Science & Technology
Facilities Council

STFC Physical and Personnel Security Policy:

Management of Physical and Personnel Security

September 2016

Contents

Appendices

1. PURPOSE

The physical security of employees, sites and assets is a primary responsibility for any employer on behalf of their shareholders and/or stakeholders. All employers have a 'duty of care' to their staff in respect to their physical security, safety, when working on their behalf on and off operated sites.

STFC as a Non Departmental Public Body (NDPB) is subject to the physical security polices and standards established by the UK Government in ensuring effective management and use of resources, the HMG Security Policy Framework.

STFC has sites in the UK and overseas; employs ~2000 staff and has assets totaling ~£1.6B. The scope and financial value of STFC assets does not represent the economic and reputational value of these assets in the national and international collaborations of which the STFC is part.

As an NDPB STFC has a high profile within its stakeholder community for which the reputational damage arising from significant breaches of physical security could be detrimental.

This code establishes the framework of responsibilities and controls for identifying and managing physical security risks for STFC, its staff, and its tenants, facility users, contractors and visitors when working at STFC sites.

A key principle with regard to physical security is that all staff must take responsibility for the security of STFC assets.

2. SCOPE

This code applies to the physical security of:

- STFC staff;
- STFC equipment/assets; and
- STFC estate (sites and buildings operated by the STFC),

and Personnel security.

The nature of STFC sites is such that they are occupied and used by others such as tenants, facility users, contractors and visitors. STFC through its leases and general 'duty of care' to those working on STFC sites has limited responsibilities to them. This code applies to tenants, facility users, contractors and visitors and their equipment/assets when present on STFC sites.

Where STFC occupies premises/buildings for which it is not the responsible operator, for example Swindon Office, this code establishes the minimum standards by which the physical security measures employed by the operators of these premises/buildings are assessed.

This code applies where STFC staff transport equipment and materials between STFC sites and to other locations in the UK or overseas. STFC responsibility for the security of these materials ceases at the contractually agreed point of receipt/acceptance of responsibility by the receiving organisation.

Specific exemptions to this code include:

- The physical security/safety of STFC staff while travelling on council business, see SHE Code 8 Travel on Council Business;
- The establishment of site emergency management and controls, see SHE Code 32 Fire and Emergency Management;
- The consequences of physical loss or damage to STFC sites, assets or people and those co-located on STFC sites, see STFC and Departmental Business Continuity Plans;
- The management of Physical Security frequently requires the collection, holding and use of personal information for staff and others. This code does not address the consequential Data Protection implications of holding this information, or potential for Freedom of Information requests; and
- Information Security which is addressed by this code's sister policy the STFC Information Security Policy . However this code does apply to the physical security of assets through which STFC information is employed and stored, for example PCs, servers etc.

3. DEFINITIONS

3.1 Physical Security

The term Physical Security encompasses all those measures/controls and processes that deter and prevent the physical loss or damage of STFC sites, assets and people. These can include but are not limited to:

- Site perimeter security systems, for example, fences, lighting, security teams;
- People access control systems, for example site reception procedures and issue of security passes/badges, security vetting etc.;
- Site vehicle access control systems, for example Automatic Number Plate Recognition (ANPR); vehicle inspections;
- Parcel, mail and delivery receipt, handling and inspection procedures;
- Building and specific offices/laboratories/workshops/server room access control systems, for example swipe, key and numeric keypad access systems, padlocks, door locks; and
- Building walls, doors/frames, windows, ceilings, floors, vents and other potential access points: and
- Use of specialist security technologies for example Closed Circuit TV (CCTV) http://staff.stfc.ac.uk/core/security/information/Policy/STFCCCTVPolicy.pdf; Perimeter Intrusion Detection (PID) systems; asset marking; SmartWater marking, signage etc.

3.2 Security Risk Assessment (SRA)

Security controls are necessary to reduce risk to an acceptable level and maintain the resilience of STFC sites. The implementation of security controls should be based on a sound Security Risk Assessment (SRA) process. Guidance for conducting an SRA can be found in Appendix 1.

3.3 STFC Security Officer

Within this code and the STFC the term 'STFC Security Officer' is employed to refer to the 'Departmental Security Officer (DSO)', see reference 5.1, to avoid confusion with the STFC's internal departmental structure.

3.4 Site Security Manager

Site Security Managers, generally reporting through Estates Operations teams are responsible for the physical infrastructure security controls at a specific site(s) and act as focus for site(s) security matters.

4. RESPONSIBILITIES

4.1 STFC Chief Executive Officer (STFC Accounting Officer) shall:

4.1.1 Ensure sufficient funding and manpower resources are made available to ensure that the STFC wide Physical Security controls established under this code are implemented, leading by example their application.

4.1.2 Appoint in writing at STFC Executive Director level (template letter of appointment) an individual responsible for both Information and Physical Security. This individual would assume the formal role of STFC Senior Information Risk Owner (SIRO), recording their appointment in the STFC SHE Directory. This role is generally undertaken by the Director responsible for CICT and Estates.

