POLICY

Title: PHYSICAL AND PERSONAL SECURITY

Policy owners	Head of Information Security (Suffolk) and Head of Professional Standards (Norfolk)
Policy holder	Information Security Manager (Suffolk) and Information Security and Vetting Manager (Norfolk)
Author	Information Security Manager (Suffolk) and Information Security and Vetting Manager (Norfolk)

Policy No.	158

Approved by

Legal Services	√
Policy owner	√

Publication date	30.03.12.
Review date	30.03.14.

Note: *Please send the original Policy with both signatures on it to the Norfolk CPU for the audit trail.*

Index

1 Purpose of this Policy 3
2 Personnel Security 3
3 Personal Security 3
4 Responsibility for Security of Premises 4
5 Principles for the Physical Protection of Information 4
6 Perimeter Security 5
7 Premise Design/Construction 6
8 Delivery/Loading Areas 7
9 Premises Entry Control 7
10 Control of Visitors and Identification (ID) 7
11 Challenging Unidentified Individuals (not applicable to those in custody) 8
12 Asset Security 9

Legal Basis

(Please list below the relevant legislation which is the legal basis for this policy). You must update this list with changes in legislation that are relevant to this policy and hyperlink directly to the legislation.

Legislation specific to the subject of this policy document

Act (title and year)
Data Protection Act 1998
Computer Misuse Act 1990
RIPA 2000
Human Rights Act 1998
Freedom of Information Act 2000
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
Copyright, Designs and Patents Act 1988
Obscene Publications Act 1959
Telecommunications Act 1984 (computer transmission of obscene or indecent images via public telecommunications system)
Protection of Children Act 1978 (re possession/distribution of indecent photos of children)
Criminal Justice Act 1988 (re possession/distribution of indecent photos of children)
Official Secrets Act 1989

Other related Documents:

ACPO Community Security Policy	Information Technology Standard 17799:2005
ACPO Vetting Policy	ISO 27001 – Information Security Management
MOPI	Home Office Police Buildings Design Guide
Cabinet Office HMG Security Policy Framework	Home Office Custody Design Guide
HMG Infosec Standards	Secured by Design and Standards LPS1175 and BSPAS24
CESG Memorandum (Passwords)	Information System Codes of Connection (CoCos)
Clear Desk and Screen Policy	Electronic Information Security Policy
Government Protective Marking Scheme Policy	Information Security and Management Policy
Management and Reporting of Security Incidents Policy	Anti-Virus Incident Response Policy
Secure Management of Confidential Information Systems Policy	

NORFOLK	SUFFOLK
INFORMATION SECURITY SINGLE POINT OF CONTACT	
Jim McIntyre MCINTYREJR@NORFOLK.PNN.POLICE.UK 01953 425699 Ext 2809	Lee Scott LEE.SCOTT@SUFFOLK.PNN.POLICE.UK 01473 613815
ICT SINGLE POINT OF CONTACT	
Joint ICT Service Desk ICTSERVICEDESK@NORFOLK.PNN.POLICE.UK 01953 424747 (1)	

1 Purpose of this Policy

1.1 To ensure:

- measures and documented requirements ensure security as per the ACPO Community Security Policy and Data Protection Act 1998;
- staff are afforded an appropriate level of security;
- building design is considered in terms of security;
- information security is maintained and developed to a high standard; and
- Constabularies asset inventories are centralised and maintained.

2 Personnel Security

2.1 The Vetting Unit vets applicants, staff, contractors, consultants and some suppliers. See the Vetting Policy for further information.

2.2 Human Resources must ensure:

- employment terms and conditions define employee security responsibilities;
- job definitions cover security roles and responsibilities;
- staff sign out to a Confidentiality Agreement and the Official Secrets Act;
- certain roles are supplied additional agreements.

2.3 Staff violating security policy/procedure may be formally disciplined.

3 Personal Security

3.1 Managers should arrange responsibilities to reduce vulnerability or temptation to commit fraud/error (e.g. split purchase order raising and placing). Ensure, where possible, that collusion must occur to bypass operational security.

3.2 The Constabularies remind all staff, regardless of role, that they are responsible for ensuring that they properly use information systems and assets. Information Asset/System Owners and managers must implement robust procedures to prevent instances where superiors can instruct subordinates to inappropriately bypass necessary processes and controls.

3.3 Managers shall risk assess the need to give potentially coerced staff network/Contact and Control Rooms linked duress alarms via radio and mobile data.

3.4 Managers shall risk assess the allocation of security responsibilities based on the individuals personal vulnerability and where this presents an issue consideration should be given to their present and potential condition. Consideration should be given regarding if the individual has any disabilities or is restricted duties and how this could affect their ability to fulfil any assigned security responsibilities.

4 Responsibility for Security of Premises

4.1 Those responsible for a premise are responsible for its security. Typically, this will be Commanders for premises on areas, the Head of Protective Services for PHQ and Heads of Departments for specialised locations. Outsourcing contracts, which delegate this responsibly to the supplying contactor, may cover particular locations.

