SERVICE DEFINITION
PHYSICAL SECURITY TESTING

Our address
Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

Give us a call
0333 939 8080

Send us a message
hello@jumpsec.com

Find out more
www.jumpsec.com

About JUMPSEC

JUMPSEC is a UK-based cyber security consultancy, established in 2012, with a proven track record in offensive testing, incident response, managed detection, and advisory services for both public and private sector organisations. Our work is led by skilled professionals with extensive experience in red teaming, security engineering, and incident response, ensuring that our services are rooted in real-world knowledge and practical expertise.

We place a premium on assurance. Our teams include CHECK and CREST-qualified penetration testers, as well as NCSC CIR-approved incident responders and NCSC CIE-accredited Incident Managers, enabling us to deliver a wide range of government-level security engagements. We have deep experience deploying and managing Microsoft security technologies such as Microsoft Defender and Sentinel, particularly within regulated environments. Our approaches and documentation are consistent with recognised standards including the NIST Cyber Security Framework, CIS Controls and CAF, and our reporting is clear and purposeful, catering to both technical specialists and executive decision-makers.

Clients use JUMPSEC to achieve three outcomes:

- **to reduce the risk of significant security incidents**
- **to speed up the detection and containment of threats, and**
- **to demonstrate robust governance to stakeholders such as boards, auditors, and insurers**

Our services are transparent and collaborative—clients are given clear scopes, well-defined engagement terms, daily updates during testing, and strong evidence to support their security posture. We prioritise remediation advice based on business impact, not just automated scan results.

Protecting client data is at the heart of our operations. JUMPSEC acts as a data processor under UK GDPR and DPA, adheres to principle-of-least-privilege access, and only retains evidence for periods agreed with clients. Where necessary, our personnel hold BPSS or SC clearance, and we can provide reports and artefacts in accessible formats to meet WCAG 2.1 AA standards.

Our public sector experience covers central and local government, healthcare, education, and critical national infrastructure. In the private sector, we support clients in finance, manufacturing, logistics, and technology. We often deliver projects alongside complementary services, such as red and purple teaming, detection engineering, and incident response retainers, to drive measurable improvements and tangible returns.

We continually refine our services to address the evolving needs of our clients, frequently developing tailored solutions to unique challenges. Our approach is adaptable and shaped by each client's specific situation, so the best way to understand how we can help is to discuss your needs directly with us before RFP release.

This overview outlines JUMPSEC's broad capabilities and demonstrates how our expertise can be applied to deliver practical, threat-focused security for your organisation. To find out more about how we can address your cyber security requirements, please get in touch for a straightforward conversation.

Example use cases

Local authority — Civic centre access via public events route

We conducted reconnaissance to track footfall during a public consultation at the civic centre. JUMPSEC entered with display materials, followed event stewards past reception, and reached the back-of-house corridors without a badge. We used a side stairwell to access a floor located near democratic services. We identified a comms cupboard secured by a generic euro-cylinder and found a disposal trolley containing unlocked laptops awaiting a wipe. Staff offered directions but did not challenge our movement or check our lanyard status.

To remediate these issues, JUMPSEC formalised event routing using barriers and staffed checkpoints, required visible visitor passes beyond reception, and relocated back-of-house stairwell exits behind controlled doors. We upgraded plant-room cylinders to a restricted profile and locked interim asset trolleys. Our security team conducted spot checks during evening sessions. During a verification walk-through, we consistently checked badges, secured plant areas, and controlled access throughout public events.

Airport operator (CNI) — Contractor routes and device planting risk

During reconnaissance, we observed that contractor entrances led directly to technical areas, with only light supervision during tool drops. JUMPSEC testers, dressed in contractor PPE, entered with a small toolkit and reached a network cabinet in a mezzanine corridor. We placed a benign, tagged device on an unused switch port for a timed interval and later retrieved it under observation. No one raised any alerts or challenged our presence.

To remediate, JUMPSEC introduced asset quarantine for unregistered devices, enforced port security and NAC on technical networks, and required electronic work orders at contractor turnstiles. We also added patrols with unpredictable routes. During a verification check, we observed port security events and saw appropriate intervention when making a controlled placement attempt.

National charity — HQ reception and post-room crossover

We presented a tester as a volunteer and directed them to the post-room for induction forms. The post-room connected to back-of-house corridors and an unlocked stationery store where we found surplus laptops awaiting disposal. We also discovered an unattended hot-desk with a logged-in device. Staff only offered friendly directions and did not challenge our movement.

