### UK SBS Physical Security Policy

**Version** | **Date** | **Author** | **Owner** | **Comments**
--- | --- | --- | --- | ---
1.0 | 16 June 14 | Head of Risk, Information and Security Compliance (Mel Nash) | Senior Information Risk Owner (Andy Layton) | 1st Issue following TU consultation

**Next Review Date** | June 15
Contents:

1. Aim and Scope
2. Responsibilities
3. Risk Assessments
4. Physical Security Measures
5. Security Procedures
6. Housekeeping / Good Practice
7. Physical Security for Information Assets
8. New Build and Refurbishment
9. Monitoring and Review

Relevant Policies:

Information Assurance Policy
Vetting Policy
Health & Safety Policy
Risk Management Policy
Business Continuity Policy
Visitor Policy
1. **Aim and Scope**

Physical security measures aim to either prevent a direct assault on our premises or reduce the potential damage and injuries that can be inflicted should an assault occur.

The aim of this policy is to ensure that our physical security stance involves an appropriate and 'layered' mix of general good housekeeping, liaison with landlords and investment in processes, structures, equipment and systems that will deter, detect and delay any attacker - protecting against criminal acts such as theft, vandalism, unauthorised entry and terrorism, while addressing general health and safety concerns. Our primary guidance for physical security will be taken from the Cabinet Office Security Policy Framework.

The policy applies to all company sites. Its priorities are to:

- Protect employees, contractors and visitors
- Protect the contents of our estate – ‘The Business Assets’
- Protect the fabric of our estate

It is recognised that many of the measures within this policy are relevant to the threats from terrorism and extremism. However, they will also assist in crime prevention, reducing crime and the fear of crime and improving the quality of life for staff and visitors. Some measures will only be implemented if the local or national threat levels demand it and there is a clear threat to our people, assets or buildings. Measures at this level will only be implemented on the authority of the CEO.

2. **Responsibilities**

The company Senior Information Risk Owner (SIRO) has the overall responsibility for physical security and will liaise and obtain support at Director / Board level.

The Head of Risk, Information and Security Compliance acts as the Departmental Security Officer (equivalent) with day to day responsibilities for security. He/she also acts as the company physical security specialist.

The IT Security Officer (ITSO) has the day to day responsibility for technical security issues and will contribute to physical security risk assessments and decision making.

The Protective Security Working Group (PSWG) will be advised by the Head of Risk, Information and Security Compliance and will assess threats/risks to all employees and visitors, buildings and equipment owned, supported or used by the company and will agree the implementation of effective and proportionate security tools. The group will carry out a 2 monthly (prior to the Audit, Risk and Controls Forum (ARC)) review of security risks, issues and actions and will escalate issues to the ARC as deemed appropriate by the Chair (SIRO).

The Accommodation / H&S Manager will act as the physical security link to the company Estates Directorate.

Information Asset Owners (IAO's) will understand and address risks to the information assets that they ‘own’ and provide assurance to the SIRO on the security and use of those assets.
They will seek physical security guidance from the Head of Risk, Information and Security Compliance as required.

All Managers are responsible for implementing relevant security policies within their business areas.

All Employees, contractors and visitors must adhere to this and other security / H&S policies and procedures, report security incidents and ensure that they undergo security briefings as directed. Failure to comply with this policy may lead to disciplinary action.

3. Risk Assessments

We recognise that physical security arrangements should be prioritised according to the prevailing Security Response Level\(^1\), the security risks to sites and the risks to individual operations or the parts of the business that allow those operations to take place. This priority is based on:

- An assessment of site profile
- The importance of the site/operation to the continuity of company business
- The prevailing Security Response Level

Physical security risk assessments will be carried out at all sites and guide the proportionate, appropriate and cost effective deployment of security measures. A physical security risk assessment template is at Appendix 1.

4. Physical Security Measures

The deployment of physical security measures will be in line with the HMG document ‘Guide to Producing Operational Requirements for Security Measures – February 2010’ and must not breach Health & Safety regulations. In liaison with landlords and contractors where appropriate, we will:

Access Control:

- Ensure that an efficient reception area is in place to control access, staffed by appropriately trained personnel or invest in a good quality access control system operated by swipe or contact proximity cards supported by PIN verification if needed.
- Keep access control points to a minimum, denying access through side or rear entrances to all but authorised personnel.

Security Passes:

- Implement a pass system, insisting that personnel wear their passes at all times while on site and ensure that the issue of passes is strictly controlled and regularly reviewed.

---

\(^1\) Response Levels are issued by HMG and provide a broad indication of protective security measures that should be applied at any particular time. Response levels tend to relate to sites, whereas threat levels relate to broad areas of activity.
• Foster a culture where employees can challenge all those not showing security passes.

• Implement a visitor control policy.

Screening and Patrolling:

• Maintain the ability to carry out the random searches of hand baggage on entry. These searches will only be implemented on the authority of the CEO and Corporate HR will ensure that the TU is fully briefed. Searches will only be implemented at the ‘Exceptional’ response level, that being when an attack is expected imminently.

• Ensure that security contracts include the routine internal and external patrolling of sites.

• Ensure that mail receipt, screening and delivery is controlled in accordance with the security requirements of specific sites and is in line with prevailing threats.

Traffic and Parking Controls:

• Ensure appropriate vehicle access control measures, traffic calming measures and well-lit parking areas.

• Keep vehicles away from buildings if the situation dictates.

