WORKSMAIL COMMS

Streamlined Communication for Enhanced Productivity.

At Worksmail, we recognize that your trust in us is our most valuable asset. That's why we've designed our network from the ground up with security in mind — and why privacy protection is built into every aspect of our business, from software updates to backups to staff training. We regularly assess potential threats and vulnerabilities, and take proactive steps to adopt even stronger security protocols and practices.

While we go to great lengths to ensure account security and data protection, it is also the customer's and end-user's responsibility to take reasonable precautionary measures to keep their accounts free from intrusion. Security starts with you.

Below, we provide some details on the specific measures we take, on our end, to keep your data as safe as possible.

Best-in-class physical security

Our servers are colocated with Aptum Technologies in Montreal, Canada. Only authorized personnel have access to our facilities, which can only be entered by scanning a badge and passing a biometric scan. Security cameras provide video surveillance throughout the facilities, and we regularly review video recordings of our space.

Actively monitored network infrastructure

Our network is constructed of redundant Cisco Nexus 9300 series switches, ensuring maximum uptime. Trunks run at a lightning-fast 40gbps, while edge access runs at 10gbps. All physical network infrastructure is properly trunked and secured, while internal and external monitoring stations test all services every minute, 24/7, using Alertra.com.

Proactively secure staff policies

We screen all staff members with rigorous background checks. All staff are required to sign non-disclosure and confidentiality agreements, ensuring that all communication about our services remains exclusively in-house.

Leading-edge email encryption

Access to data is mediated through SSL / TLS1.2, which provides Perfect Forward Secrecy for Webmail / IMAP / SMTP and POP3 email services. We leverage HTTP Strict Transport Security, and maintain an updated Content Security Policy to further enhance the security of our webmail system. All our servers are firewalled, and only used service ports are made accessible. Only in the very rare cases when a recipient cannot be reached through our standard encrypted channels (SSL/TLS) will a message be sent without encryption.

Up-to-date open-source software

We believe in using open-source software, running on an open-source OS. Our entire platform runs on FreeBSD, a high-performance operating system designed with security in mind. We perform regular updates not only on the OS, but also on all software running on that OS — such as Dovecot, Haraka and Qmail, to which we apply the latest security patches.

Irreversibly encrypted passwords

We use bcrypt to hash customer passwords. bcrypt() is an irreversible function, which means the password can never be recovered from the hash data. We support Application Passwords, enabling users to define unique application passwords in order to segregate access, and quickly identify points of entry in case of a suspected security breach. In addition, we provide two-factor authentication (2FA) for all our users, and encourage them to enable it to safeguard their email accounts and control panels.

Vigilant and detailed logging

We routinely review access logs, looking for patterns that may indicate a potential security breach, and proactively warning customers about possibly undesired attempts to access their account (via the Security tab in the Admin Panel). We provide each customer and end-user with access to a "Last Logins" page, which details all recent instances of access to their account.

Zero third-party data sharing

We never share any customer data or metadata with any third party. While we do utilize the Amazon CloudFront content delivery network (CDN) to speed up email load times, this network only processes static content such as images, fonts and javascript files — it never sees the actual content within any email message.

Daily backups and dependable logs

We perform daily backups of all customer data, and retain it for 30 days before destroying it. Metadata logs are retained for a full 180 days. When a customer terminates their account, we retain the data for up to 30 days in case recovery is needed — but upon direct request, we will immediately destroy all data associated with a terminated account.

Secure payment processing

We process all payments through Stripe.com, an encrypted third-party payment processor. We never store, or ask for, any customer's payment details.

Closing words

From physical infrastructure, to software policy, to communication, to staffing, Worksmail is committed to providing users with end-to-end communication security. Our primary goal is to safeguard your data, and our entire organization is designed with this aim in mind.