

<b>Policy Domain</b>	<b>Information Security Policy</b>	<b>Creation Date</b>	10 <sup>th</sup> Feb 2021
		<b>Classification</b>	Internal
		<b>Version</b>	1.0
		<b>Doc. Owner</b>	IT Head

- Information shall be protected against unauthorized access;
- Confidentiality of Information is assured at all times;
- Integrity of information is maintained;
- Availability of right type of information at the right place is maintained;
- Regulatory and legal requirements regarding intellectual property rights, data protection and privacy of personal information are met;
- Risk treatment plan is established, maintained and tested and
- All employees are given adequate training/awareness on Information Security.

All breaches of information security actual or suspected are reported and investigated at appropriate level to ensure understanding of the root cause, prepare knowledge repository to eliminate/minimize future occurrence and to take corrective/ preventive measures.

Any action that may expose the Company to risks of unauthorized access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action up to any including termination of employment and / or criminal prosecution.

#### 4.2 Purpose

All employees at AETL share the Information Technology infrastructure at AETL. These facilities are provided to employees for the purpose of disbursing AETL's business.

AETL does permit a limited amount of personal use of these facilities, including computers, printers, email and Internet access. However, these facilities must be used responsibly by everyone, since misuse by even a few individuals has the potential to negatively impact on productivity, result in disruption of company business and interfere with the work or rights of others. Therefore, all employees are expected to exercise diligence and have ethical behaviour when using the company's information and information processing facilities.

Any action that may expose the Company to risks of unauthorized access to data, disclosure of information, legal liability, or potential system failure is prohibited and may result in disciplinary action up to any including termination of employment and / or criminal prosecution.

#### 4.3 Policy Disclaimer

The use of the AETL information and information processing facilities in connection with company business and limited personal use is a privilege but not a right, extended to various Company employees. Users of AETL computing facilities are required to comply with all policies referred to in this document.

Users also agree to comply with applicable country and local laws and to refrain from engaging in any activity that would subject the company to any liability. AETL reserves the right to amend these policies and

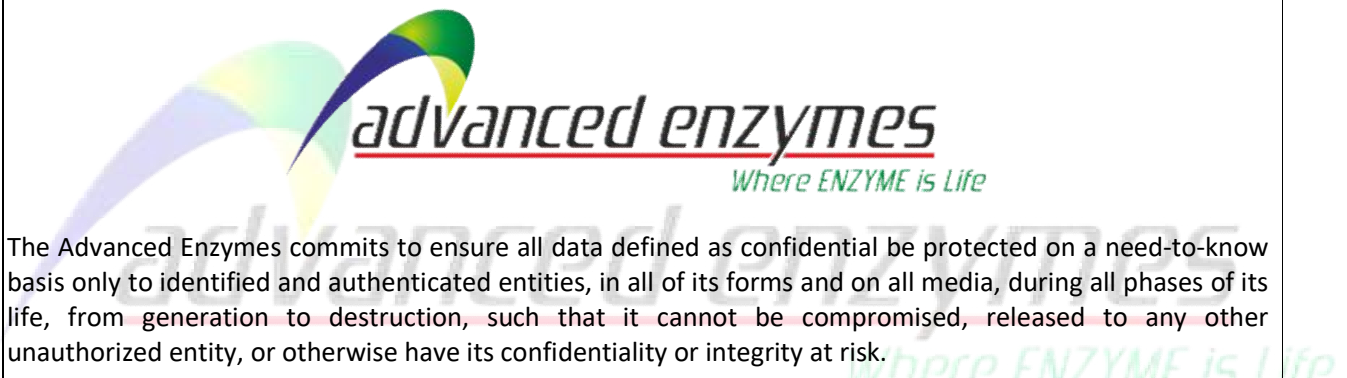
<b>Policy Domain</b>	<b>Information Security Policy</b>	<b>Creation Date</b>	10 <sup>th</sup> Feb 2021
		<b>Classification</b>	Internal
		<b>Version</b>	1.0
		<b>Doc. Owner</b>	IT Head

practices at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with applicable laws.

To protect the integrity of AETL information and information processing facilities and its users against unauthorized or improper use of those facilities, and to investigate possible use of those facilities in violation of AETL policies, AETL reserves the right, without notice, to limit or restrict any individual's use, and to inspect, copy, remove, or otherwise alter any data, file, or system resource which is used in violation of AETL rules or policies. AETL also reserves the right periodically to examine any system and other usage and authorization history as necessary to protect its information and information processing facilities. AETL disclaims any responsibility for loss of data or interference with files resulting from its efforts to maintain the privacy and security of those computing facilities or from system malfunction or any other cause.

