A deep dive into Security at Zoho Creator

TABLE OF CONTENTS

4.0 Customer controls for security

5.0 Reach out to us

1.0 Overview

Zoho provides Software as a Service (SaaS) products to millions of users worldwide to solve their business problems. Security is a key component in our offerings, and is reflected in our people, process, and products. In this document, we share the various standard measures we take to ensure security for our customers and their data.

1.1 Infrastructure security

Why is infrastructure security crucial?

IT infrastructure security is important for the prevention of unauthorized users and devices from accessing our network and data centers. Zoho uses world-class security technologies and best practices to prevent breaches and mitigate the risks associated.

Network security

Our network security and monitoring techniques are designed to provide multiple layers of protection and defense. We use firewalls to prevent our network from unauthorized access and undesirable traffic. Our systems are segmented into separate networks to protect sensitive data. Systems supporting testing and development activities are hosted in a separate network from systems supporting Zoho's production infrastructure.

We monitor firewall access with a strict, regular schedule. A network engineer

reviews all changes made to the firewall everyday. Additionally, these changes are reviewed every three months to update and revise the rules. Our dedicated Network Operations Center team monitors the infrastructure and applications for any discrepancies or suspicious activities. All crucial parameters are continuously monitored using our proprietary tool and notifications are triggered in any instance of abnormal or suspicious activities in our production environment.

Network redundancy

All the components of our platform are redundant. We use a distributed grid architecture to shield our system and services from the effects of possible server failures. If there's a server failure, users can carry on as usual because their data and Zoho services will still be available to them.
We additionally use multiple switches, routers, and security gateways to ensure device-level redundancy. This prevents single-point failures in the internal network.

DDoS prevention

We use technologies from well-established and trustworthy service providers to prevent DDoS attacks on our servers. These technologies offer multiple DDoS mitigation capabilities to prevent disruptions caused by bad traffic, while allowing good traffic through. This keeps our websites, applications, and APIs highly available and performing.

Our dedicated Network Operations Center team monitors the infrastructure and applications for any discrepancies or suspicious activities. All crucial parameters are continuously monitored using our proprietary tool and notifications are triggered in any instance of abnormal or suspicious activities in our production environment.

Server hardening

All servers provisioned for development and testing activities are hardened (by disabling unused ports and accounts, removing default passwords, etc.). The base Operating System (OS) image has server hardening built into it, and this OS image is provisioned in the servers, to ensure consistency across servers.

Intrusion detection and prevention

Our intrusion detection mechanism takes note of host-based signals on individual devices and network-based signals from monitoring points within our servers. Administrative access, use of privileged commands, and system calls on all servers in our production network are logged. Rules and machine intelligence built on top of this data give security engineers warnings of possible incidents. At the application layer, we have our proprietary WAF which operates on both whitelist and blacklist rules.

At the Internet Service Providers (ISP) level, a multi-layered security approach is implemented with scrubbing, network routing, rate limiting, and filtering to handle attacks from network layer to application layer. This system provides clean traffic, reliable proxy service, and a prompt reporting of attacks, if any.

1.2 Data security

Why is data security crucial?

Data is the lifeblood of businesses of all sizes, from a small startup to a global conglomerate. Protecting your and your customer data protects your company from financial loss, reputation damage, consumer confidence disintegration, and brand erosion. We follow a holistic approach of hardened security to ensure that your data remains protected.

Secure by design

Every change and new feature is governed by a change management policy to ensure all application changes are authorised before implementation into production. Our Software Development Life Cycle (SDLC) mandates adherence to secure coding guidelines, as well as screening of code changes for potential security issues with our code analyser tools, vulnerability scanners, and manual review processes.

Our robust security framework based on OWASP standards, implemented in the application layer, provides functionalities to mitigate threats such as SQL injection, Cross site scripting and application layer DOS attacks.

Data isolation

Our framework distributes and maintains the cloud space for our customers. Each customer's service data is logically separated from other customers' data

using a set of secure protocols in the framework. This ensures that no customer's service data becomes accessible to another customer.

The service data is stored on our servers when you use our services. Your data is owned by you, and not by Zoho. We do not share this data with any third-party without your consent.

Encryption

In transit: All customer data transmitted to our servers over public networks is protected using strong encryption protocols. We mandate all connections to our servers use Transport Layer Security (TLS 1.2/1.3) encryption with strong ciphers, for all connections including web access,API access,our mobile apps, and IMAP/POP/SMTP email client access. This ensures a secure connection by allowing the authentication of both parties involved in the connection, and by encrypting data to be transferred. Additionally for email, our services leverages opportunistic TLS by default. TLS encrypts and delivers email securely, mitigating eavesdropping between mail servers where peer services support this protocol.

We have full support for Perfect Forward Secrecy (PFS) with our encrypted connections, which ensures that even if we were somehow compromised in the future, no previous communication could be decrypted. We have enabled HTTP Strict Transport Security header (HSTS) to all our web connections. This tells all modern browsers to only connect to us over an encrypted connection, even if you type a URL to an insecure page at our site. Additionally, on the web we flag all our authentication cookies as secure.

At rest: Sensitive customer data at rest is encrypted using 256-bit Advanced Encryption Standard (AES). The data that is encrypted at rest varies with the

services you opt for. We own and maintain the keys using our in-house Key Management Service (KMS). We provide additional layers of security by encrypting the data encryption keys using master keys. The master keys and data encryption keys are physically separated and stored in different servers with limited access.

Please click here for detailed information about encryption at Zoho and click here to understand what data we encrypt in our services.

Data retention and disposal

We hold the data in your account as long as you choose to use Zoho Services. Once you terminate your Zoho user account, your data will get deleted from the active database during the next clean-up that occurs once every 6 months. The data deleted from the active database will be deleted from backups after 3 months. In case of your unpaid account being inactive for a continuous period of 120 days, we will terminate it after giving you prior notice and option to back-up your data.

A verified and authorized vendor carries out the disposal of unusable devices. Until such time, we categorize and store them in a secure location. Any information contained inside the devices is formatted before disposal. We degauss failed hard drives and then physically destroy them using a shredder. We crypto-erase and shred failed Solid State Devices (SSDs).

1.3 Identity and Access control

Why is IAM crucial?

Identity and Access Management (IAM) is an important part of an enterprise security management system. It allows IT administrators to automate numerous user account related tasks such as standardizing and managing identities, authentication, and authorization, boosting the efficiency and effectiveness of access management across an organization while reducing risk to the business.

Single Sign-On (SSO)

Zoho offers single sign-on (SSO) that lets users access multiple services using the same sign-in page and authentication credentials. When you sign in to any Zoho service, it happens only through our integrated Identity and Access Management (IAM) service. We also support SAML for single sign-on that makes it possible for customers to integrate their company's identity provider like LDAP, ADFS when they login to Zoho services

SSO simplifies login process, ensures compliance, provides effective access control and reporting, and reduces risk of password fatigue, and hence weak passwords.

Multi-Factor Authentication

It provides an extra layer of security by demanding an additional verification that the user must possess, in addition to the password. This can greatly reduce the risk of unauthorized access if a user's password is compromised. You can configure multi-factor authentication using Zoho One-Auth. currently, different modes like biometric Touch ID or Face ID, Push Notification, QR code, and Time-based OTP are supported.

We also support Yubikey Hardware Security Key for multi-factor authentication.

Administrative access

We employ technical access controls and internal policies to prohibit employees from arbitrarily accessing user data. We adhere to the principles of least privilege and role-based permissions to minimize the risk of data exposure.

Access to production environments is maintained by a central directory and authenticated using a combination of strong passwords, two-factor authentication, and passphrase-protected SSH keys. Furthermore, we facilitate such access through a separate network with stricter rules and hardened devices. Additionally, we log all the operations and audit them periodically.

1.4 Operational security

Why is operational security important?

The operational security policy defines the responsibilities and authorization, as well as disciplinary actions in case of breaches. It establishes clear guidelines on what employees are allowed to do and what they are not allowed to do. This ensures that strict procedure and documentation is followed for every specific action taken in our security measures—from restricting employees to blocking malware.

Logging and Monitoring

We monitor and analyse information gathered from services, internal traffic in our network, and usage of devices and terminals. We record this information in the form of event logs, audit logs, fault logs, administrator logs, and operator logs. These logs are automatically monitored and analyzed to a reasonable extent that helps us identify anomalies such as unusual activity in employees' accounts or attempts to access customer data. We store these logs in a secure server isolated from full system access, to manage access control centrally and ensure availability.

Detailed audit logging covering all update and delete operations performed by the user are available to the customers in every Zoho service.

Vulnerability management

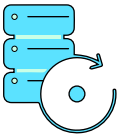
We have a dedicated vulnerability management process that actively scans for security threats using a combination of certified third-party scanning tools and in-house tools, and with automated and manual penetration testing efforts. Furthermore, our security team actively reviews inbound security reports and monitors public mailing lists, blog posts, and wikis to spot security incidents that might affect the company's infrastructure.

Once we identify a vulnerability requiring remediation, it is logged, prioritized according to the severity, and assigned to an owner. We further identify the associated risks and track the vulnerability until it is closed by either patching the vulnerable systems or applying relevant controls.

Malware and spam protection

We scan all user files using our automated scanning system that's designed to stop malware from being spread through Zoho's ecosystem. Our custom anti-malware engine receives regular updates from external threat intelligence sources and scans files against blacklisted signatures and malicious patterns. Furthermore, our proprietary detection engine bundled with machine learning techniques, ensures customer data is protected from malware.

Zoho supports Domain-based Message Authentication, Reporting, and Conformance (DMARC) as a way to prevent spam. DMARC uses SPF and DKIM to verify that messages are authentic. We also use our proprietary detection engine for identifying abuse of Zoho services like phishing and spam activities. Additionally, we have a dedicated anti-spam team to monitor the signals from the software and handle abuse complaints. For more information, click here

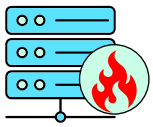


Backup

We run incremental backups every day and weekly full backups of our databases using Zoho Admin Console (ZAC) for Zoho's DCs. Backup data in the DC is stored in the same location and encrypted using AES-256 bit algorithm. We store them in tar.gz format. All backed up data are retained for a period of three months. If a customer requests for data recovery within the retention period, we will restore their data and provide secure access to it. The timeline for data restoration depends on the size of the data and the complexity involved.

To ensure the safety of the backed-up data, we use a redundant array of independent disks (RAID) in the backup servers. All backups are scheduled and tracked regularly. In case of a failure, a re-run is initiated and is fixed immediately. The integrity and validation checks of the full backups are done automatically by the ZAC tool.

From your end, we strongly recommend scheduling regular backups of your data by exporting them from the respective Zoho services and storing it locally in your infrastructure.



Disaster recovery and business continuity

Application data is stored on resilient storage that is replicated across data centers. Data in the primary DC is replicated in the secondary in near real time. In case of failure of the primary DC, secondary DC takes over and the operations are carried on smoothly with minimal or no loss of time. Both the centers are equipped with multiple ISPs.

We have power back-up, temperature control systems and fire-prevention systems as physical measures to ensure business continuity. These measures help us achieve resilience. In addition to the redundancy of data, we have a business continuity plan for our major operations such as support and infrastructure management.

1.5 Incident Management

What is the purpose of incident management?

Incident management, as the name suggests, is the process that is used to manage the lifecycle of all incidents with proper records of past similar incidents and their resolutions. Incidents can be identified by technical staff, reported and detected by event monitoring tools, be conveyed by communications from users (usually through a telephone call to the service desk), or reported by third-party suppliers and partners.

Reporting

We have a dedicated incident management team. We notify you of the incidents in our environment that apply to you, along with suitable actions that you may need to take. We track and close the incidents with appropriate corrective actions. Whenever applicable, we will identify, collect, acquire and provide you with necessary evidence in the form of application and audit logs regarding incidents that apply to you. Furthermore, we implement controls to prevent recurrence of similar situations.

We respond to the security or privacy incidents you report to us through incidents@zohocorp.com, with high priority. For general incidents, we will notify users through our blogs, forums, and social media. For incidents specific to an individual user or an organization, we will notify the concerned party through email (using their primary email address of the Organisation administrator registered with us).

Breach notification

As data controllers, we notify the concerned Data Protection Authority of a breach within 72 hours after we become aware of it, according to the General Data Protection Regulation (GDPR). Depending on specific requirements, we notify the customers too, when necessary. As data processors, we inform the concerned data controllers without undue delay.

1.6 Organizational security

What is the purpose of organizational security?

Organizational security policy establishes the minimum administrative, technical, and physical safeguards that will be utilized to protect sensitive information from unauthorized access and disclosure. These set of procedures guide employees' interactions with data and data processing systems so that our security efforts always stay aligned with the goals of our business.

We have an Information Security Management System (ISMS) in place which takes into account our security objectives and the risks and mitigations concerning all the interested parties. We employ strict policies and procedures

encompassing the security, availability, processing, integrity, and confidentiality of customer data.

Employee background checks

Each employee undergoes a process of background verification. We hire reputed external agencies to perform this check on our behalf. We do this to verify their criminal records, previous employment records if any, and educational background. Until this check is performed, the employee is not assigned tasks that may pose risks to users.

Security Awareness

Each employee, when inducted, signs a confidentiality agreement and acceptable use policy, after which they undergo training in information security, privacy, and compliance. Furthermore, we evaluate their understanding through tests and quizzes to determine which topics they need further training in. We provide training on specific aspects of security, that they may require based on their roles.

We educate our employees continually on information security, privacy, and compliance in our internal community where our employees check in regularly, to keep them updated regarding the security practices of the organization. We also host internal events to raise awareness and drive innovation in security and privacy.

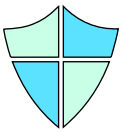
Dedicated security and privacy teams

We have dedicated security and privacy teams that implement and manage our security and privacy programs. They engineer and maintain our defense systems, develop review processes for security, and constantly monitor our networks to detect suspicious activity. They provide domain-specific consulting services and guidance to our engineering teams.

Internal audit and compliance

We have a dedicated compliance team to review procedures and policies in Zoho to align them with standards, and to determine what controls, processes, and systems are needed to meet the standards. This team also does periodic internal audits and facilitates independent audits and assessments by third parties.

For more details, check out our compliance portfolio.



Endpoint security

All workstations issued to Zoho employees run up-to-date OS version and are configured with anti-virus software. They are configured such that they comply with our standards for security, which require all workstations to be properly configured, patched, and be tracked and monitored by Zoho's endpoint management solutions. These workstations are secure by default as they are configured to encrypt data at rest, have strong passwords, and get locked when they are idle. Mobile devices used for business purposes are enrolled in the mobile device management system to ensure they meet our security standards.

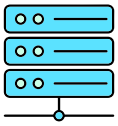
1.7 Physical security

What is the purpose of physical security?

The objective of physical security is to safeguard personnel, information, equipment, IT infrastructure, facilities and all other company assets. Rigorous controls at our offices and datacenters are installed to keep out external threats.

At workplace

We control access to our resources (buildings, infrastructure and facilities), where accessing includes consumption, entry, and utilization, with the help of access cards. We provide employees, contractors, vendors, and visitors with different access cards that only allow access strictly specific to the purpose of their entrance into the premises. Human Resource (HR) team establishes and maintains the purposes specific to roles. We maintain access logs to spot and address anomalies.



At Data Centers

At our Data Centers, a co location provider takes responsibility of the building, cooling, power, and physical security, while we provide the servers and storage. Access to the Data Centers is restricted to a small group of authorized personnel. Any other access is raised as a ticket and allowed only after the approval of respective managers. Additional two-factor authentication and biometric authentication are required to enter the premises. Access logs, activity records, and camera footage are available in case an incident occurs.

Monitoring

We monitor all entry and exit movements throughout our premises in all our business centers and data centers through CCTV cameras deployed according to local regulations. Back-up footage is available up to a certain period, depending on the requirements for that location.

2.0 Compliance at Zoho Creator

Certifications

IS 642819
ISO/IEC 27001

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.

Applicable to- All cloud services and on-premise products of Zoho, ManageEngine, Site24x7, WebNMS and GSP Solution.

PM 732705
ISO/IEC 27701

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 organisations to demonstrate compliance with the various privacy regulations around the world that are applicable to them.

Applicable to- All business units, cloud services and on-premise products of Zoho, ManageEngine, Site24x7, WebNMS which function in the capacity of a PII controller and/or as a PII Processor.

CLOUD 714132
ISO/IEC 27017

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.

Applicable to- All Cloud services of Zoho, Manage Engine and Site24x7.

PII 714133
ISO/IEC 27018

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).

Applicable to- All Cloud services of Zoho, Manage Engine and Site 24x7.

SOC 2

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.

Applicable to- All cloud services and on-premise products of Zoho, ManageEngine, Site24x7, WebNMS and GSP Solution.

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'.

SOC 2 + HIPAA

Applicable to- Zoho CRM, Zoho Desk, Zoho Mail, Zoho Creator , Zoho Projects, Zoho Workdrive (including Zoho Writer, Zoho Sheet, Zoho Show), Zoho Sign, Zoho People, Zoho Books, Zoho Invoice, Zoho Inventory, Zoho Subscriptions, Zoho Expense, Zoho Checkout, Zoho Payroll, ManageEngine Desktop Central and ManageEngine ServiceDesk Plus Cloud.

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.

Zoho, being PCI compliant, consistently adheres to a set of guidelines set forth by companies that issue credit cards.

Applicable to- All the Zoho finance Plus products (ie) Zoho Books, Zoho Invoice, Zoho Inventory, Zoho Subscriptions, Zoho Expense, Zoho Checkout and Zoho Commerce.The Payments module of Zoho Creator uses Zoho Checkout, which is PCI compliant.

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.

Applicable to- Zoho Corporation

3.0 More security for your apps

To add to the various security measures offered by Zoho, at a product level, Zoho Creator also provides more security features to protect your apps, and the data in them. Let's learn about them in detail.

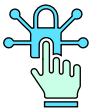
Audit trails

If you want to exercise effective governance, you need to have complete visibility of your application. With Zoho Creator's rich metadata, everything is traceable and auditable. It enables users to supervise every minute detail of their application with audit trails. It captures the history of changes made to a record, for viewing/auditing purposes. When a user updates a record with new values or deletes an existing record, the updated or deleted record values gets logged along with the entire activity log such as old value, modified value, user who modified/deleted the record and more. Learn more about Audit Trails here.

