Document Statistics

Type of Information	Document Data
Organization	**Panacea Bioedge Pvt. Ltd**
Document Name	Reward and Recognition Policy
Classification	Internal
Date of Release	01-08-2025

Document Revision History

Version Number	Revision Date	Description for Change	Reason for Change	Affected Section	Prepared By	Reviewed By	Approved By
1.0	00	-	New Document	--	QM	Lead-ESG	DO

1. Purpose

Table of Contents

1. Introduction 3
2. Purpose 3
3. Scope 3
4. Policy Statement 3
5. Organizational Responsibilities 4
5.1 Senior Management: 4
5.2 Human Resources Department: 4
5.3 Information Security Manager: 4
5.4 Line Managers of Security Testing Team: 4
5.5 STT Employees: 4
6. Policy Requirements 5
6.1 Criteria for Security Testing Team 5
6.1.1 Quantitative Parameters: 5
6.1.2 Qualitative Parameters: 5
6.2 Programs and Initiatives 5
6.2.1 Quarterly Security Champion: 5
6.2.2 Annual Distinguished Security Advocate 6
7. Policy Administration 6
7.1 Version Control 6
7.2 Review Cycle 6
7.3 Exceptions 6
8. Enforcement 6

Introduction

Panacea Bioedge Pvt Ltd is committed to developing a robust information security management system (ISMS) as per ISO 27001 standard. The Security Testing information security controls and posture.

This policy outlines a comprehensive framework for motivating, recognizing and rewarding the efforts, achievements and leadership demonstrated by STT personnel towards advancing the organization's information security objectives in alignment with ISO 27001 guidelines.

Purpose

The purpose of this policy is:

a) To foster an information security conscious culture and motivate STT members to implement sound cybersecurity practices that contribute towards the ISO 27001 ISMS objectives.

b) To institutionalize mechanisms for acknowledging the accomplishments of STT personnel in continuously identifying, assessing and mitigating critical information security related risks and vulnerabilities.

c) To incentivize behaviours and initiatives focused on collective responsibility and leadership towards achieving organization-wide information security goals.

d) To enable the attraction, growth and retention of specialized talent with capabilities and potential to elevate information security preparedness as per ISO 27001 best practices.

Scope

This policy is applicable to all current employees who are part of the Security Testing Team at Panacea Bioedge Pvt Ltd. The scope covers initiatives tied to rewards and recognitions focusing specifically on information security achievements.

Policy Statement

Panacea Bioedge Pvt Ltd is committed to identifying, assessing and mitigating information security risks continually in alignment with the ISO 27001 standard. The organization also endeavours to build a work culture where employees are motivated to realize the ISMS objectives through individual discipline and collective contribution.

This policy mandates the institution of formal reward and recognition programs to drive information security focused behaviours and outcomes across all activities undertaken by the STT department.

Organizational Responsibilities

Senior Management:

Ensure adequate budget allocation for executing this policy effectively.

Provide leadership direction and visibility to information security initiatives recognizing employee rewards and recognitions.

Human Resources Department:

Design programs for information security specific reward and recognition categories as per guidelines from Information Security Manager

Facilitate the assessment process through tools and templates mapping to policy criteria.

Information Security Manager:

Finalize appropriate metrics and criteria for information security related rewards and recognitions in alignment with business priorities and ISO 27001 controls

Participate in the assessment and nomination process for finalizing reward recipients

Line Managers of Security Testing Team:

Reinforce information security focused behaviours through positive feedback, coaching and mentoring STT personnel

Provide mandatory inputs during annual/ periodic reviews to determine eligibility for performance based rewards

STT Employees:

Adhere to this policy and associated information policies of the organization in letter and spirit

Proactively attend information security trainings and certifications to enhance knowledge and competence

Policy Requirements

Criteria for Security Testing Team

The criteria for rewards and recognitions focusing on STT's contribution to information security shall include:

Quantitative Parameters:

Number of critical/high severity vulnerabilities discovered and addressed

Quick identification, escalation and resolution of information security incidents

Innovative solutions directly enhancing security of infrastructure, applications, products and services

Adoption of tools, technologies and practices to improve information security controls

Qualitative Parameters:

Demonstrated commitment towards evolving the organization's information security capabilities in alignment with industry best practices and ISO 27001 standard

Consistent compliance with existing information security policies and support during new policy roll-outs

Responsible application of skills and expertise to strengthen ISMS objectives

Collaboration with diverse teams to drive organization-wide information security initiatives

Programs and Initiatives

The programs instituted to encourage and felicitate STT for noteworthy contributions to information security shall include:

Quarterly Security Champion:

Two top performers from STT shall be recognized as “Quarterly Security Champion” basis selection criteria. Benefits include:

- Certificate of Appreciation
- Gift Voucher Worth Rs 2000
- Display photograph on STT Information Security board.

Annual Distinguished Security Advocate

The STT member demonstrating year-on excellence across quantitative and qualitative information security contributions shall be recognized as "Annual Distinguished Security Advocate" and facilitated during the annual Founders Day event with:

- Letter of Appreciation from CEO
- Trophy
- Cash Award of Rs 10,000

Policy Administration

Version Control

All policy revisions shall be tracked via document version numbers and change log in adherence to ISO 27001 Clause 8.1.

Review Cycle

This policy shall be reviewed annually in alignment with the Information Security Policy review framework. Recommendations for revisions shall be submitted to the Information Security Manager.

Exceptions

Any deviations sought from this policy shall be processed per the Information Security Policy Exception Procedure.

Enforcement

Any non-conformance to this policy by STT personnel shall be addressed as per the organization's employee disciplinary process.

The Panacea Bioedge Pvt. Ltd. is the owner of this document and is responsible for ensuring that this policy document is reviewed in line with the review requirements stated above.

A current version of this document is available to all members of STT staff.

This policy was approved by, CEO and is issued on a general company policy under his/her signature.

Signature: Date: