Cryptography Policy

To ensure the confidentiality, integrity, and authenticity of information across the organization, cryptographic controls must be applied to all sensitive data in storage and in transit. Only cryptographic algorithms that are currently approved by recognized standards bodies, such as NIST or ISO/IEC, are permitted. Acceptable algorithms include AES with a minimum key length of 256 bits, RSA with a minimum key length of 2048 bits, SHA-256 or stronger, and elliptic curve cryptography using curves of at least P-256. The use of deprecated or broken algorithms—including but not limited to MD5, SHA-1, and DES—is strictly forbidden under all circumstances.

All cryptographic key material must be managed in accordance with NIST SP 800-57 or its equivalent, with keys being securely generated, stored, distributed, rotated, and destroyed. Keys must be protected within FIPS 140-2 Level 2 (or higher) compliant hardware security modules whenever technically feasible. Symmetric encryption keys must be rotated at least once every 12 months, while asymmetric keys must be rotated at least every 24 months. No key material may be stored in plaintext or in user-accessible locations such as shared directories or local filesystems.

Sensitive data must be encrypted using approved cryptographic methods whenever it is stored or transmitted. All network transmissions containing confidential, regulated, or proprietary data must use TLS version 1.2 or higher. Full-disk encryption is mandatory for all company-owned laptops, mobile devices, and workstations used to access internal systems. All emails containing sensitive or confidential data must be encrypted using enterprise-approved tools, such as S/MIME or PGP, depending on the classification of the content and the recipient.

All public certificates must be issued by a trusted Certificate Authority and must meet a minimum RSA 2048-bit or ECC P-256 requirement. Internal certificates must be issued and managed by the organization’s Public Key Infrastructure (PKI), with certificate validity not exceeding two years. Certificates must be renewed no later than 30 days prior to expiration to prevent service disruptions.

Access to cryptographic systems and materials is restricted to authorized personnel with a valid business need, and all such access must be protected by multi-factor authentication. All interactions with cryptographic services, including key usage and administrative actions, must be logged and retained for a minimum of 12 months. These logs must be monitored for unauthorized or anomalous activity on a continuous basis by the security operations team.

Any exceptions to this policy must be formally documented and approved in writing by the Chief Information Security Officer. Exception requests must include a risk assessment, justification, and compensating controls. Violations of this policy may result in disciplinary action up to and including termination of employment or contract, and may trigger legal action if warranted. This policy is to be reviewed at least annually, or immediately following significant changes to cryptographic technologies, threat landscape, or regulatory requirements.

This policy draws upon and aligns with the following standards and guidelines: NIST Special Publications 800-57 and 800-52, ISO/IEC 27001 and 27002, and FIPS 140-2/140-3.