CYBER GUIDANCE DOCUMENT

VETTING REQUIREMENTS FOR POLICING

ABSTRACT:
This guidance describes the vetting requirements for access to Policing assets including premises, information, and information systems. This document should be read in conjunction with the Statutory Vetting Code of Practice and Authorised Professional Practice on Vetting.

ISSUED	October 2023
PLANNED REVIEW DATE	September 2024
DISTRIBUTION	Community Security Policy Framework Members

STANDARD VALIDITY STATEMENT
This standard is due for review on the date shown above. After this date, the standard may become invalid.

Members should ensure that they are consulting the currently valid version of the documentation.

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
0.1	PDS Cyber	Initial version	05/10/22
0.2	PDS Cyber	Updated following National IAO & National Vetting leads consultation	28/07/23

Approvals

Version	Name	Role	Date
1.0	National Cyber Policy & Standards Working Group	National Approving Authority for Guidelines	04/10/23

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2022	07/2022
ISO 27002:2022 - Information security, Cybersecurity, and privacy protection – Information security controls	v2022	02/2022
CIS Controls	v8	05/2021
NIST Cyber Security Framework	v1.1	04/2018
10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021
CPNI Role based Protective Security Risk Assessment Guidance - final-role-based-protective-security-risk-assessment-211.pdf (cpni.gov.uk)	Summer 2022	Summer 2022
Statutory Vetting Code of Practice for England & Wales (www.college.police.uk)	20 July 2023	20 July 2023
College of Policing Authorised Professional Practice – Vetting APP on Vetting (college.police.uk)	2023	2023
National Community Security Policy (NCSP) – People Management Standard		

Contents

Community Security Policy Commitment

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National Policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This standard in conjunction with the National Policing Community Security Policy (NPCSP) Framework and associated documents sets out National Policing requirements.

Introduction

It is well established that one of the most significant threats to any ICT system is that of legitimate users misusing systems and data. Police users have legitimate access to significant volumes of sensitive information and are open to coercion directly, or through family, friend or social connections, from several sources, including serious and organised crime, investigative journalists, other criminals, as well as the more traditional threat from Foreign Intelligence Services (FIS).

Access to Police systems, both local and national, is limited to Police vetted individuals. This approach is essential to meet legislative requirements, support operational Policing, ensure successful prosecution, and protect the health and safety of Police officers, staff and members of the public.

Vetting alone cannot prevent unauthorised disclosure, but it can mitigate the risk. The consequences of inappropriate disclosure of Police information can be significant and have included: financial penalties from the Information Commissioner, cancelling or rescheduling active Police operations, impact on future ability to disrupt crime or gather intelligence, threat of injury and loss of life (through disclosure of covert human intelligence sources), collapse of court proceedings, legal action, reputational damage and risk to safety of operational officers and staff.

This standard supports the requirements described by the NPCSP (People Management Policy Heading) and associated standard(s);

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this guidance is to assist community members in demonstrating compliance with the following NPCSP policy statements (People Management Policy Heading):

- Embed information security into each stage of the employment lifecycle (including personnel vetting, induction, employment contracts, ongoing management, and termination).

Furthermore, this guidance helps;

- To ensure that the risks to Policing information and IT systems is managed within risk appetite.
- To reduce the risk of insider threat affecting the Policing Community of Trust.
- To ensure that only appropriately vetted personnel with a lawful business need have access to policing information, IT systems and premises.
- Adherence to the Statutory Code of Practice and Authorised Professional Practice on Vetting.

Audience

This document applies to any member of the Policing Community of Trust as defined in the National Community Security Policy (herein referred to as a 'member'.)

This document is expected to support Senior Information Risk Owners (SIRO) and Vetting Managers as well as inform HR directors, Force Vetting Managers, and any person involved in appointing personnel to fulfil roles. It will also support those undertaking compliance and audit activities.

Scope

1. This guidance applies to all roles (permanent and temporary) that are expected to access National Policing IT systems, Force IT systems, premises, and physical information assets (including documents and artefacts).
2. It should be applied across the through-life journey of information assets and IT systems.
3. It applies to all member personnel who have a lawful business need to access National or Force IT systems, premises, or information assets. This includes temporary (contract), sworn and permanent personnel engaged in supporting policing activities.

4. It applies to third parties who have lawful business need to access National Policing IT systems, Force IT systems, premises, and physical information assets.
5. This guideline does not affect access by individuals who are provided police information by the police in the course of their professional duties, solely for the purpose of performing those duties, such as regulatory audit and inspection bodies. Refer to Vetting APP 2021 paragraph 7.39.

Responsibilities Matrix

Note: equivalent roles should be applied for non-Force members.

