Association of Chief Police Officer of England, Wales & Northern Ireland

Association of Chief Police Officers in Scotland

ACPO / ACPOS

Information Systems Community Security Policy

Status:	Version 3.3 - Approved by ACPO IMBA on 29th September 2009
Implementation Date:	March 2009
Review Date:	March 2010

CONTENTS PAGE

SECTION 1 - PREFACE

1 STRATEGIC AIMS OF THIS POLICY

1.1 Enable the delivery of core operational policing by providing appropriate and consistent protection for the information assets of member organisations.

1.2 Comply with statutory requirements and meet ACPO/ACPOS expectations of the Police Service to manage information securely.

1.3 Help assure Her Majesty's Government that Police Service elements of the Critical National Infrastructure (CNI) are appropriately protected.

1.4 Facilitate effective participation with Transformational Government strategies.

SECTION 2 – POLICY

2 INTRODUCTION

2.1 The Association of Chief Police Officers of England, Wales and Northern Ireland and the Association of Chief Police Officers in Scotland (ACPO/ACPOS) recognise that information, including the supporting processes, systems and networks, is a valuable asset to the Police Service, other members of the wider Pan Government Community and contracted third parties.

2.2 Responsibility for determining Information Assurance policy, implementing that policy and acting as the regulatory authority is invested in the Police Information Assurance Board (PIAB) which reports to the ACPO Information Management Business Area (IMBA) and includes representation from ACPOS.

2.3 In line with 1.2 above, this policy is owned and maintained by the PIAB.

3 PURPOSE

3.1 The ACPO/ACPOS Information Systems Community Security Policy (CSP) details the strategy for the security of information processes throughout the police community and forms a framework for other subordinate policies including:

- System Interconnection Security Policies
- Force Information Security Policies
- Risk Management and Accreditation Document Sets
- Codes of Connection to National Systems and Services
- Business Continuity Plans,
- Security Operating Procedures

4 GOALS AND PRINCIPLES

4.1 Information exists in many forms and can be printed or written on paper, stored electronically, transmitted by post or electronic means, shown on films or spoken in conversation. ACPO/ACPOS supports the need for appropriate safeguards and the effective management of all information processes, and are committed to helping protect all community member information assets from identifiable threats, internal or external, deliberate or accidental, ensuring Confidentiality, Integrity, Availability and Non-repudiation of information.

4.2 This policy provides the necessary controls to mitigate against the consequences of the Police Service being exposed to unacceptable business risks. These risks include the safety of operational Police Personnel, the compromise of sensitive operations and ultimately loss of public confidence.

4.3 Information Assurance will be achieved by undertaking risk assessments and implementing appropriate controls, covering policies and procedures for physical security, personnel security and technical security.

4.4 The Police Service shall ensure that information systems and processes comply with all applicable legislation and regulatory requirements which include:

- The Data Protection Act 1998
- The Human Rights Act 1998
- The Computer Misuse Act 1990
- The Official Secrets Acts 1911-1989
- The Copyright, Designs and Patents Act 1988
- The Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Equivalent Legislation applicable to community members outside England and Wales.

4.5 Compliance with these requirements is primarily the responsibility of two ACPO portfolios. The Data Protection (DP) and Freedom of Information (FOI) legislation portfolio is responsible for ensuring that police information and processing complies with the principles contained in Data Protection and Freedom of Information legislation. The Information Assurance portfolio is responsible for ensuring that the necessary measures are taken to protect the confidentiality, integrity and availability of all its information systems. Conflicts with obligations placed on the service by DP and FOI legislation shall be referred to the DP and FOI portfolio for decision.

5 THE THREAT

5.1 Generic threats to information security emanate from many sources including Foreign Intelligence Services (FIS), subversive organisations, terrorist and criminal groups, investigative journalists, disaffected personnel, members of the public and natural disasters including fire and flood. These threats may manifest themselves via the unauthorised activities of personnel (due to inadequate awareness training, disinterest, disaffection or coercion), the interception of communications (electronic and manual), physical disruption (including criminal damage and theft) and unauthorised penetration (internal and external). All such breaches of security may result in the loss of Confidentiality, Integrity and Availability or the incorrect repudiation of information and information assets.

5.2 In conjunction with other Government agencies, regular assessments will be undertaken to identify specific threats to police systems. These will be provided to the PIAB and promulgated by the NPIA Information Assurance team.

