



SECURITY CONTROLS AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY AND PRIVACY OF DATA

Tivarri manages risks to our information systems, data and operations through a comprehensive framework incorporating a substantial range of security measures and controls aligned with recognised industry practices. These controls support our own security posture and demonstrate the extensive standards and capabilities we apply when helping clients strengthen the security and resilience of their IT environments. Our areas of control are:

Devices and Network

Perimeter Layer Protection

- Dedicated on-site security appliances are deployed and managed where required, with centrally managed firewall controls restricting unauthorised external access and supporting secure VPN connectivity for remote users.
- Firewall rules and traffic policies are centrally maintained in accordance with defined operational and security requirements.
- Network traffic and security events are centrally logged. Firewall and network security configuration changes are reviewed and recorded through the change management process.

Endpoint Protection

- Microsoft Defender for Endpoint provides continuous Endpoint Detection and Response (EDR) across managed PCs and laptops for malware, ransomware and suspicious activity.
- Security detections generate alerts to the Tivarri Helpdesk and, where applicable, the client. Containment and response actions are initiated through the EDR platform.

Mobile Device Management (MDM) through Microsoft Intune

- Microsoft Intune app protection policies separate corporate data from personal applications and restrict transfer of business information to unmanaged storage, personal email and other unauthorised applications.
- Mobile device storage encryption and minimum six-digit PINs are enforced.
- Selective wipe removes corporate data from enrolled mobile devices without deleting the user's personal information.

Identity and Access

Logical Access

- Access to corporate systems and information is governed through Microsoft Entra Conditional Access policies.
- Multi-factor authentication (MFA) or passkeys are enforced across user accounts, with additional access restrictions applied through device trust, geographic and risk-based Conditional Access policies where configured.
- Single Sign-On (SSO) integrates supported third-party applications with the customer's Microsoft identity, inheriting tenant-level authentication and access controls.
- High-risk authentication attempts can be blocked automatically and escalated to the Tivarri Helpdesk. Third-party application access is controlled through Microsoft tenant permissions and policies.

Password Controls

- Password requirements are centrally enforced in accordance with the organisation's security policy, with MFA or passkeys providing an additional authentication layer beyond username and password credentials.
- Repeated unsuccessful authentication attempts are subject to automated throttling and account-lockout controls to mitigate password-guessing and brute-force attacks.

Secure Foundations

Physical and Environmental Security

- Client information is hosted within Microsoft data centres operating to ISO 27001 and SOC 1 Type 2 and SOC 2 Type 2 information security management standards.

- Client data hosted in Tivarri's UK data centres meet both ISO 27001 and Cyber Essentials standards.

Cloud Data Storage

- Client data hosted within Microsoft 365 services, including email and SharePoint, is typically stored within the UK and replicated to a secondary Microsoft data centre multiple times per hour.
- Microsoft 365 data can be backed up outside the Microsoft environment to a Tivarri UK Sovereign data centre¹, providing separation between primary and backup infrastructure.
- Timed recovery testing is available to demonstrate actual data restoration times and provide Mean Time to Recovery (MTTR) evidence for audit purposes.

Encryption

- Managed devices are protected using Microsoft BitLocker with AES-256 encryption.
- Microsoft 365 data is encrypted at rest using AES-256 and in transit using TLS 1.2.
- Backup data is encrypted using AES-256 and stored on infrastructure isolated from the Microsoft environment, with separate authentication controls and encryption keys.

Threat Prevention

Email Security

- Microsoft Defender for Office 365 analyses email attachments within an isolated Microsoft environment prior to delivery.
- Safe Links performs time-of-click inspection of URLs contained within email messages.
- External auto-forwarding is blocked by default, and messages originating outside the organisation are identified through external sender tagging.

URL and Web Filtering

- Microsoft Defender for Endpoint web content filtering restricts access to malicious and inappropriate content, including specified website categories such as personal email and file-sharing services.
- Microsoft Defender Safe Links performs time-of-click URL inspection and blocks access to destinations identified as unsafe after message delivery.

- Web filtering and URL inspection controls are applied to reduce exposure to malicious and emerging web-based threats.

Detection and Assurance

Independent Penetration Testing

- Independent third-party penetration testing is conducted weekly against Tivarri data centre infrastructure and client environments hosted within Tivarri facilities. Findings are reviewed through the vulnerability management process.
- Full-scope penetration testing with formal reporting is available for client environments to support insurance, audit and compliance requirements.

Vulnerability Management

- Microsoft Defender Vulnerability Management continuously assesses managed devices and software for known vulnerabilities and security exposures.
- Remote Monitoring and Management (RMM) software is used to deploy patches to PCs, laptops and servers at least weekly and identify systems with missing security updates.
- Out-of-cycle patching can be initiated through the RMM platform where an imminent security threat requires immediate remediation.



