Policy

Alliance information security

J-P-015

Version 2.1
Effective date 09/11/2020
Version date 11/05/2026
Review date 20/01/2028

Host Force Devon & Cornwall Police
Host Policy Unit Devon & Cornwall Police
Policy Owner Head of Alliance Information Management
Policy Author Alliance Information Security Manager

Associated procedures
J-Pr-005 Alliance information security procedure

1. Policy summary

1.1 This policy applies to all police officers, police staff, special constables, police volunteers, agency staff and contractors (referred to as members of the police workforce) working within Devon & Cornwall Police (DCP) and Dorset Police (DP) (referred to as both forces throughout this document) and aims to provide consistency in respect of information security across both forces which will be practical, usable, appropriate and achievable.

1.2 The purpose of this policy is to protect both forces information assets from all threats, whether internal or external, deliberate, or accidental. It is concerned with the preservation of the 3 pillars of information security as outlined by the United States National Institute of Standards and Technology (NIST) (NIST SP 1800-25):

- Confidentiality – preserving authorised restrictions on information access and disclosure, including means of protecting personal privacy and proprietary information.
- Integrity – guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.
- Availability – ensuring timely and reliable access to and use of information.

1.3 The term ‘asset’ when used in the context of this policy describes tangible (physical items such as hardware, firmware, computing platforms, network devices or other technology components) or intangible (data, information, software, service, trademark, intellectual property, image, or reputation) items.

1.4 This policy and its associated procedure and IA guidance will deliver a security conscious culture to help protect policing information through establishing compliance with relevant legal, regulatory, and procedural obligations, establishing both personal and organisational responsibilities.

1.5 The technological and physical controls outlined in this policy and associated procedure demonstrate a commitment to delivering an appropriate and systematic approach to information security, focussing on risk management and compliance, and thus delivering the Information Security Management System (ISMS) across both forces.

2. Purpose, standards, and legal basis

2.1 The strategic objective of this policy is to provide reassurance to the Joint Senior Information Risk Officer (SIRO) and respective Chief Constables, that both forces systems, networks, information, and physical estate are protected, maintained, and managed effectively through the ISMS.

2.2 The ISMS consists of several measures and includes the following: (not exhaustive)

- Both forces employ a secure by design approach in partnership with the Information and Communication Technology (ICT) Department and British Telecom (BT) via the shared managed service contract to deliver against:
  - Police Digital Services (PDS) cyber security procedures, standards, guidance, and blueprints
  - Adherence to the principles of International Organisation for Standardisation (ISO) / International Electrotechnical Commission (IEC) 27001/2.

- To evidence and provide greater visibility of both forces security status, the PDS Security Assessment for Policing (SyAP) methodology is maintained. Regular assessments are undertaken, culminating in a PDS led annual report submitted to the Joint SIRO for Executive scrutiny.

- As a handler of cardholder information, both forces are required to comply with the Payment Card Industry Data Security Standard (PCI DSS) to ensure that all cardholder data is processed in a secure environment.

2.3 Both forces are obliged to abide by all relevant legislation. The requirement to comply with this legislation shall be devolved to members of the police workforce of the relevant Force, who may be held personally accountable for any breaches of information security. This includes but is not limited to:

- The Data Protection Act 2018 and UK General Data Protection Regulation (GDPR)
- The Data (Use and Access) Act 2025
- The Health and Safety at Work Act 1974
- Human Rights Act 1998
- Freedom of Information Act 2000 (FOIA)
- Copyright, Designs and Patents Act 1988
- The Computer Misuse Act 1990
- The Health and Safety at Work Act 1974
- Regulation of Investigatory Powers Act 2000
- Equality Act 2010
- Authorised Professional Practice (APP)
- National Decision Model
- Force Purpose, Objectives and Priorities
- Equality and diversity matters including the Public Sector Equality Duty and Code of Ethics (ethical policing principles and guidance for ethical and professional behaviour in policing).

3. Roles and responsibilities

3.1 To deliver the ISMS effectively across both forces and embed a security conscious culture, information security needs to be everyone's responsibility. Specific activities will be allocated appropriately across the organisation with clear lines of accountability.

3.2 To establish a framework to initiate and control the implementation and operation of information management within the Alliance, the following roles must be appointed, appropriately trained, qualified and actively engaged within the organisation(s):

- Senior Information Risk Owner (both forces share a Joint SIRO).
- Information Assurance (IA) Manager.
- Information Asset Owners (IAO), or equivalent role.

3.3 Chief Constable - ultimate responsibility for information management rests with the Chief Constable of each Force as the Data Controller, although oversight and management of information risk is delegated to the Joint SIRO.

3.4 Governance of IA and risk management is delivered through the Joint Information Board (JIB) as the Executive level forum. It is chaired by the Joint SIRO. Please see Force Strategic Meetings - Terms of Reference.

3.5 Within DCP, the Tactical Force Security Group focuses on security matters with a terms of reference based on the National Protective Security Authority. The meeting is chaired by the Assistant Chief Constable for Contact & Strategic Planning, reporting into the JIB.

3.6 Joint SIRO - as an Executive member of the Alliance, the Joint SIRO is responsible for managing information risk from a business, rather than technical perspective. The Joint SIRO provides board-level accountability and greater assurance that risks are addressed. The Joint SIRO considers the individual forces risk appetite and ensures they are considered against the delivery of individual Force, Alliance, regional, and national objectives.

