Parliamentary
and Health Service
Ombudsman

PARLIAMENTARY AND HEALTH SERVICE OMBUDSMAN

SECURITY POLICY

November 2012

Contents

1. Purpose

1.1. This document sets out the framework policy for security in PHSO. It provides the Policy from which all security controls, procedures, advice and education are drawn; sets out how the Office manages security; and who is responsible for delivering the policy.

1.2. This document covers protection of buildings and other assets (including our information), contractor and third party issues, personnel security, and security education and awareness.

1.3. Detailed information on PHSO's security procedures can be found in the security guidance notes on the intranet. Any questions relating to this policy should be addressed to the Security Officer in the first instance.

2. Policy Statement

2.1. PHSO recognises that security is about protecting the confidentiality, integrity and availability of its assets from an increasingly wide range of threats. An asset is anything that is of value to and necessary for the successful achievement of our business objectives e.g.: people, records, information systems, data, equipment, money, property, etc.

2.2. PHSO fully supports the aims and principles of good security practice and the security policies and procedures required to achieve these. Good security means protecting PHSO from incidents and risks that could damage our ability to operate and/or our reputation.

2.3. Our Security Policy is aimed at supporting achievement of our business aims and objectives. In designing the policy and in its operation, we are mindful of the need to ensure that our security procedures complement - rather than complicate - the ability to do our work safely, efficiently and effectively. Security controls will be risk-based and implemented proportionately. Their operation will be monitored effectively; all breaches and incidents investigated thoroughly; and action taken promptly to amend procedures where appropriate.

3. Scope

3.1. This policy applies to all permanent, contract and temporary staff and any organisation or body acting as agents of PHSO where contractual arrangements are in place.

3.2. In pursuing these policies, PHSO will comply with all relevant laws including the Official Secrets Act, Health and Safety legislation, the Data Protection and Human Rights Acts.

3.3. All Crown Servants and Contractors are, by virtue of their employment, subject to the provisions of the Official Secrets Act. Any member of staff or former member of staff who deliberately passes sensitive material to unauthorised individual(s) may be subject to prosecution under the Act. Unauthorised disclosure (leaking) of information by any member of staff will be treated as a serious disciplinary matter.

4. Key Principles

4.1. PHSO's security policies will seek to set out clearly the policies, standards and guidance we follow to ensure that appropriate levels of security and good practice is followed. We will therefore:

4.2. Use a risk management based approach to security and ensure it is widely understood what our priorities are:

4.2.1. Balance effective security controls and counter-measures with the business needs of the Office;

4.2.2. Be flexible and pragmatic where possible;

4.2.3. Be cost effective and simple in delivery;

4.2.4. Promote the benefits of good security practice as a business enabler;

4.2.5. Reflect in our security arrangements the culture and principles of the Office and of the public service generally;

4.2.6. Conduct regular audits and reviews of our security arrangements to ensure compliance with procedures, and take action on any non-compliance as appropriate;

4.2.7. Deal with security policy breaches through positive management action and learn from security incidents;

4.2.8. Ensure that requests for information from those with a right to access are handled with necessary care;

4.2.9. Only pass information on to those with a need to know and handle such information with necessary care;

4.2.10. Recruit reliable people and ensure their positive commitment through pre-employment security checking, and good HR and line management support thereafter;

4.2.11. Induct new staff and continue to educate existing staff on security issues to increase and maintain awareness and understanding;

4.2.12. Do everything practical to ensure our information systems are protected from accidental or malicious attack;

4.2.13. Ensure that the protection and welfare of our staff are a high priority.

5. Objectives

5.1. The key objective of this policy is to protect and maintain the confidentiality, integrity and availability (CIA) of PHSO assets in support of business delivery:

5.1.1. ***Confidentiality*** means the restriction of information and assets to authorised individuals;

5.1.2. ***Integrity*** means the maintenance of assets in their complete and proper form;

5.1.3. ***Availability*** means the continuous or timely access to assets by authorised individuals.

5.2. Other key objectives are to:

5.2.1. Model best practice in security;

5.2.2. Maintain a culture which recognises the benefits, importance and value of good security practices; and

5.2.3. Define clear responsibilities for managers and staff. These are set out in Annex 3.

6. Outcomes

6.1. Fully implemented and embedded this policy will deliver the following outcomes:

6.1.1. An established governance framework for managing security issues within PHSO;

6.1.2. High awareness of security issues and responsibilities among staff;

6.1.3. Effective controls in place to ensure that all assets are adequately protected;

6.1.4. Effective monitoring, reporting and review of security issues;

6.1.5. Security risks and threats regularly reviewed and reported, and appropriate actions taken.

7. Monitoring and Review

7.1. Security will be reviewed in accordance with the cycle set out in Annex 2. This policy will be reviewed annually by the Security Committee taking into account any changes affecting the existing risk assessment, significant security incidents or new vulnerabilities.