4.2 Facilities are responsible for installing and maintaining both non-structurally integral security controls and structurally integral security controls.

4.3 Information Security is responsible for premise security audits.

4.4 Staff should be aware of security issues (e.g. open doors/windows/faulty security equipment), personally rectifying or reporting to an appropriate department (e.g. Facilities).

4.5 Staff leaving an office at the end of a shift must secure all windows and doors.

4.6 Only authorised audio/visual recording equipment may be used on Constabularies premises (e.g. CCTV, ANPR, training video, photo shoot, etc).

4.7 Any member of staff issued with security devices, such as keys, access control cards and ID cards, are responsible for their use and security at all time. When not in use, these musts be securely stored.

4.8 Consideration must be given to staff members who are disabled, in poor health or on restricted duties that may be more vulnerable and therefore it may be unsuitable for them to hold their security devices at home. In such circumstances, line managers should discuss with the individual as to whether they have any concerns and, where raised, consider alternatives in consultation with Information Security.

5 Principles for the Physical Protection of Information

5.1 Physical security protection should be based on defined perimeters (or areas) and achieved through a series of strategically located barriers throughout the location. The requirements and siting of each security barrier should depend upon the value of the assets and services to be protected, as well as the associated security risks and current protective measures.

5.2 Each level of physical protection should have a defined security perimeter around which a consistent level of security protection is maintained. This will range from obstructions (such as screens) to physically separated and secured areas.

5.3 The following are guidelines for the improvement of physical protection for information. The security of the perimeter should be consistent with the value of the assets or services under protection.

- Protectively marked information should not be displayed or otherwise processed in areas of public or insecure accommodation (corridors, reception areas etc.).
- Support functions and equipment (e.g. photocopiers and fax machines) should be located to minimise the risks of unauthorised access to secure areas and secured information.
- Physical barriers should, if necessary, be extended from floor to ceiling to prevent unauthorised entry.
- Other personnel should not be made aware unnecessarily of the activities within a secure area.
- Prohibition of individuals working alone should be considered, both for safety and to prevent opportunities for malicious activities.
- Computer equipment should be housed in dedicated areas separate from third party-managed computer equipment.
- When vacated, physically secure areas should be locked and periodically checked.
- Support services personnel should be granted access to secure areas only when required and authorised. Where appropriate, their access should be restricted (particularly to secured information) and their activities monitored.
- Areas of public access (e.g. Public Enquiry Offices) should be clearly defined. No sensitive material, systems or activities should be undertaken in areas subject to public access.
- The receipt, storage and disposal of equipment should follow the Protective Marking procedures to ensure building and computer room security is not compromised and that any holding areas remain secure.
- A clear desk policy is in place throughout all Constabularies premises in order to reduce risks of loss or compromise to information.

6 Perimeter Security

6.1 Where deemed necessary by risk assessment, and proportional to assessed risk, Constabularies premises must have, as per physical standards:

- the security perimeter should be clearly defined with warning notices where appropriate;
- adequate security measures to prevent unauthorised access to premises;
- CCTV systems;

- perimeter security lighting (possibly motion sensor activated);
- motion sensors/alarms.

6.2 When maintenance/changes occur at secure areas, assess security issues and implement tighter controls (e.g. staff supervision, reactivating access systems, etc).

6.3 Security guards will be considered (if necessary) to provide a deterrent to criminals and to others who might plan a covert attack.

6.4 Photography, recording or video equipment should not be allowed, unless authorised within the security perimeters.

7 Premise Design/Construction

7.1 All premises should allow information processing to take place in a secure environment appropriate to the protective marking of information held or processed in the premises. Controls and procedures to maintain Business Continuity, including regular risk assessments, should be followed to protect against theft, fire, explosions, flooding, power loss or surges and any other forms of natural and man made disasters.

7.2 All rooms and network equipment rooms and any other office processing or supporting critical business activities should be protected by physical barriers and be located away from areas of public access. Additional considerations and assessment should be given to the risks of theft, fire, explosions, flooding, power loss or surges and any other forms of natural and man made disasters.

7.3 A premises structure must be assessed in accordance with the Home Office Police Buildings Design Guide and Home Office Custody Design Guide. All measures to create 'secure rooms' are to be risk assessed and approved by a suitable advisor (e.g. Special Branch Counter Terrorism Security Advisor, Information Security).

