ComplyJet

Data Encryption Policy Template

A free, adaptable template covering data classification, encryption requirements for data at rest and in transit, and SOC 2 / ISO 27001 / HIPAA / PCI DSS / GDPR alignment.

Company: _____

Effective date: _____

Policy owner: _____

Review cycle: Annually, and at every new system or data type

HOW TO USE THIS TEMPLATE

Replace every bracketed placeholder with your organization's specifics, adapt the classification examples to your own data inventory, and route the completed policy through your normal internal-approval process before treating it as adopted. This template is a starting point, not legal advice — see ComplyJet's full Data Encryption Policy guide for the reasoning behind each section.

1. Purpose

This policy defines what data [Company Name] must encrypt, where (at rest, in transit, or both), and the compliance requirements that apply. It establishes a data classification scheme and maps encryption requirements to that scheme, so that any engineer, auditor, or customer security reviewer can determine encryption requirements for a given system without a case-by-case judgment call.

2. Scope

This policy applies to all data created, processed, stored, or transmitted by [Company Name], across production, staging, and development environments, and including data held by third-party vendors and subprocessors on the company's behalf. It covers data at rest (databases, file systems, backups, cloud storage) and data in transit (API calls, internal service-to-service traffic, file transfers, email).

This policy scopes *what* must be encrypted and where. It does not cover approved algorithms, key generation, or key rotation — see [Company Name]'s Cryptography Policy for that technical implementation detail.

3. Data Classification

All company data is classified into one of four tiers. The tier determines the encryption requirement below. If exposing a piece of data would cause real regulatory, financial, or reputational harm, it belongs in a tier that requires encryption both at rest and in transit.

Classification Tier	Examples	Encryption Requirement
Public	Marketing content, published documentation	None required

Classification Tier	Examples	Encryption Requirement
Internal	Internal wikis, non-sensitive internal communications	Encouraged in transit; not mandatory at rest
Confidential	Business plans, internal financial data, source code	Required at rest and in transit
Regulated / Restricted	Customer PII, credentials, payment data, health data	Required at rest and in transit, with the strictest access controls

3.1 Categories That Are Commonly Missed

- **Backups and archived data.** Production data gets encrypted; the backup of that same data often doesn't.
- **Logs and monitoring data.** Application logs can capture sensitive fields without anyone deciding that should happen.
- **Non-production and staging environments.** Treated as lower-risk by default, even when they contain copies of real production data.
- **Data held by third-party vendors and subprocessors.** Scope this explicitly rather than assuming a vendor's own practices are sufficient.

4. Encryption Requirements

4.1 Data at Rest

Full-disk or database-level encryption is required for all Confidential and Regulated/Restricted data in storage, including databases, file systems, and cloud storage. Backups of this data must be encrypted with keys managed separately from the backup itself. Plaintext sensitive data must not appear in logs or exports.

4.2 Data in Transit

All Confidential and Regulated/Restricted data in transit — including internal service-to-service traffic, not just customer-facing traffic — must use a current, company-approved transport encryption protocol. Legacy, insecure protocols are explicitly prohibited.

> **MOST COMMON GAP**
>
> Customer-facing traffic gets HTTPS; internal service-to-service traffic or backups quietly stay unencrypted, on the assumption an internal network is inherently safe. It isn't — apply the same requirement to internal traffic as external.

5. Framework Alignment

How this policy's requirements map to the compliance frameworks most companies encounter. This is a starting reference, not a substitute for reading each framework's current text.

Framework	Where It Lives	What It Requires
SOC 2	Trust Services Criteria (risk-based)	No mandated algorithm; encryption decisions must be justified against the company's own risk assessment and data classification.
ISO 27001	Annex A control 8.24, Use of Cryptography	Requires documented rules for appropriate cryptography use; leaves algorithm selection to the organization.
HIPAA	Security Rule, 45 CFR §164.312(a)(2)(iv) / (e)(2)(ii)	Currently "addressable": encryption or an equivalent alternative must be implemented and justified. A 2026 proposed rule would make it mandatory.
PCI DSS 4.0	Requirements 3.5-3.6 (stored data), 4.2 (transmission)	Requires protecting stored cardholder data and its keys, plus TLS 1.2+ for transmission over open networks.
GDPR	Article 32, Security of Processing	Names encryption as an example "appropriate technical measure"; not mandated outright but treated as evidence of compliance.

6. Roles and Responsibilities

Role	Responsibility
[Policy Owner]	Accountable for this policy's accuracy, enforcement, and annual review.
Engineering / Platform team	Implements and maintains encryption controls for systems they own; classifies new data stores before launch.
Security / Compliance team	Audits actual encryption status against this policy; manages the exceptions process.
Vendor management	Confirms vendor and subprocessor encryption practices meet this policy as part of onboarding.

7. Exceptions Process

Any exception to this policy requires documented approval from [Policy Owner / Security Lead] and a compensating control, logged in [exceptions register / ticketing system]. Exceptions must be reviewed at the same cadence as this policy and re-justified or remediated, not renewed indefinitely by default.

8. Rollout and Policy Maintenance

1. **Assign an owner** — usually the IT or security lead, accountable for the policy and its enforcement.

2. **Classify existing data** against the tiers defined in Section 3, system by system.
3. **Identify any unencrypted sensitive data**, currently at rest or in transit, against that classification.
4. **Remediate gaps**, prioritized by classification tier, Regulated/Restricted first.
5. **Get leadership to formally approve** the policy once it reflects reality, not before.
6. **Set a review cadence** tied to new systems and data types, not just a fixed calendar date.

> **BEFORE CALLING ROLLOUT COMPLETE**
>
> Walk every production data store against the classification table in Section 3 and confirm its actual encryption status matches its assigned tier. A policy that hasn't been checked against reality yet isn't rolled out — it's just written.

9. Sample Policy Clauses

Ready-to-adapt clause language for the two sections most reviewers ask about directly.

Sample Clause — Data Classification and Encryption Requirements

CLAUSE 4.1

All company data is classified as Public, Internal, Confidential, or Regulated/Restricted. Data classified as Confidential or Regulated/Restricted must be encrypted at rest using company-approved encryption standards and encrypted in transit whenever it moves across a network, including internal service-to-service traffic. Backups of Confidential or Regulated/Restricted data must be encrypted with keys managed separately from the backup itself.

Sample Clause — Data in Transit

CLAUSE 4.2

All Confidential and Regulated/Restricted data transmitted over any network, public or internal, must use a current, company-approved transport encryption protocol. Legacy protocols no longer considered secure are explicitly prohibited. Exceptions require documented approval and a compensating control, logged under this policy's exceptions process (Section 7).

Sample Clause — Vendor and Subprocessor Encryption

CLAUSE 7.1

Any third-party vendor or subprocessor that stores, processes, or transmits Confidential or Regulated/Restricted data on [Company Name]'s behalf must demonstrate encryption practices meeting or exceeding this policy's requirements as part of vendor onboarding and annual vendor review.