7.2. The outcome of this will be the Security Officer's Annual Security Assurance Statement to the Ombudsman.

7.3. This report will include:

7.3.1. A revised PHSO security risk assessment taking account of the CPNI (Security Service) Annual Threat Assessment and other relevant material;

7.3.2. A review of security incidents, breaches, thefts and other losses, specific physical security issues and any recommendations for change, identified during the past 12 months;

7.3.3. A review of pre-employment security checking and any recommendations for change;

7.3.4. A review of Information Security arrangements and any recommendations for change;

7.3.5. A review of the security education programme from reception and induction through to general reminders of the importance of security to all staff and any recommendations for change.

8. PHSO Security Committee

8.1. Terms of Reference

8.1.1. To co-ordinate the delivery of security advice and guidance to the Office;

8.1.2. To discuss and develop policy responses to security events and issues;

8.1.3. To review existing security arrangements looking at risk assessment, policy, implementation and evaluation;

8.1.4. To participate in reviewing PHSO's Security Policy Framework and the Security Policies and Procedures, and to contribute to the Security Officer's annual review of security for the Ombudsman.

8.2. Membership

Chief Operating Officer
Director of Service Delivery (Chair)
Security Officer/ITSO
Deputy Director of Customer Services & Assessment
Head of HR Operations
Head of FOI/DPA
Deputy Security Officer (Secretary)
Head of the Office of the Ombudsman and COO
Parliamentary Business Manager
Director of Clinical Advice
Director of Complex Health Investigations
Head of Information & Records Management
Communications Business Manager
Head of Customer Services

8.3. Frequency of Meetings

8.3.1. Quarterly; more frequently as required.

9. Annual Security Review Cycle

9.1. Throughout the year:

9.1.1. Risk assessments following changes to vulnerabilities and threats;

9.1.2. Building security assessments;

9.1.3. Incidents and trend analysis;

9.1.4. Review/amend the security policies and procedures, and the Security Policy as necessary.

9.2. April

9.2.1. CPNI (Security Service) Annual Threat Assessment received and considered.

9.3. May

9.3.1. Security Officer completes Annual Security Assurance Statement for the Ombudsman and Executive Board. Any changes to existing security policies and procedures proposed and considered.

9.4. Proposals for change fed into business planning cycle as necessary.

10. Responsibilities

10.1. The Ombudsman is ultimately responsible for security at PHSO.

10.2. The Chief Operating Officer (COO) is PHSO's Executive Board member with specific responsibility for security matters, and is accountable to the Ombudsman for the effectiveness of security arrangements. As such, she is also the Senior Information Risk Owner (SIRO).

10.3. The Security Committee responsibilities and membership are set out in Annex 1.

10.4. The Director of Service Delivery is responsible to the COO for delivering physical and IT security on a day to day basis, assisted by the Security Officer/ITSO.

10.5. The Security Officer co-ordinates and reports on all security arrangements including compliance with, and maintenance and review of, the policy. The postholder is responsible for ensuring that the detailed security notes and procedures are kept up to date and for issuing regular reminders to the Office on security issues. The postholder is also responsible for liaising with the landlord on building security issues.

10.6. The Security Officer/ITSO provides technical advice and guidance on ICT security matters, and has responsibility for advising the Director of Service Delivery on the development, implementation and monitoring of ICT policy.

10.7. The Head of Information & Records Management is responsible to the COO for delivering information security, including liaising with the Information Commissioner's Office regarding data breaches.

10.8. The Head of Human Resources is responsible for ensuring all PHSO staff, including agency and temporary staff, undergoes the appropriate pre-employment security checks, and for advising on any disciplinary procedures following a breach of security.

10.9. Certain key posts in the Office are deemed to require the holder to undergo a higher form of security clearance - National Security Vetting (NSV). The Security Officer is responsible for offering advice on which posts need such clearance and the procedures entailed for securing a clearance. The Deputy Security Officer is responsible for ensuring that the list of NSV post holders is kept updated.

10.10. All Directors and Heads of Functions are responsible for ensuring that PHSO security policies are implemented within their business areas, and for compliance by their staff.

10.11. Individual members of staff and contractors have a personal responsibility to ensure they adhere to PHSO security policies and procedures.

11. Detailed Security Procedures

11.1. Detailed security procedures are set out in the Security guidance on the intranet within the following framework:

11.1.1. Information Security;

11.1.2. Security governance;

11.1.3. Risk management;

11.1.4. Compliance;

11.1.5. Asset Control

11.1.6. Protective marking;

11.1.7. Personnel security;

11.1.8. Physical security.

11.2. Security in relation to Business Continuity Management (BCM) is covered within PHSO's separate BCM policy framework and guidelines.