Signal365

Signal365 – Security Policy

Version 1.0 – January 2026

1. Purpose of This Policy

This policy provides a high-level overview of how Signal365 approaches security.

It is intended for customers and procurement teams and does not disclose sensitive internal controls or implementation details.

2. Security-by-Design

Signal365 is designed with security as a core principle, including:

Least-privilege access

Tenant isolation

Defence-in-depth

Secure defaults

We aim to minimise the amount of data accessed and stored while still delivering meaningful insights.

3. Infrastructure & Hosting

Signal365 is hosted on secure, reputable cloud infrastructure, including:

Microsoft Azure

Managed database and storage services

These platforms provide:

Physical security controls

Redundancy and resilience

Regular security patching

4. Data Protection

We apply reasonable technical and organisational measures to protect data, including:

Encryption in transit (TLS/HTTPS)

Encryption at rest where supported by underlying services

Secure key management practices

Segregation of customer data

5. Access Controls

Access to Signal365 systems is restricted and controlled through:

Role-based access controls

Least-privilege permissions

Strong authentication methods

Limited administrative access

Access is reviewed and adjusted as required.

6. Monitoring & Logging

We monitor Signal365 for:

Availability issues

Security events and anomalies

Errors and unexpected behaviour

Logging is used to support:

Incident detection and response

Troubleshooting and reliability improvements

Audit and accountability

7. Third-Party Security

Signal365 relies on third-party providers (such as Microsoft and Stripe) to deliver parts of the service.

We:

- Select reputable providers with strong security practices
- Rely on their certifications and compliance programmes
- Monitor integrations and dependencies for risk

8. Vulnerability Management

We take a proactive approach to security risks by:

- Applying updates and patches in a timely manner
- Reviewing platform changes for security impact
- Investigating reported vulnerabilities

Responsible disclosure of security issues is encouraged via: support@signal365.co.uk

9. Incident Response

If a security incident occurs:

- We investigate promptly
- Take steps to contain and remediate
- Communicate with affected customers where appropriate

Incident handling is covered in more detail in our Incident & Breach Notification Policy.

10. Compliance & Standards

Signal365 is designed with recognised security standards in mind, including:

- UK GDPR principles
- ISO 27001-aligned practices

- Microsoft security baseline concepts

This does not imply formal certification unless explicitly stated.

11. Customer Responsibilities

Customers are responsible for:

- Securing their own Microsoft 365 tenant
- Managing user access and permissions
- Protecting their account credentials
- Reviewing outputs and acting responsibly

Security is a shared responsibility.

12. Changes to This Policy

We may update this policy from time to time.

If changes are material, we will provide reasonable notice.

Continued use of Signal365 means you accept the updated policy.