## 5. ISMS Policy Statement

### Information Security Policy



The Advanced Enzymes commits to ensure all data defined as confidential be protected on a need-to-know basis only to identified and authenticated entities, in all of its forms and on all media, during all phases of its life, from generation to destruction, such that it cannot be compromised, released to any other unauthorized entity, or otherwise have its confidentiality or integrity at risk.

Maintain integrity and availability of information by facilitating access; exchange of information within the organization on a need-to-know basis only to identified and authenticated entities; and institutionalization of secure work environment by complying with all contractual, regulatory requirements and protect proprietary information in all forms.

Establish and evaluate systematic risk management strategies, impart training to users (including third parties) to equip them to be aware of security weakness and report security incidents, security weakness and software/hardware malfunctions.

Formulate, implement, test and maintain a practicable business continuity plan to facilitate continual customer satisfaction.

<b>Policy Domain</b>	<b>Information Security Policy</b>	<b>Creation Date</b>	10 <sup>th</sup> Feb 2021
		<b>Classification</b>	Internal
		<b>Version</b>	1.0
		<b>Doc. Owner</b>	IT Head

## 6. Information Security Awareness

- Protecting AETL Information Assets is a key responsibility for all employees.
- Each employee ensure that he/she must be aware of his/her roles and responsibilities.
- In this endeavour, Information Security team send IS security awareness emails and IS policy to all new joiners on AETL domain (employees and named contractual ids).
- To ensure each employee (AETL domain & contractual employee) must be aware of Information Security, all employees will again get notified periodically with awareness emails, documents and IS policy.

## 7. Compliance Requirements

- It is mandatory for all employees to ensure that they have read and understood the ISMS policy;
- In case of any doubts, they need to contact their respective manager for clarity;
- Non-compliance due to ignorance shall be treated as wilful ignorance;
- Non-compliance to ISMS policy may result in disciplinary action; and
- Any non-compliance due to technical or business feasibility, the same is required to be validated by the respective line of business including acceptance of risk.

## 8. 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

<b>Policy Domain</b>	<b>Information Security Policy</b>	<b>Creation Date</b>	10 <sup>th</sup> Feb 2021
		<b>Classification</b>	Internal
		<b>Version</b>	1.0
		<b>Doc. Owner</b>	IT Head

## 9. Roles and Responsibilities

- **IT Team :**
  - Shall review this document at least once in a year and/or when there is a significant change in the organization, technology adopted, business objectives, identified threats, external events
  - Policy Ownership,
  - Development and Maintenance Compliance audit & risk reviews
  - Coordinate for security compliance audit, minimum once in a year as per schedule.
  - Shall be responsible for maintaining updated copy of this document and its effective communication.
  - Conduct periodic training and security awareness programs for all users on security and system usage responsibilities.
- **Security Operations / IT Team:**
  - Procedure Development and Maintenance
  - User Provisioning and De-provisioning
  - Internet Security Configuration, Implementation and Administration, Monitoring
- **Users:**
  - Shall attend security awareness training arranged by AETL.
  - Shall use Internet service judiciously.
  - Understand that Information Security is everybody's responsibility.
  - Report any security incident to IT team immediately.
  - Discharge his or her responsibility for information security.
  - Responsible for taking backups as well as for restoration of files residing on their desktop/Laptops.

## 10. Risk for Non-Compliance

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

- Unauthorized Access
- Malicious Code or virus propagation
- Information leakage, violation of IPR
- Misuse of the internet facility given to the employees, third parties of AETL
- Threat to Image & reputation of AETL
- Information disclosure,
- Violation of laws and regulation,
- Unavailability of service,
- Insecure IT operation,
- Inadequate security posture



<b>Policy Domain</b>	<b>Information Security Policy</b>	<b>Creation Date</b>	10 <sup>th</sup> Feb 2021
		<b>Classification</b>	Internal
		<b>Version</b>	1.0
		<b>Doc. Owner</b>	IT Head

## 11. References

- **Information Security standard ISO27001:**

- Control Objective A.5.1 – Information Security Policy
- Control Objective A.12.1 – Security requirements of information systems.
- Control Objective A.12.4 – Security of system files.
- Control Objective A.13 – Information security incident management.
- Control A.15.1.1 from Annexure A – Identification of applicable legislation
- Control A.15.1.2 from Annexure A – Intellectual Property Rights (IPR)
- Control A.15.1.4 from Annexure A – Data protection and privacy of personal information

## 12. ISMS Steering Committee Members

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

## 13. AETL IT Helpdesk Contact Details

- Logging an online support request: <https://192.168.2.7:8080>
- Email: [it.helpdesk@advancedenzymes.com](mailto:it.helpdesk@advancedenzymes.com)
- Telephone: **022 41703234**

*advanced enzymes*  
Where ENZYME is Life