4.1.3 Submit to Cabinet Office, via the STFC's parent government Department, an annual 'Commentary on protective security risks'.

4.2 Executive Director responsible for Physical and IT security shall:

4.2.1 Undertake the role of SIRO responsible for:

- the risk profile of the STFC;
- identifying all of the risks; and
- making sure that appropriate mitigations are in place so that the risks can be accepted.

4.2.2 Appoint in writing (template letter of appointment) a competent STFC Security Officer ensuring that they have been Baseline Personnel Security Standard (BPSS) checked, see Appendix 2, attend any required training, see Appendix 4, and their appointment is recorded in the STFC SHE Directory.

4.2.3 Appoint in writing (template letter of appointment) for each site a competent Site Security Manager responsible for site security as defined in this code ensuring that they have been BPSS checked, see Appendix 2, attend any required training, see Appendix 4, and their appointment is recorded in the STFC SHE Directory.

4.2.4 Ensure sufficient funding and manpower resources are made available to ensure that the site wide Physical Security controls established under this code are implemented, leading by example their application.

4.2.5 Co-ordinate and lead an annual review of STFC Physical Security, drafting and collating the 'Annual Statement of Assurance'/'Commentary on protective security risks' and ensure that this is reviewed by Executive Board prior to submission by the STFC Chief Executive Officer, and in the light of planned changes to STFC operations for which there may be significant security implications.

4.3 STFC Security Officer shall:

4.3.1 Ensure that a generic STFC Security Risk Assessment (SRA) is undertaken for the Council. The STFC SRA should be reviewed annually or when significant change occurs and be informed by prevailing national and Government security levels. The recommended format and content of the STFC and other SRAs is presented in Appendix 1.

4.3.2 Based on the STFC SRA, that an STFC Security Plan is developed. The STFC Security plan establishes corporate security controls relevant to all STFC sites and operations. The recommended format and content of the STFC and other Security Plans is presented in Appendix 1.

4.3.3 Ensure that all new starters are subject to BPSS checks undertaken by HR through the STFC's Shared Service Centre, and that access to specific assets/areas is provided to personnel on a risk assessed needs basis and subject to on-going review. Additional checks may be undertaken for specific roles and responsibilities.

4.3.4 Establish and chair the STFC Security Committee reporting and reviewing physical security incidents, reviewing changing national and Government security levels and as appropriate updating the STFC SRA and Security Plans to improve STFC physical security controls. Appendix 3 presents the terms of reference for this committee, see Appendix 3.

4.3.5 Respond to changes in the alert states identified by the UK Threat Levels as appropriate convening the STFC Security Committee to consider the change.

4.3.6 Ensure a process is established to ensure that Physical Security incidents can be reported by STFC staff and others working at STFC sites, communicating these incidents to relevant Site Security Managers for investigation.

4.3.7 Ensure that the STFC SRA and STFC Security Plan are held securely and access provided only to those with a need to access them.

4.3.8 Establish an audit programme for the implementation of this code, as appropriate undertaken by external specialists or internal auditors. The audit frequency shall be determined by the STFC Security Committee.

4.4 Site Security Manager shall:

4.4.1 Ensure an SRA is undertaken for their site(s) for the physical security controls provided most effectively at site level. The SRA should consider but not be limited to:
- theft of STFC, tenant, contractor, visitor and facility user property by staff and others with access to the site(s);
- damage to STFC and Tenant property and site(s);
- threats to STFC and tenant operations.

The Site SRA should be reviewed annually or when prompted by significant change, internally or externally and a copy sent to the STFC Security Officer. The recommended format and content of the SRAs is presented in Appendix 1.

4.4.2 Based on the Site SRA, ensure that a 'Site Security' Plan is developed for their site(s). The recommended structure and content of Security plans is outlined in Appendix 1. The Site Security Plans should be reviewed annually or whenever the site security risk assessment is updated, and a copy sent to the STFC Security Officer.

4.4.3 Ensure that the Site SRA and Site Security Plans are held securely and access provided only to those with a need to access them.

4.4.4 Implement the Physical Security controls established by the Site Security Plan effectively across their site(s). Ensure that where CCTV is employed their use is recorded in the CCTV list in the Information Systems Register (http://csd.stfc.ac.uk/security/isr/Lists/CCTV%20Systems/AllItems.aspx).

4.4.5 Investigate all Physical Security Incidents, documenting the investigation's findings and implementing corrective actions to minimise the likelihood of the incident's repetition, sending a copy of the incident investigation report to the STFC Security Officer, and as appropriate informing the STFC Information Security team where information controls may have been compromised.

4.4.6 Respond to changes in the alert states identified by the UK Threat Levels considering the immediate impact for their site.

4.4.7 Ensure that site emergency exercise programmes, see SHE Code 32 Fire and emergency management, periodically rehearse and test the response of site security to relevant security scenarios including theft of radioactive material.