6 APPLICABILITY

6.1 This Policy is mandated for all members of the police community currently defined as those forces and agencies constituted under the Police Act 1996; the Police (Scotland) Act 1967; British Transport Police (BTP), Guernsey Police, Isle of Man Constabulary, Ministry of Defence Police (MDP), Police Service of Northern Ireland (PSNI), States of Jersey Police, Serious Organised Crime Agency (SOCA), Scottish Police Services Authority (SPSA), and the National Policing Improvement Agency (NPIA).

6.2 ACPO/ACPOS or the PIAB may also consider and identify other organisations to which this policy will apply.

7 SCOPE

7.1 The CSP encompasses all manual and electronic information processing systems and provides a mechanism by which Community members and contracted third parties can develop, implement and measure effective information security management systems/strategies and countermeasures to identified threats and vulnerabilities.

7.2 The CSP applies to all information assets owned by members of the Community whether or not such information is being stored or processed on their premises and should be considered as the primary reference document when developing local information assurance policies where applicable.

8 RESPONSIBILITIES

8.1 Each member will implement and maintain strategies enabling information to be managed and secured ensuring Confidentiality, Integrity, Availability and Non-repudiation.

8.2 When required to do so, members must demonstrate compliance with this policy using the current methodology promulgated by the PIAB.

9 COMPLIANCE STANDARDS

9.1 ACPO / ACPOS has adopted a number of Government and Industry compliance standards that provide the foundation and framework for applying, implementing, managing and measuring effective information assurance controls to common criteria.

9.2 Compliance with these standards is necessary to provide assurance to ACPO / ACPOS, Pan Government Departments and other community members that the risk to community information and interconnected community systems can be shown to have been mitigated to acceptable levels.

9.3 The following standards have been adopted and together form the foundations upon which this policy is based and shall be used by the community to which this policy applies as benchmark requirements:

- Cabinet Office HMG Security Policy Framework[1] which includes HMG Information Assurance Standards[2] and Memoranda (published on behalf of HMG by CESG)
- ISO/IEC 27001:2005 Information Technology - Security techniques - Specification for an Information Security Management System
- Statutory Code of Practice on the Management of Police Information 2005
- ACPO Guidance on the Management of Police Information (MoPI) 2006
- Electronic Information Processing Security Notices (S(E)N) issued by Cabinet Office Security Policy Division.
- HMG Information Assurance Maturity Model and Assessment Framework
- The ACPO National Vetting Policy for the Police Community (and the equivalent vetting standards in non Police agencies)

10 COMPLIANCE REQUIREMENTS

10.1 In order to comply with the requirements of the CSP, members must:

- Undertake a risk assessment and accreditation process approved at local SIRO level for systems with connections to the CJX and other national information systems.
- Submit Risk Management and Accreditation Document Sets (RMADS) for member's domains connecting to national systems to the National Accreditors for Police Systems.
- Complete and submit on an annual basis a CSP compliance return as determined by the PIAB via the NPIA National Accreditors for Police Systems. (Currently the CSP Matrix)
- Provide evidence of independent auditing in accordance with any audit requirements issued by PIAB.
- Immediately report via PolWarp or the NPIA Information Assurance Team any incident that has the potential to compromise the security of national systems.
- Submit a quarterly return of lower level incidents to NPIA via Polwarp to enable patterns and trends to be analysed.

[1] Available via the CPNI Extranet.

[2] The mandatory measures contained within the Government report Data Handling Procedures in Government – June 2008 generally known as the Hannigan report have been incorporated in HMG Information Assurance Standard No. 6)

11 REFERENCE DETAILS

11.1 CESG

CESG is the Information Assurance (IA) arm of GCHQ based in Cheltenham. It is the UK Government's National Technical Authority for Information Assurance. As the National Technical Authority, CESG produces a number of HMG Information Assurance and COMSEC Standards and Memoranda, which provide guidance and national policy. All CESG Memoranda and Standards form part of the Government framework. They must be considered and their applicability assessed in all cases where Government (including Police) information is being held and processed.