Encryption

Zoho Creator is regulated with the EU GDPR Regulation Act. You can choose to encrypt the Zoho Creator Fields which are identified to contain any PII. Fields like Name and Email in Zoho Creator are optimized to protect the privacy of your respondents and safeguard any personally identifiable information (PII). You can also label sensitive PII to be encrypted while in transit and at storage. Set compliance checks to adhere to industry regulations. For example, a healthcare organization can mark a field that contains HIPAA-sensitive data as ePHI (electronic protected health information). Please refer here to know more.

All customer data transmitted to our servers over public networks is protected using strong encryption protocols. We mandate all connections to our servers use Transport Layer Security (TLS 1.2/1.3) encryption with strong ciphers, for all connections including web access, API access, our mobile apps, and IMAP/POP/SMTP email client access. This ensures a secure connection by allowing the authentication of both parties involved in the connection, and by encrypting data to be transferred. Additionally for email, our services leverages opportunistic TLS by default. TLS encrypts and delivers email securely, mitigating eavesdropping between mail servers where peer services support this protocol. Learn more



Role-based access controls

Decide what people can access based on their roles in your organizational hierarchy. Roles and Permissions in Zoho Creator help you regulate who can access your application, how much of it can be accessed, and what actions can be performed. You can create roles for different users and define form, report and even record-level read, write and edit permissions. For more information on how user management works, please refer Users , Roles & Permissions.

Identity and access management

Zoho supports strong authentication with multiple enterprise systems. Users can authenticate via:

- SAML 2.0
- Active Directory
- MFA

User passwords are hashed and stored, to prevent brute-force attacks. Customized Password policy can also be set for an Organization by means of Zoho Directory/Active Directory.

Single sign-on

Provide seamless login experience to users with single sign-on (SSO). It allows users to access different services using the same sign-in page and authentication credentials, thereby reducing the risk of password fatigue. We also support SAML for single sign-on that simplifies integration with your company's identity provider like LDAP, ADFS etc.

Moreover, using ADSync tool you can maintain all user identities in a single place and eliminate the time required to manage users and groups manually. Learn how to set up SSO for your account here.

Vulnerability and penetration testing

To identify Security Vulnerabilities existing in the application and infrastructure, we conduct Network Vulnerability scans and Penetration Tests. Network vulnerability scans are performed for all internet facing endpoints, once in a week by an Industry-standard-external third party tool and Penetration Tests (Application Layer Penetration) are done by our Application Security team once in every 6 months. Also, we have BugBounty program to encourage external hackers to contribute to our security and get them rewarded.

User passwords are hashed and stored, to prevent brute-force attacks. Customized Password policy can also be set for an Organization by means of Zoho Directory/Active Directory.

Zoho OAuth 2.0

OAuth 2.0 is an industry standard protocol specification that enables third-party applications (clients) to gain delegated access to protected resources in Zoho via an API.

With OAuth:

- Clients are not required to support password authentication or store user credentials
- Clients gain delegated access, i.e., access only to resources authenticated by the user.
- Users can revoke third-party application's delegated access anytime
- OAuth access tokens expire after a set time. If the client faces a security breach, user data will be compromised only until the access token is valid.

Learn more about OAuth here.

Zoho Creator's GDPR readiness

Addressing rights of Data Subjects

The following are the Data Subject Rights that GDPR identifies, and how Zoho Creator helps you address them in your apps:

» **Right to be informed:** Add an add notes field to your form

- The Data Subject has a right to be informed on how their personal data was, is, and will be processed. By adding an add notes field to your form (next to the fields in which you're collecting their personal data), you can explain why you need said data, what you will be using it for, and how it will be processed. You can also insert a hyperlink (in the note) to your organization's privacy policy.

» **Right to access, right to erasure, and right to be forgotten:** You need to forward the requests you receive from your users to support@zohocreator.com. Our Support team will analyze the request and guide you on how to act on it.

- With their right to access, the Data Subject can demand Data Controllers to furnish the following: the personal data (of the Data Subject) that was collected and processed, how it was obtained, how it is processed, and to whom it was shared with — all the details from point of collection to point of storage

- With their right to erasure, the Data Subject can demand that Data Controllers erase all their personal data

- With their right to be forgotten, the Data Subject can demand for their data to be completely erased

» **Right to rectify:** Users can edit their records by accessing the respective reports

- The Data Subject has a right to obtain from the Data Controllers, without undue delay, the rectification of inaccurate personal data concerning them, and also complete any incomplete data point.

» **Right to object to processing of their personal data:** Add a decision box to your form

- Use separate decision box fields to capture the Data Subject's consent to process their personal data, and define your workflows such that these permissions are checked for before they are processed. To give or take away their permission, the Data Subject can simply update the relevant decision box field accordingly.

