Bitwarden Security and Compliance

Bitwarden envisions a world where no one gets hacked. This is reflected in a steadfast Bitwarden commitment to security, privacy, and compliance with international standards.

Read the Security Whitepaper

Bitwarden privacy and product security

Third-party audited

External experts regularly review Bitwarden products, ensuring strong and trusted security.

Zero-knowledge, end-to-end encryption

Compliant with privacy and security standards

Get Bitwarden products quickly approved by your internal IT and security teams with industry compliance.

Trust and transparency powered by open source

An open source codebase enables the security of Bitwarden products to be easily audited by independent security researchers, notable security firms, and the Bitwarden community.

Trusted open source architecture

The Bitwarden codebase on GitHub is regularly reviewed and audited by millions of security enthusiasts and active Bitwarden community members.

Read the code >

Source code assessment

Bitwarden completes annual source code audits and penetration tests for each client including web, browser extension, and desktop — in addition to the core application and library.

Access the reports >

Network security assessment

Bitwarden completes annual network security assessments and penetration tests by reputable security firms.

Access the reports >

HackerOne bug bounty

Independent security researchers are rewarded for submitting potential security issues.

Check out the program >

Keeping your data secure

As your password manager and credential security provider, Bitwarden utilizes trusted security measures and encryption methods to protect user data.

Zero-knowledge, end-to-end encryption

Bitwarden uses end-to-end encryption for all vault data, which only your master password can decrypt. With a zero-knowledge architecture, Bitwarden does not have the ability to read any encrypted data in your vault.

Learn more about encryption

Multifactor encryption

Multifactor encryption is an additional layer of encryption that protects your stored information. This makes it practically impossible for a bad actor to break into your vault, even if they were able to gain access to your encrypted vault data.

Learn more about multifactor encryption

Self-hosting options

Choose to deploy and manage Bitwarden on-premises in your private network or infrastructure with self-hosting options. Self-hosting allows customers to have more detailed control over their stored information.

Learn how to self-host Bitwarden

Security compliance

Bitwarden adheres to industry security standards with an ISO 27001 certification, SOC2 and SOC3 certifications, and HIPAA compliance.

SOC2 and SOC3

System and Organization Controls (SOC) comprise a set of control frameworks that are used to validate an organization's security systems and policies. Bitwarden is SOC2 Type II and SOC3 certified.

SOC2 Reports available upon request.

Read the SOC3 report >

HIPAA

Bitwarden is HIPAA compliant and undergoes annual third-party audits for HIPAA Security Rule compliance.

Read about Bitwarden HIPAA compliance >

ISO 27001

Bitwarden is ISO 27001 certified and in compliance with ISO 27001 control sets surrounding data security.

Privacy compliance

Bitwarden prioritizes protecting the personal data of users and ensuring compliance with key privacy standards across the globe.

CCPA & CPRA

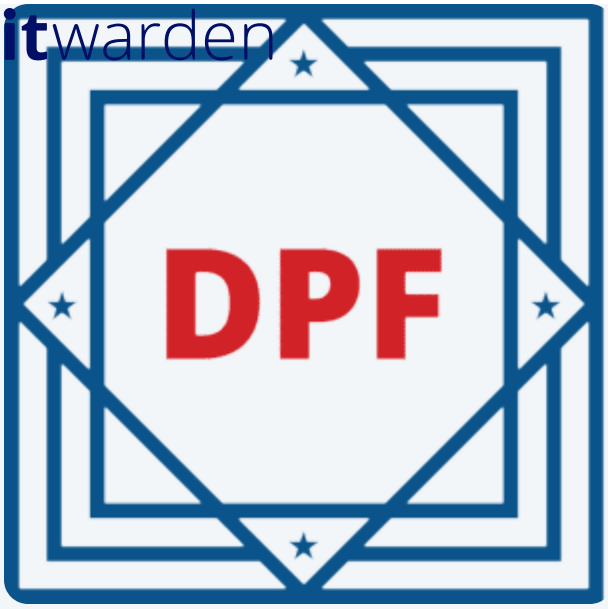
Bitwarden is compliant with the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA).

See the Bitwarden Privacy Policy >

GDPR

Bitwarden complies with GDPR, current EU data protection rules, and EU Standard Contractual Clauses (SCCs).

See the Bitwarden Privacy Policy >



Data Privacy Framework

Bitwarden complies with the Data Privacy Framework (DPF), previously called Privacy Shield, which defines the safe transfer of personal data.

See the Bitwarden Privacy Policy >

Learn about Bitwarden security, privacy, and compliance.

Download the whitepaper

Meet your security compliance standards with Bitwarden

Bitwarden is more than a password manager; it's a foundational tool for achieving and maintaining industry compliance with key security standards. Through secure sharing, monitoring capabilities, centralized management, and robust data protection, Bitwarden strengthens your organization's cybersecurity posture to meet compliance needs.

ISO 27001

ISO 27001, an international standard, sets the foundation for creating, maintaining, and developing information security management systems (ISMS), including data management.

Read the full resource >

SOC 2

Service Organization Control 2 (SOC 2) reports are often requested by customers and business partners of outsourced solution providers. Companies seeking SOC 2 compliance can leverage a SOC 2-compliant password manager to help meet requirements.

Read the full resource >

NERC

The North American Electric Reliability Corporation (NERC) is a non-profit international regulatory body dedicated to setting compliance standards that help reduce risks to the electricity grid and power systems serving hundreds of millions of people in the United States, Canada, and part of Mexico.

Read the full resource >

NIS2

NIS2 is a set of requirements for securing network and information systems across the EU. The directive mandates businesses identified as operators of essential services to implement appropriate measures to enhance cybersecurity and comply with legal obligations.

Read the full resource >

NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) provides guidance and best practices for organizations to follow, in order to help businesses, non-profits, and other private-sector institutions to improve cybersecurity risk management.

Read the full resource >

SOX

Sarbanes-Oxley Act (SOX) compliance involves adhering to a set of security requirements designed to ensure the integrity of financial reporting.

Read the full resource >

Password Management Maturity Model

This framework helps organizations understand their password manager maturity level — based on their current operations — and identify what steps are necessary to strengthen their security and improve their existing classification.

Read the full resource >

Learn more about Bitwarden commitment to data privacy in the Bitwarden Privacy Policy.

Read the Bitwarden Privacy Policy

FAQs

Can the Bitwarden team see my passwords?

How do you keep the cloud servers secure?

Is Bitwarden audited?

What happens if Bitwarden gets hacked?

Where is my data stored in the cloud?

Why should I trust Bitwarden with my passwords?

Does Bitwarden use a salted hash for my password?

How is my data securely transmitted and stored on Bitwarden servers?

What encryption is being used?

What information is encrypted?

Where is my data stored on my computer/device?

Get page details as PDF

English