<table>
<thead>
<tr>
<th>Document Name</th>
<th>National Policing Information Risk Management Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Name</td>
<td>National Policing Information Risk Management Policy v2.doc</td>
</tr>
<tr>
<td>Authors</td>
<td>David Critchley</td>
</tr>
<tr>
<td>Reviewer</td>
<td>Dave Jamieson</td>
</tr>
<tr>
<td>Authorisation</td>
<td>Police Information Assurance Board</td>
</tr>
<tr>
<td>Signed version held by</td>
<td>National Policing Information Risk Management Team (NPIRMT)</td>
</tr>
</tbody>
</table>
# Table of Contents

1. Introduction ......................................................................................3  
2. Purpose .............................................................................................3  
3. IRM Governance ................................................................................3  
4. Risk Assessments and Accreditation .................................................4  
5. Risk Appetite ....................................................................................5  
7. Shared ICT Services Risk Management .............................................5  
8. Training and Awareness ....................................................................5  
9. References ........................................................................................5  
Control page ...........................................................................................6
Information Risk Management Policy

1. Introduction

This policy stipulates the Information Risk Management (IRM) requirements necessary to enable appropriate levels of reassurance to be gained. This is due to:

- the increased reliance on National Information Systems\(^1\) and policing information by Forces, Agencies, Criminal Justice, local government partnerships and others;
- the ever changing threat landscape to and introduction of new technologies in UK Policing;
- collaborative working;
- changes in data handling requirements and legislation;
- increased personal, organisational liability and accountability; and
- the need to protect this information and the assets used to deliver it is greater than in previous years.

To address these issues it is necessary to ensure National Information Systems and assets are robustly, but proportionately and cost effectively risk managed.

2. Purpose

This policy outlines the governance requirements, the appropriate roles and responsibilities, and methodologies to be employed for ensuring the continued protection of National Information Systems/assets. These will be achieved by the identification, review, escalation and treatment of risks, and how these risks will be proportionately and cost effectively managed.

This policy is owned by the National Senior Information Risk Owner\(^2\) (SIRO) (Chair IMBA) and supports the National Policing Information Systems Community Security Policy (CSP) and the National Approach to IA by ensuring Police National Information Systems/assets and related information risks are regularly assessed and managed.

3. IRM Governance

Information Risk Management is governed through the following Police Business Areas:

The Information Management Business Area (IMBA) provides senior leadership under the Professional Practices Committee and Chief Constables’ Council, for information assurance and data protection including information risk management. The National Senior Information Risk Owner’s (SIRO) responsibilities are described in this policy.

---

\(^1\) National Information Systems and Services are described in the document “Definition of "National System" within the context of national accreditation” approved by PIAB 24 July 2012 and published on POLKA /IA.

\(^2\) The National SIRO is a member of ACPO and is the chair of IMBA.
The Police Information Assurance Board (PIAB) provides support to the National SIRO through policy development, advising and reporting on information risks. PIAB also provides a policy, guidance and reporting function to IMBA and the CSP Community of forces and agencies.

The National SIRO has responsibility for ensuring all National Information Systems are appropriately risk assessed and identified risks are managed in accordance with the National Policing Accreditation Policy. This also includes risks identified during Third Party Suppliers or Delivery Partners security reviews, Police Assured Secure Facilities (PASF) audits and audits of non police users of PNC.

The National SIRO represents the Chief Constables’ Council for all matters in relation to this Policy and is the final arbiter for all related matters. Further information on the governance can be found in the National Policing IA Governance guidance document.

The National SIRO ensures identified risks are registered in the National Risk Statement and these risks are reviewed on a regular basis in line with current requirements.

Each National Information System/Asset (or data set) is identified in an Information Asset Register (IAR) and is assigned to a National Information Asset Owner\(^3\) (National IAO). The National IAO is the appropriate National Policing Business Area Lead or individual nominated by the National Policing Business Area Lead to take responsibility for the data held in the National Information System related to the Business Area. A List of current IAOs is held by NPIRMT.

The NPIRMT provides advice and accreditation services, in supports of this policy, to UK Policing, IMBA, PIAB and the National SIRO under its mandate from PIAB.

