Policy Domain	Incident Management 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.	Incident Management 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).

Table of Contents

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

1. Overview

Business users expect smooth business operations without any disturbance. However, in reality it is a challenge to achieve with the available complex infrastructure components and applications. Proactive approach to incident management eliminates major incident occurrence.

2. Purpose

The purpose of this policy is to make the organization resilient to any accidental or deliberate security incidents to Information Assets and the supporting infrastructure.

3. Scope

The scope of this policy includes all (but not limited to) Organization personnel and service/support contractors who have access to Organization information and supporting.

4. Policy

4.1 General information

The goal of Incident Management policy is to restore service operations as quickly as possible and minimize the adverse impact of a service outage or degradation on the organization. The activities associated with Helpdesk Support Portal Management primarily deal with recording the details of the incident, classifying the incident, investigating the incident, and ultimately resolving the incident.

4.2 Incident Reporting Procedure

a) Users need to logged incident request by sending mail or manually adding incident request on Helpdesk Support Portal.

b) Please refer **AETL Helpdesk Support Portal User Guide** for more information.

4.3 Incident Response Procedure

4.3.1 After the incident is reported, Location IT In-charge, shall immediately analyze the incident and categorize whether it is minor or major.

4.3.2 Manager IT shall try to find the damage caused by the incident to AETL's information processing facilities. However, if the severity of the incident is high and the resolution process is not within the purview of IT In-charge, it shall be escalated to Head IT / HOD.

4.3.3 The System Admin/ Incident response team should first apply short-term solution to contain the damage and minimize the risk, which is critical to an incident.

4.3.4 Identifying the type and severity of the compromise is essential to see what kind of resources is required to be allocated. It needs to be labeled based on the severity level like High, medium and low Priority.

4.3.5 The "exact" nature of the incident needs to be identified for an effective counter measure procedure.

4.3.6 Determine the incident point of origin where exactly it is coming from. (For e.g. Single point or Multi point)
4.3.7 Also, identify the systems that have been compromised.
4.3.8 Identify if AE has to move the business functions to its Disaster recovery site. If so initiate the process.
4.3.9 Identify the evidences of the incidence and collect them all. It is essential to protect the collected evidence.
4.3.10Where action against a person or organization involves the law, either civil or criminal, the evidence collection and presentation will conform to applicable laws. This will include compliance with any published standard or code of practice for the production of admissible evidence.
4.3.11All investigations of alleged criminal or abusive conduct will be treated as restricted information to preserve the reputation of the suspected party until charges are formalized or disciplinary action taken.
4.3.12All internal investigations of information security incidents, violations, and problems will be conducted by staff authorized.

3.1 Recovery

In case of security incident like theft, start the procurement of the new device. If case of security incidents involving hacking or virus or other system related incidents bring back the systems to original state. The systems need to be brought back online in the minimum possible time. The following steps should be carefully carried out for an effective resumption of the work and to prevent any reoccurrence.

3.1.1 **Eradication –** Remnants of the incident (attacker toolkits, Trojan horse programs, viruses, etc.) must be removed from the system(s) affected by the incident.
3.1.2 **Operations Restoration –** Systems must be rebuilt, recovered, or replaced.
3.1.3 **Mitigate Reoccurrence Risk** - System vulnerabilities and inadequate controls exploited by the attacker must be addressed.

5. Monitoring & Control

5.1 It is the responsibility of the Head IT to monitor and review that internal IT team/Outsource Service Provider is adhering to the defined Policy Norms.
5.2 In case it is found by Head IT or by internal audit team that the employee is not adhering to the terms defined under the policy, the same shall be highlighted to the Director for required action.

6. 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.

7. Roles & Responsibility Matrix (RACI)

Role Activity	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. Roles and Responsibilities

Below are the specific roles and responsibilities for the defined policy:

- **User**
  - Shall formally report the incident.
  - Shall fill request in Helpdesk support portal tool with complete details and impact assessment.

- **Change Manager, IT Head**
  - Shall determine the impact of incident.
  - Basis the severity of impact IT Head will notify Director/MD, Employees and any third party to be impacted by the implementation.
  - shall suggest and approve the corrective action to control the impact and approve.

- **Incident Controller (IT Head/Local IT In Charge)**
  - Shall Implement strategies as suggested by IT.
  - Shall notify any parties to be impacted by the implementation.
  - Shall confirm once the implementation sequence is completed.
  - Shall communicate the result of the implementation to the relevant parties.

9. Risk for Non-Compliance

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

- Data/Configuration integrity loss,
- System crash and avoidable interruptions,
- Security failures
- Loss of unavailability of important data

Compliance with this policy initiates the following key controls:

- Incidents are reported and contained.
- Changes are implemented as per priority and in a controlled manner.
- All the incidents are adequately documented for audit trail and proactive management.

10. ISMS Steering Committee Members

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

11. AETL IT Helpdesk Contact Details

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