Activity	Accountable	Responsible	Consult	Inform
Vetting exemption decisions for access to National Information Assets or access to, design and build of National IT systems.	National SIRO	National IAO	NPCC vetting & PDS Cyber Services Audit, Risk and Compliance Team	
Vetting exemption decisions in Force regarding clearance exemption for access to Force or member Premises / IT Systems / Assets	Force SIRO	IAO	Force ISO & Professional Standards (Vetting) or member equivalent Lead	Force IT manager – to manage access
In-Force vetting clearance decisions	Force Professional Standards (vetting) Lead	Force Vetting Units	Line managers, HR teams	Individuals
Define and maintain Access requirements for National Systems e.g. Police National Database (PND)	National SIRO	National IAOs	NPCC Vetting portfolio	
Access requirements for Force Systems, information, or premises	Force SIRO	Force IAOs	Force ICT Lead & Force ISO where ICT outsourced	
Maintains in-Force threat assessments	Force SIRO	Force Information Security Officer / PSD	Force Professional Standards (Vetting) lead	Force IAOs

		Counter Corruption		
Maintains a National Policing threat Assessment	National CISO / NCA	PDS NMC	PDS Cyber Compliance	
Maintains a list of permanent and temporary role profiles which includes required vetting clearances.	HR Director / Vetting Manager	HR teams	Force Vetting Manager & Line Managers	
Ensures lawful business need to know through implementing & maintaining information security controls.	Force SIRO	IAOs	Force Information Security Officer (ISO) Force Vetting Manager	All personnel and contractors

Overarching Requirements

The following table describes the minimum requirements to assist members in reducing the risk of access to policing systems or information.

Reference	Minimum requirement	Control reference	Compliance Metric
VRP0	Authentication – The individual's identity documents must be checked and validated against National standards to confirm identity.	APP on Vetting section 7.1 on	Records of authentication of individuals.
VRP1	Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks. Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	ISO 27001 A.7.1.1 NIST CSF PR.IP.11	Register or list of designated roles / posts that require enhanced clearances such MV, NPPV 3 or SC &DV. Number of personnel not holding clearances vs holding current clearances. Number of personnel with interim clearance exemptions.

			Duration of interim clearance exemptions.
VRP2	Vetting clearances must be granted before an individual is appointed, employed or otherwise authorised to access police premises or information that is not in the public domain. This is because the vetting process can uncover information that shows the individual is unsuitable to be appointed, employed or otherwise given unsupervised access to police assets.	APP on Vetting 2021 Page 12 Para 3.2 And APP on Vetting 2021 Page 17 Para 4.4.3	Number of personnel with vetting clearance before access granted vs number of personnel granted access without clearance.
VRP3	Where a provisional or conditional clearance is considered, a full rationale – including review dates and any other safeguards – should be recorded and maintained by the force vetting manager (FVM) until the full vetting process has been completed.	APP on Vetting 2021 Page 13 Para 3.6	Number of personnel with provisional or conditional clearance. Evidence of reviews Details of safeguards in place.
VRP4	A role based protective security risk assessment should be undertaken and maintained in partnership with the Force / member organisation vetting unit, Information Asset Owners and HR team.	APP on Vetting 2021 Page 53 Para 7.30 CPNI RB-PSRA guidance	Register or list of designated roles / posts and prioritised risk assessment.
VRP5	Processes should be in place to describe and manage third party access to premises, IT systems and information to ensure appropriate clearances are in place prior to access.	APP on Vetting 2021 Page 12 Para 3.2 NCSP Third Party Policy heading & associated standard(s)	Process in place to ensure third party access controlled according to clearance. Records of exceptions and risk management decisions.
VRP6	The requirement for appropriate security vetting clearance to access police assets should be communicated to all personnel, this should include contract relevant contacts and escalation points.	NCSP People Management Policy heading and associated standard(s)	Regular awareness programme with records of attendees. Induction training with records of attendees.

Minimum clearance requirements by role or access

This section describes the minimum vetting clearance level by role or access. Each should be considered in line with a risk assessment and in liaison with Force ISO and local vetting units or member equivalents.