Security Monitoring

- Identity Threat Detection and Response (ITDR) detects, investigates and mitigates identity-based attacks in real time. Where supported by client licensing, Microsoft Risky User and associated risk-based controls identify suspicious user and sign-in activity. Predefined risk thresholds or behaviour patterns can trigger automated remediation, access blocking and Tivarri investigation.
- XDR (Extended Detection and Response) collects data from endpoints, networks, cloud services, email, SaaS applications and identity systems for real-time detection, investigation and response. Analytics, AI and machine learning identify anomalies, suspicious patterns and attack techniques across correlated security data. In customer environments, XDR can combine Defender for Endpoint telemetry with Microsoft Exchange email-flow data and Entra ID access logs.
- Risk-based Conditional Access policies can apply additional authentication requirements, including MFA, where access is assessed as suspicious or unusual.
- Identity Security Posture Management (ISPM) is available as an optional service, providing continuous assessment of Microsoft 365 identities, access rights and configurations.
- Cloud Security Posture Management (CSPM), provided as part of Tivarri's SOC services, continuously monitors customer cloud environments for misconfigurations, compliance gaps and security risks.
- 24/7 Security Operations Centre (SOC): Tivarri's standard services use automated rules to block account access when predefined threat-risk thresholds are met. The optional 24/7 SOC provides continuous human-led review and response by security specialists as part of the wider Identity Threat Detection and Response (ITDR) posture.

Governance and Resilience

Backup Verification and Recovery Testing

- Backup data can be manually restored by an engineer to verify successful recovery.
- Backup and restore procedures are tested quarterly to verify backup integrity and recoverability.

- Quarterly recovery testing is documented through formal test reports providing evidence of successful restore validation.

IT Change Management

- System and service changes are managed through a formal ticketing process, providing an auditable record of the request, action and associated timeline.
- Changes requiring client approval are restricted to authorised client contacts.
- Changes to client environments are controlled and traceable through the change management process.

Business Continuity and Disaster Recovery

- Tivarri maintains documented Business Continuity and Disaster Recovery arrangements within its ISO 27001 Information Security Management System (ISMS).
- Recovery procedures are manually tested twice yearly, with automated backup and recovery checks performed daily to verify backup integrity and recoverability.

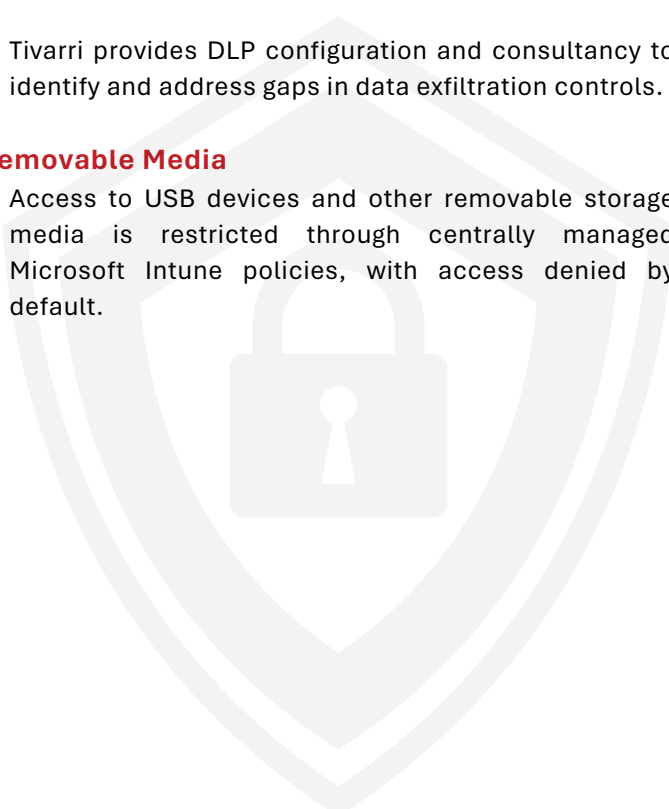
Data Protection

Data Loss Prevention (DLP)

- DLP controls are configured to prevent or detect unauthorised data exfiltration, including transmission of tagged documents to external recipients or upload to external websites.
- Tivarri provides DLP configuration and consultancy to identify and address gaps in data exfiltration controls.

Removable Media

- Access to USB devices and other removable storage media is restricted through centrally managed Microsoft Intune policies, with access denied by default.



People

Cybersecurity Awareness Training

- Cybersecurity awareness training is available as an optional service, covering phishing, social engineering and credential compromise.
- Training is delivered online or in person using practical scenarios and can be tailored to organisational requirements.
- Completion certificates are valid for 12 months.

Certification and Accreditations

Independent Assurance

- Tivarri holds ISO/IEC 27001:2022 (Certificate No. 291512018) and Cyber Essentials.
- Tivarri is a Certified B Corporation.
- Tivarri is an approved supplier on the UK Government's G-Cloud 15 framework.



HM Government
G-Cloud
Supplier



¹Tivarri provides secure UK-based data centre infrastructure, enabling organisations to keep data within the UK while supporting compliance, resilience and greater control over data residency.