SAFE & SECURE

How we safeguard your information.

Spark nz | SPARK BUSINESS MESSAGING

Your company creates, collects and communicates valuable data. It holds the trust of customers, staff and vendors and is bound by the law. Here's how we protect that data and maintain your trust.

Why you should trust us?

Our cloud based messaging platform is built to offer highly available, scalable and secure cloud services. We are trusted by large, varied organisations across the world, in a range of critical industries, including; finance, IT, Government, health and education. In 2021 we celebrated 20 years of providing trustworthy, secure, reliable service.

What security measures do we take?

We start with password hashing and salting, least privilege access, security focussed software development and regular penetration testing.

How do we protect access?

Staff access to Spark Business Messaging's platform is limited to authorised personnel, secured with TLS (Transport Layer Security) 1.2, strong passphrases, VPN (Virtual Private Network) and MFA (Multi Factor Authentication). We continually refine these controls to maintain security.

How do we keep our application and your data secure?

Our services are primarily written in PHP, Go and Typescript. These follow security best practices from organisations such as the OWASP Foundation. We continually adopt a privacy and security by design approach that includes a regular cadence to scan the platform for vulnerabilities and remediate findings that impact customers.

How do we protect your data when we rollout improvements?

Changes to our code base go through a suite of automated tests as well as peer reviews before changes are pushed to the production environments.

How do we respond to privacy and security incidents?

We maintain an incident response plan that follows triage, investigation & remediation of incidents. In the event of a breach, affected customers are notified as part of our commitment to security and privacy in accordance with NZ law privacy principles and GDPR.

How secure is our data center?

Our platform is deployed to AWS which has a robust security and compliance program, including controls that are ISO 27001 certified. For more information on AWS processes, please visit: https://aws.amazon.com/compliance/programs/

What other things do we do to protect your information?

Our staff undergo formal security awareness training on hire, complete a criminal and identify check, and are required to report suspicious activity. Our offices are secured via keycard access.

How does our product protect your data?

We provide native in-product protection and mechanisms that give you greater visibility and control over your data. Product users can securely communicate with the platform with SAML 2.0. All data is secured in-flight using TLS 1.2 or greater.

How do we secure your information?

All production data is encrypted at rest with AES 256.

How do we restrict access to your information?

Our platform is a multi-tenant web application. User authentication, logical database separation & session management controls are implemented to restrict access to only your Account.

To learn why some of NZ's leading businesses trust us to deliver intelligent messaging, or for how we can meet your needs, email sparksupport@modicagroup.com or call 0800 776 630 or text 'SBM' to 8526

SAFE & SECURE

How we safeguard your information.

How do we ensure reliability and business continuity?

We offer insights into real-time and historical platform status with a 99.9% uptime commitment to all our customers. Our platform is cloud native and is hosted in AWS Australia across multiple availability zones.

Our platform is built to automatically and securely backup data daily and across multiple AWS availability zones. This is coupled with DR processes to restore services in the event of catastrophic failures.

How do we help protect the privacy of your information?

We're committed to protecting your data and have a robust privacy program that aligns with all applicable regulations. We provide in-product administrative features such as IP whitelisting, fine grained permissions and more that are designed to give you greater control over your data.

How do we maintain the confidentiality of your information?

We treat all customer data as confidential. Access to your data is restricted to only those who require such information as part of their job and only where it is required to provide a specific service to you as a customer.

For how long is your information retained?

We retain your information only for the period necessary to provide services to you as a customer.

How do we preserve data sovereignty?

Our platform is designed to preserve data sovereignty. Your data resides only in AWS Australia and is only accessible by Modica staff and approved-third parties.

What other user access methods do we support?

Managing access to your information plays a key role in making sure that only approved and authorised users have access to your information. We recommend integrating and setting up federation along with Single Sign On (SSO) using your identity platform with ours so that you have complete control over the policies and processes that work best for your organisation like removing access when a staff member leaves, strong password policies and more.

If integrating your identity management isn't an option, we highly recommend switching on two-factor authentication (2FA) paired with strong passwords. This gives you an additional level of protection and keeps the bad guys out. If you'd like more information, talk to one of our Service Delivery Managers who'd be happy to help you.

Can I restrict access so that employees can only access this portal from approved IP addresses?

If you'd like to lock down access to authorised staff from known locations, we also offer the option for you to use IP whitelisting. It's as easy as adding a list of approved IP addresses that are permitted to access the platform. If you'd like more information, talk to one of our Service Delivery Managers who'd be happy to help you.

Still have questions?

Please contact your Account Manager. They will work with our Security team to answer your questions. For general queries, please contact Call 0800 776 630