Trimble Connect

Security Whitepaper

Last Updated: May 12, 2026

Disclaimer

This document provides information related to customer data and security in Trimble Connect. The content and Trimble's operations, procedures, and controls are subject to change without notice. Trimble Connect services and related products are subject to the Trimble Offering Terms. The content of this document is informational only and does not establish any contractually binding obligations on Trimble.

Contents

Introduction

Trimble Connect Overview

Trimble Connect serves as the central hub for cloud-based collaboration within the engineering and construction sectors. By providing a unified platform accessible via Desktop, Mobile, and Web, it enables global project teams to view, share, and manage critical information from any location at any time. Our architectural mission is to deliver a scalable, resilient environment that empowers customers to enhance productivity and efficiency through modernized digital construction workflows.

Document Purpose and Scope

This whitepaper provides a comprehensive overview of the security architecture, information security protocols, and operational safeguards governing the Trimble Connect platform. It is designed to provide transparency into Trimble's security, data privacy, and operational data protection strategies and to clarify the shared responsibility model. This model establishes the boundary between the robust security measures managed by Trimble and the administrative controls explicitly granted to and managed by the customer.

The scope of this document primarily encompasses the security implementations for the Trimble Connect platform. Trimble Connect leverages foundational enterprise services for centralized identity management, subscription and entitlement validation, automated data transformation, and secure file storage. While these core components are managed by centralized Trimble engineering teams, they are governed by the same rigorous corporate-level security frameworks and independent third-party audits - including ISO 27001 and SOC 2 - referenced throughout this document. While our foundational infrastructure services already maintain SOC 2 Type II status, Trimble Connect is currently transitioning from Type I to Type II, with completion anticipated in 2026. Audit certifications for these shared infrastructure services are available to customers via the Trimble Trust Portal.

Trimble Security Framework

Core Security Principles

Trimble is deeply committed to protecting the Confidentiality, Integrity, and Availability (CIA) of customer information. Our security framework is built upon ISO 27001 best practices and an Integrated Management System (IMS) that aligns with ISO 27701 for privacy management. We operate under a "Secure by Design" philosophy, designed to ensure that security and privacy protections are integrated at every stage of the Trimble Secure Development Lifecycle

(TSDLC). This is supported by secure operational workflows and persistent monitoring to counter evolving threats and maintain global regulatory standards.

Governance and Oversight

Trimble's cybersecurity program is led by the Chief Information Security Officer (CISO) and is supported by the Office of Data Protection (ODP). To ensure security remains a core pillar of development, Trimble fosters a Security-First Engineering Culture. Every member of the Trimble Connect engineering team undergoes specialized secure coding training, and dedicated security reviews are integrated directly into the sprint and release cycles. This approach ensures that security is treated as an essential component of software quality rather than an external check.

Identity and Access Management

Customer Access Controls

Trimble Connect is built on a "Private by Default" architecture. Project data is isolated and remains undiscoverable to all users until an explicit invitation is issued by a Project Administrator. Once invited, project members maintain control over their data environments. This includes the ability to audit project membership through exportable listings, assign dynamic roles such as "Project User" or "Project Administrator," and revoke access manually to immediately terminate a user's connection to project data. Furthermore, access can be refined using granular permissions - Read, Read/Write, or No Access - which can be applied to individuals or User Groups to ensure members only interact with relevant information.

Authentication and Password Policy

Trimble Connect leverages the Trimble Identity (TID) service, which is a foundational enterprise service, to enforce rigorous authentication standards across the entire ecosystem. To protect against credential theft and phishing, Multi-Factor Authentication (MFA) is mandatory for all users authenticated via TID.

Authentication methods for users relying on Trimble Identity vary based on their user type and include:

- **Native TID Users:** Trimble promotes a "passkey-forward" approach, utilizing phishing-resistant, biometric-based digital keys stored on the user's device. Additionally, the platform supports time-based one-time passwords (TOTP) via authenticator apps and email-based one-time passcodes (OTP).

- **Federated Identities:** For organizations utilizing Identity Federation (SSO), authentication policies - including MFA enforcement - are governed and managed by the customer's third-party Identity Provider (IdP). As technical verification protocols vary between external providers, federated organizations maintain the responsibility for enforcing their internal security and MFA standards prior to users accessing Trimble services.
- **Managed Users in Constrained Environments:** Certain specialized workflows utilize Managed Users who may operate in environments with limited access to smartphones or utilize specialized hardware that does not support standard security keys. For these specific use cases, Trimble is currently evaluating alternative authentication factors to balance rigorous security requirements with the practicalities of field-based and specialized hardware operations.

Data Privacy and Personal Information

Trimble processes certain personal information, such as for user authentication, provision of support and services, and invoicing, as shown in the table below. Trimble Connect users solely determine and control any other information, including personal information, that is processed in connection with their use of Trimble Connect.

