[MSP LOGO]

[MSP name]
SECURITY ASSURANCE

CLIENT POSTURE BROCHURE

Prepared by [MSP name] for managed Microsoft 365 customers.

Your Microsoft 365 security posture, monitored continuously by *[MSP name]*.

Read-only. UK-hosted. Designed for ongoing assurance, not one-off audits.

01 WHAT [MSP NAME] IS DOING FOR YOU

[MSP name] uses a continuous control assurance platform to monitor your Microsoft 365 security posture, scan after scan. The platform looks at how your security controls are actually configured, where the meaningful gaps are, and what changes between reviews.

The point is not to add another tool to your stack. It is to give [MSP name] a clearer, more structured view of where your Microsoft 365 environment stands today, so the conversations you have together about security are grounded in current evidence rather than scattered admin-centre screenshots or quarterly spreadsheets.

02 WHAT YOU WILL SEE

Posture reports
A regular summary of where your Microsoft 365 security controls stand, delivered by [MSP name] on the cadence you have agreed.

Prioritised remediation requests
When something needs attention, [MSP name] explains what, why, and what is being done about it.

Drift and change summaries
If your Microsoft 365 configuration changes between scans, [MSP name] can see it and follow up.

Framework readiness summaries
Useful when your clients, insurers, or auditors ask security questions.

03 READ-ONLY BY DESIGN

The platform [MSP name] uses a read-only connection to your Microsoft 365 environment. It does not modify your Microsoft tenant in any way.

Any remediation work is planned and executed by [MSP name], with your authorisation, in the relevant Microsoft admin centres. The platform's role is to provide visibility, evidence, and workflow support. The decisions and the work remain with the people who own them.

UK-hosted
Data held in the UK environment.

ICO registered
Operated with UK data protection registration.

Read-only
No tenant changes made by the platform.

Regular reporting
Current posture evidence on an agreed cadence.

04 WHY THIS MATTERS

The security questions your business gets asked are changing. Customers, insurers, procurement teams and internal stakeholders now expect current evidence about how Microsoft 365 is being managed, rather than annual assurance statements.

Microsoft 365 itself is not static. Users join, apps gain permissions, guest accounts arrive, admin policies are edited, conditional access rules change. A review done three months ago does not answer today's question.

Continuous monitoring lets [MSP name] spot changes early, explain them, and put them on the agenda for your next review. It also produces a record of where your posture stands and how it has improved over time.

05 WHAT THIS IS NOT

- Not a compliance certificate.
- Not a replacement for formal audit, certification, or legal advice.
- Not an automatic remediation engine.
- Not a tool that changes your Microsoft tenant.
- Not a broad assessment of non-Microsoft platforms.

06 HOW THE EVIDENCE HOLDS UP

> ScanPosture shows alignment and readiness against selected technical controls. It does not itself certify compliance or replace formal assessment, certification, or legal advice.

- The platform supports readiness and evidence conversations with clients, insurers, procurement teams, and your own audit or risk reviewers.
- Framework views are bounded to observable technical controls. Each one names what it covers and what it does not.
- People, physical security, organisational policy and similar areas cannot be observed from Microsoft 365 configuration, and the platform does not claim to assess them.
- Where a control cannot be read automatically from Microsoft APIs, you may be asked to confirm it through an attestation workflow.

07 WHO TO ASK

[MSP name] service desk

For findings, remediation, reporting, or service scope questions.

SUPPORT	**[MSP support contact]**
WEB	**[MSP website]**