Client Security Statement

Revision	Details of Amendments/Additions	Date	Who
V002	Section name changes, addition of Perimeter Vulnerability Scanning and Hybrid SOC	29/07/2024	Russell Gower-Leech

As your trusted IT partner, it is vital that our own security standards and procedures mesh with your business. Security is a complex topic which needs a layered (or defence in depth) approach.

This statement outlines the tooling, services, and policies we provide to help protect your business.

Tooling and services

As a WorkTogether customer we provide the following to your business:

Automated Windows Patch Management	While patching helps to add new functionality or address bugs, it is also a powerful security tool, closing identified vulnerabilities before they can be exploited.
Managed anti-virus & ED	We help to ensure all your business assets are protected by a centrally managed AV and EDR solution, providing greater visibility into potential security events and ensuring that it is always on, always up to date and that detected threats are investigated and resolved before they negatively impact the business
Web filtering	Many threats including malware, phishing, botnets and ransomeware rely on DNS based services or luring your staff to unsafe locations on the web. By providing protective services we can significantly reduce the likelihood of these threats landing at all, as well as their impact should they slip through the net.
Perimeter Vulnerability Scanning	Identify and close external vulnerabilities before they are exploited. An alarming number of security incidents come from ports and services which have either been left open by accident or potentially opened by a malicious actor as part of their attack.
Hybrid SOC	We work with a dedicated 24/7 Security Operations Centre (SOC) to ensure there is a second set of trained eyes reviewing security telemetry from the tooling and services we provide to protect our clients

	infrastructure. This enhances: Intrusion Detection - Identify potential intrusions. No one layer is fool proof and the bad guys may get into your network. Being able to detect this presence allows you to both eject these intruders but also more crucially identify how they entered so that gap can be closed Threat Hunting - Human operators working round the clock with machine learning to identify security incidents and provide clear remediation steps to stop issues in their tracks.
Staff Security Awareness Testing andTraining	Technology is a fantastic tool but is not infallible. Providing testing and training helps sharpen a business's best last layer of defence – its staff. Testing and training keep the threat front of mind in small manageable chunks.
Dark Web Monitoring	Passwords are the keys to the kingdom, but sadly they are often lost, copied, or stolen. We monitor Dark Web forums looking out for possible password leaks so our clients can update their passwords before they are misused.

Security policies

As a business we understand that our clients and their data are our crown jewels, we have a robust set of policies and procedures which govern our staff and ensure they do their utmost to keep our clients protected.

ID and DBS Checks	Starting from the recruitment phase, all staff are vetted in line with current employment law, with relevant ID checks. We also carry out DBS checks for all technical staff that may visit client sites.
Non-Disclosure Agreements	All staff are required to sign a company NDA.
Role-Based Access	We have a 'role-based access' policy ensuring staff are granted the minimum system access required to perform their specific roles.

Password Management and Multi-Factor Authentication	We continually employ and refine strict policies when it comes to password management and MFA, secure data handling and device management, ensuring our staff undergo security awareness training as well as specific technical training.
Annual Audits	The business is audited annually for both ISO 27001 and Cyber Essentials, but we also live by these standards' day in day out.
Security Operations Centre	We also utilise an independent SOC service to ensure there is a second set of trained eyes reviewing the security telemetry of our infrastructure.

All of this helps to ensure we protect our clients and can offer them the very best advice and services when it comes to security best practices.