

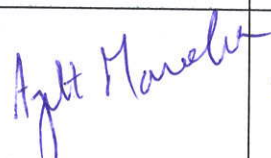


**TITLE: INFORMATION SECURITY POLICY****POLICY NUMBER: S/IT/ISMS/ISP/001****DOCUMENT CLASSIFICATION: Confidential****VERSION NUMBER: 004****EFFECTIVE DATE: 01.02.2023****1. Authorized Signatures:**

This Information Security Policy has been reviewed by the following Subject Matter Experts (SME) for its completeness / accuracy and is approved for implementation.

This document is prepared, reviewed and approved by the following personnel.

Responsibility	Name of the Personnel	Signature	Date
Prepared by	Tejas Patel IT compliance – Deputy Manager		30 Jan 2023
Reviewed by	Shikha Singh Deputy Manager Legal Department		30 Jan 2023
Approved by (CIO)	Ajit Manocha Chief Information Officer		30 Jan 2023

**2. Table of contents:**

- 1. Authorized Signatures: ..... 1
- 2. Table of contents: ..... 2
- 3. Objective:..... 5
- 4. Scope: ..... 5
- 5. Definitions ..... 5
- 6. Information Security Management Policy ..... 8
  - 6.1 Information Security Management (A.5.1.1) ..... 8
  - 6.2 Review of Information Security Policy (A.5.1.2) ..... 8
- 7. Organization of Information Security Policy ..... 9
  - 7.1 Internal Organization (A.6.1) ..... 9
  - 7.2 Mobile Devices and Teleworking (A.6.2)..... 10
- 8. Human Resources (HR) Security Policy ..... 11
  - 8.1 Prior to Employment (A.7.1)..... 11
  - 8.2 During Employment (A.7.2) ..... 11
  - 8.3 Termination or change of employment (A.7.3.1)..... 12
- 9. Asset Management Policy ..... 13
  - 9.1 Responsibility for Information Assets (A.8.1) ..... 13
  - 9.2 Classification and Handling of Information Assets (A.8.2)..... 13
  - 9.3 Media Handling (A.8.3) ..... 15
- 10. Access Control Policy ..... 16
  - 10.1 Business Requirements for Access Control (A.9.1) ..... 16
  - 10.2 User Access Management (A.9.2) ..... 16
  - 10.3 User Responsibilities (A.9.3)..... 18
  - 10.4 System Access Control (A.9.4)..... 19
- 11. Cryptography Policy ..... 21

11.1 Cryptographic Controls (A.10.1.1).....21

11.2 Key Management (A.10.1.2) .....21

12. Physical and Environmental Security Policy.....22

12.1 Secure Areas (A.11.1).....22

12.2 Equipment Security (A.11.2).....24

13. Operations Management Security Policy .....26

13.1 Operational Procedures and Responsibilities (A.12.1).....26

13.2 Protection from Malware (A.12.2).....27

13.3 Backup (A.12.3).....27

13.4 Logging and Monitoring (A.12.4) .....28

13.5 Control of Operational Software (A.12.5) .....29

13.6 Technical Vulnerability Management (A.12.6) .....29

13.7 Information Systems Audit Considerations (A.12.7) .....30

14. Communications Security Policy .....31

14.1 Network Security Management (A.13.1).....31

14.2 Information Transfer (A.13.2) .....32

15. System Acquisition, Development and Maintenance Policy.....34

15.1 Security Requirements of Information Systems (A.14.1).....34

15.2 Security in Development and Support Processes (A.14.2).....34

15.3 Test Data (A.14.3).....34

16. Supplier Relationship Policy .....35

16.1 Information Security in Supplier Relationships (A.15.1) .....35

16.2 Supplier Service Delivery Management (A.15.2).....36

17. Information Security Incident Management Policy.....37

17.1 Management of Information Security Incidents and Improvements (A.16.1).....37

18. Business Continuity Management Policy .....40

- 18.1 Planning Information Security Continuity (A.17.1.1) .....40
- 18.2 Implementing Information Security Continuity (A.17.1.2).....40
- 18.3 Verify, Review and Evaluate Information Security Continuity (A.17.1.3).....41
- 18.4 Availability of Information Processing Facilities (A.17.2.1) .....41
- 19. Information Security Compliance Policy .....42
  - 19.1 Compliance with Legal and Contractual Requirements (A.18.1).....42
  - 19.2 Information Security Reviews (A.18.2).....43
- 20. Mobile Device Management Policy .....44
- 21. Acceptable Usage Policy .....45
- 22. Exceptions .....50
- 23. Revision History:.....50