» **Right to data portability:** Data submitted by your users can be exported as spreadsheets and PDFs

- The Data Subject has a right to receive all their personal data, submitted to the Data Controller. To do this, users can simply export their records from reports.

Implement some best practices

You can leverage the features and capabilities of Zoho Creator to implement the following in your apps:

» **Denote fields that contain personal data:** The Contains personal data field property helps you define if the concerned field is one in which your users will be entering some personal data.

» **Encrypt data: Upon enabling this field property, the data your users enter in that field will be stored in an encrypted format.** Lean more

» **Capture location:** Forms in your Zoho Creator app can, with your user's consent, capture the geographical location from where they submit their entries. Learn more

» **Capture IP address:** Forms in your Zoho Creator app can capture the public IP address using which your users submit their entries. Learn more

» **Getting consent:** Data Subjects have a right to be informed on why your app, or a form in your app, is collecting data, and how it will be processed. Also, as a Data Controller, you may need to show if your users gave their consent for this. Here's how you do it:

- If consent is required along with the data a form is already collecting, then add an add notes field (which will display information on why you need to collect certain data points, and how you will process them), and a decision box field (marked mandatory) that lets your users give their consent

- If consent is required on the app level, add a new form and use the combination of add notes and decision box fields as given above

- To let your users know what they consented to, you can send them an email saying they've given their consent (and copy-paste the add notes field's content in the email's message)

» **Provision a double opt-in mechanism for your form or app:** Double opt-in is a widely used mechanism to get the intended audience to confirm before proceeding. You can put in place a double opt-in before you let your users access any form in your app. Here's how you do it:

- Add a new form to your app, which contains an add notes field (where you can add whatever information you want your users to know), an email field (to which you'll send an email) and a decision box field (to capture if user yours consent to receiving an email)

- The email you send on form submission must contain the link to your intended form

4.0 Customer controls for security

So far, we have discussed what we do to offer security on various fronts to our customers. Here are the things that you as a customer can do to ensure security from your end:

» Choose a unique, strong password and protect it.

» Use multi-factor authentication

» Use the latest browser versions, mobile OS and updated mobile applications to ensure they are patched against vulnerabilities and to use latest security features

» Exercise reasonable precautions while sharing data from our cloud environment.

- Classify your information into personal or sensitive and label them accordingly.

- Monitor devices linked to your account, active web sessions, and third-party access to spot anomalies in activities on your account, and manage roles and privileges to your account.

- Be aware of phishing and malware threats by looking out for unfamiliar emails, websites, and links that may exploit your sensitive information by impersonating Zoho or other services you trust.

4.1 Understanding shared responsibility with Zoho

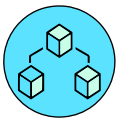
Our customers can collaborate with us and take individual responsibility towards cloud security and privacy. Zoho takes responsibility for building products that are secure, reliable, and robust. While we maintain the cloud infrastructure, you are responsible for securing your data and the settings you configure within the Zoho applications.

When you use Zoho, data security and privacy is a shared responsibility between you and us. Here's a model that describes the high-level architecture of our cloud environment, which is Software as a service (SaaS), and the associated responsibilities.

Customer's Responsibility	Shared Responsibility	Zoho's Responsibility
Data accountability	Identify and access management	Data security
Passwords	Data management	Availability
Client and endpoint security	Managing data to other parties	Business continuity
	Encryption	Network controls
	Backups	Host infrastructure
	Incident management	Physical security
	Awareness and training	
	Policy and compliance	

We have put together this guide to help you understand what Zoho does to keep your account safe, what you can do to secure your data, and how we can work together to achieve a safe cloud environment.

4.2 Customer's responsibility



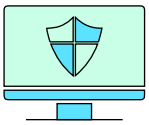
Data accountability

You are responsible for:

- The data you share and receive over the cloud. You decide whom you share it with, the period, and the means of sharing.
- Ensuring the privacy of data you handle using Zoho services, to ensure that you do not accidentally or willingly make any private content publicly available.
- Maintaining the accuracy of the data that you process in your system.
- Ensuring that your Zoho service account is not used by you or others on your behalf for spamming or illegal activities, that Zoho's services are only used for their intended purposes.

Passwords

You are responsible for creating a strong password and safeguarding it when you use it to log in and access the cloud.



Client and end-point security

- The compromise of one of your endpoints (whether your laptop, desktop, or smart phone) will render all other controls ineffective.
- You are responsible for your end-point security and are expected to keep your browser services, mobile OS, and mobile applications updated to the latest version and patched against vulnerabilities.

4.3 Shared responsibility

Responsibility of control that will apply to both you and Zoho.

Identity and access management

We provide infrastructure for managing user accounts through Identity and Access Management (IAM) service by facilitating:

- User registration, de-registration options, and specifications on how to use them.
- Functionality for managing access rights of your cloud users.
- Strong authentication techniques such as Multi-Factor Authentication and IP address restrictions.