4.4.8 Where a site holds radioactive materials subject to Environment Agency permitting ensure a specific Radioactive Materials SRA is undertaken for the security of these materials at site level. This should be developed with the advice of the Radiation Protection Adviser (RPA)/Radioactive Waste Adviser (RWA). The SRA should be maintained in the light of significant change, internally or externally and a copy sent to the STFC Security Officer. The recommended format and content of the SRAs is presented in Appendix 1.

4.4.9 Based on the Site Radioactive Materials SRA, develop a specific 'Site Radioactive Materials Security' plan developed for their site(s) addressing the controls detailed in the Site Radioactive Materials SRA. The recommended structure and content of Security plans is outlined in Appendix 1. The site security plans should be reviewed annually or whenever the site security risk assessment is updated, and a copy sent to the STFC Security Officer.

4.5 **STFC Directors or Senior Managers of Tenant companies shall***:*

4.5.1 Take responsibility for security of their respective assets.

4.5.2 Where following discussion with the Site Security Manager, and as appropriate the site Radiation Protection Adviser (RPA)/Radioactive Waste Adviser (RWA), it is determined that STFC and site-based physical security controls are not sufficient to assure the security of Departmental or Tenant assets and activities they shall appoint in writing (template letter of appointment) a Security Representative (SR). SRs should be BPSS checked prior to appointment, see Appendix 2. SR appointments should be recorded in the STFC SHE Directory and the STFC Security Officer and relevant Site Security Manager(s) informed.

4.5.3 Ensure where STFC and site-based physical security controls are not sufficient to assure the security of Departmental/Tenant assets and activities a local SRA is undertaken and Security Plan developed. A copy of the local SRA and Security Plan shall be sent to the STFC Security Officer and relevant Site Security Manager(s).

4.5.4 Ensure that the Local SRA and Security plan are held securely and access provided only to those with a need to access them.

4.5.5 Ensure sufficient funding and manpower resources are made available to ensure that Department and Tenant specific Physical Security controls documented in the local SRA and Security Plan are implemented, leading by example in their application.

4.5.6 Where scientific facilities are operated for external users, ensure that the names of users coming to STFC sites are provided in advance and checked on arrival through photo identification.

4.5.7 Contribute to the STFC annual review of Physical Security.

4.6 **Security Representative (SR) shall:**

4.6.1 Provide a focus for Department/Tenant Physical Security matters, acting as a communication focus for the Department/Tenant with Site and STFC security management, championing Departmental/Tenant company Physical security, and leading by example in implementing physical security controls.

4.6.2 Document the local SRA for their Department or company, see Appendix 1, and ensure that the controls detailed in the local SRA are implemented.

4.6.3 Attend the twice yearly SR Security Review meeting on behalf of their Department or company.

4.7 **Managers, Contract Supervising Officers, Tenant Management shall:**

4.7.1 Take responsibility for security of their respective assets.

4.7.2 When recruiting new staff be assured that they have undertaken a BPSS check, see Appendix 2, prior to arrival. This process is managed by HR, see STFC Induction Checklist, and routinely undertaken by the STFC Shared Service

Centre. Where BPSS clearance has not been completed on arrival consider the security implications of their work until clearance is granted.

4.7.3 When managing contractors, and as appropriate their sub-contractors, working at STFC sites be assured that their employer has undertaken a BPSS check or an equivalent verification of their employee(s), see Appendix 2. This is a routine specification within STFC Framework contracts but may need to be requested for agency, sub-contractors or other contractors. In the absence of such checks, agency, sub-contractors or other contractors should not be given unsupervised access to any area.

4.7.4 As appropriate undertake a dedicated local SRA where valuable materials/ equipment are transported off STFC sites, with advice of the SR and site/STFC security management. The scope of the SRA should extend to the point at which the receiving party signs acceptance/receipt of the materials/equipment.

4.7.5 Ensure their staff, and others working at or visiting STFC sites (for example tenants, contractors and their sub-contractors, facility users, visitors), are made aware of the relevant aspects of STFC and site security through attendance of relevant site induction training. As appropriate ensure that individuals, and short term visitors, are made aware of any Departmental level local security controls, for example through ‘tool box’ talks etc.

4.7.6 Implement the STFC, Site and as appropriate Departmental Security controls detailed in the Departmental SRA and dedicated material/equipment transport SRAs.

4.7.7 Encourage all staff, or others they are responsible for, to report all instances of actual or suspected breaches of STFC physical security, see 3.1, to those responsible for site security, and record such incidents here information.security@stfc.ac.uk.

Radioactive materials and wastes

4.7.8 Inform the Site Security Manager and RPA/RWA prior to new, open or closed, radioactive materials being brought to STFC sites by staff, contractors or others to discuss and agree appropriate security measures. Inform the Site Security Manager and RPA/RWA prior to new radioactive materials being created on STFC sites by staff, contractors or others to discuss and agree appropriate security measures unless under existing agreed arrangements.

