

Information Security Management Systems

Information Security Policy

V-Guard Industries Ltd & Subsidiary Companies (V-Guard)

Classification: Public

1. DOCUMENT CONTROL

Rule Profile		
General	Title	VGIL-ISMS-05-Information Security Policy
	Summary	This document contains the Information Security policy and objectives of VGIL.
	Prepared By	VGIL
	Reviewed By	CISO
	Approved By	Management Committee
	Last Revision	1.1
	Validity From	16-Feb-2026
	Number of Pages	7 Pages
Responsibility	Ownership	CISO
	Distribution List	All V-Guard Employees
	Documentation	This Document is available in Intranet portal and Available for public in V-Guard Website
Other Documents	Annexes	Nil
	Further Applicable Regulations	Nil

2. CHANGES AND REVISION HISTORY

Version No	Date	Summary Details of Changes	Responsibilities of Changes	
1.0	15-Oct-2024	New	Author	PBC
			Reviewer	CISO
			Approver	Management Committee
1.1	21-Jan-2026	Included Policy Applicability	Author	Info Sec
			Reviewer	CISO
			Approver	Management Committee

Internal

3. TABLE OF CONTENTS

1. Document Control 1

2. Changes and Revision history..... 2

3. Table Of Contents 3

4. Introduction 4

5. Policy Applicability 4

6. Purpose..... 4

7. Scope 4

 7.1. Scope Statement 4

 7.2. Physical Scope and Processes 5

8. Goals..... 5

9. Intended Outcome and IS Objectives..... 5

10. Information Security Management System Policy 5

 10.1. Policy Statement 5

 10.2. Information Security Policy 6

Internal

4. INTRODUCTION

This document contains the policies for the Information Security Management System (ISMS) based on ISO / IEC 27001:2022, to preserve Confidentiality, Integrity and Availability of systems and information used by V-Guard.

5. POLICY APPLICABILITY

This policy applies to **V-Guard Industries Ltd. and its Subsidiary Companies**, which shall mean and include:

- **V-Guard Industries Ltd.**
- **V-Guard Consumer Products Limited.**
- **Guts Electro-Mech Ltd.**
- **Sunflame Enterprises Private Ltd.**

All the above entities are hereinafter collectively referred to as "**V-Guard.**". This policy is binding on all employees, contractors, consultants, third-party service providers, and any individual or entity acting on behalf of V-Guard. Compliance with this policy is mandatory for all activities, operations, processes, information systems, and resources managed or controlled by **V-Guard.**

6. PURPOSE

The ISMS is based on the overall business risks of V-Guard. The ISMS is designed to ensure adequate and proportionate security controls that adequately protect information assets and give confidence to V-Guard. management, customers, suppliers and other interested parties.

The purpose of this policy is to provide governance and ensure: -

- The confidentiality, integrity and availability of critical information.
- Critical information is protected from intentional or unintentional - unauthorized access, use, disclosure, modification and disposal.
- All applicable legal, regulatory and contractual requirements with regard to information security are complied.
- All stakeholders adhere to the policy and the Management has rights to take necessary action in case of violation.

7. SCOPE

This policy applies to employees, temporary staff and all other stakeholders of V-Guard. This policy is also applicable to all information assets within the ISMS scope and boundaries.

7.1. Scope Statement

The scope statement for V-Guard, is mentioned as follows –

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) FOR SUPPORT AND MAINTENANCE OF IT INFRASTRUCTURE, IT OPERATIONS AND IT APPLICATIONS FOR INTERNAL OPERATIONS.

7.2. Physical Scope and Processes

The Scope of ISMS is applicable at the below-mentioned Location:

V-Guard Industries Limited, Regd. office: 42/962, Vennala High School Road Vennala, Kochi - 682 028.

The processes under the scope of certification are

- ❖ **IT Infrastructure**
- ❖ **IT Operations**
- ❖ **IT Applications**

8. GOALS

Compliance: Organization's awareness towards compliance and adherence towards information security to meet accepted standards and follow best practices while delivering in all operational areas.

Business Continuity: To ensure robust processes and systems are in place and thereby ensuring the operation is process driven with right and competent people such that business continuity is never hampered.

Customers: Robust and absolute security of client data to ensure and establish trustworthy client relationships

9. INTENDED OUTCOME AND IS OBJECTIVES

The main objectives of **Information Security Management** may be summarized as:

1. Designing a security policy (in collaboration with customers and suppliers) that is aligned with the needs of the business.
2. Ensuring compliance with the agreed security standards.
3. Minimizing the security risks threatening continuity of service.

ISMS Objectives are periodically monitored, measured and articulated in order to ensure effective implementation of V-Guard's ISMS framework.

10. INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

10.1. Policy Statement

V-Guard has agreed to adopt an **Information Security Management System (ISMS)** that complies with the **ISO/IEC 27001:2022 Standard**. It is the intention of the V-Guard 's Corporate Management Board to maintain compliance/certification with the Information Security Standard for the following reasons:

1. V-Guard has an obligation to its customers, employees, suppliers, and service providers to protect and ensure stringent and effective maintenance of the **Confidentiality, Integrity** and **Availability** of information assets and ensure the organization is compliance driven.
2. To ensure business continuity and minimize disruption to business functions by preventing and minimizing the impact of security incidents.
3. To affirm trust among the customers and global market for ensuring healthy business relationships and partnerships
4. Fostering a secure work environment by engaging and involving employees towards achieving the best security standards and processes.
5. To ensure best security processes are implemented so that the right information is available to the right resource at the right time.

10.2. **Information Security Policy**

This Information Security Policy demonstrates the direction and commitment of V-Guard towards information security in order to protect its own information assets and those provided to the V-Guard by their Interested parties.

Our information security management system will ensure that:

1. Critical information is protected from unauthorized access, use, disclosure, modification, and disposal.
2. The **Confidentiality, Integrity** and **Availability** of such information, whether acquired, provided or created, are ensured at all times.
3. Awareness programs on Information Security are available to all employees and wherever applicable to third parties viz. subcontractors, consultants, vendors etc.
4. All contractual requirements with respect to information security are met wherever applicable and comply with all relevant information security laws, regulations.
5. Any incident of Policy infringement will be reported, and corrective actions are taken.
6. The management is committed towards the continual improvement of the information security management system.

All interested parties should understand their obligations to protect these assets and implement security practices consistent with the security manual. Compliance will be checked periodically through reviews, audits, and then corrective actions will be initiated.

Internal