You are responsible for:

- Implementing strong user access management controls.
- Configuring strong passwords based on the organization's policy and protecting them.
- Enabling Multi-Factor Authentication for your organization's users.
- Administering user accounts and privileges—configuring user roles according to the principal of least privilege.
- Defining the administrator(s) of the organization's account and having a proper process for ownership transfers. Taking necessary steps to ensure that your organization does not lose control of its administrator accounts.
- Periodically reviewing the list of users with access to data and removing access for anyone who should not have it.
- Frequently reviewing devices linked to the organization's user accounts and removing unused or unauthorized devices.
- Monitoring your organization's user accounts for malicious access or usage.
- Notifying Zoho of any unauthorized use of your organization’s accounts.
- Educating your users on the importance of good password management, the risks on credential reuse, social logins, and phishing attacks.

Data Management

We provide a platform for you to manage your data with:

- Data sharing features for administrator and user-level controls.
- Audit features on customer data to provide transparency on important activities and to track changes.
- Data interoperability—the option to take a complete backup of data and configurations to migrate all or a part of your data to another SaaS provider.
- Data retention and disposal—we hold the data in your account as long as you choose to use Zoho Services. Once you terminate your Zoho user account, your data will get deleted from the active database during the next cleanup that occurs once every six months. The data deleted from the active database will be deleted from backups after three months.
- Access limitations features to limit employees from accessing customer data and ensure that they can only do so if there is a specific reason.

You are accountable for:

- Due diligence while processing information belonging to special categories (for example, personal/sensitive data) by applying appropriate controls to comply with the requirements of applicable legislation.
- Configuring proper sharing and viewing permissions.
- Regularly reviewing audit reports to identify any suspicious activity.

- Maintaining up-to-date contact information with Zoho.
- Taking your data out of the system once you stop using our services. Otherwise it will be subjected to permanent deletion without any scope for recovery.

Managing data to other parties

We work towards having secure integrations and extensions to our applications by:

- **Marketplace applications:** Performing functional testing, security testing, and privacy testing once an application is submitted to us. We also perform product review and content review.
- **Sub-processors:** Evaluating the security and privacy practices of sub-processors whom we wish to contract to ensure that they are in line with Zoho's information security and privacy standards. We then execute appropriate data protection agreements with them.
- We review the privacy policy and terms of service of our vendors and ensure that their operations stick to it.

We expect you to:

- Enable or disable third-party integrations after taking into consideration the data that gets shared to third-party environments. You must review the terms and the privacy policy of the third-party service regarding the collection, use, or disclosure of data.

- Mark your preference on whether you would like to share your details with vendors every time an extension is installed.
- Assess the suitability of the Marketplace Apps and the reasonableness of the requested permissions prior to installation.
- Notify Zoho of any malicious behaviour identified in the Marketplace Apps.

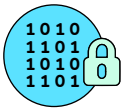
Data subject rights

We are accountable for:

- Providing features that enable customers to cater to and protect the rights of your customers.
- Notifying you of requests from your customers when they contact us directly for exercising their rights.

You are obliged to:

- Honor and handle requests from customers for data access, rectification, deletion, and restrictions in processing of their personal information.



Encryption

We safeguard your data using encryption at transit and at rest in the following ways:

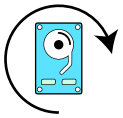
- **Data in transit:** Customer data transmitted to our servers over public networks is protected using strong encryption protocols. We mandate all connections to our servers use Transport Layer Security (TLS 1.2/1.3) encryption with strong ciphers for all connections including web access, API access, our mobile apps, and IMAP/POP/SMTP access.

- **Data at rest:** Sensitive customer data is encrypted at rest using Advanced Encryption Standard (AES) 256-bit algorithm. The data that is encrypted at rest varies with the services you opt for. We own and maintain the keys using our in-house Key Management Service(KMS).

We suggest you to:

- Determine your encryption needs. For data at rest, in many instances while using our services, you may be responsible for defining which of the fields need to be encrypted.

- When the data from our cloud is downloaded or exported into your environment or synced within integrations in Zoho or with any other third-party integration, you need to ensure that relevant encryption controls are applied. For example, enable disk encryption on your devices and use the export feature with password protection enabled, etc.



Backups

We are equipped with a robust system to:

- Maintain system-level backups encrypted with AES-256 bit algorithm and stored securely. Automatically run integrity and validation checks of the full backups.

- Enable requests for data restoration and provide secure access to it within the retention period. Provide customers a feature to export and take a backup of their data.

From your end, you can:

- Schedule a backup for your data, export it from its respective Zoho services, and store it locally in your infrastructure, if necessary. You are responsible for storing it in a secure manner.