4.7.9 All radioactive materials and wastes should be the subject of a dedicated documented SRA and Site Security Plan based on OCNS regulations and undertaken by the responsible manager in consultation with the Site Security Manager and Radiation Protection Adviser/Radioactive Waste Adviser, to whom final copies should be sent. The SRA Site Security Plan should be reviewed and exercised annually or when significant changes to the radioactive inventory or their controls take place. The manager is responsible for implementing the controls established by the SRA and their on-going maintenance.

4.8 Radiation Protection Adviser (RPA)/Radioactive Waste Adviser (RWA) shall:

4.8.1 Provide advice and guidance with regard to the security requirements and Site Security Plan necessary for the storage and use of radioactive materials, in particular but not limited to High Activity Sealed Sources.

4.9 **Staff, tenants, facility users, and contractors (and their sub-contractors) shall:**

4.9.1 Ensure they undertake relevant site induction training for the site(s) they are working at addressing STFC security.

4.9.2 Staff and tenants shall take responsibility for security of their respective assets.

4.9.3 Staff and tenants hosting visitors to STFC sites shall take responsibility for the security of STFC assets in respect to their visitors and ensure visitors understand their responsibility for their assets while on STFC sites.

4.9.4 Follow and implement all physical security controls established as part of the STFC's Physical Security policies, this code and as appropriate Department SRAs.

These include but are not limited to:
- carrying and displaying at all times their site pass;
- challenging or reporting to site security any individual not displaying their site pass or acting suspiciously;
- do not 'tail gate' or allow others to 'tail gate' through controlled access points;
- taking responsibility for the security of their workplaces remaining vigilant to and addressing potential security threats, for example closing doors, locking cupboards etc.; and
- ensure STFC property remains secure at all times, on and off site.

4.9.5 Take full responsibility for the security of personal belongings brought onto STFC sites (and for staff while travelling on Council business), for example: wallets/purses, handbags, mobile phones and vehicles.

4.9.6 Contractors, and their sub-contractors, shall take full responsibility for the security of, and liability for the loss of their belongings: tools, materials etc. while on STFC sites.

4.9.7 Report all instances of actual or suspected breaches of STFC physical security, see 3.1, to those responsible for site security **immediately**, and after the event recording such incidents here information.security@stfc.ac.uk.

4.10 **Head of Business Incubation shall:**

4.10.1 Ensure that all tenant staff undertake BPSS checks prior to arrival on site and that the content of this Physical Security Code are implemented by tenants.

5. References

5.1 UK Centre for Protection of National Infrastructure (CPNI) website - http://www.cpni.gov.uk/default.aspx

5.2 CPNI Guide to Producing Operational requirements for Security Measures http://www.cpni.gov.uk/documents/publications/2010/2010001-op_reqs.pdf?epslanguage=en-gb

5.3 CPNI assurance scheme for destruction services
http://www.cpni.gov.uk/about/Who-we-work-with/manufacturers/Manufacturers-and-service-providers/

5.4 Home Office Surveillance Camera code of practice https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

5.5 STFC CCTV policy
http://staff.stfc.ac.uk/core/security/information/Policies/Policy/STFCCCTVPolicy.pdf

5.6 STFC Data Protection policy
http://staff.stfc.ac.uk/core/security/DataProtection/Pages/default.aspx

5.7 Cabinet Office HMG Security Policy Framework https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

5.8 Cabinet Office HMG Baseline Personnel Security Standard https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/365602/HMG_Baseline_Personnel_Security_Standard.pdf

5.9 UK Government Service Design Manual – Information Security
https://www.gov.uk/service-manual/making-software/information-security.html

Appendix 1: Generic structure and content of Security Risk Assessment and Site Security Plans

Modern approaches to security need to be holistic. Effective management of physical security is predicated on the presence of effective personnel security and effective information security systems. The absence of any one of these three management systems undermines the effective security of all.

Effective physical security management should be based on a Security Risk Assessment (SRA). An SRA is an assessment of the threats to the CONFIDENTIALITY, INTEGRITY and AVAILABILITY of the assets which enable the STFC to conduct its business. An SRA ensures that current security measures are not based on past history but on an objective assessment of what attacks could occur and the impact they would have. The on-going review of SRAs in the light of new assets, facilities or buildings being acquired; and/or changing circumstances will ensure that physical security measures remain effective and proportionate.

Physical security controls are intended to protect individuals and valuable physical assets from attack/theft by those who are not authorised to have access to them. Such controls often combine control of entry through a secure perimeter, with one or more layers of further physical security controls closer to the assets. Installing security measures into new builds at the outset or subsequent renovations can be significantly cheaper than retrofitting security measures which can often be implemented at low or even no cost - for example keeping keys secured in a key press, locking valuables in cabinets or rooms, or securing items which can be used as tools to breach security e.g. ladders, power tools, fork lift trucks.

