CYBER SECURITY POLICY

Stylam Industries Limited

Head Office: SCO 14, Sector 7C, Madhya Marg
Chandigarh – 160019, India

DOCUMENT CONTROL

Field	Details
Document Name	Cyber Security Policy
Document ID	SIL-IT-POL-CSP-001
Version	1.0
Effective Date	20-01-2026
Created By	Sandeep Kumar
Reviewed By	Rajiv Jindal
Approved By	Anurag Jain

CONFIDENTIALITY STATEMENT

1. INTRODUCTION

Stylam Industries Limited recognizes that its information and cyber assets are critical to its business operations, customer trust, and overall reputation.
The organization is committed to protecting its digital ecosystem by ensuring the Confidentiality, Integrity, and Availability (CIA) of all information assets.

2. VISION & MISSION

Vision

To build a secure, resilient, and trusted digital environment that supports business growth and minimizes cyber risks.

Mission

To implement and maintain a robust cyber security framework that safeguards information assets from unauthorized access, disruption, or loss.

3. OBJECTIVES

- Ensure secure access to systems for authorized users
- Protect information assets from cyber threats
- Implement effective cyber risk management practices
- Ensure compliance with legal and regulatory requirements
- Promote cyber security awareness among employees
- Establish effective incident response mechanisms
- Continuously improve cyber security posture

4. SCOPE & APPLICABILITY

This policy applies to:

- All employees of Stylam Industries Limited
- All IT systems, applications, networks, and data owned or managed by Stylam

5. CYBER SECURITY PRINCIPLES

Stylam Industries Limited shall adhere to the following CIA principles:

Principle	Description
Confidentiality	Prevent unauthorized access to information.
Integrity	Protect data from unauthorized modification.
Availability	Ensure timely and reliable access to information.

6. POLICY STATEMENTS

Ref	Area	Policy Statement
6.1	**Risk Management**	Cyber risks shall be identified, assessed, and mitigated through formal processes.
6.2	**Access Control**	Access to systems shall be granted based on business need and authorization.
6.3	**Data Protection**	Sensitive data shall be protected throughout its lifecycle.
6.4	**Incident Management**	All cyber incidents shall be reported, investigated, and resolved promptly.
6.5	**Monitoring & Detection**	Systems shall be implemented to monitor and detect cyber threats.
6.6	**Awareness & Training**	Employees shall receive regular cyber security awareness training.
6.7	**Continuous Improvement**	Cyber security controls shall be reviewed and improved periodically.

7. REVIEW & GOVERNANCE

- Policy shall be reviewed annually or upon significant changes
- Approved by senior management
- Updated based on evolving threats and technologies

8. CONCLUSION

Stylam Industries Limited is committed to maintaining a strong cyber security posture through proactive risk management, continuous monitoring, and adherence to best practices.

APPROVAL

Role	Name	Signature	Date
Prepared By	SANDEEP KUMAR		
Reviewed By	RAJIV JINPAL		
Approved By	ANURAG JAIN		