Rapid Security Customer Statement

This document provides an overview of the security measures implemented to protect the Rapid service, aiming to offer high-level assurance and address common questions. For more specific security inquiries, please get in touch with our security team.

1) Security Accreditations & Compliance

ISO 27001 – Rapid is built on a platform that complies with ISO 27001 requirements, the international standard for information security management systems. This ensures we maintain systematic security controls and risk management processes to protect your data.

GDPR – We comply with the requirements of GDPR, protecting sensitive data with comprehensive data protection measures.

Cyber Essentials – Our platform follows Cyber Essentials requirements, meaning we maintain technical defences approved by NCSC standards against common cyber threats.

NCSC & NIST Compliance – We follow National Cyber Security Centre (NCSC) and NIST cybersecurity framework best practices to maintain robust defences against modern cyber threats, ensuring our security measures align with government-recommended standards.

2) Data Security & Infrastructure

All data is stored securely in UK data centres, ensuring your information remains within UK jurisdiction and meets local data residency requirements. We implement bank-grade security with robust encryption for data in transit and AES-256-bit encryption for stored data, protecting your information throughout its lifecycle. Your data is protected by enterprise-grade cloud infrastructure with access only through secure authentication methods (Microsoft Entra SSO or native MFA), whilst user access operates on the principle of least privilege, ensuring individuals only access data and functions necessary for their role.

3) Access Control & Monitoring

Secure access is enforced through robust authentication policies, supporting both native MFA and Microsoft Entra integration for seamless enterprise security. All systems are continuously monitored with comprehensive audit trails for all activities. We conduct regular security assessments and penetration testing to ensure ongoing protection against evolving threats, providing complete visibility for security analysis, compliance reporting, and incident investigation.

4) Business Continuity & Data Management

Rapid is provisioned on a scalable, high-performance architecture with comprehensive disaster recovery capabilities and secure data backup using resilient infrastructure to ensure reliable service delivery. Clear data retention policies ensure information is kept only as necessary, with secure deletion procedures and data minimisation following privacy-by-design principles. We maintain a comprehensive incident response plan with defined procedures for security incidents, including GDPR-compliant breach notifications.

5) Secure Software Development

We follow secure coding practices and implement security controls throughout the development process, ensuring vulnerabilities are identified and addressed before deployment. All third-party components and libraries are regularly updated and monitored for known security vulnerabilities, maintaining a secure software supply chain. Our development process includes automated security scanning and manual security reviews to identify potential weaknesses before they reach production systems, ensuring Rapid is built with security as a core principle.

6) Network & Infrastructure Security

Our network infrastructure is protected by enterprise-grade firewalls and intrusion detection/prevention systems that monitor and block malicious activity in real-time. We implement comprehensive vulnerability management processes, including regular patch management schedules, to ensure all systems remain protected against known security threats. Physical security measures protect our infrastructure through restricted access controls, whilst our cloud-first approach minimises on-premises security risks by leveraging secure data centre facilities with 24/7 monitoring and environmental controls.

7) Operational Security & Risk Management

All staff undergo thorough background checks and receive regular security awareness training to maintain high security standards and recognise potential threats. We conduct comprehensive third-party risk assessments for all vendors and suppliers, ensuring our security standards extend throughout our supply chain through strict contractual arrangements. Business continuity is validated through regular disaster recovery testing schedules, ensuring our recovery procedures remain effective and our high availability commitments can be met during various failure scenarios.