11.2 Cabinet Office HMG Security Policy Framework

Issued in December 2008, the Security Policy Framework (SPF) contains the primary internal protective security policy and guidance on security and risk management for HM Government Departments and associated bodies. It is the source on which all localised security policies should be based. The framework supersedes the Manual of Protective Security and has been made publicly available for the first time; however, it has clearly been necessary to restrict access to some technical and procedural material on security grounds. Whilst it is recognised that security policies will differ according to the range of business and risks faced by each organisation, the framework does set out the minimum security requirements which are mandatory for all Government Departments and Agencies. The framework also provides technical information, advice and guidance to support implementation of the policy requirements.

11.3 ISO/IEC 27001

ISO/IEC 27001 is an auditable international standard which defines the requirements for an Information Security Management System (ISMS). The standard is designed to ensure the selection of adequate and proportionate security controls. The standard adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS.

11.4 Cabinet Office Security Electronic Notices

Security Electronic Notices [S(E)N] are issued by the Cabinet Office on an ad-hoc basis to provide guidance on how to counter a specific threat. In most cases, this guidance will become policy in due course.

11.5 Guidance on the Management of Police Information

The ACPO (2006) Guidance on the Management of Police Information (MoPI) follows the publication in July 2005 of a code of practice on the Management of Police Information developed by the Home Secretary, under the Police Act 1996. It forms part of the government's response to recommendations 8-11 of the Bichard Inquiry.

This guidance is designed to provide a common national framework for the management of police information, highlighting the importance of common standards in high risk areas of activity and together with the code of practice forms a package that chief officers will have regard to under the terms of the Police Act.

The guidance describes the processes for managing information which support the high level principles set out in the code. It outlines the processes for the collection, recording, evaluation, sharing, review, retention and disposal of police information.

11.6 Centre for the Protection of the National Infrastructure (CPNI)

CPNI was formed in February 2007 from the merger of the National Infrastructure Security Co-ordination Centre (NISCC) and a part of MI5 (the UK's Security Service), the National Security Advice Centre (NSAC.

CPNI provides integrated (combining information, personnel and physical) security advice to the businesses and organisations which make up the national infrastructure. Through the delivery of this advice, it aims to protect national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats.

Advisers working for CPNI cover the full range of security disciplines and are highly experienced in providing advice to national infrastructure organisations. A protected CPNI Extranet web site provides access to CPNI advice, guidance and alerts.

11.7 PolWarp

WARPs (Warning, Advice and Reporting Points) are part of CPNI's (Centre for the Protection of National Infrastructure) information sharing strategy to protect the UK's Critical National Infrastructure from electronic attack. As police forces and related agencies come to rely more and more on local and national infrastructures, there needs to be in place a capability to provide information, advice, guidance and, where necessary, broadcast alerts to force and agencies where a serious threat to local or national infrastructures is likely or actually occurring. At the request of ACPO, the police WARP (PolWARP) was registered with CPNI. PolWARP serves the police community and related agencies on the CJX.

12 REVIEW

12.1 The CSP will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance strategy to ensure that the Community continues to meet the strategic aims linked to this policy.

13 AMENDMENT HISTORY

Issue	Status	Date	Reason	Author
Version 1.0	Final	28/04/99	Publication	PITO ISO
Version 1.1	Draft	19/06/01	Review	PITO ISO
Version 1.2	Draft	18/09/01	Rewrite	Wilts Pol ISO
Version 1.3	Draft	12/10/01	Rewrite	Wilts Pol ISO
Version 1.4	Final Draft	12/11/01	Consultation	Wilts Pol ISO
Version 1.5	Final draft for ACPO IMBA	16/09/02	Rewrite for ACPO IMBA	PITO ISO
Version 2.0	Final	06/02/03	Publication	PITO ISO
Version 2.1	Draft	20/04/06	Review & update	PITO
Version 2.2	Draft	05/06/06	Amendments from PIAB	PITO
Version 3.0	Final	27/06/06	Publication	PITO
Version 3.1	Draft	25/01/09	Review & Update	Dorset ISO Chair PIAAG
Version 3.2	Draft	26/02/2009	Minor Amendments	Dorset ISO / NAPS
Version 3.3	Draft	20/03/2009	Consultation (PIIAG) & Minor Amendment	Dorset ISO Chair PIAAG
Version 3.3	Final	23/04/2009	Approved by PIAB	ACC R Toner Chair PIAB
		29/09/2009	Approved by ACPO IMBA	Ailsa Beaton Chair IMBA