There are recommended standards for physical security controls for radioactive sources which can be obtained from the STFC Radiation Protection Advisor (RPA).

Security Risk Assessment (SRA) Process

This generic security risk assessment process can be employed at site or Departmental levels.

1. Identify assets, value and ownership

Determine what assets - physical items, personnel, etc need protection. Determine their replacement cost (if applicable), persons responsible. Start with assets your Department values the highest. Items with a low individual replacement cost may be included if aggregated into large quantities or if they pose another element of risk from their loss, e.g. interruption to normal business or reputational harm.

2. Identify Hazards - the security threats and vulnerabilities to the assets

Think about whether items are attractive for theft and whose location is well-known; use knowledge of crime and other security incidents; consider the terrorism threat level. In the absence of detailed threat information, consider vulnerability: a risk-based approach of what could occur due to insufficient protection. Consider how an attack would be mounted – what would someone need to be successful?

3. Assess level of security Risk to each asset

Security Impact is an assessment of the harm caused to the integrity, confidentiality and availability of assets. It may involve a financial cost, delay or cessation of STFC projects, harm to people, and/or reputational cost. **Impact can be scored: Low; Moderate or High**.

A key error in security risk assessment is being swayed by historic events when determining the Likelihood of a security breach - whether a lack of security incidents (leading to complacency); or the painful memory of an incident which occurred can lead to overreaction and insufficient consideration of other threats. It is not possible to assess Likelihood (and impact) in a quantitative manner, it will to some degree depend on the judgment of those undertaking the assessment and should as far as practicable be undertaken by a team to avoid such bias introduced by one individuals experience. These considerations together form your estimate of the probability of a loss or harm occurring – its likelihood. **Likelihood can be scored: Low, Moderate or High**.

Together the Security Impact and its Likelihood determine the Security Risk to the organisation, where - Risk = Impact x Likelihood.

From the **Security Risk Matrix** below the Security Risk for a specific asset can be determined.

Likelihood	High (3)	Low (3)	High (6)	Very high (9)
	Moderate (2)	Low (2)	Moderate (4)	High (6)
	Low (1)	Very low (1)	Low (2)	Low (3)
		Low (1)	Moderate (2)	High (3)
		Impact		

Depending on the risk score further security measures may need to be implemented to reduce the risk. If it is within the risk appetite of the asset owner risk scores of low or very low are normally deemed acceptable and do not require further action if controls are maintained. Risk scores of **Moderate, High and Very High** need further mitigation.

4. Identify measures to reduce the risk

Physical Security measures that can be employed include those relating to the following:

- Document handling - including transfer, accounting, copying and classification;
- Buildings;
- Doors, windows, frames, floors, ceilings, vents;
- Rooms, including secure rooms;
- Security containers, safes;
- Locks including keyed interlocks;
- Entry and Access Control Systems;

- Site Security Officers;
- Intruder alarms;
- Intruder detection;
- Perimeter security, including the use of CCTV and intruder detection;
- Destruction of protectively marked waste and other valuables ;
- Working on protectively marked assets away from official premises, for example, at home or when travelling; and
- Planning for accommodation moves

Personnel Security measures include:

- Assessing who has a clear business need to access assets or data;
- Ensuring that those with legitimate access wear identification;
- Challenge any who do not show valid identification (''Can I help you?'');
- Recognising that temporary access for non-staff may require escort or other arrangements such as working hours' access only;
- Completion of background security checks (BPSS or higher as required);
- Ensuring that those with access to a certain area or project are not publicised; and
- Ensuring that access is removed when personnel no longer have a business need For more information, see In.focus Core services/Security/Personnel security [TBA]

Information Security measures include:

- Using passwords that meet STFC Password Standards and never sharing them;
- Locking PCs when unattended;
- Using anti-virus software so personal or business information and systems integrity are not compromised; and
- Adhere to the STFC Information Security Policy.

For more guidance, consult STFC Intranet in.focus/Core Services/STFC Information Security Team or contact your local IT Service Desk.

It is important to remember, all protective security measures should be employed because they can reduce the risk in a specific way. They must be considered in a holistic way to avoid weak links reducing the effectiveness of the other protective measures which have been adopted. For example, using a code-locked container and then recording the entry code in a document on a shared network drive allowing illegitimate access without a trace. Purchasing typical security measures like CCTV must be due to an appreciation of their utility in the situation – they may provide deterrence only. The approach should be the adoption of commensurate measures which mitigate risk in a specific way.

5. & 6. Review Residual Risk – are additional mitigating security measures required to reduce the security Risk further?

What negative outcome to the asset would be costly or harmful?
How could it occur – what would I do if I were the attacker?
What could reduce the likelihood and/or impact of the attack occurring?
What further measures can prevent loss to an acceptable level or provide detection and delay until response arrives?
Consult the STFC Security Officer, Site Security Manager or Departmental Security Representative for further guidance on available security measures.