For more information about how Trimble collects and uses personal information, please visit the Trimble Privacy Center.

Personally Identifiable Information	
Email Address	Required
First Name	Required
Last Name	Required
Job Title	Optional
Employer Name	Optional
Country	Required
State/Province/Region	Required
Street address	Required when purchasing products
City	Required when purchasing products
Zip code	Required when purchasing products
Telephone	Required when purchasing products

Personally Identifiable Information	
Email Address	Required
First Name	Required
Photo	Optional

Data Management and Protection

Encryption and Cryptographic Practices

Information protection is maintained through rigorous cryptographic standards. All data transmitted to or from Trimble Connect is encrypted using Transport Layer Security (TLS) 1.2 or higher. For data at rest, project files and sensitive metadata are secured using AES-256 or equivalent strong algorithms, designed to ensure that cleartext data remains inaccessible on physical storage media.

Data Residency, Portability, and Sanitization

To support global performance and data sovereignty requirements, project administrators select a storage region upon project creation. These regions are hosted within specific sovereign jurisdictions, including the United States, Ireland, United Kingdom, Singapore, and Australia.

Customers maintain full control over their data throughout their subscription. Trimble Connect provides native tools that allow administrators to export project files and metadata at any time. When data is deleted or storage resources are decommissioned, Trimble follows industry-standard media sanitization practices that meet or exceed NIST 800-88 standards, ensuring that data is rendered permanently unrecoverable. For granular information on data lifecycle policies, please refer to our published Trimble Connect Data Retention Standards and Procedures.

Operations and Infrastructure Security

System Hardening and Resilience

Trimble Connect infrastructure is hosted in top-tier data centers managed by Amazon Web Services (AWS) and Microsoft Azure, following a "defense-in-depth" approach. Facilities employ 24/7 on-site security, biometric access controls, and environmental protections like

redundant power and fire suppression. Our services are deployed across multiple AWS Availability Zones (AZs) designed to ensure resilience against localized data center failures.

Operational security is further maintained through strict system hardening and risk-based patch management. Services are configured according to the principle of "least functionality," disabling unnecessary ports and services to reduce the attack surface.

Availability, Continuity, and Monitoring

Trimble provides real-time transparency via the Trimble Connect Status Dashboard. We maintain a robust Disaster Recovery (DR) plan with a Recovery Point Objective (RPO) and Recovery Time Objective (RTO) of 24 hours for critical services. These plans are verified through annual exercises. Additionally, Trimble operates a 24/7/365 Security Operations Center (SOC) that utilizes SIEM solutions for rapid threat detection and response.

Secure Software Development

TSDLC and Vulnerability Management

The Trimble Secure Development Lifecycle (TSDLC) embeds security into every phase of the software journey, from initial threat modeling and peer reviews to automated static (SAST) and dynamic (DAST) analysis. Additionally, we partner with independent 3rd party vendors to conduct penetration tests annually where the vendor uses both automated and manual techniques to find vulnerabilities. Beyond internal testing, Trimble collaborates with the global security research community through our Vulnerability Disclosure Program (VDP). Hosted on a leading crowdsourced security platform, this program provides a responsible and transparent mechanism for identifying and remediating potential vulnerabilities across Trimble-owned endpoints. For more information or to report a security finding, please visit the Trimble Trust Center.

Compliance and Industry Alignment

Audited Certifications

Trimble Connect and its foundational enterprise services - including identity management, entitlement validation, and secure storage infrastructure - undergo annual independent third-party audits to maintain ISO/IEC 27001:2022 certification.

Regarding the SOC 2 framework, our foundational infrastructure services already maintain SOC 2 Type II certifications. Trimble Connect currently holds SOC 2 Type I status, with the

platform's transition to SOC 2 Type II currently underway and anticipated for completion in 2026.

Beyond these core certifications, the platform and its underlying identity and storage services align with NIST 800-171 for the protection of Controlled Unclassified Information (CUI). Additionally, to support project requirements in the United Kingdom, Trimble UK Limited maintains Cyber Essentials Plus certification, providing independent verification of technical security controls against common cyber threats.

Industry Standards Alignment

Trimble Connect provides the foundational data governance framework required to execute an ISO 19650-compliant Common Data Environment (CDE). By leveraging granular access controls, immutable activity trails, and extensible metadata schemas, the platform enables project teams to enforce the rigorous information states - WIP, Shared, Published, and Archived - stipulated by international BIM standards. Our 'Open BIM' architecture is designed to ensure that information integrity is maintained across the entire project lifecycle, providing a secure, vendor-neutral audit trail for all stakeholders.

Conclusion and Contact

Trimble remains dedicated to a "Secure by Design" philosophy, providing the infrastructure and granular controls necessary for the world's most complex construction projects. For further inquiries, please contact connect-support@trimble.com or visit the Trimble Trust Center at https://trust.trimble.com.