7.4 Secure Rooms are locations and equipment (e.g. Radio (e.g. Base Stations, Comms centre), Telephone (PABX), IT Rooms, MIR, CAIU, etc). Secure Rooms may require extra security, subject to a risk assessment of the whole premises, such as:

- additional door controls (e.g. Digi Lock, SALTO) to restrict staff access;
- being windowless, above ground floor or accessed via a locked room;
- holding secure room keys in a key safe accessible to authorized staff (holding spares separately from working keys in a secured container);
- a key register for signed in/out keys, showing who, when, where, why;
- only issuing code pad codes/swipe cards to authorised persons;
- performing code changes on a regular basis and if compromised;
- if an equipment room, extra visitor and/or key sign in/out books;

- implementing CCTV/motion sensor intruder alarms to prevent and detect;
- security standard approved door locks (e.g. 5-lever mortice, deadlock).

8 Delivery/Loading Areas

8.1 Where possible and practical, delivery/loading areas should:

- be located away from other building areas to minimize biohazard cross contamination or explosion damage;
- have an incident policy with management conducting regular staff training/drills of appropriate action;
- have a secure holding area for valuable and sensitive electronic goods and controlled stationery (e.g. blank official pre-printed forms/cheques);
- restricted holding area access to authorised staff and designed to allow unloading of supplies without accessing the rest of the building;
- secure the external holding area door when the internal door is open.

9 Premises Entry Control

9.1 An entrance is a controllable barrier that must have the following implemented subject to a risk assessment of the whole premises under Secured by Design and standards LPS1175 and BSPAS24:

- outer and inner door locks to a standard that prevents forced entry (Consult Crime Reduction Officer/ Head of Estates / Facilities. Contact IST for supplementary checklists/security product specifications);
- controlled distribution of keys/cards and disclosure of access codes;
- Automated Access Control System including protected power supplies. These fail safe for evacuation purposes, so remain vigilant if this happens. Access should only be granted to authorised personnel and such access permissions are to be immediately revoked when no longer required;
- CCTV systems for sensitive buildings and rooms;
- Suitable configured intruder alarms.

10 Control of Visitors and Identification (ID)

10.1 Entry controls should be employed to gain access to Force premises. All personnel must wear identity passes. Visitors will be issued with a temporary pass and the date, time of entry and of departure should be recorded.

10.2 Police staff and approved visitors must wear suitable ID cards/visitor passes for clear identification. Staff must not let anyone tailgate them (following into police premises) unless identifiable and wearing an ID card/visitor pass.

10.3 An individual issued with ID or keys which enable access to

Constabularies premises and/or assets must return any and all IDs and keys on leaving the employment of either Constabularies or third party partner through which their access has been authorised.

10.4 All Constabularies premises must have a visitor's booking system to log non-staff visits (e.g. contractors, volunteers or other Police/agencies). Visitors should be booked in and out. Sensitive departments/premises (e.g. Major Investigations, Child Abuse) should require visiting staff to sign in and out.

10.5 Reception/front desks must issue visitor passes with a start/expiry (not exceeding a week post start) dates. (Reissuing passes for longer periods.) Visitors must clearly position their pass for easy identification when entering 'staff only' areas, as they lack appropriate ID.

10.6 Visitors should present two forms of ID (i.e. staff ID card and/or personal ID (e.g. preferably photo ID (i.e. drivers license, passport)) or credit/bank card) before receiving their pass, without this visitors might not get a pass. Minors do not have to supply photo ID but staff can request to see photo ID.

10.7 Staff members collecting visitors must escort the visitor/s until discharged to other staff or the visitor/s leaves the premises. Only visiting Police employees with ID cards can be 'unescorted'.

11 Challenging Unidentified Individuals (not applicable to those in custody)

11.1 Staff must challenge those found on Constabularies premises without recognised police ID (visitors/unidentified staff) or acting suspiciously, without waiting for others to do so.

11.2 Staff should ask the challenged individual(s) to verify their identity as a requirement of staying on the premises. The challenged individual (including officers and staff) should allow ID inspection and verification if staff are suspicious of their identity.

11.3 If unable to verify an identity, staff must request the individual(s) to accompany them to a manager. If the individual(s) refuses to comply with the request, then the challenger must alert surrounding staff and immediately inform a manager, who should decide on appropriate action. If staff or a visitor improperly fail to allow identity verification, staff should bring this to the attention of their Commander/Departmental Head for a decision on appropriate action.

11.4 Report incidents identified by challenging via the Information Security Incident form so that necessary measures or investigation are instigated. The Constabularies support those who comply with the policy.

11.5 Managers should have local guidance for social functions, open days etc.

12 Asset Security

12.1 The Constabularies pinpoints and values assets (information and others) through various department's asset inventories as follows:

Department	Inventory of
Estates	Building / environmental services assets
Finance	Financial assets
Transport Services	Transportation assets
ICT (Information Communications Technology)	ICT assets
Records management	Information assets
Commanders and Heads of Departments	General furniture and equipment
Human Resources	Human resource assets

12.2 The Constabularies have in place an Asset Management Policy that should be referred to for further information.

12.3 Staff must not remove Constabulary assets from Constabularies premises without appropriate manager authority. Anyone removing assets from premises is personally responsible for its security and subject to sanction if incompliant with policy (e.g. discipline/loss of access).