Technical Fact Sheet: Totara Data Encryption

1. Data In Transit (In Motion)

This refers to data moving between the user's browser and the Totara server, or between Totara and integrated third-party systems.

- **Protocol:** Mandatory use of **TLS (Transport Layer Security)**, typically version 1.2 or 1.3.
- **Mechanism:** SSL Certificates encrypt the communication channel.
- **Application Settings:** * **Enforced HTTPS:** Admins can enforce HTTPS for the entire site or specifically for login pages via *Quick-access menu* > *Security* > *HTTP security settings*.
    - **Secure Cookies:** Session cookies are flagged as Secure and HttpOnly to ensure they are only sent over encrypted connections and are inaccessible to client-side scripts.
- **API Security:** All outgoing and incoming Web Service calls (REST, SOAP) are performed over HTTPS to prevent "man-in-the-middle" (MITM) attacks.

---

2. Data At Rest (In Storage)

This refers to data stored within the database, the file system (dataroot), and backup files.

A. Application-Level Encryption (Secrets)

Totara uses an internal encryption framework to protect specific sensitive strings (secrets) within the database.

- **Algorithm: AES-256-CBC** (Advanced Encryption Standard).
- **What is encrypted:** API keys, OAuth2 client secrets, external service passwords, and authentication tokens.
- **Key Management:**
    - Encryption keys are stored in a file named encryption_keys.json located in the dataroot folder (outside the public web directory).
    - **Rotation:** Administrators can rotate keys using CLI tools (php admin/cli/add_encryption_key.php).

  - **Isolation:** Each encrypted value is tied to the specific model and instance that created it; it cannot be decrypted if moved to another record.

B. Infrastructure-Level Encryption (TDE)

Most Totara environments (especially in Cloud or Partner-hosted setups) utilize **Transparent Data Encryption (TDE)**.

- **Database:** The physical database files (MySQL, PostgreSQL, or SQL Server) are encrypted on the disk using industry-standard ciphers.
- **File Storage:** User-uploaded files (PDFs, SCORM packages, etc.) stored in the dataroot are encrypted at the hardware level by the storage provider (e.g., AWS EBS or S3 encryption).
- **Backups:** Off-site backups are encrypted before being transferred to long-term storage.

---

3. Compliance and Standards Summary

Requirement	Totara Implementation Method
GDPR Compliance	Achieved via AES-256 storage and granular "Purge Types" for data deletion/anonymization.
Encryption Standard	**AES-256** for data at rest; **TLS 1.2+** for data in transit.
Integrity Checks	Database hashes and OpenSSL modules ensure data hasn't been tampered with.
Key Storage	Securely located in dataroot/encryption_keys.json, inaccessible via the web.