Document Name	**National Policing Community Security Policy**
File Name	Community_Security_Policy_FINAL v4_3.doc

Authorisation	Information Management Business Area
Signed version held by	*National Police Information Risk Management Team*

For additional copies, or to enquire about the content of the document, please contact the National Police Information Risk Management Team at the following e-mail address information.assurance@homeoffice.pnn.police.uk

Control page

Controlling documents

Description	Document reference	Revision
SPF	HMG Security Policy Framework	Latest version
IA National Approach	National Policing National Approach 2014 – 2017	Latest version
Threat Model	National Policing Information Threat Model	Latest version
polWARP	Procedures for Use of the Police Warning, Advice and Reporting Point	Latest version

Contents

1. Introduction

1.1 National Policing recognise that information, systems and networks, are valuable assets to the police community, members of the criminal justice community, delivery partners and contracted third parties.

1.2 The information, systems and networks must be safeguarded to ensure the Police Service can meet their statutory and regulatory responsibilities. The Police Service meets these responsibilities by the implementation of this Community Security Policy (CSP) which encompasses appropriate Information Assurance (IA) policies and guidance.

2. CSP Membership

2.1 Organisations which are members of the CSP are listed at Annex A.

2.2 The Police community or the Police Information Assurance Board may also consider and identify other organisations to which this policy will apply.

3. Threat

3.1 The threats to the Police Service are well understood and are documented in the National Policing Information Threat Model.

3.2 The Police Service support 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.

3.3 To ensure these threats are suitably addressed the CSP and supporting IA policies and guidance, when implemented, and maintained by members will provide the necessary protection of police information, systems and networks assuring their confidentiality, integrity and availability.

4 Strategic Aims of CSP

4.1 The strategic aims of the CSP are to:

4.1.1 Enable the delivery of policing by providing appropriate and consistent protection for the information assets of member organisations whether national, collaborative or local assets;
4.1.2 Comply with statutory requirements and meet the expectations of the Police Service to manage information securely;
4.1.3 Help assure Her Majesty's Government that Police Service elements of the Critical National Infrastructure (CNI) and Police Service connections to HMG networks and services are appropriately protected;
4.1.4 Facilitate effective participation with the National Security Strategy, Cyber Security Strategy and any future Government information strategies.

5 Objectives

5.1 The key objective of the CSP is to enable forces, agencies and relevant organisations to understand the need to implement the IA policies identified herein, so the Police Service is able to meet its legal, statutory and regulatory requirements to a common standard, which is appropriate to ensure the continued:

5.1.1 Confidentiality of police information, systems and networks, to ensure only those authorised to access police data can do so;
5.1.2 Integrity of police information, systems and networks, so the accuracy and completeness of data is maintained and can be trusted;
5.1.3 Availability of police information, systems and networks, such that data is available to forces, agencies and other relevant organisations when required.

5.2 The supplementary objective is that by implementing and maintaining the policies, standards and guidance identified in this document there is assurance that:

5.2.1 Individual member forces, agencies and organisations of the community have the confidence that other members of the community are protecting police information, systems and networks to common standards;
5.2.2 All members of the community implement and maintain information risk management strategies and processes with appropriate risk ownership aligned with the National Policing National Approach 2014 – 2017;
5.2.3 Ownership and management of IA risks and issues will be clear and understood by individuals, teams, partners and partnerships, enabling proper consultation with stakeholders prior to IA decisions.

6. Responsibilities

6.1 Responsibility for determining IA policy, implementing the CSP and acting as the regulatory authority is invested in the Police Information Assurance Board (PIAB), which reports to the Information Management Business Area (IMBA).

6.2 In line with 6.1 above, this policy is owned and maintained by the PIAB.

6.3 All CSP member forces, agencies and organisations ensure that adequate competent resources are assigned to IA activities including:

6.3.1 Information risk management activities, including production and review of force/system Risk Management and Accreditation Document Sets (RMADS);
6.3.2 Timely completion of annual Community Codes of Connection (CoCo) returns;
6.3.3 Timely completion of annual Protective Security Risk Management Overview (PSRMO) including the Information Assurance Maturity Model (IAMM);
6.3.4 Support for compliance audits by independent professional bodies, e.g. HMIC/HMICS, and/or agents of the PIAB;

6.3.5 Thorough security incident investigation and quarterly reporting returns through polWARP in accordance with current policies and standards

6.4 There are two ACPO portfolios, which have responsibility for Information Assurance, Data Protection (DP) and Freedom of Information (FoI) compliance. The Information Assurance portfolio is responsible for ensuring that the necessary measures are taken to protect the confidentiality, integrity and availability of all Police Service information systems. The DP and FoI portfolio are responsible for ensuring that police information and processing complies with the principles contained in the Data Protection and Freedom of Information legislation. Conflicts with obligations placed on the service by DP and FoI legislation shall be referred to the DP and FoI portfolio for resolution.