To address these issues, JUMPSEC separated public-facing and back-of-house routes, locked interim asset stores, and mandated screen-locks with rapid timeouts on hot-desks. We provided reception with a concise challenge script for anyone moving without a badge. When we conducted a short re-run, we observed correct routing of volunteers and secured asset areas.

Service Overview

JUMPSEC conducts independent assessments of premises security and on-site processes to determine whether an attacker can gain access, move within the estate, and reach sensitive areas or assets. Engagements cover reconnaissance, entry attempts, movement, asset access, and controlled device placement. Activities follow strict safety gates and legal permissions, using non-destructive methods and clear cease criteria.

Objectives

- Test real-world access controls, from perimeter to critical rooms
- Validate staff challenge culture, visitor flows, and contractor handling
- Assess protection of assets such as comms rooms, end-user devices, and backups
- Provide precise, testable improvements for people, process, and technology

Approach

Work begins with a planning workshop to agree rules of engagement, operating hours, areas in scope, and abort criteria. Reconnaissance maps entrances, guard routines, delivery routes, and badge/lock types. Controlled attempts then exercise entry, movement, and asset access with real-time oversight. Evidence is gathered through time-stamped notes and photography where permitted.

Method

- **Plan** — objectives, locations, scenarios, authority matrix, safety and legal approvals, evidence handling
- **Reconnaissance** — observe flows, uniforms, deliveries, signage, and access technologies
- **Attempt entry** — use agreed pretexts, timing, and techniques to gain access safely
- **Move and validate** — reach agreed zones, evidence access to assets without disruption
- **Debrief** — present findings, owners, acceptance criteria, and a verification path

Deliverables

- Executive briefing describing successful routes, control gaps, and priority actions
- Physical Security Assessment Report covering perimeter, reception and visitor management, access control and surveillance, asset protection, secure areas, device handling, guard force posture, and contractor processes
- Evidence bundle (sanitised) with timelines, annotated photos where allowed, and route diagrams Improvement plan with practical changes to policy, process, signage, training, access technology, and guard routines

- Optional verification letter after fixes and a light re-run
- Standards and alignment (embedded) referencing NPSA physical security guidance, NCSC personnel security principles, and ISO 27001 Annex A physical controls for governance context

Outcomes and benefits

- Reduced likelihood of unauthorised entry and asset compromise
- Clear ownership for fixes across Facilities, Security, and suppliers
- Improved staff challenge culture and visitor handling
- Audit-ready artefacts for boards, regulators, and insurers

Pricing model

Fixed price per site or campus band, or time-and-materials for complex estates. Price drivers include site size, hours in scope, scenario count, required observers, and verification depth.

Timelines

- Planning and approvals in 1–2 weeks
- Execution windows as agreed, aligned to shift patterns and deliveries
- Report issue in 5–10 working days after testing completion
- Optional verification by agreement

Security and assurance

Practitioner-led delivery using peer-reviewed methods and internal QA. Evidence is reproducible and traceable. Reports and artefacts are available in accessible formats

Team and roles

- **Engagement Lead** — scope, governance, quality management, stakeholder alignment
- **Physical Security Tester(s)** for on-site execution and evidence capture
- **Coordinator** — logistics, communications, evidence handling, action tracking

Buyer responsibilities

- Nominate a senior sponsor and single engagement lead

JUMPSEC responsibilities

- Operate strictly within rules of engagement and legal permissions

- Provide site lists, floor plans where available, and emergency contacts
- Arrange landlord and supplier permissions as required by lease or contract
- Provide letter of attestation for engagement approval
- Avoid disruption, respect privacy, and stop on any safety concern
- Handle evidence securely and retain only for agreed periods

Data protection and privacy

The buyer is data controller; JUMPSEC acts as processor. Only minimum necessary evidence is collected and retained. Secure transfer, strict access control, and agreed retention periods apply. Artefacts are returned or securely destroyed on completion.

Constraints and assumptions

- Non-destructive techniques only and no coercion
- No hazardous areas without specialist permits and escorts
- Third-party sites and shared campuses require written consent Personnel with BPSS/SC available where required
- Reports available in accessible formats (WCAG 2.1 AA)

Related services

- Social Engineering Testing
- Rogue Client / Rogue Device Assessment
- Threat-Led Penetration Testing / Red Teaming

Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

0333 939 8080

hello@jumpsec.com

www.jumpsec.com