The Leveson Inquiry into the Culture Practices and Ethics of the Press

Exhibit Ref: JK/4

Witness: ACC Jerry Kirkby

Date Produced: 21 March 2012

Description: Surrey Police Acceptable Use of Surrey Police Computers Procedure

Signature: ....

Document Attached.

Procedure

Force Information Security

Governing Policy : Force Information Security Policy
Aim :

Surrey Police recognises the importance of all Force information assets and the need for proper, effective management of all information processes within the Force. Therefore, it is important that there be in place sufficient and adequate information security safeguards and countermeasures to provide the continued availability, integrity and confidentiality of force information and information systems.

The Force Information Security Policy provides the overall strategy for information security throughout the Force. This policy forms the framework for policies relevant to information security including the SPIKE System Security Policy, Security Operating Procedures and Firewall Flow Policies.

Introduction

The Force Information Security Policy has been produced to provide baseline security requirements in order to safeguard the confidentiality, integrity and availability of all information held by Surrey Police. The purpose of this policy is not to obstruct but enable the information sharing processes of Surrey Police. All personnel with access to information owned by Surrey Police will be made aware of and required to comply with the provisions of the policy.

The policy sets out to implement the requirements of the ACPO/ACPOS Information Systems Community Security Policy together with the business and operational demands of Surrey Police.

Index

The Strategy or Surrey Police
Roles and Responsibilities
Security Incidents
Development and Implementation of IT Applications
Expectation of Privacy and Audit
Audit
Training and Awareness
Discipline
Documentation

Text

The Force and its employees have an obligation to comply with United Kingdom and European Community legislation in respect of the use of information processing

systems. This legislation includes:

- The Data Protection Act 1998
- The Human Rights Act
- The Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990
- The Official Secrets Act.

The Force Information Security Policy applies to all manual and electronic information processes owned by Surrey Police. The policy provides a common basis for the Force to develop, implement and measure effective information security management practice.

The policy applies to all personnel contracted to work for the Surrey Police, Special Constables, temporary personnel and trusted employees from agencies and organisations who by the nature of their role require access to Surrey Police information systems.

In compliance with the ACPO/ACPOS Information Systems Community Security Policy, the information security policies and procedures will be based on sections 1–12 of the British Standards Code of Practice for Information Security Management (BS7799) covering both technical and non – technical aspects. These include the following:

- Security policies
- The security structure
- Asset classification and control
- Physical and environmental security
- Communication and operational management
- Access control
- Systems development and maintenance
- Contractual controls
- Training and awareness
- Business continuity planning
- Compliance checking

THE STRATEGY OF SURREY POLICE

To meet the requirements of managing the 'electronic' information, the Force is employing the HMG Information Security Standard, Security Policy Portfolios. The policies, procedures and countermeasures provided by this security standard comply with the requirements of BS7799 in respect of data processing security. These same policies also provide many of the procedures and countermeasures that are generic to all information security.

This document is one of a set of policies that will dictate the procedures and countermeasures relevant to all information security in Surrey Police. This set of policies includes:

The SPIKE System Security Policy. - This document will identify the threats and vulnerabilities that the SPIKE wide area network and every application connected to it is exposed to. The policy will undertake a risk assessment of those threats and vulnerabilities and based on various assertions, mandate procedural and technical countermeasures that will enable Surrey Police to manage the risk. This document also identifies to independent security auditors both the rationale and method behind the Force's approach to compliance with the Community Security Policy.

The SPIKE Security Operating Procedures – This document will describe the way in which the system is to be managed and used to ensure that it conforms to the System Security Policy. The Security Operating Procedures for SPIKE describe the responsibilities of the Director of Information Services, System Administrators/Services Managers, the Force Information Security Officer and users of the system.

System Interconnection Security Policy – These policy documents may also be known as Firewall Flow Policies. The purpose of these documents is to manage the Firewall and associated software that protects the SPIKE wide area network at every external connection.

Stand alone systems and mobile computing - Stand-alone workstations or systems working on a local area network not connected to the SPIKE wide area network will require individual System Security Policies and Security Operating Procedures. Laptop computers and other mobile computing systems that are capable of being attached to the SPIKE wide area network will be used in accordance with the SPIKE System Security Policy.

ROLES AND RESPONSIBILITIES

Ownership of the Force Information Security Policy.