7. Compliance

7.1 Forces, agencies and organisations are required to demonstrate compliance with the CSP. Compliance provides assurance to PIAB, relevant HMG organisations and other community members that risks to community information is being managed to a level acceptable to the wider CSP community.

7.2 Demonstrable compliance is provided through:

7.2.1 Timely annual submission of Community CoCo returns signed by the Force Senior Information Risk Owner to the National Accreditors for Police Systems (NAPS), acting on behalf of PIAB;
7.2.2 Evidence from force/system RMADS to support the CoCo;
7.2.3 Timely submission of the Annual Protective Security Risk Management Overview (PSRMO) signed by the Chief Constable / AO;
7.2.4 Independent audits whose scope includes elements of the required IA standards described in this policy, undertaken by HMIC/HMICS, suitable accredited auditors and/or agents of PIAB.

8. IA Standards & Guidance

8.1 This section stipulates the minimum IA policies, standards and guidance to be used for the security of information processes throughout the police community. It also forms a framework for other subordinate policies including Force Information Security Policies, Risk Management & Accreditation Document Sets, Community Codes of Connection, Business Continuity Plans, Cryptographic Control Policies and System Security Policies.

8.2 CSP IA policies, standards and guidance include as a minimum baseline:

8.2.1 HMG Security Policy Framework - The Security Policy Framework (SPF) is published by the Cabinet Office. The SPF provides central internal protective security policy and risk management for government departments and associated bodies. It is the source on which all localised police security policies should be based;
8.2.2 National Policing and PIAB approved policies, standards and guidance;

8.2.3 HMG Information Assurance Standards - The Cabinet Office and CESG co-own the HMG Information Assurance Standards which define high level policy and standards with which organisations bound by the HMG Security Policy Framework must comply. The current Information Assurance Standards cover such subjects as risk management, accreditation, cryptographic matters, user authentication and secure disposal of systems/data;

8.2.4 CESG Good Practice Guides (GPG) and other guidance - The National Technical Authority for Information Assurance, CESG, produce these documents. These documents form part of the Government IA Policy Portfolio. They must be considered and their applicability assessed in all cases where Government (including Police) information is being held and processed;

8.2.5 CESG IA Notices (CIAN) - CIANs provide a mechanism for issuing interim updates to policy and guidance. These are generally time limited and will normally be superseded within 12 months of publication, usually by being incorporated into an HMG IA Standard or CESG Good Practice Guide;

8.2.6 ISO/IEC27001 - is the international standard that defines the management system required to deliver IA within an organisation. It covers technical and non-technical aspects of Information Assurance/Security Management;

8.2.7 Guidance on the Management of Police Information - The ACPO (2010) Guidance on the Management of Police Information (MoPI) followed the publication in July 2005 of a code of practice on the Management of Police Information. For Scotland, Guidance on the Management of Police Information 2006 is the current standard. 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.

9. Review

9.1 The CSP will be reviewed at least annually (from the date of publication) and following any major change to IA strategy or the membership of the CSP community. This ensures IA requirements are reviewed and that the CSP continues to meet the objectives and strategies of the police service.

Change control

Version	Date	Record of change	Authority	Evidence of approval
0.1	13 Feb 2012	Initial Draft		
0.2	21 Feb 2012	Second Draft		
3.4	19 Mar 2012	Final Draft For PIAB		
4.0	30 Mar 2012	Final	IMBA	Minutes
4.1	1 Nov 2013	Update following organisational changes		
4.2	21 Jan 2014	Final Draft for PIAB		Minutes

Annex A – Membership of the CSP

CSP members include those forces and agencies constituted under the Police and Justice Act 2006; Police Act 1996; The Police and Fire Reform (Scotland) Act 2012. It also includes:

ACPO Central Business Area,
National Policing business areas,
TAM,
British Transport Police (BTP),
States of Jersey Police,
Guernsey Police,
Isle of Man Constabulary,
Police Service of Northern Ireland (PSNI),
Ministry of Defence Police (MDP),
National Crime Agency (NCA),
Police Service of Scotland (PSoS), (branded as "Police Scotland"),
Scottish Police Authority (SPA).,
MoD Service Police Bureau,
Civil Nuclear Constabulary (CNC)
The College of Policing.
.