Role	Minimum Clearance Level required	Comments, additional controls
General clearance and access (as described in APP for Vetting 2021)		
No access required to classified material.	NPPV 1	See APP for Vetting 2021 Page 56 Para 7.33 Physical access controls
Up to OFFICIAL-SENSITIVE on police premises or remote access. No systems access.	NPPV 2 (abbreviated)	See APP for Vetting 2021 Page 57 Para 7.34 Lawful business need-to-know controls
Police classified material up to OFFICIAL-SENSITIVE and occasional access to SECRET. Unsupervised access to police premises or systems.	NPPV 2 (full)	See APP for Vetting 2021 Page 58 Para 7.35 Lawful business need-to-know controls
Police classified material or unsupervised access to SECRET and occasional access to TOP SECRET. Unsupervised access to Police premises or systems.	NPPV 3	See APP for Vetting 2021 Page 59 Para 7.36 Lawful business need-to-know controls
Police classified material up to and including OFFICIAL-SENSITIVE & occasional access to Government SECRET (as described in UK Government Classification Scheme)	RV + authentication	See APP for Vetting 2021 Page 33 Para 7.11.5 Lawful business need-to-know controls
Police classified material up to SECRET and occasional access to TOP SECRET (Police assets only – does not include Government assets)	MV	See APP for Vetting 2021 Page 40 Para 7.20.1 Lawful business need-to-know controls

Within Police premises:		
Escorted visitors, including contractors	None	Visitor management standards must be applied including verification of identity, recording in a visitor log and safety & security brief. Must always be escorted by a person with clearance for areas accessed. Areas to be visited to approve visit and put in place appropriate risk management controls. Escorts to be aware of the risk of "overlook" of screens, documentation, whiteboards. No access to any ICT systems.
Visiting Employees and unescorted visitors with no ICT access	RV, NPPV 2[1] or DV[2]	Visitor management standards must be applied including verification of identity, recording in a visitor log and safety & security brief. Note: DV in isolation does not allow unescorted access.
Employees and unescorted visitors with ICT access	NPPV 2 full	Only access to systems required for their role and lawful business need. System Owner / Information Asset Owner authority. All access subject to system Acceptable Use Policy (normally need to sign AUP) and training/briefing.
Employees and unescorted visitors with ICT access to systems which may be of increased interest to threat actors and a compromise is likely to cause increased damage.	MV or NPPV 3	Acceptable Use Policy (AUP) in place and mandatory training completed. UKSV SC or DV may additionally be required for access to areas and systems carrying HMG sensitive information.

[1] NPPV clearance may be carried out by any Police force, following the vetting policy. Where the vetting is carried out by Warwickshire, as part of the national scheme, it should be noted that Warwickshire only do the higher NPPVL3 (not NPPVL2), with an optional SC check.

[2] DV is not designed to counter threat to Police information. It does provide a high degree of assurance and, in certain situations, under local risk management, it may be permissible to accept DV as a sufficient level of clearance.

Within Council (local authority) or other "shared" premises: (Not managed service providers)		
Where possible, the guide given above is generally appropriate but, in some cases, it may be difficult to insist on vetting for colleagues from other agencies who share the same area but have no direct Police ICT access. Countering "overlook" then becomes a real issue. Any direct access to Police ICT systems must follow the direction as above.		
Role	**Minimum Clearance Level required**	**Comments, additional controls**
Data centres holding Police data:		
Guards	NPPV2 Full	NPPV3 if privileged access needed e.g. access control / CCTV administration
Guards with access control administrator rights to areas where NPPV is required.	NPPV 3	Logs must be regularly, independently checked.
Employees and unescorted visitors with ICT access to Police systems	MV or NPPV 3	AUP and mandatory training. SC or DV may additionally be required for access to areas and systems carrying HMG sensitive information. Consideration must be given to level of protective monitoring. Consideration to baggage inspection.
Research areas, including MoJ. Note: An Information Sharing Agreement should be in place which defines the scope of access / information to be shared.		
Access to sanitised copies of Police data	None	But care must be taken that the "sanitisation" is adequate, e.g. post codes may need to be clustered.
Access to un-sanitised copies of Police data	NPPV 2 full	But only the minimum dataset should be provided. If SC required NPPV 3 will be needed.
Read access to entire datasets, e.g. PNC	NPPV 2 full	But consideration must be given to SC or DV due to level and source of threat.
Read access to entire datasets, PND	NPPV 3	But consideration must be given to SC or DV due to level and source of threat.
Write access to entire / large datasets, e.g. PNC / PND	NPPV 3	But consideration must be given to SC or DV due to level and source of threat.

Access to Police data in Government Departments:		
Role	**Minimum Clearance Level required**	**Comments, additional controls**
Access to “low level” Police data, e.g. PNC driver details. Likely to be classified OFFICIAL.	BPSS or higher	Enforce lawful need-to-know System AUP and mandatory training.
Access to Police data likely to be classified OFFICIAL.	NPPV 2 full	Enforce lawful need-to-know System AUP and mandatory training.
Access to sensitive Police data, where there may be threat to life or the safety of an individual. Likely to be classified as OFFICIAL-Sensitive	NPPV 3	Enforce lawful need-to-know AUP and mandatory training. SC or DV may additionally be required for access to areas and systems carrying HMG sensitive information.
Project staff, commercial, Home Office, Police Digital Service:		
Access to live data (e.g. not test data) or security related information including OFFICIAL-Sensitive.	NPPV 3	Enforce lawful need-to-know General IA awareness training and briefing on threat to Police information
Vetting requirements for those in receipt of PNC data		
Regular users of PNC and auditors of PNC	NPPV 2 full	It is impractical to suggest all professions such as Solicitors, barristers, judges, Prison officers, Social & mental health workers and Trading Standards hold current NPPV2 clearance and not desirable to ask

