



2026 Charter and Terms and Conditions

This Charter sets out what CM Security Ltd will do for you, what we need from you and the terms and conditions that apply to every product, subscription and service we supply. It replaces all documents of its type including our 2025 Charter and fees

Who we are:

CM Security Ltd is an independent managed security service provider based in London. We supply, configure and support email security, web security, cloud application security, encrypted backup, compliant archiving and security awareness training from the vendor partners listed at www.cmsecurity.co.uk. Our managed services run on annual, and multi-year contracts paid in full and advance. Multi-year contracts can alternatively be paid annually in advance

Our accreditations:

- **Cyber Essentials.** CM Security is authorised to deliver Cyber Essentials, the UK Government-backed scheme that protects organisations against the most common cyber-attacks. We prepare you for assessment, fix the gaps we find and take you through to certification.
- **ISO/IEC 20000.** Our IT service management is certified to the international standard.
- **G-Cloud.** We are an approved supplier on the Government Commercial Agency (GCA) frameworks, Currently G Cloud 15 so public sector customers can buy from us without a separate tender.
- **Microsoft Partner.** Our engineers work within Microsoft's certification programme.

This charter covers vendor product support supplied with product contracts. Our management fees can be bundled with vendor product or taken separately and cover social engineering protection, identity protection and Security Operations Centre (SOC) monitoring.

What we protect you against

Protection against social engineering, that often leads to brand damage, identity theft or Ransomware, is our priority. Most attacks on organisations like yours don't start with a technical break-in. They start by tricking a member of staff, and end with a stolen identity or criminals trading on your name. Our services are built to break that chain at each step.

Social engineering

Phishing, fake invoices, business email compromise and criminals posing as your directors or suppliers, increasingly using AI-generated email, voice and video. We counter this with email security that detects impersonation, security awareness training with simulated phishing, and advice on payment checks so one convincing email can't move money.

Identity theft and account takeover

Stolen passwords and hijacked Microsoft 365 accounts expose your data, contacts and bank details. We protect identities with multi-factor authentication, Zero Trust checks on every user and device, and SOC monitoring that alerts on unusual sign-ins.

Brand damage

A spoofed email in your name, a lookalike domain or a publicised breach can cost you customers long after the fix. We lock down your email domain against spoofing (SPF, DKIM and DMARC), keep encrypted backups and archives so you can recover and show what happened, and take you through Cyber Essentials so customers and insurers can see you meet a recognised standard.

These services reduce your risk. No provider can remove it entirely, and our liability is set out under Liability and your responsibilities below.

Our Service and Consultancy

Our engineers are certified systems engineers with more than 20 years' experience, working within Microsoft's certification process. Your requests go straight to engineers who know the products and your network.

We are independent of any single vendor, so our recommendations are based on your budget, your business fit and how easy a product is to own and run. We deal with you honestly, keep your information confidential and tell you what to expect before we deliver it.

We are advocates of Zero Trust networking, where no user, device or connection is trusted until it has been verified. We lead workshops that guide your team through adopting Zero Trust and getting the most from it, from mapping who needs access to what, through to rolling out access controls in stages without disrupting your users.

Consultancy covers the full cycle: recommendations, product demonstrations and proof-of-value trials, deployment and ongoing support. We work as a co-managed security resource alongside your IT team, covering Zero Trust Network Access, SOC monitoring, MDR and SASE. We recommend a review at least once a quarter, including perimeter and supply chain risk.

When we visit your premises we follow your site rules, and before any work we tell you how long it will take and what disruption to expect.

Confidentiality and Data Protection

We protect your confidential information and personal data in line with UK GDPR, the Data Protection Act 2018 and the requirements of the government frameworks we supply under, including G-Cloud. Where we process personal data on your behalf, we do so only on your written instructions.

Your ideas and plans are your business advantage. We won't use our position to gain an advantage for ourselves or anyone else, or to your detriment. Our Privacy Policy, Subject Access Request Policy and GDPR Compliance Statement are published at www.cmsecurity.co.uk.

Support

We offer two levels of support. Tier 1 comes with every product subscription. Tier 2 is included in our chargeable Managed Service and is what we recommend.

Tier 1 level - Self-Managed Support

- Customer manages all configurations independently.
- Access to the Knowledgebase for self-service troubleshooting.
- Ticket portal available for bug fixes and service outages.

