Signal365

Signal365 – Incident & Breach Notification Policy

Version 1.0 – January 2026

1. Purpose of This Policy

This policy explains how Signal365 responds to security incidents and data breaches, and how we communicate with customers when an incident may affect them.

It is designed to set clear expectations without creating unnecessary alarm.

2. What Is an Incident?

An incident may include:

- Unauthorised access to Signal365 systems
- Loss, disclosure, or alteration of customer data
- Service disruption caused by a security event
- Confirmed or suspected data breaches

Not all incidents result in a data breach.

3. Incident Detection & Investigation

When an incident is suspected or detected, we will:

- Investigate promptly
- Assess the scope and impact
- Take steps to contain and mitigate the issue
- Preserve relevant logs and evidence where appropriate

4. Breach Assessment

If an incident involves personal data, we assess:

- The type of data involved

The number of affected individuals or tenants

The potential risk to individuals' rights and freedoms

Whether notification is required under UK GDPR

5. Customer Notification

If a breach is likely to result in a risk to customers or individuals, we will:

Notify affected customers without undue delay

Provide a summary of what happened

Describe the data involved (where known)

Outline actions taken or planned

Share recommended customer actions (if applicable)

Notifications will normally be provided by email or through the platform.

6. Regulatory Notification

Where required by law:

We will notify the Information Commissioner's Office (ICO)

Notifications will be made within required timeframes

We will cooperate with regulatory authorities as necessary

7. Third-Party Incidents

Signal365 relies on third-party services such as Microsoft and cloud infrastructure providers.

If an incident originates from a third party:

We will monitor their response

Assess any impact on Signal365 customers

Communicate relevant information where customers are affected

8. Customer Responsibilities

Customers are responsible for:

Securing their own Microsoft 365 tenant

Monitoring access to their accounts

Promptly reporting suspected security issues

Security concerns should be reported to: security@signal365.co.uk

9. Post-Incident Review

After a significant incident, we may:

Review root causes

Improve controls or processes

Update policies or procedures

Implement additional safeguards

10. Relationship to Other Policies

This policy should be read alongside:

Security Policy

Privacy Policy

Terms of Service

If there is any conflict, the Terms of Service take precedence.

11. 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.