The National Senior Information Risk Manager (NSIRM), as head of the NPIRMT, is the principal advisor to the National SIRO, manages the National Risk Statement on behalf of the National SIRO and is the central liaison officer for National IAOs and the National SIRO (for all matters relating to this policy).

The National Accreditation Manager, within NPIRMT is supported by a team of National Accreditors for the Police Service (NAPS), advises the National SIRO, through the NSIRM, on all risks raised through the accreditation of National Information Systems and manages the Accreditation Policy and processes on behalf of the National SIRO.

### 4. Risk Assessments and Accreditation

All National Information Systems (proposed, new or existing) are subject to accreditation using the technical risk methodology and risk treatment defined in the National Policing Accreditation Policy, which complies with the HMG Information Assurance Standard 1&2. This includes Privacy Impact Assessments where systems or services include the collection, use or disclosure of personal data.

\(^3\) IAO responsibilities are defined in the Cabinet Office document “Guidance on Mandatory Roles”
5. **Risk Appetite**

All National Information Systems/Services are subject to the National Policing Risk Appetite Statement. This stipulates the current Risk Appetite to be applied to all accreditation and information risk assessments. It establishes the delegation authority for information risks in the escalation case process. This is set by the National SIRO, endorsed by IMBA and PIAB and reviewed annually.

6. **National Systems Information Risk Summary**

The National Systems Information Risk Summary summaries the risks to national systems by recording and monitoring risks identified through the Accreditation process or reported separately to NPIRMT.

These statements are maintained by NPIRMT on behalf of PIAB and IMBA.

7. **Shared ICT Services Risk Management**

Where National Information Systems and ICT Services are shared with other organisations the National SIRO (or nominated representative\(^4\)) will represent the Police Service and in conjunction with the SIRO(s) of the other organisation(s) of the shared service will have a joint responsibility for establishing a governance framework. Each SIRO will retain the information risks of their own information assets processed on the shared service. They will agree an acceptable Risk Appetite Statement and ensure adherence to the Shared Service Security Policy, the Risk Appetite and any other requirements\(^5\) as necessary for the secure management of the shared system or service.

8. **Training and Awareness**

All roles identified in this policy must hold the required competencies. In a rapidly changing field, there is an expectation that everyone filling such roles will have received appropriate training and awareness briefings.

9. **References**

- HMG Security Policy Framework (SPF)
- HMG/CESG IS1 & 2 – Information Risk Management
- National Policing Information Systems Community Security Policy
- National Policing Accreditation Policy
- National Policing Information Risk Management Guidance
- National Policing IA Governance Guidance
- Cabinet Office Guidance on Mandatory Roles
- CESG Good Practice Guide (GPG) 47 Information Risk Management

\(^4\) The nominated representative will usually be the National System Information Asset Owner or other individual with delegated authority to represent the National SIRO. This role is limited to decide upon risk issues in accordance with the National Risk Appetite Statement (delegation matrix).

\(^5\) Further guidance and requirements on Shared services can be found in the CESG Good Practice Guide 47 Information Risk Management Chapter 3
## Control page

### Change control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Authority</th>
<th>Evidence of approval</th>
<th>Record of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>06/12/12</td>
<td></td>
<td></td>
<td>Initial draft of document for discussion with PIAAG</td>
</tr>
<tr>
<td>0.2</td>
<td>09/01/13</td>
<td></td>
<td></td>
<td>Submitted to PIAB for Acceptance and referral to ACPO Cabinet for Approval.</td>
</tr>
<tr>
<td>0.3</td>
<td>22/01/13</td>
<td></td>
<td></td>
<td>Minor correction made to Section 6 National Information Risk Summary from National Risk Statement.</td>
</tr>
<tr>
<td>1.0</td>
<td>18/02/13</td>
<td></td>
<td></td>
<td>Submitted to ACPO Council for Approval from IMBA</td>
</tr>
<tr>
<td>1.1</td>
<td>29/11/2013</td>
<td></td>
<td></td>
<td>Minor update to terminology and references.</td>
</tr>
<tr>
<td>2.0</td>
<td>1/2/14</td>
<td>CoP</td>
<td></td>
<td>Updated – Approved by College of Policing</td>
</tr>
</tbody>
</table>