Where the residual security risk remains High or Very High after implementing all practical security measures, active consideration should be given to ensuring that these security risks are highlighted through the STFC Risk Assurance process.

Record steps 1-6 in the SRA template below.

<table>
<tr><td colspan="2">Asset:</td><td colspan="2">Start Date:
End Date (optional):</td><td colspan="2">Date of Risk Assessment:</td></tr>
<tr><td colspan="6">Risk assessment completed by (name, position):</td></tr>
<tr><td>1. Asset (Inc. value and owner)</td><td>2. Identify Hazards (threats or vulnerabilities related to personnel, physical items or information)</td><td>3. Assess Risk (Likelihood multiplied by Impact - low, medium, high)</td><td>4. Identify mitigating security measures</td><td>5. Residual risk</td><td>6. Actions to implement measures</td></tr>
<tr><td><i>e.g. Secure valuable laboratory equipment in store room</i></td><td><i>Theft risk due to mechanical code lock, code not changed for 5 years</i></td><td><i>2 x 3 = 6 High risk</i></td><td><i>Mechanical code lock replaced by electronic access control and access approvals regularly reviewed</i></td><td><i>1 x 3 = 3 Low risk</i></td><td><i>Contact Estates Helpdesk to arrange survey and quotation; Identify who needs access and at what times / days</i></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

The SRA should be marked Official Sensitive when complete; see the STFC Information Security Policy for further guidance.

This template may also be suitable for Departments reviewing security protection measures for their physical, personnel and information assets. For high risk / high value assets (those which would have a significant detrimental effect on business operation) consult your Departmental Security Representative to formulate an appropriate response.

Review SRA periodically or when circumstances change

It is common for security measures to slip over time as they have the intended effect and the sense of risk reduces. Becoming more relaxed about leaving assets insecure for short periods can become tempting. Security measures may become less effective due to environmental changes such as building works removing a perimeter, obstructions appearing in front of CCTV cameras. Maintaining a Security Risk Assessment document for all significant assets will help avoid these pitfalls, provided it is reviewed periodically when changes occur or after security incidents are reported.

Site Security Plan template:

This template is intended to document or review the site security measures established as a result of a Security Risk Assessment (SRA) by Site Security Managers, it should relate to the security controls detailed in columns 4. and 6. in the SRA. Consequently it is important that an SRA is completed first to ensure the grounds for the measures are justified.

It may also provide a useful basis for Departmental Security Risk Plans.

Official Sensitive (when complete)

Section 1: PERIMETER	
Site or area to be secured	
Gatehouse, reception or lodge	
Access points: pedestrian and vehicle control - gates, turnstiles, barriers	
Fences e.g. welded mesh, palisade, expanded metal, chain link; height and topping. Consider climbing aids or attack tools nearby and temporary works which cause an opening	
Security lighting. Consider type, mode of operation (motion-activated, switchable, timed)	
Perimeter Intruder Detection systems (PIDS) & area Intruder Detection Systems (IDS) Consider monitoring method and response times, activation times/days, key-holders	
Closed circuit television (CCTV) system (pan, tilt, zoom, monochrome, colour, day/night etc). **CCTV systems must be only be installed with the agreement of Site Security Manager**	
Automatic Access Control Systems	
Physical locking systems (key locks, mechanical code locks, padlocks, reinforced doors) including estimated delay time to defeat the measure	
Any other features or arrangements which add to the security of the assets	
Section 2: SECURITY AND STAFFING ARRANGEMENTS	

Pass system for employees	
Issue of temporary passes to visitors, contractors and others	
Vehicle Checks	
Access arrangements for employees – identification, security vetting, buddy system, out of hours access	
Access arrangements for contractors (including any escort arrangements) - identification, security vetting, escorting, out of hours access	
Access arrangements for visitors (including any escort arrangements) identification, security vetting, escorting, out of hours access	
Search arrangements (entry/exit, personnel/bags/vehicles, normal/heightened/exceptional threat response levels)	
Key control for rooms, areas and locked gates	
Section 3: RESILIENCE OF SECURITY SYSTEMS	
Tests at specified intervals (e.g. weekly)	
Details of standby power which switches in automatically in the event of a mains failure	
Procedures for reporting / repairing of security system faults	
Procedures for maintaining the security regime in the event of security equipment failure or while routine maintenance or minor repair work is carried out	
Provide details of your contingency plans for security events / incidents and instructions to staff	
State the arrangements for an annual test of security related contingency plans	
List security instructions provided for guidance of staff and security personnel	
List pre-planned options for upgrading security in the event of an increase in threat	

Appendix 2: Baseline Personnel Security Standard (BPSS) Checks

1 STFC Policy

In accordance with Cabinet Office instructions, STFC has a policy of carrying out a simple pre-employment check for all new employees.