Doors, Windows and Walls:

• Ensure that the physical structure of our buildings is in line with the security requirements of the assets that we are protecting.

• Ensure that the fabric of our buildings is regularly maintained to ensure effectiveness.

• Ensure that all faults and deficiencies are rectified as soon as practical.

Integrated Security Systems:

• Ensure that intruder alarms, CCTV systems and security lighting are integrated so that they work together in an effective and coordinated manner.

• Ensure that alarm systems are linked to an appropriate responding organisation (police or security company) and that relevant contracts are monitored to ensure compliance.

5. Security Procedures

In Liaison with landlords and contractors where appropriate, we will ensure that we have appropriate and incremental security procedures in place and that these procedures are communicated, reviewed and tested regularly. Security procedures will include but will not be limited to:

• Mail screening and the delivery of post

• Bomb threats
• Suspicious objects
• Building search
• Fire and explosion actions and evacuation / invacuation
• Demonstrations
• Chemical, Biological and Radiological (‘White Powder’) attacks
• Crime Prevention – Reducing the likelihood of theft and vandalism
• The incremental deployment of security measures. See Appendix 2.

6. **Housekeeping / Good Practice**

Good housekeeping will improve the ambience of our sites and reduce the opportunity for criminal activity. In Liaison with landlords and contractors where appropriate, we will:

• Keep public and communal areas clean and tidy.
• Keep external areas clean and tidy.
• Prevent the concealment of suspicious objects as far as is practical.
• Ensure that our premises look well cared for, well maintained and controlled.

7. **Physical Security for Information Assets**

We will ensure the physical security of our information assets by providing controls in line with specific Cabinet Office guidance for the protection of assets at different classification levels. Guidance will be taken from the Cabinet Office document ‘Government Security Classifications. Annex – Security Controls Framework’.

8. **New Build and Refurbishment**

We will work with landlords and contractors to ensure that the design of new builds and refurbished accommodation captures the security requirements of the assets that the accommodation will house. When planning new builds or considering refurbishments, we will review:

• Access and movement
• The building structure
• Methods of appropriate surveillance
• Ownership
• Physical protection
• Activity and management

• Maintenance

9. **Monitoring and Review**

The Head of Risk, Information and Security Compliance will review this policy at least annually or whenever legal or business reasons dictate. He/she will recommend changes as required to the SIRO and Senior Leadership Group for final approval. Changes will be implemented following consultation with the Trade Unions.
Appendix 1 to
Physical Security Policy
Dated 16 June 14

<table>
<thead>
<tr>
<th>Site:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Date:</td>
<td></td>
</tr>
<tr>
<td>Conducted By:</td>
<td></td>
</tr>
<tr>
<td>The Threat:</td>
<td></td>
</tr>
<tr>
<td>Assets Protected:</td>
<td></td>
</tr>
<tr>
<td>Vulnerabilities:</td>
<td></td>
</tr>
<tr>
<td>Highest Protective Marking/Classification:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Physical Measure</th>
<th>Comments - Detect, Delay, Deter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perimeter Fence</td>
<td></td>
</tr>
<tr>
<td>Doors</td>
<td></td>
</tr>
<tr>
<td>Walls</td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td></td>
</tr>
<tr>
<td>Intruder Alarms</td>
<td></td>
</tr>
<tr>
<td>CCTV</td>
<td></td>
</tr>
<tr>
<td>Lighting</td>
<td></td>
</tr>
<tr>
<td>Access Control</td>
<td></td>
</tr>
<tr>
<td>Housekeeping</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Procedures</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone Threats</td>
<td></td>
</tr>
<tr>
<td>Evacuation</td>
<td></td>
</tr>
<tr>
<td>Delivered Items</td>
<td></td>
</tr>
<tr>
<td>Fire</td>
<td></td>
</tr>
<tr>
<td>Search</td>
<td></td>
</tr>
<tr>
<td>Demonstration</td>
<td></td>
</tr>
<tr>
<td>Business Continuity</td>
<td></td>
</tr>
<tr>
<td>Internal Liaison for multi-occupancy</td>
<td></td>
</tr>
<tr>
<td>Local Security Environment / Crime Mapping</td>
<td></td>
</tr>
<tr>
<td>External Liaison - Emergency Services</td>
<td></td>
</tr>
</tbody>
</table>

Page 8 of 9
Appendix 2 to
Physical Security Policy
Dated 16 June 14

This matrix provides guidance on our protective security measures and in particular sets an incremental approach to our response to the threat from terrorism. It should be noted that response will be in line with the national threat levels detailed below. THE MATRIX IS ISSUED SEPARATELY AND IS NOT TO BE CIRCULATED OUTSIDE OF THE COMPANY.

The matrix is held and administered by the Head of Risk, Information and Security Compliance.

There are 3 levels of response:

<table>
<thead>
<tr>
<th>Response Level</th>
<th>Description</th>
<th>Related Threat Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Routine protective security measures appropriate to the business concerned</td>
<td>Low and Moderate</td>
<td>Low – An attack is unlikely. Moderate – An attack is possible but not likely.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Heightened</td>
<td>Additional and sustainable protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk</td>
<td>Substantial and Severe</td>
<td>Substantial – An attack is a strong possibility. Severe – An attack is highly likely</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exceptional</td>
<td>Maximum protective security measures to meet specific threats and to minimise vulnerability and risk</td>
<td>Critical</td>
<td>An attack is expected imminently</td>
</tr>
</tbody>
</table>