Data Protection

Overview

Version 1.1 | April 2025

Introduction

We understand that entrusting a third party with your data is a significant decision—and at Totara, we take that responsibility seriously.

Protecting data requires a rigorous and proactive approach to meet the demands of evolving threats and shifting regulatory landscapes. That's why we prioritize security and compliance at every level, ensuring data is never compromised, misused, or disclosed without authorization.

From the ground up, Totara's technology has been built with security and privacy embedded into its core. Our controls are based on industry best practices, designed to ensure data is processed securely and in compliance with applicable requirements such as GDPR. These measures are regularly tested and validated through internal reviews and independent third-party audits to ensure ongoing effectiveness.

Below, you'll find a summary of our Data Protection controls. For more detailed information, please contact us at Security@Totara.com.

Compliance	Totara’s Information Security Program adheres to industry best practices and data protection laws, including alignment with ISO 27001, Cyber Essentials and the General Data Protection Regulation (GDPR). Totara is actively working toward achieving ISO 27001 and Cyber Essentials Plus certifications in 2025.
Security Governance	Totara has a dedicated security team responsible for ensuring that data is processed in compliance with applicable data protection laws and regulatory frameworks.
Security Testing	Penetration tests are performed annually by a third-party vendor. A summary of the report is available upon request. Customers interested in performing their own security tests should contact Security@Totara.com
Access Control	Access to Totara’s systems is based on the concept of least privilege and uses an assortment of controls including Single Sign-On (SSO), User and Entity Behavior Analytics and multi-factor authentication. We conduct quarterly evaluations of all access rights. This proactive approach ensures that permissions remain appropriate and reflect any role changes, maintaining a secure environment.
Supply Chain Risk	Totara mitigates supply chain risk by implementing robust supply chain risk management, vendor monitoring, and strict access controls to protect customer data. We carefully assess third-party vendors to ensure they meet our high security and compliance standards, reducing potential vulnerabilities in the supply chain.

Incident Management	Totara maintains security incident management policies and procedures to manage suspected or actual breaches of confidentiality, integrity, or availability. Totara will notify impacted Customers without undue delay or within 72 hours of any unauthorized disclosure of their respective data.
Personnel Policies and Procedures	All employees and contractors are subject to background checks prior to joining. These checks include substantiation of previous employment, credit history, address verification and international criminal checks, as applicable. Upon commencing employment, all Totara employees and contractors are contractually committed to confidentiality clauses to ensure that they adhere to Totara's commitment to security and confidentiality for its customers. Upon termination, access is removed by close of business on the final day of employment.
Security Awareness Training	All employees and contractors at Totara receive information security and privacy awareness training within 5 days of commencing employment. Additional role-based training (e.g., Secure SDLC) may also be required. Refresher training is provided annually.
Change Management	Totara utilizes a formal, documented, change management process for all changes to Services.
Physical Security	All customer data is secured with appropriate physical access controls and security to ensure only authorised individuals have access to areas & computer equipment. Totara facilities are protected using access control mechanisms that authenticate the identity of personnel prior to them being granted access to

	the office space. Totara offices are also protected using a monitored alarm system. Vendors, contractors, and visitors are always escorted while in Totara offices and a record of the visit is maintained in the visitor log. (Totara-hosted customers only) Details about the physical security of AWS data centers can be found here: https://aws.amazon.com/compliance/data-center/controls/
Encryption	TLSv1.2 an v1.3 is used for all transmissions between a Customer's network and Totara Services. Any data that is collected and persisted is encrypted at rest using 256-bit AES encryption using AWS managed keys.
Vulnerability Management	We conduct both regular and ad hoc scans to identify potential risks, monitoring the Common Vulnerabilities and Exposures (CVE) database and staying vigilant against emerging threats.
Patch Management	Patches are prioritized based on their severity when they are required. All OS/Vendor updates are first applied to non-production resources and then applied to production systems only after testing has been completed.
Virus Protection	Endpoint Detection and Response (EDR) software is installed on all Totara systems.
Resource Hardening	Totara applies secure configurations derived from industry best practices (e.g., CIS Benchmarks).
Intrusion Detection	Totara services are monitored 24/7 by our Security Operations Center.

	Key activities within our Cloud environment and infrastructure are logged and stored for 13 months within our SIEM solution.
Application Security	Totara follows a secure software development process, beginning with design reviews, threat modeling, and risk assessment. Our software development methodology includes security control touchpoints built into the software development lifecycle (SDLC). Each phase of our SDLC has clear quality and security exit criteria, ensuring that potential problems are identified and resolved as early as possible. Our Engineering and Product Security teams conduct extensive development and post-development testing to be certain our applications are secure. This includes code analysis and independent penetration. At Totara, we prioritize application security by embedding robust measures throughout our software development lifecycle (SDLC). Our approach includes: • **Secure Development Practices**: We follow a rigorous set of secure development practices, including monitoring for new vulnerabilities in related platforms and ensuring our code remains secure. • **Security Control Integration:** Security controls are integrated into every phase of our SDLC, with clear quality and security exit criteria to identify and resolve potential issues early, including use of SAST and DAST. • **Comprehensive Testing:** Our Engineering and Product Security teams conduct extensive testing, including code analysis and independent penetration tests, to ensure our applications are secure.

	By implementing these practices, Totara ensures that our applications are secure, reliable, and aligned with industry best practice.
Data Retention *(Totara-hosted customers only)*	Following the end of a customer contract, we will maintain the site data for 30 days, during which time you can request a copy of all data we hold or request the removal of the data associated with your site, including the site database and filesystem. After this period, we will remove all data in the site database and filesystem. Refer to our Totara contractual agreement for more information on data processing.
Data Segregation (Totara-hosted customers only)	Totara's architecture is designed to segregate and restrict customer data storage and access based on business needs. Customer environments are fully segregated within our hosting environment. Each environment has its own dedicated database and allows the use of customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, including staging and development. No production data is transferred into non-production environments.
Employee Access to Customer Data *(Totara-hosted customers only)*	Totara will not access or modify data except where necessary as directed by Customers to provide Services or resolve or prevent errors.
Backups *(Totara-hosted customers only)*	All site data required to regenerate the customer's site is backed up by an automated nightly backup process, then stored securely encrypted in AWS S3. Nightly versioned backups are kept for a period of 2 weeks in S3 before being transferred to S3 Glacier. S3 Glacier is an immutable long-term backup.

Disaster Recovery *(Totara-hosted customers only)*	Totara has developed Disaster Recovery plans to ensure operations can continue with minimal impact in the event of a disaster. BC/DR plans are tested annually.
Network Security *(Totara-hosted customers only)*	We run a web application firewall (WAF) in front of our load balancer to filter malicious requests before they reach the application.
Data Processing Locations *(Totara-hosted customers only)*	Totara hosts its services in Amazon Web Services (AWS) data centers located in North America, Europe, and Asia Pacific. Customers may choose which data center their tenancy is hosted in. We currently offer hosting in the following regions, with additional regions being added as demand dictates: • Virginia, United States (AWS region: us-east-1) • London, United Kingdom (AWS region: eu-west-2) • Dubai, United Arab Emirates (AWS region: me-central-1) • Sydney, Australia (AWS region, ap-southeast-2)