Regular users which have rights in addition to read access.	NPPV 3	them to do so, so a judgement needs to be made around when occasional access becomes regular enough and in sufficient volume to mean that the professional standards and obligations of individuals need to be strengthened by vetting. The decision on whether NPPV clearance is necessary should ideally be done on a case-by-case basis, however the broad rule is that: • If the subject in the course of their professional work sees PNC data on an individual directly in relation to their role as part of case papers, prison transfer data etc. then NPPV is not required. • If the subject handles or has regular access to significant amounts of data in relation to multiple individuals or has unrestricted access to data on past and current cases, such as would be the case for those with access to an intelligence/investigation database, then NPPV should be required.
National Systems Audit roles		
Role	**Minimum Clearance Level required**	**Comments, additional controls**
Auditor Police & Police Staff or member permanent staff Non Police Law Enforcement Agencies	MV + SC NPPV3 + SC	Minimum Level specified based upon PND Vetting Levels

National Auditor Police & Police Staff or member permanent staff Non Police Law Enforcement Agencies	MV + DV NPPV3 + DV	Minimum Level specified based upon PND Vetting Levels

Handling exceptions to clearance requirements

As described in the APP on Vetting 2021[3], authentication underpins all levels of Force and National Security Vetting and must be completed before the vetting process is started.

Authentication is used to confirm an individual's identity, nationality, employment eligibility and residency qualification. On its own it does not allow access to police information that is not in the public domain, nor does it allow unescorted access to any police or member premises.

Before any consideration of temporary access to police information, systems or premises, authentication checks must be carried out through the following stages;

- Identity check
- Nationality check
- Employment eligibility
- Checkable history

It should be noted that vetting clearance cannot be granted if the applicant has not been resident in the UK for the relevant minimum period (see below) and if comparable vetting enquiries cannot be made in jurisdictions where the individual has been residing.

- non-police personnel vetting – three years
- recruitment vetting – three years
- management vetting – five years

Where it is not possible to authenticate an individual access should not be considered, as there is no likelihood of successfully gaining vetting clearance. This is likely to be the case for overseas individuals any risk assessment must start with satisfactory completion of the authentication stage and supported by the good practice of collecting personal details of the applicant's family and co-residents, as these details may support any subsequent investigation or enquiry.

3 APP on Vetting 2021 Page 26 Para 7.1

The following table describes risk management measures that should be applied to help assure the Senior Information Risk Owner (SIRO). These measures are only applicable once the individual has successfully completed the authentication stage and has submitted their completed vetting application forms.

Requirements for exception / temporary access		
Scenario	**Clearance normally expected**	**Minimum requirement to risk manage (for a fixed duration only)** NB: Below only applicable when individual has completed authentication stage and submitted completed forms for clearance.
Access to information already in the public domain.	None	Authentication only, application submitted for clearance.
Access to low level Police data – limited data sets and read only	RV / BPSS	Force or member achieves baseline maturity of 2.0 in a recent PCAF (SyAp) assessment
Access to Police data Regular use of PNC	NPPV 2	As above plus: Lawful business need to know. Auditing of access and activity.
Privileged access such as; Physical access to sensitive / critical areas Modify access to PNC data Access to complete Police datasets of live data (including PII) Enhanced / admin / root access to ICT system(s) Unrestricted developer access to ICT system. This would include remotely connected contractors.	MV / NPPV 3	Force or member achieves baseline maturity of 2.0 in a recent PCAF (SyAp) assessment. Privileged access (System Administrators) AUP and mandatory training. SC or DV may additionally be required for access to areas and systems carrying HMG sensitive information. . Consideration must be given to level of protective monitoring. Physical Security controls following a physical security risk assessment such as NPSA -Surreptitious Threat Mitigation Process (STaMP) also see NPCSP Physical & Environmental Management standard.

Communication approach

This document will be communicated as follows:

- Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

This guideline should be socialised with the target audience to help complete an initial gap analysis which can inform any implementation plan. This implementation plan can be shared with your Force SIRO / Security Management Forum. Consideration should also be given to raising awareness amongst Force personnel of the implementation of this standard where it may affect them.

Measurables generated by adopting this standard can also form part of regular Cyber management reporting.

Review Cycle

This guideline will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed and that the policy continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

(Adapt according to Force or PDS Policy needs.)