Incident management

From our side, we ensure to:

- Report all incidents of breach that we are aware of and that applies to you along with impact details and suitable actions. For incidents specific to an individual user or an organization, we will notify the concerned party through email registered with us.

- Track such incidents and close them.

- Implement controls to prevent recurrence of similar incidents.
- If requested, we will provide additional evidence related to the incident that applies to you.

We expect you to:

- Take actions suggested by Zoho in case of a breach.
- Meet your data breach disclosure and notification requirements, such as notifying your end users and data protection authorities when relevant.
- Report security and privacy incidents that you are aware of to incidents@zohocorp.com.

Awareness and training

We take complete responsibility for:

- Training our employees to be security-conscious and to adhere to a secure development standard. Newly hired employees take part in mandatory security and privacy training in addition to receiving regular security awareness training via informational emails, presentations, and resources available on our intranet.
- Training our employees on appropriate handling of cloud service customer data.

You are responsible for training cloud users on:

- Standards and procedures for the use of our services.
- How the risks related to our services are managed.
- Risks on the general system and the network environment.
- Applicable legal and regulatory considerations.

Policy and compliance

We adhere to set of guidelines, such as:

- We have a comprehensive risk management program in place and effectively implement the controls.
- We operate within the law of various jurisdictions where we operate from.
- We provide evidence of compliance with applicable legislations and based on our contractual requirements.
- We will assist in DPIA assessments of our customers to the extent allowed by the applicable laws.

We expect you to:

- Evaluate regulations and laws that are applicable to you and to review our compliance with regulations and standards that are needed for your

business. You can request for additional information to serve as evidence of our compliance.

» Understand our policies, our policy assessment methods, and how we process data.

» Conduct DPIA as required by the data protection laws applicable to your organisation before / while processing data

» Before you process any personal/sensitive data, assess your lawful basis. In case your lawful basis is consent, ensure you obtain the consent from your customers.

» Assess the suitability of our cloud-based services based on the information we provide and ensure it is sufficient to meet your compliance needs.

» Understand the risk profile and sensitivity of the data hosted in the Zoho services and apply appropriate controls.

4.4 Zoho's responsibility

We are responsible for the protection 'of' the cloud and related controls that run all Zoho services.

Data security

- We are responsible for the isolation of your data stored with us. Each customer's service data is logically separated from other customers' data using a set of secure protocols in the framework.
- We are responsible for the confidentiality of your data stored with us at rest, in transmission, and during processing.
- We are responsible for the integrity of both your data and system data such as logs and configuration data.
- We are responsible for traceability and control of your data, such that at any given time, the physical location and processing of data can be known.

Availability

- We are responsible for ensuring that our services are available as per our uptime SLA of 99.9% by handling hardware/software failures and threats like denial of service attacks.

» As a customer, you can visit status.zoho.com at any time to view the current site status, as well as past disruptions.

Business continuity

» We are responsible for having a business continuity plan in place for our major operations such as support and infrastructure management.

» We will ensure that the application data stored on resilient storage is replicated across data centers. Data in the primary DC is replicated in the secondary in near real-time, and we can switch to the secondary in case of any disaster.

Network controls

» We are responsible for operating a secure production network. We use firewalls to prevent our network from unauthorized access and undesirable traffic. Access to production networks is strictly controlled.

Host infrastructure

» We are responsible for protecting and securing the host infrastructure. All servers provisioned in the production network are hardened according to the standards. OS patch management, baseline configuration, and Host intrusion detection technologies are adopted to maintain a secure infrastructure.

Physical security

» We are responsible to ensure that our infrastructure is protected from unauthorized physical access, intrusion, and disasters.

Note:

The shared responsibility model for cloud security provides clarity on security expectations for cloud users and cloud service providers. However, an understanding of the expectation is just the first step. Users must take action on these responsibilities by creating policies and procedures for their portion of cloud security. Zoho will continue to work hard to keep your data secure—like we always have—and will strive to work towards a secure cloud environment.

For any further queries on this topic, feel free to contact us at **security@zohocorp.com**

5.0 Reach out to us

Security of your data is your right and a never-ending mission of Zoho. We will continue to work hard to keep your data secure, like we always have.

For any further queries on this topic, take a look at our FAQs or write to us at security@zohocorp.com.

About Us

At Zoho Creator, we've always worked towards a single purpose—enabling problem solvers of varied technical skills to build business solutions that make a difference.

Equipped with features like a drag-and-drop interface, predictive analysis, and prebuilt integrations, we empower users to build and deploy custom applications 10x faster than conventional methods. Build tailor made solutions from scratch, or choose from our extensive range of prebuilt apps to kickstart your digital transformation.

Contact Us

We'd love to talk! Reach out to us at
hello@zohocreator.com

Zoho.com/creator