



INFORMATION SECURITY POLICY

Authorized by:	Board of Directors
Version number:	1.1
Implementation date:	30 th January 2024
Last revision date:	31 st March 2025

INFORMATION SECURITY POLICY

A) INTRODUCTION

- We at Usha Martin Limited (hereinafter referred to as “UML” or “Company”) recognize that information is one of our most valuable assets belonging to our business operations, which helps us in maintaining and augmenting our competitive advantage. We recognize that Information Security is the responsibility of everyone in the organization. The achievement of our business goals depends on our ability to safeguard the information we create or possess by ensuring its confidentiality, integrity and availability at all times.
- The purpose of this Information Security Policy is to establish and maintain an effective framework for protecting Usha Martin's information assets, including but not limited to data, systems, networks, and intellectual property, from unauthorized access, disclosure, alteration and destruction. The Company endeavours to align its information security practices with globally recognized framework such as ISO 27001:2013.
- This policy shall apply to all employees, contractors, vendors, value chain parties and third parties who have access to Usha Martin's information assets.
- All Business Heads / Department Heads are directly responsible for ensuring compliance with our information security policy in their respective business domains.
- This policy is complemented with Internal SOPs, which are communicated to all employees through the company's Intranet.

B) POLICY FRAMEWORK

Information assets shall be classified based upon their business value and risk exposure and accordingly adequate controls shall be applied to business requirements.

The Company shall continuously strive to improve and strengthen our Information Security initiative and make it as part of our identity and business action.

We shall achieve this by ensuring that:

- i. Information assets and IT assets are protected against unauthorized access
- ii. Information is not disclosed to unauthorized persons through deliberate or careless action.
- iii. Information is protected from unauthorized modification.
- iv. Information is available to authorized users when needed.
- v. Applicable regulatory and legislative requirements are met.
- vi. Disaster recovery plans for IT assets are developed, maintained and tested as far as practicable.
- vii. Secure collection, processing, and storage of third-party information through robust security controls.
- viii. Training is imparted to all IT users including all employees, contractors, and third parties, with regular refresher sessions to strengthen their knowledge on information security-related issues.
- ix. All information security breaches are reported and investigated.
- x. Violation of policies is dealt with a disciplinary action.
- xi. Achieve a 100% resolution rate for reported security incidents
- xii. Ensure 100% of employees, contractors, and third parties complete annual information security awareness training.

C) REPORTING AND GRIEVANCE REDRESSAL MECHANISM

The Company has developed a structured reporting mechanism for employees, third parties, and stakeholders to report information security breaches and related concerns. Grievances and breaches can be submitted via email to the Information Security Officer at grievance@ushamartin.co.in.

G. Anand



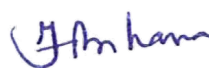
All reports will be handled with strict confidentiality, protecting the identity of whistleblowers and maintaining the integrity of the process. The company upholds a non-retaliation policy, ensuring that individuals reporting in good faith face no adverse consequences. All reported concerns will be thoroughly investigated, and necessary corrective measures will be implemented to strengthen the company's information security framework.

D) GOVERNANCE MECHANISM

The Board of Directors is in charge of implementing, monitoring, reviewing and continuously enhancing the Information Security Policy. The committee will oversee regulatory compliance, identify emerging security concerns, and apply required protections.

E) AMENDMENTS

The policy will be reviewed annually to ensure that it is effective and in line with changing business requirements, technological improvements, and regulatory revisions. Any improvements or modifications identified will be made as soon as possible.

Signature: 
Designation : Whole-time Director
Date : 31st March 2025