This has been carried out for new employees since December 2008. A similar basic check is to be extended retrospectively to any member of staff in the following categories:

- STFC Directors who are also Gold level Emergency Controllers
- All Silver level Emergency Controllers
- Members of the Security Review Committee
- All Security Officers
- Staff with IT security responsibilities
- Staff who have routine and unsupervised access to radioactive materials that fall within the High Activity Sealed Sources (HASS) Directive

BPSS checks should also be carried out for contractors and visitors who are to be given unsupervised access to High Risk Areas.

2 What does it comprise?

For the pre-employment check STFC uses the Cabinet Office approved Baseline Personnel Security Standard (BPSS). Despite its name the BPSS is not a formal security clearance, it is however a precursor to such clearances if these are required. The BPSS sits at the bottom of a hierarchy of security checks which can be carried out where an employer feels there is a need for such checks or the Cabinet Office mandates them. The BPSS is a package of checks that represent good recruitment and employment practice and aims to provide an appropriate level of assurance as to the trustworthiness, integrity and probable reliability of employees.

The BPSS is conducted to set standards and comprises the following:

- Checks on the individual’s right to work in the UK and immigration status if applicable;
- An identification check;
- A criminal records check; and
- A previous employment check (three years).

The full BPSS guidance document can be accessed by following this hyperlink: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/365602/HMG_Baseline_Personnel_Security_Standard.pdf

The checks for **existing** employees are similar to those used in the pre-employment process but do not ask for a CV; details of references; previous employers details; home contact details nor does it give authority for STFC (or its agents) to approach the Driver Vehicle Licensing Authority for details of motoring convictions.

Appendix 3: STFC Security Committee Terms of Reference (ToR)

Remit:

To meet on a monthly basis to share information and advise the STFC Security Officer and the SIRO/Director responsible for security.

Allocated budget:

None

Overall

1. The Security Group reports to the SIRO/Director of Corporate Services and is made up of representatives from all sites within STFC (and DLS).

2. The Security Group is chaired by STFC Security Officer, who will provide structure for the meetings, documentation related to the meetings and guidance for the activities to take place outside the meeting.

3. The remit of the Security Group is to share information and provide guidance on security matters including but not limited to:

   3.1 Report security incidents and shared learning;
   3.2 Update on current threat levels;
   3.3 Provide any information which may have security implications;
   3.4 Update on security initiatives;
   3.5 Highlight areas of concern; and
   3.6 Identify opportunities to cascade information via security staff, in-Brief and other appropriate media.

Specific Deliverables

4. The Security Group will deliver the services set out below:
   4.1 Input to the annual security review (Security Policy Framework (SPF) and Statement on Internal Control (SIC));
   4.2 Review and update the risk register;
   4.3 Respond to incidents/events/threats;
   4.4 Escalate any items requiring senior management attention or decisions;
   4.5 Assist internal/external audits as necessary; and
   4.6 Review these Terms of Reference in the January meeting each year.

Mode of Operation STFC (and DLS) Security Group

- To meet at least monthly (first Tuesday of the month wherever possible) and more frequently if required.
- Meetings to be held at RAL with video conferencing at the other sites.
- All necessary papers to be distributed prior to each meeting and actions circulated as soon as possible after each meeting.

Membership

Role(s)		Job Title
Security Group	Role	
Chair	DSO	STFC Security Officer
		Regional Head of Estates & FM South
		Manager RAL Operations/Services
		Regional Head of Estates & FM North
		Manager DL Operations/Services
	‘Site Security Manager’	Diamond Light Source (DLS)
	Site Security Manager	ROE
	Site Security Manager	DL
	Site Security Manager	RAL
	Site Security Manager	Head of Support Services SO
	ITSO	STFC Information Technology Security Officer
		Departmental Security Representatives
		SO IT
		STFC Head of Stakeholder Engagement

Appendix 4: Competence and Training

Role	Competence			Commentary
	Knowledge / Training	Skills / Experience	Attitude / Behaviours	
STFC Security Officer (Department Security Officer)	Understanding of local, national and international security threats and geopolitical affairs. Thorough knowledge of Risk Management. Sound understanding of STFC's strategic goals. Understanding of the Mandatory Requirements set out in the Cabinet Office Security Policy Framework (SPF). Attend annual CPNI / Cabinet Office briefing (or delegate).	Experience of Corporate Governance and risk management. Information-gathering skills.	Highest integrity and sound judgement. A comprehensive analytical approach toward enabling STFC goals in a secure way.	To hold Security Check (SC) clearance for regular unsupervised access to assets marked up to 'Secret' or occasional supervised access to assets marked 'Top Secret'.
Site Security Manager	Security Management Diploma (e.g. ISMI, CSMP) or higher security related qualification from a respected body (e.g. University degree)	Security, Military or Police experience at supervisory level.	Adopt 'Business partner' role towards supporting security across STFC departments.	To hold SC clearance, see above.
Security Representative (SR)	No specific training is required for this role except a thorough understanding of the content of this code.	Thorough understanding of the security risks arising from their respective Department's activities.	The will and ability to communicate a positive security message within department.	To hold BPSS clearance.

