

Encryption Standards and Practices

(Classification and Handling -Safeguarding Sensitive and Confidential Information)

Version: 1.2

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party.

Document Revision History:

VERSION NO.	REVISION DATE	AUTHOR	REVIEWED BY	APPROVED BY	DESCRIPTION
1	28/6/2022	Gyan Singh	P.Sahoo	Amit Sobti	Reviewed
1.1	28/6/2023	Gyan Singh	P.Sahoo	Amit Sobti	Reviewed
1.2	28/7/2024	Gyan Singh	P.Sahoo	Amit Sobti	Reviewed

1. Purpose

The purpose of this Encryption Policy is to ensure that sensitive information, both in transit and at rest, is protected through encryption mechanisms. This policy applies to all employees, contractors, and third parties with access to company data and systems. The goal is to safeguard the confidentiality, integrity, and availability of sensitive company information and comply with applicable data protection regulations.

2. Scope

This policy applies to:

- All company data, both in transit and at rest, that is stored on company-owned devices, servers, or cloud-based systems.
- All personnel, including employees, contractors, and third parties, who handle sensitive information.
- All encryption methods and technologies used within the company's IT infrastructure, including software, hardware, and network communication.

3. Types of Encryption

The company will utilize the following encryption types:

- Data-at-Rest Encryption: Encryption of stored data on devices, servers, and storage systems.
- Data-in-Transit Encryption: Encryption of data while being transmitted over networks, including email, websites (HTTPS), and VPN connections.
- End-to-End Encryption: Encryption of messages or data from one endpoint to another, ensuring only the sender and receiver can decrypt the data.
- Full Disk Encryption (FDE): Encryption of entire disk drives on devices (e.g., laptops, desktops) to protect against data theft in case of device loss or theft.

4. Encryption Standards

- Encryption Algorithms:
 - AES-256 (Advanced Encryption Standard) will be used for encrypting sensitive data, both at rest and in transit.

- RSA-2048 or greater will be used for encrypting data in transit where applicable (e.g., SSL/TLS certificates).
 - For email encryption, we will use PGP (Pretty Good Privacy) or S/MIME (Secure/Multipurpose Internet Mail Extensions) where necessary.
 - **Key Management:**
 - Key Generation: Encryption keys will be generated using secure methods and will be managed through a central key management system (KMS).
 - Key Rotation: Encryption keys will be rotated on a regular basis (e.g., annually) to minimize the risk of exposure.
 - Key Storage: Keys will be stored in a secure, encrypted vault or key management system to prevent unauthorized access.
 - **Data Deletion:**
 - When encryption keys are retired or data is deleted, all associated encrypted data will be destroyed or rendered irretrievable using industry-standard data-wiping methods.
-

5. Roles and Responsibilities

- **IT Security Team:**
 - Ensure the proper implementation of encryption technologies and tools.
 - Perform regular audits of encrypted data to verify compliance with encryption policies.
 - Manage the encryption key lifecycle, including generation, rotation, and storage.
- **System Administrators:**
 - Implement and maintain encryption systems on company devices, storage systems, and servers.
 - Ensure that encrypted backups are performed as part of the company's disaster recovery plan.
- **End Users:**
 - Adhere to encryption requirements for handling sensitive data, including using encrypted communication channels and devices.

6. Encryption in Different Environments

- **Endpoints (Laptops, Desktops, Mobile Devices):**

- All endpoint devices containing sensitive data must have full disk encryption enabled, using a company-approved encryption solution (e.g., BitLocker, FileVault, or similar).
- **Servers:**
 - All servers storing sensitive data must use encryption for both the data stored on disk (data-at-rest) and data transferred over the network (data-in-transit).
- **Cloud Services:**
 - Data stored in cloud-based services must be encrypted, both at rest and in transit, using strong encryption methods and compliant with the cloud provider's encryption capabilities.
- **Email Communications:**
 - Sensitive or confidential information should be sent through encrypted email methods such as S/MIME or PGP.
- **Network Communications:**
 - All internal and external network communication involving sensitive data must use encryption protocols like TLS (Transport Layer Security), HTTPS, or VPN encryption.

7. Encryption Management Procedures

- **Access Control:**
 - Only authorized personnel should have access to encryption keys. Access will be logged and monitored.
 - Encryption keys will be stored separately from the data they encrypt to minimize the risk of compromise.
- **Encryption Deployment:**
 - The IT security team will ensure that encryption tools are deployed in all relevant systems, including servers, workstations, and mobile devices.
- **Auditing:**
 - Regular audits will be conducted to verify that encryption is applied correctly to all sensitive data across systems.
- **Incident Response:**
 - In case of a security breach involving encrypted data, a clear incident response plan will be followed to identify the source of the breach and mitigate the risks to the encrypted data.

8. Training and Awareness

- Employee Training:
 - All employees will receive training on the importance of encryption and how to use encryption tools appropriately.
 - End users will be informed about the risks of unencrypted communication and data storage and will be provided with the necessary tools to ensure encryption.

9. Exceptions

- Any exceptions to this encryption policy must be documented and approved by the IT Security team and senior management. Exceptions may only be granted in specific cases where encryption is not technically feasible or presents a significant operational challenge.

10. Monitoring and Enforcement

- Continuous Monitoring: The IT security team will continuously monitor systems to ensure encryption compliance.
- Enforcement: Violations of this policy, such as failure to encrypt sensitive data or bypassing encryption systems, may result in disciplinary action, including access revocation and termination.