Tier 2 level - 9x5 Support (Recommended)

- Email and Telephone Support available 9x5 (Monday to Friday).
- Assistance with configuration issues beyond standard troubleshooting.
- Ideal for businesses that need direct access to support during working hours. SLA in appendix I below
- Direct access to 2nd line technicians provided for product and product in the network from cm security ltd. Support requests are not triaged by junior staff
- Quarterly Consultancy on site visits concerning emerging technology such as ZTNA, Perimeter defence, MDR, 24/7 SOC monitoring and SASE

Tier Two Support services premier grade services as defined above. Cover for matters relating to Remote Connectivity and App Protection; Adaptive Defence; Continuous Security Validation and Compliant Archiving are offered as additional services and charged separately.

We reserve the right to charge fees for on-site support and particularly charge fees where emergency call out is requested. Our services include AI security protection includes but is not restricted to attack mitigation, Microsoft Federation Services, Remote working, O365, Identity Services and Security Breach and Attack Simulation.

Training is encouraged. Training is charged separately. Security Awareness Training is proven more appropriate than support. Security Awareness Training is subscription based as SaaS. AI awareness and how to stop maximise the use of tools such as Open AI, Gemini, ChatGpT, Claude, CoPilot and the difference between Enterprise version of AI and privately subscribed AI that threatens Zero Trust

Support cover for devices or systems which do not form part of the business network (such as personal computers used from time to time for work access) is not provided without charge.

The defined levels of support form part of a comprehensive cover under our Managed Service under annual subscription and paid monthly

Service Levels

Our support lines are open 09:00 to 17:30 (UK time), Monday to Friday, excluding bank holidays. Email requests sent outside these hours are logged and handled from the start of the next business day. Log requests at support@cmsecurity.co.uk or for Tier 2 by phone on 0203 307 0370.

We acknowledge every ticket on receipt. The targets below apply to Tier 2 and measure the time until an engineer starts work on your issue. They are response times, not resolution times.

Issue Level	
Category	Description
Severity A (Critical)	Infrastructure outage on the network , service disruption on the network. Network, not available and no workaround exists.
Severity B Degraded (High)	The network service is usable but degraded. Significant reduction experienced in network performance
Severity C General (Medium)	A problem, which outside of the expected operation of the network but causes only minor inconvenience to the customer, requests for information, service requests or feature requests. Failure of one or more system functions making use of the systems difficult (eg service still running and operational, but not at full capacity)

SEVERITY LEVEL	Hours (GMT) Business Days	Standard Support and Target response
SEV A (Critical)	09.00 to 17.30	4 business hours. This is response to the issues defined above
Sev B degraded (High)	09.00 to 17.30	6 business hours
Sev C General (Medium)	09.00am to 17.30	24 business hours

Subscriptions, renewals and termination

A subscription to any of our services entitles you, for the subscription period, to Tier 1 support, free software updates, and offers to buy add-ons and upgrades. An update is a minor change that corrects errors or adds patches, bug fixes or small improvements. An upgrade is a new version or added functionality and may be charged.

All subscriptions, including Managed Services, consultancy and support, renew automatically for the same term. To stop a renewal you must give us written notice at least 90 days before the renewal date.

Products supplied by our vendor partners are also subject to the vendor's own licence terms.

Fees and Payments

Support, Consultancy and Managed Services are professional services. They are invoiced and paid directly to CM Security Ltd, separately from product subscription fees, including where products are ordered through G-Cloud or another government framework.

Prices are set according to your requirements. All prices exclude VAT.

Item		Charge
Professional Services		Min £5000 a year, paid in full before contract start date
Managed Service		Annual Contract, payable monthly.
Emergency call out		Minimum £1,500 a day, plus travel and any overnight costs at cost

Liability and your responsibilities

Security is shared. For our services to work, you agree to:

- give us accurate, complete and timely information about your systems and any incident
- tell us promptly about changes to your network, users or suppliers that affect our services
- act on our security recommendations, or tell us in writing that you have chosen not to
- make sure your staff follow your security policies and complete the training you buy

Our services reduce the likelihood and impact of attacks, including social engineering, identity theft and damage to your brand. They cannot guarantee that no attack will succeed.

We are not liable for indirect or consequential loss, loss of profit, revenue, data or goodwill, or damage to reputation. Nothing in these terms limits liability for death or personal injury caused by negligence, for fraud, or for anything else that cannot be limited by law.