Staff with unsupervised access to HASS sources	While not offered routinely periodic seminars by Environment Agency and CTSA provide training on HASS security.	N/A	Trustworthy individual with responsible attitude.	To hold BPSS clearance as minimum.
Site Security Officers	Minimum NVQ2 Certificate in Providing Security Services or equivalent. First aid at work. Fire awareness training. Radiation awareness training. Rescue set training.	Previous experience in security / police / military desirable. Ability to adhere to STFC policies and Standard Operating Procedures.	Communication and customer service skills. Integrity and ability to handle sensitive information with appropriate discretion.	To hold BPSS clearance as minimum.
Staff, tenants, contractors, visitors and facility users	HR induction checklist and relevant Site induction training.	N/A	N/A	To hold BPSS clearance as minimum.

Appendix 5: Audit Checklist

Ref	Item	Evidenc e	Rating	Comment s
4.1.2	Has CEO appointed in writing SIRO?			
4.2.2 4.2.3	Has SIRO appointed in writing a competent STFC Security Officer and site specific Security Managers?			
4.2.4	Has SIRO submitted annual statement of assurance on security risks?			
4.3.1 4.3.2 4.3.7	Has STFC Security Officer undertaken and documented the STFC SRA and Security Plan? And is it being held securely?			
4.3.3	Are BPSS checks being undertaken for all new starters?			
4.3.4	Are STFC Security Committee meetings being held and records thereof available			
4.3.6	Is there a security incident reporting system? And is it being employed by staff?			
4.3.8	Has an audit programme been established to assess the implementation of this policy?			
4.4.1 4.4.2 4.4.3	Has site security manager undertaken and documented the site SRA and Security Plan? And is it being held securely?			
4.4.4	Are controls detailed in Site Security plan in place and effective?			
4.4.5	Are all security incidents investigated and actions taken to minimise their recurrence?			
4.4.7	Have site emergency exercises been undertaken?			
4.4.8 4.4.9	Have sites holding radioactive materials undertaken specific SRA and Security plans for these materials?			
4.5.2	Where site security measures are considered insufficient for a particular Departments assets has a Director appointed in writing a Department Security Representative			
4.5.3	Have Department Security Representatives undertaken and documented the STFC SRA and Security Plan? And is it being held securely?			
4.7.3	Have contractors and others working at STFC sites been subject to BPSS checks?			
4.7.5 4.7.7	Are staff and others aware of their site and any local security controls? And the need to report security incidents?			
4.7.8	Has Site Security Manager been informed of all radioactive materials on site? And are they the subject of a dedicated SRA?			
4.9.1	Have all staff undertaken site induction training that addresses their site security and the reporting of security incidents?			
4.9.4	Do staff wear site passes visibly and challenge those that do not?			

Appendix 6: Document Retention Policy

Records Established	Minimum Retention Period	Responsible Record Keeper	Location of Records	Comments/Justification
STFC Security Risk Assessment (SRA)	Current and past 5 years	STFC Security Officer	Local record systems	Reviewed annually, stored securely and access restricted to those with a need to have access
STFC Security Plan	Current and past 5 years	STFC Security Officer	Local record systems	Reviewed annually, stored securely and access restricted to those with a need to have access
Site Security Risk Assessment (SRA)	Current and past 5 years	Site Security Manager	Local record systems	Reviewed annually, stored securely and access restricted to those with a need to have access
Site Radioactive Materials Security Risk Assessment	Current and past 5 years	Site Security Manager	Secure Local record systems	Reviewed annually, stored securely and access restricted to those with a need to have access
Site Security Plan	Current and past 5 years	Site Security Manager	Local record systems	Reviewed annually, stored securely and access restricted to those with a need to have access
Site Radioactive Materials Security Plan	Current and past 5 years	Site Security Manager	Secure Local record systems	Reviewed annually, stored securely and access restricted to those with a need to have access
Local Security Risk Assessment (SRA)	Current and past 5 years	Departmental Director	Local record systems	Reviewed annually, stored securely and access restricted to those with a need to have access
Transport SRAs for valuable materials/ equipment	Current and past 5 years	Relevant manager	Local record systems	Reviewed on completion of the transportation and receipt of materials/equipment.
Physical Security Incident report	All	STFC Security Officer	Local record systems	Reviewed annually, stored securely and access restricted to those with a need to have access
Physical Security Incident Investigation Reports	All	Site Security Manager	Local record systems	Reviewed annually, stored securely and access restricted to those with a need to have access
CCTV recordings	At least 15 days	CCTV Data Controller	Local record systems	
Access control system journals	3 years	Site Security Manager or	Local record systems	

		access control system owner		
Appointments:				
STFC Security Officer	Most Recent	SHE Group	SHE Directory	
Site Security Manager	Most Recent	SHE Group	SHE Directory	
Security Representative (SR)	Most Recent	SHE Group	SHE Directory	