COMPASS

Software Cybersecurity Compliance

March 2022

RISC Compass

RISC Compass is composed of trusted 3rd party software to create a cloud based, automated, and organized compliance system for firms to gather data, perform reviews, produce reports, and maintain firmwide organization.

In accordance with industry guidelines, RISC Compass gives security and privacy the utmost importance. We do not sell, or share your information with 3rd parties except with your consent, to comply with laws, to provide services pursuant to contracts, or to fulfill business obligations during everyday business.

The RISC Compass privacy policy can be found at any time online at:
https://risccompass.com/privacy-policy.

Data Entered

All information uploaded or entered into RISC Compass forms or modules is held in the strictest confidence and is deemed the exclusive property of the Client. For this reason, the Firm has full control over data maintained in RISC Compass. Any information the Firm deletes is permanently deleted at the moment the validation pop-up is confirmed. Certain modules have the option to delete disabled to protect the integrity of the associated records, and Firm must contact RISC Compass directly for further assistance. RISC Compass Portal access levels must be properly assigned in order to restrict the ability to delete records to the appropriate personnel.

RISC Compass Drive

The Firm does not have the ability to delete any attestations, forms, reports uploaded to the RISC Compass Drive. The Firm may access or download these items at any time, and are periodically provided links to download all files. No files will be deleted by RISC Compass without confirmation of download or electronic/physical delivery.

Zoho

RISC Compass utilizes Zoho, a cloud software used to create custom applications. Compass does not gather or store any sensitive information like credit card details, passwords, or social security numbers. Furthermore, Compass and Zoho adhere to GDPR's guidelines by classifying specific fields as “personal data” for any data that can directly or indirectly help identify a natural person. This includes, but is not limited to: name, address, phone number, email address, IP address, traveling habits, and photos.

https://www.zoho.com/privacy-commitment.html
https://www.zoho.com/security.html
https://www.zoho.com/security-faq.html
https://www.zoho.com/privacy.html
https://www.zoho.com/compliance.html

With nearly 30 million users worldwide accessing Zoho services, individuals, small, medium and large organizations count on Zoho security and data protection to meet their needs. We take security very seriously and have developed a comprehensive set of practices, technologies and policies to help ensure your data is secure.

If you are currently maintaining your data on personal computers or your own servers, the odds are that we offer a better level of security than what you currently have in place.

This document outlines some of the mechanisms and processes we have implemented to help ensure that your data is protected. Our security practices are grouped in four different areas: Physical Security; Network Security; People Processes and Redundancy and Business Continuity.

Physical Security

Our datacenters are hosted in some of the most secure facilities available today in locations that are protected from physical and logical attacks as well as from natural disasters such as earthquakes, fires, floods, etc.

- 7x24x365 Security. The data centers that host your data are guarded seven days a week, 24 hours a day, each and every day of the year by private security guards.
- Video Monitoring. Each data center is monitored 7x24x365 with night vision cameras.
- Controlled Entrance. Access to the Zoho data centers is tightly restricted to a small group of pre-authorized personnel.
- Biometric, two-Factor Authentication. Two forms of authentication, including a biometric one, must be used together at the same time to enter a Zoho data center.
- Undisclosed locations. Zoho servers are located inside generic-looking, undisclosed locations that make them less likely to be a target of an attack.
- Bullet-resistant walls. Zoho servers are guarded safely inside bullet-resistant walls.

Network Security

Our network security team and infrastructure helps protect your data against the most sophisticated electronic attacks. The following is a subset of our network security practices. These are intentionally stated in a very general way, since even knowing what tactics we use is something hackers crave. If your organization requires further detail on our network security, please contact us.

- Secure Communication. All data transmission to Zoho services are encrypted using TLS 1.2 protocols, and we use certificates issued by SHA 256 based CA ensuring that our users have a secure connection from their browsers to our service. We use the latest and strong ciphers like AES_CBC/AES_GCM 256 bit/128 bit keys for encryption, SHA2 for message authentication and ECDHE_RSA as the key exchange mechanism.
- IDS/IPS. Our network is gated and screened by highly powerful and certified Intrusion Detection / Intrusion Prevention Systems.
- Control and Audit. All accesses are controlled and also audited.
- Secured / Sliced Down OS. Zoho applications run inside a secured, sliced-down operating system engineered for security that minimizes vulnerabilities.
- Virus Scanning. Traffic coming into Zoho Servers is automatically scanned for harmful viruses using state of the art virus scanning protocols which are updated regularly.

People Processes

Designing and running data center infrastructure requires not just technology, but a disciplined approach to processes. This includes policies about escalation, management, knowledge sharing, risk, as well as the day to day operations. Zoho's security team has years of experience in designing and operating data centers and continually improves our processes over time. Zoho has developed a world class practices for managing security and data protection risk.

- Select Employees. Only employees with the highest clearance have access to our data center data. Employee access is logged and passwords are strictly regulated. We limit access to customer data to only a select few of these employees who need such access to provide support and troubleshooting on our customers' behalf.
- Audits. Audits are regularly performed and the whole process is reviewed by management.
- As-Needed Basis. Accessing data center information as well as customer data is done on an as-needed only basis, and only when approved by the customer (i.e. as part of a support incident), or by senior security management to provide support and maintenance.

Redundancy and Business Continuity

One of the fundamental philosophies of cloud computing is the acknowledgment and assumption that computer resources will at some point fail. We have designed our systems and infrastructure with that in mind.

