Microsoft Security & Governance Services

G-Cloud 15 — Terms & Conditions

Supplier: Inetum Digital Services UK Ltd

Services overview

Design, implement and operate Microsoft-centric security services across identity (Entra), threat protection (Defender XDR), SIEM/SOAR (Microsoft Sentinel), information protection and compliance (Purview), and cloud posture (Defender for Cloud). Services include assessment, architecture, deployment, integration, governance, MDR/SOC operations, incident response, Security Copilot enablement, and continual improvement.

Service scope and activities

Security strategy, Zero Trust roadmap and architecture assurance.
Entra ID: IAM design, identity governance, access reviews, lifecycle.
Defender XDR: deployment, tuning, hunting, incident response and containment.
Microsoft Sentinel: SIEM design, data onboarding, analytics, SOAR runbooks.
Purview: information protection, DLP, Insider Risk, records management.
Defender for Cloud: policy, posture management, workload protections.
Vulnerability management and secure baseline hardening coordination.
Security Copilot: use cases, guardrails, operational integration and training.
Adoption and change: role-based training, playbooks, comms and champions.
Operations: monitoring, MDR/SOC, service reviews and continuous improvement.

Data backup, restore and disaster recovery

Security platforms are Microsoft SaaS or PaaS services with built-in data durability. We document and evidence restore procedures (e.g., Sentinel workbooks/analytics, Purview policies/labels) and establish runbooks for configuration export, versioning and rehydration. Where workloads rely on Azure services, we apply Azure-native backup/DR patterns under change control.

Onboarding and offboarding

Onboarding: kick-off, RACI, access model, toolchain setup, telemetry baseline and data connectors.
Offboarding: artefact and configuration handover, documentation, knowledge transfer, access revocation and exit report.

Service constraints

Remote-first delivery; on-site support subject to Buyer facilities access and vetting. Requires active Microsoft licences (Entra, Defender, Sentinel, Purview). SIEM outcomes depend on available telemetry and connectors. Data residency follows Buyer tenant region; security aligned to NCSC principles under Call-Off. Cyber Essentials compliance applies. SLAs assume timely approvals, SME availability and required integrations.

Service levels (performance, availability, support hours)

Essential: UK business hours; L2/L3 across Entra, Defender, Sentinel, Purview; portal/email/Teams; triage and monthly reporting.
Enhanced: adds L1 triage, extended hours, co-managed Sentinel, hunting, vuln mgmt coordination; named Security Service Manager; weekly/monthly reviews.
Premium: 24×7 P1/P2; SOC/MDR, SOAR playbooks, on-call engineering; quarterly exercises and AI-safety reviews; optional forensics retainer.

After-sales support and governance

A named Security Service Manager runs governance, KPI reporting, risk/issues, roadmap and continuous service improvement. Includes release notes, KEDB/runbook updates, and enablement refreshers.

Technical requirements

Buyer tenant(s) and relevant Microsoft security licences/subscriptions.
Administrative access model; just-in-time elevation and audit logging.
Connectivity for hybrid/on-prem telemetry; firewall and proxy allowances for connectors.
Access to ticketing/CMDB; optional case integration with Sentinel/Defender.
Evidence sources for compliance reporting (e.g., audit logs, asset inventories).

Outage and maintenance management

Planned changes follow change control with maintenance windows and defined rollback. Emergency changes use expedited approvals with post-implementation review. Microsoft advisories are monitored; regressions are tested in non-production before phased deployment.

Hosting options and locations

Microsoft security services are Microsoft-hosted SaaS/PaaS; no customer infrastructure to manage. Data residency follows the Buyer tenant region. Government-cloud options may be available subject to eligibility.

Access to data (upon exit)

Buyer retains ownership of data and configurations. We support structured exports (analytics rules, workbooks, hunting queries, policies, labels) and hand over documentation, scripts and runbooks. All Inetum access is revoked with evidence.

Security

Least-privilege RBAC, MFA and Conditional Access; privileged access workstations recommended.
DLP and information protection policies; data minimisation and secure collaboration controls.
Audit, logging and alerting integrations; Customer Lockbox where enabled.
Personnel screening aligned to Buyer requirements; supplier oversight of sub-processors.

Roles, responsibilities and support levels

Service delivered by L1 SOC (optional), L2 Security Engineers, L3 Security Architects/Threat Hunters, and a named Security Service Manager. Responsibilities are defined in the onboarding RACI and Call-Off.

Service reporting and continual improvement

Monthly/quarterly reviews covering SLAs, incidents, threat trends, change success, vulnerability posture, compliance status and adoption/usage, with a prioritised improvement backlog (automation, resilience, coverage, value realisation).

Accessibility

Buyer-facing artefacts are available in accessible formats. Templates follow WCAG 2.1 AA guidance where applicable; we provide inclusive training and documentation.

Assumptions and dependencies

Timely Buyer decisions/approvals and SME availability.
Access and licences granted on schedule; data sources and connectors enabled.
Non-functional requirements (security, DR, performance) agreed and reviewed annually.

Pricing model

Projects: fixed-price based on scope, deliverables and timeline. Managed services: time & materials against the G-Cloud rate card, with optional reserved capacity and SLAs. Expenses and VAT follow Framework rules.

Contact and ordering

Available via the Digital Marketplace under G-Cloud 15. Framework Agreement and Call-Off govern, with service-specific terms applied as applicable. For queries, contact your Inetum account manager or the assigned Security Service Manager.

.