Zoho Security Practices, Policies & Infrastructure

With more than three million users worldwide and a growing number of small, medium and large sized companies using Zoho services from every industry, security and data protection are two of the most important aspects of our offering. Needless to say, we take security very seriously and have developed a comprehensive set of practices, technologies and policies to ensure you that your data is secure.

If you are currently maintaining your data on laptops, flash drives or other media as well as on your corporate or company 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 ensure that your data is protected. Our security practices are grouped in four different areas: Physical Security; Network Security; People, Process and Monitoring; Redundancy and Business Continuity.

Physical Security

Physical security is the first line of defense. Our datacenters are hosted in 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 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.

- **256-bit SSL**. The communication between your computer and our servers is encrypted using a strong 256-bit key. What this means is that even if the information traveling between your computer and our servers were to be intercepted, it would be nearly impossible for anyone to make any sense out of it. Please check our product pages for details on which applications support SSL.
- **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 implementing data center infrastructure requires not just technology, but a disciplined approach to process. 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 has improved the process over time. Zoho has developed a world class process 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.** Are regularly performed and the whole process is reviewed by management
- **As-Needed**. 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.
- **Compliance.** While not formerly certified for any particular vertical industry such as health care, our team is preparing for eventual certification and has implemented policies that are in line with the strictest industry standards such as HIPPA and SaaS 70.

Monitoring, Redundancy and Business Continuity
One of the fundamental philosophies of computing in general, is the acknowledgment and assumption that computer resources will at some point fail. So 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 the basic server unit will eventually fail so 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. Please note geo mirroring is available on select products and plans.
- **Fire Prevention**. The Zoho data centers are guarded by industry-standard fire prevention and control systems.
- **Data Protection & Back-up.** All user data is backed-up at least three times and a fourth copy is sent off site to another secure, redundant tier 4 data center

located across the country further protecting users data in the unlikely event of a natural disaster*.

*A note on customers wanting to get their data from Zoho: Our stated customer data policy is that our customers own their data and can retrieve it from Zoho upon request. In some Zoho applications, users can simply select an option to download or export copies of their documents using the built-in feature available in the application.

Additional Information:

While we cannot list all the details of our infrastructure for security reasons, rest assured that Zoho's Security, Practices, policies and Infrastructure are proven and reliable.

For more information about Zoho and our Security please contact:
zohosecurity@zohocorp.com