- Distributed Grid Architecture. Zoho services run on a distributed grid architecture. That means a server can fail without a noticeable impact on the system or our services. In fact, on any given week, multiple servers fail without our customers ever noticing it. The system has been designed knowing that server will eventually fail - we have implemented our infrastructure to account for that.
- Power Redundancy. Zoho configures its servers for power redundancy – from power supply to power delivery.
- Internet Redundancy. Zoho is connected to the world –and you- through multiple Tier-1 ISPs. So if any one fails or experiences a delay, you can still reliably get to your applications and information.
- Redundant Network Devices. Zoho runs on redundant network devices (switches, routers, security gateways) to avoid any single point of failure at any level on the internal network.
- Redundant Cooling and Temperature. Intense computing resources generate a lot of heat, and thus need to be cooled to guarantee a smooth operation. Zoho servers are backed by N+2 redundant HVAC systems and temperature control systems.
- Geo Mirroring. Customer data is mirrored in a separate geographic location for Disaster Recovery and Business Continuity purposes.
- Fire Prevention. The Zoho data centers are guarded by industry-standard fire prevention and control systems.
- Data Protection & Back-up. User data is backed-up periodically across multiple servers, helping protect the data in the event of hardware failure or disaster.

Security Certifications

SOC Reports

Service Organization Controls (SOC) Reports, known as SOC 1, SOC 2, or SOC 3, are frameworks established by the American Institute of Certified Public Accountants (AICPA) for reporting on internal controls implemented within an organization. Dropbox has validated its systems, applications, people, and processes through a series of audits by an independent third-party, Ernst & Young LLP.

SOC 2 + HIPAA - An independent third-party audit firm has examined the description of the system related to Application Development, Production Support and the related General Information Technology Controls for the services provided to customers, from Zoho offshore development centre, based on Security, Privacy and breach requirements set forth in the Health Insurance Portability and Accountability Act (“HIPAA”) Administrative Simplification. The responsibility of Zoho is limited to the extent it acts as a 'Business Associate'.

ISO Certifications

The International Organization for Standardization (ISO) has developed a series of world-class standards for information and societal security to help organizations develop reliable and innovative products and services. Dropbox has certified its data centers, systems, applications, people, and processes through a series of audits by an independent third-party, Netherlands-based EY CertifyPoint.

ISO/IEC 27001 is one of the most widely recognized independent international security standards. This certificate is awarded to organizations that comply with ISO's high global standards. Zoho has earned ISO/IEC 27001:2013 certification for Applications, Systems, People, Technology, and Processes

ISO/IEC 27701 is an extension to the ISO/IEC 27001 and ISO/IEC 27002 standards for privacy management within the context of the organization. The certification standard is designed to enhance the existing Information Security Management System (ISMS) with additional requirements in order to establish, implement, maintain, and continually improve a Privacy Information Management System (PIMS). This standard enables organizations to demonstrate compliance with the various privacy regulations around the world that are applicable to them.

ISO/IEC 27017 gives guidelines for information security controls applicable to the provision and use of cloud services by providing additional implementation guidance for relevant controls specified in ISO/IEC 27002 and additional controls with implementation guidance that specifically relate to cloud services.

Zoho is certified with ISO/IEC 27017:2015 - Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

ISO/IEC 27018 establishes commonly accepted control objectives, controls and guidelines for implementing measures on safeguarding the PII that is processed in a public cloud. These controls are an extension of ISO/IEC 27001 and ISO/IEC 27002, ISO/IEC 27018 which provide guidance to organizations concerned about how their cloud providers are handing personally identifiable information (PII).

ISO 9001 is defined as the international standard that specifies requirements for a Quality Management System (QMS). Organizations use the standard to demonstrate the ability to consistently provide quality products and services that meet customer and regulatory requirements. Zoho Desk, Zoho HRMS and Finance suite of applications comply with ISO 9001 requirements.

Zoho is SOC 2 Type II compliant. SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the AICPA's Trust Services Principles criteria.

Payment card industry (PCI) compliance refers to the technical and operational standards that businesses must follow to ensure that credit card data provided by cardholders is protected. PCI compliance is enforced by the PCI Standards Council, to ensure that all businesses that store, process or transmit credit card data electronically do so in a secure manner that helps reduce the likelihood that cardholders would have sensitive financial data stolen.

GDPR is a pan-European regulation that requires businesses to protect the personal data and privacy of EU citizens for processing of their personal data.
Zoho has always demonstrated its commitment to its user's data privacy by consistently exceeding industry standards. Zoho welcomes GDPR as a strengthening force of the privacy-consciousness that already exists in it.

Zoho's offerings have privacy features that comply to GDPR, and Zoho's processing of its customer's data adheres to the data protection principles of the GDPR. To know more about how Zoho complies with GDPR, click here.

CCPA is a data privacy law specific to the processing of personal information of California residents that requires businesses to protect their personal information and provides privacy. Zoho has always demonstrated its commitment to its user's data privacy by consistently exceeding industry standards. Zoho welcomes CCPA as a strengthening force of the privacy-consciousness that already exists in it.

Zoho's offerings have privacy features that enable it's users to comply with the CCPA, and Zoho's processing of its Californian customer's data adheres to requirements of the CCPA. To know more about this, click here.

TRUSTe Review Zoho’s privacy policy, platform, website, and support portal have been reviewed by TRUSTe for compliance with their program requirements.
Zoho Corporation is certified to be compliant with the SWISS-U.S. PRIVACY SHIELD FRAMEWORK.

Signal spam reports help in providing FBL data, primarily technical information for identification of spammers and marketing abuse, from major ISPs like Orange.fr, SFR.fr, and so on. It has many spam reporting plugins for third-party browsers and email clients, focused at the French communities worldwide. It’s important for both Zoho corporation and our customers to know all the recipients who mark or report the emails they receive as ‘spam’, so that we can remove them from the lists. Hence, this certification protects our network reputation in the French region.