SFJ Awards

NaCTSO NATIONAL COUNTER TERRORISM SECURITY OFFICE

Level 3 Award in **Counter-Terrorism Protective Security and Preparedness**

Protective security checklist for businesses

Protective security checklist for businesses

Protective security is the coordinated management of people, physical assets, information, and operational systems to reduce the likelihood and impact of security threats.

This checklist helps leaders and operational decision-makers identify gaps, prioritise action, and understand where professional expertise can add long-term resilience.

You can use this checklist as:

- a leadership tool to understand the organisation's strengths and vulnerabilities.
- a planning framework to help inform budgets, risk mitigation, and security strategy.
- a conversation starter to highlight where actions are needed, assess skills gaps or the need for trained professionals to bring expertise, structure, and independence.

1. Governance and strategic oversight

1.1 Security ownership and responsibilities

□ Has a senior leader been formally designated as the security lead?

□ Are roles and responsibilities for security (physical, personnel, technical, and cyber) clearly defined and communicated?

□ Are security responsibilities included in job descriptions for key roles?

1.2 Policy and frameworks

□ Does the organisation have a current protective security policy aligned to risk?

□ Does the organisation have any other policies aligned to security and risk (e.g. business continuity or resilience policies)?

□ Are related and supporting policies (IT security, lone working, incident management, access control) up to date?

□ Is there a documented annual review cycle?

1.3 Culture and awareness

□ Are employees trained on recognising and reporting suspicious behaviour?

□ Do leaders promote a culture that values vigilance and transparency?

□ Are there mechanisms for staff to confidentially report concerns?

2. Threat and risk assessment

2.1 Threat identification

□ Has the organisation mapped relevant threats (e.g., theft, cyber attack, physical attack, insider threat, protest activity, hostile reconnaissance, supply chain compromise)?

□ Are local environmental or sector risks taken into account (e.g., critical infrastructure, high footfall, sensitive data)?

2.2 Risk assessment process

□ Is there a formal, documented protective security risk assessment?

□ Does it evaluate likelihood, impact, vulnerabilities, and existing controls?

□ Are assessments updated after incidents, near misses, or environmental changes?

2.3 Mitigation strategy

□ Are mitigation measures prioritised based on risk?

□ Are budgets aligned to security priorities?

□ Do leaders regularly review the organisation's risk appetite?

3. Physical security

3.1 Access control

□ Are physical entry points secured with appropriate controls (e.g., ID cards, PINs, biometrics, visitor sign-in)?

□ Are visitor management processes consistently followed?

□ Are contractors and temporary workers appropriately vetted?

3.2 Surveillance and monitoring

□ Are CCTV systems maintained, compliant, and fit for purpose?

□ Is there a clear policy on monitoring, data retention, and review?

□ Is CCTV regularly checked for blind spots or technical issues?

□ Are staff members sufficiently trained in CCTV operation?

3.3 Barriers, perimeters and internal protection

□ Are external boundaries secured (e.g. fencing, lighting, gates)?

□ Are critical areas (e.g. server rooms, cash handling, control rooms) restricted to authorised staff?

□ Are alarms and intrusion detection systems tested and maintained?

3.4 Building management and housekeeping

□ Are fire exits and evacuation routes secured from intrusion but safe for emergency egress?

□ Are security-sensitive materials stored safely (e.g. keys, passes, tools, uniforms)?

□ Are deliveries and loading bays managed and supervised?

4. Personnel security and insider threat

4.1 Vetting and screening

□ Are new employees screened to appropriate levels (references, ID checks, right-to-work, DBS if required)?

□ Are periodic re-checks conducted for staff in sensitive roles?

4.2 Access to information and assets

□ Is access to systems and facilities based on "need to know / need to access"?

4.3 Behavioural awareness

□ Are managers trained to recognise signs of insider threat or vulnerability?

□ Is there a clear, supportive escalation pathway for concerns?

5. Information security (in coordination with IT/security specialists)

5.1 Data handling and storage

□ Is sensitive data classified, labelled, and stored securely?

□ Are physical files locked and logged?

5.2 IT security controls

□ Are multi-factor authentication, strong passwords, and patch management in place?

□ Are backups tested regularly?

□ Are remote access arrangements secure?

5.3 Human factors

□ Do staff receive regular training on phishing, social engineering, and data protection?

□ Are simulated phishing exercises used to test awareness?

6. Operational security (OPSEC)

6.1 Protection of sensitive operational information

□ Are operational plans, rotas, and travel patterns protected?

□ Are high-risk activities subject to additional controls?

6.2 Supply chain security

□ Are suppliers vetted proportionately to the risk they pose?

□ Are contracts clear on security expectations and breach reporting?

6.3 Handling security-sensitive events

□ Is there enhanced security planning for major events, VIP visits, or public-facing activities?

□ Are staff briefed appropriately before high-risk operations?

□ Do you have an appropriate number of trained staff for events?

7. Incident and crisis management

7.1 Incident response

□ Is there a documented incident response plan covering security breaches, threats, protests, cyber incidents, and criminal activity?

□ Are roles and communication lines clear?

□ Are first responders trained appropriately?

7.2 Business continuity and recovery

□ Is there a business continuity plan linked to security threats?

□ Are recovery arrangements tested at least annually?

□ Are lessons learned integrated back into risk and policy reviews?

7.3 Reporting and learning culture

□ Do staff understand how to report incidents quickly?

□ Are near misses recorded and analysed?

□ Is learning shared across teams and leadership?

8. Training, testing and continuous improvement

8.1 Staff competence

□ Do staff understand their responsibilities in maintaining protective security?

□ Are induction and refresher sessions consistent and engaging?

8.2 Exercises and drills

□ Are security exercises (e.g. evacuation, invacuation, lockdown, suspicious package) conducted regularly?

□ Are outcomes reviewed and actioned?

8.3 Assurance and audits

□ Are internal audits conducted to verify compliance with protective security standards?

□ Are external professionals used to validate or stress-test security arrangements?

The Workforce Development Trust

England and Wales charity no. 1143246 | Scotland charity no. SC045901