Information Transfer Policy

1. Introduction and Scope

This policy establishes the mandatory controls and procedures for the secure and compliant transfer of all organizational information, particularly **Sensitive Data**, both internally and externally. It applies to all employees, contractors, and systems involved in capturing, processing, or transferring information.

2. Policy Statement

The organization has developed formal **Information Transfer Policies** for any information captured by the organization. All information transfers must align with the organization's **Information Classification Policy** and be conducted using secure, authorized methods to protect data integrity and confidentiality.

3. Alignment with Information Classification

3.1. Classification Requirement

Every information transfer request must first identify the **classification level** (e.g., Public, Internal, Confidential, Restricted) of the data being moved, as defined in the Information Classification Policy.

3.2. Mandatory Controls

Transfer methods and security controls must be commensurate with the information classification:

- **Restricted/Confidential Data:** Requires strong encryption for data in transit (TLS 1.2+ or IPsec) and may necessitate a formal, pre-approved third-party agreement (see Section 4).
- **Internal Data:** Requires encryption and must use internal, secured, authorized channels (e.g., secure VPN, company email).
- **Public Data:** May use standard transfer methods, but secure channels are still encouraged to prevent spoofing or tampering.

4. External Information Transfer Agreements

Any data or information transfer with external parties is captured within **formal agreements** (e.g., Data Processing Agreements, Non-Disclosure Agreements, or specific Information Sharing Agreements) that are reviewed by the Legal and Security teams prior to execution.

4.1. Required Agreement Elements

All formal information transfer agreements must include, at a minimum, the following security and accountability clauses:

Requirement	Description
Traceability	Procedures detailing how both parties will track the information's journey, including audit logs, timestamps, and recipient confirmation.
Transmission	Stipulations on the approved, secure technical methods (e.g., SFTP, encrypted cloud links) and cryptographic standards (e.g., AES-256 encryption) to be used for transfer.
Labelling	Mandatory requirements for the sending party to correctly label or tag the information with its classification level (e.g., "CONFIDENTIAL") and handling instructions prior to transmission.
Security Requirements for Systems Receiving Information	A clear mandate that the receiving external party's systems must meet minimum security and privacy requirements, including access control, incident response, and required data encryption **at rest** and **in transit** for the received information.
Data Retention & Disposal	Explicit instructions for the retention period and secure disposal/deletion of the transferred information by the receiving party once the purpose of the transfer is fulfilled.

5. Information Transfer Procedures

5.1. Authorization

All transfers of **Restricted** or **Confidential** data must be pre-authorized by the data owner and the relevant department head.

5.2. Logging and Monitoring

All authorized transfers, especially those involving external parties, must be logged and monitored. Logs must include:

- Date and time of transfer.
- Data classification level.
- Sending and receiving parties.
- Method of transfer (protocol).

5.3. Prohibition

Unauthorized or ad-hoc transfer methods (e.g., personal email, unencrypted flash drives, public file-sharing services) are **strictly prohibited** for all Sensitive Data.