IT Security Features & Document Authenticity Policy

1. Introduction

Mitra S.K. Private Limited prioritizes data security, system integrity, and document authenticity. This policy defines the technical and operational measures implemented to safeguard customer data, maintain high-availability environments, and protect official certification against unauthorized alteration.

2. Document Integrity & Certificate Verification System

2.1. IMS QR Code Authentication:

- **Policy:** Every official certificate issued by MSK must carry a mandatory, system-generated IMS Certificate Number and a secure, dynamic QR Code.
- **Authentication Flow:** Scanning the QR code on any MSK certificate automatically redirects the user to MSK secure **IMS Portal**. Clients can instantly verify authentic test values and download original documents.
- **Impact:** Eliminates external tampering and unauthorized document alterations outside MSK, providing global trade partners with immediate proof of genuineness.

2.2. Unverified / Legacy Certificate Verification Protocol:

- **Policy:** If a client receives or holds an MSK certificate **without an IMS QR Code**, it must be reported immediately for manual verification prior to reliance.
- **Verification Procedure:** Clients must email a copy of the certificate to **info@mitrask.com** or contact our verification team directly at **(+91) 76050 88665**.
- **Impact:** Ensures seamless support for legacy or offline-issued documents while preventing fraudulent certificates from circulating unvetted.

3. Data Protection & System Resilience

3.1. End-to-End Encryption:

- **Policy:** Data is secured using industry-standard encryption protocols both in transit (TLS/SSL) and at rest (AES-256).
- **Impact:** Guarantees intercepted or unauthorized data transfers remain completely unreadable without valid decryption keys.

3.2. Automated Data Backups:

- **Policy:** Regular scheduled backups are performed across production systems with structured retention policies.
- **Impact:** Ensures continuous business continuity, high availability, and rapid system recovery in data loss scenarios.

3.3. Continuous Auditing & Threat Monitoring:

- **Policy:** Systems undergo 24/7 continuous monitoring combined with periodic third-party security audits to identify vulnerabilities.
- **Impact:** Enables proactive threat identification, rapid incident response, and continuous compliance alignment.
- **Client Verification Portal:** Provide direct access via our official website for seamless QR code scanning and certificate verification.