The Force Information Security Policy is owned by the Chief Constable who has authorised the Force Information Assurance Governance Board to accredit and assure compliance with the Policy. The Force Information Assurance Governance Board is also required to assure compliance with the ACPO/ACPOS Information Systems Community Security Policy.

The Information Assurance Governance Board.

The Information Assurance Governance Board shall meet as required and at least every six months. The Board is responsible for:

- Review and accredit the Force Information Security Policy and Force Security Operating Procedures.
- Review and approve specific roles and responsibilities for information security across the Force.
- Agree, promote and support the Force information security initiatives and security awareness.
- Monitor and review all reported security incidents or where a breach of

security is suspected.
- Co-ordinate the implementation of specific security measures for new systems or services.

The Information Assurance Governance Board will identify by post personnel in each Stream or Department who will implement and administer the requirements of the Force Information Security Policy and Force Security Operating Procedures.

The Director of IS

The responsibility for the management of the force Information Technology services in accordance with all force information security policies is devolved to the Director of Information Services.

All data and equipment relating to Surrey Police IT systems is under the control of the Director of IS who is also responsible for the management of all personnel and equipment within IS the Force IT infrastructure.

The Director of IS is not responsible for either the quality or content of the data when created by the users. The Director of IS is responsible for the maintenance and safeguard of the data in accordance with force information security policies.

Stream Leads and Heads of Departments

Responsibility for IT equipment and server rooms located outside of the responsibility of the Director of IS is devolved to the respective Stream Leads or Head of Department whilst still remaining under the control of the Director of IS.

Stream Leads and Heads of Department are responsible for the security and management of all information processes within their jurisdiction.

Information Security Officer

The post and role of Information Security Officer (ISO) is a requirement of compliance with the Community Security Policy. The Information Security Officer has a primary function to ensure that there is a focal point in the organisation for security issues, to provide advice on information security matters and to ensure that the Community Security Policy and the Force Information Security Policy are implemented and maintained within the Force. It is the responsibility of the Information Security Officer to report all security incidents to the Information Assurance Governance Board.

The Force Information Security Office, in compliance with the Community Security Policy has a duty to ensure that all organisations that are connected to the SPIKE wide area network comply with that policy.

Responsibilities of system users.

All system users have a duty to comply with force information security policies and to report all security incidents to the Force Information Security Officer. System

users are also responsible for the quality and content of the information that they create.

Responsibilities of line managers.

Line managers have a duty to enforce compliance with policies by the regular monitoring of staff IT accounts and information processes. All security incidents will be reported to the Force Information Security Officer.

SECURITY INCIDENTS

Employees must report any real or potential information security incident to the Force Security Advisor as soon as practicable by telephone or email and giving as much detail about the incident as is known.
An information security incident is defined as a breach of policy or an adverse event that has led or could lead to a compromise in the confidentiality, integrity, or availability of information owned or processed by Surrey Police. Incidents may be accidental or malicious. Examples of incidents are:

- unauthorised access to information
- action that leads to unauthorised denial of access to information
- unauthorised modification of information
- unauthorised disclosure of information
- failure to protect information in line with the relevant procedure (eg clear desk,
- unauthorised access to the system
- failure to comply with physical security requirements (eg not wearing your security pass or allowing unknown people to tailgate through security doors/barriers.)
- loss or theft of assets containing information
- allowing a person to start work for Surrey Police or access information prior to confirmation of their security clearance approval

This list is not exhaustive.

The Force Security Advisor will either investigate the matter directly or assist and guide the Information Asset Owner in an investigation.

At the conclusion of an investigation, the Force Security Advisor will conduct a lessons learnt exercise and recommend actions to minimise any future risk. If possible, the cost of the incident in respect of financial cost, resource cost and reputational harm will also be assessed.

The Force Security Advisor will record all information security incidents and will provide statistical information to the relevant Information Assurance Governance Body for review.

DEVELOPMENT AND IMPLEMENTATION OF IT APPLICATIONS.

Development - using the SPIKE System Security Policy as a baseline, a security

risk analysis must be undertaken for all applications with the resulting security and legislative requirements incorporated into the specification or statement of requirement. This will be carried out in consultation with the Force Information Security Officer.

Implementation - in consultation with the Force Information Security Officer, the project manager will be responsible for all aspects of Information System security in the implementation of an application or infrastructure project. This will be based on carrying out a further security risk analysis using the earlier review as a basis. No application will be implemented without a technical operating manual (for use within IS) and user operating procedures (specific to the application) being in place.

All applications must have a nominated system owner who shall ensure that applications within their responsibility are only used for their intended purpose.

Technical operating manuals will include all facets of the operation of the application including back up procedures.

Use of applications - Applications will only be used for the purposes permitted in their operating procedures. Any proposed changes in use of the application must be submitted to the System Owner. An assessment will be undertaken to identify any change in the risk relevant to the System Security Policy.

Access Data bases and spreadsheets

Access databases and spreadsheets that hold personal or restricted information will not be developed at local level. Requests to hold such information will be routed via the Force Information Security Officer who will consult with IS and advise on an appropriate course of action.

EXPECTATION OF PRIVACY AND AUDIT

All Surrey Police information processes, which includes computer applications, telephone transmissions, word processing, exchange mail, Internet E mail and Web browsing, are intended for official police purposes. Limited use for personal or private purposes is acceptable, where this use does not impact on the business of Surrey Police. Use for any other purpose such the playing of computer games, experimental programming or the removal of any computer component or article (except where specific authorisation has been given) for home use is prohibited. The following activities are expressly prohibited:

- illegal, fraudulent, or malicious activities
- political or religious lobbying or canvassing
- activities for the purposes of personal or commercial financial gain, for instance solicitation of business or services
- storing, processing or displaying offensive or obscene material, such as pornography, "hate literature
- annoying or harassing another individual, for instance, by sending chain letters, uninvited e-mail of a personal nature or by using lewd or offensive language

- using another individual's account or identity, for example, by forging e-mail
- viewing, altering or deleting other users' files or communications without appropriate authorisation or permission
- attempting to circumvent or defeat security measures without prior permission from the Director of IS.
- introducing unofficial software or files (e.g. sound, graphics files, games or screensavers) from any source (including from floppy disk, CD, e-mail or by download from the web) without appropriate authorisation or permission
- permitting any unauthorised individual to access SPIKE
- modifying or altering the operating system or system configuration without permission
- breaking copyright through scanning or electro-copying entire documents (or extracts) from commercial publications without first obtaining permission from the relevant authorities

Where it is an operational requirement to store, process or display offensive or obscene material, such as pornography and "hate literature", such activity will only be undertaken by individuals who are personally authorised by a Stream Leads / Department Head in consultation with the DCI PSD.

AUDIT

All personnel within the organisation deal with sensitive matters requiring high professional and ethical standards. In order to ensure that these high standards are maintained by all employees, telephone conversations, fax, modem, e-mail and usage of IT systems may be recorded or monitored.

Overt Monitoring

Surrey Police reserves the right to monitor all information processes within the Force. Overt monitoring shall be conducted by line supervisors in the presence of the subject of the audit. Line managers and supervisors have a responsibility to satisfy themselves that their staff are complying with the force standard.

Covert Monitoring

Covert monitoring will only be used where the level of intrusion will be proportional to the issue being investigated and/or evaluated for compliance with professional standards.

The procedures for covert monitoring are as follows:

a) The authority of an ACPO rank officer / DCI PSD must be obtained in writing.
b) The request is forwarded to IS by PSD who will record the subject and nature of the audit.
c) The audit must be for a specified time period.

Monitoring of Telephone Communications

The authority to monitor internal telephone communications within Surrey Police will be given by the Acting Deputy Chief Constable or an officer of ACPO rank.

TRAINING AND AWARENESS

All personnel in the Force will receive appropriate training with regard to information security and will be required to reaffirm compliance with the Security Operating Procedures annually.

DISCIPLINE

Contravention of this policy and any associated information security policy mandated by the Information Security Management Committee is in breach of the Police Code of Conduct and the civilian support staff discipline arrangements.

DOCUMENTATION

Information security documentation will be in the format of HMG Infosec Standard No 2, Accreditation Document Sets.

Monitoring

This policy will be reviewed at yearly intervals and more frequently as necessary

---

Approved By : (Command/Dept Head)	ACO – Support Services
Department :	Professional Standards Department
Author :	Force Security Advisor
Date Created :	04/03/2011
Consultation : (approved date)	Minor updates approved by P&P Team 09/03/2011
Next Review Due :	31/03/2012
File number :	708-6-20
Audit Status :	Data Protection - Expires 08/02/2013 Health and Safety - Expires 04/01/2013 Equality Impact - Expires TBA Human Rights - Expires TBA
See Also :	Force Information Security Policy Acceptable Use of Computers Passwords Force Information Risk Appetite Statement

Document Classification : Not Protectively Marked