3.7 Head of Alliance Information Management - strategic lead for both forces in respect of information management.

3.8 Alliance IA Team - operating as a single team across the Alliance, the IA Team provide a focal point for information, security, and compliance issues, providing advice and guidance on information, technical and physical security. Please see the IA Team SharePoint site.

- They must be contacted whenever a department is looking to implement a new system, application, or device.

- Their role will be to carry out a physical and information risk assessment, ensuring that any security controls required support the business, whilst adhering to any legislative or national compliance.

- They are also responsible for managing all information security incidents for the Alliance, including co-ordination of investigation and mitigation of breaches, both physical and cyber related.

3.9 Alliance IA Manager and Accreditor - The Accreditor is responsible for the acceptance of information processes and systems connecting to the Force Enterprise Network (FEN).

- The Accreditor acts as an impartial assessor of the residual risk affecting information systems on behalf of the Joint SIRO. If, following the risk assessment, the Accreditor determines that the risk is outside either forces information risk appetite, the risk is raised to the Joint SIRO for advice and, if necessary, a decision to accept a new level of residual risk is made.

3.10 ICT Technical Security Team/BT Managed Service Contract – The teams are responsible for protecting computers, networks, infrastructure, and data from unauthorised access or damage. They provide advice on technical security architecture and posture.

3.11 Data Protection Officer (DPO) - DCP and DP have separate DPOs. The DPO is responsible for informing and advising on compliance with data protection legislation in respect of the processing of personal data by each Force and any processor engaged by either Force.

3.12 Alliance Data Protection Team – operates across both forces and provides specialist advice on data protection matters, process the Right of Access requests for individuals, co-ordinate the remaining rights and the maintenance of Information Sharing Agreements (ISAs) with partner organisations. Please see the Data Protection SharePoint site.

3.13 Information Asset Owners (IAOs) - IAO's are senior/responsible individuals involved in running a business area/command. They have a responsibility to safeguard the use of assets (information, devices, evidential property etc) within their area of business and assist in the investigation process following a breach.

- IAO's are responsible for maintaining an Information Asset Register (IAR) accurately reflecting the information assets within their business area/command. By understanding the extent of information assets on their IAR, they will be able to ensure information is exploited and shared where possible to ensure maximum service to the public, whilst at the same time ensuring appropriate protective measures in place that matches the sensitivity of the data.

- Any information risks identified by the IAO must be recorded within the relevant IAR.

- The specific responsibilities of the IAO and their appointed Information Liaison Officer (ILO) are defined within the IAO Handbook.

3.14 Information Liaison Officer (ILO) – nominated by their IAO, ILOs provides a critical function in supporting the IAO in the maintenance of the area of business/command IAR, processes and provides the necessary liaison with the Alliance Information Management Department. ILOs are also the information champions for their department, promoting good practice and ensuring information management and information security issues are identified and addressed.

- The specific responsibilities of the ILO are defined within the IAO Handbook.

3.15 Line managers - must ensure their teams understand and comply with organisational policies, legislative and regulatory requirements in respect of information security. Line managers are responsible for ensuring IAP02 Line manager responsibilities security policy is followed and that their teams are aware of:

- The information security policies applicable in their work areas.
- Their personal responsibilities for information security.
- How to handle information in accordance with the Government Security Classification (GSC).
- How to access advice on information security matters.

3.16 All members of the police workforce will comply with relevant Force and Alliance policies and associated procedural documents. IA related policies are supported by a series of locally held policy, procedure and guidance,

providing more detailed information as required. Failure to comply with these policies, procedures and guidance may result in disciplinary action.

- Each member of the police workforce shall be responsible for the security of the assets (information, computing equipment, passwords, ID cards, security keys, vehicles etc.) they use. Please see IAP01 Personal security policy for more guidance.

4. Policy information

4.1 Controlling documents and accreditors

4.1.1 Both forces utilise a combination of primary documents and scrutiny processes that set rules, standards, and procedures in relation to information security. These documents and procedures serve as the authoritative reference point, ensuring consistency and compliance across the organisation and are the foundation upon which Force level policies and procedures are created.

4.1.2 These include:

- SyAP: Measures policing's current level of maturity regarding cyber security against "Identify, Protect, Detect, Respond, Recover" criteria.

- ISO/IIEC27001: The international standard that defines the management system required to deliver IA within an organisation. It covers technical and non-technical aspects of IA/security management. ISO/IIEC27001 specifies the requirements for an ISMS.

- Police Information Assurance Board (PIAB):
  Provides strategic leadership and support for the development, implementation, and evaluation assurance within national policing.

- The Joint Data Strategy:
  The strategy identifies an intent to be a data driven organisation and provide direction in relation to data management.

- National Policing Community Security Policy (NPCSP):
  Outlines policies for police forces to meet legal and regulatory requirements for IA and security, both technical and non-technical.

- J-P-011 Joint records management policy:
  Provides consistency across both forces, aiding alignment with other organisations and to provide guidelines and best practice for the management, governance, security and use of structured and unstructured data within both forces, ensuring legal and regulatory standards are maintained whilst maximising the value of the data held.

- Codes of Connection (CoCo) including Airwave, Police National Computer (PNC), Police National Database (PND):
  Communication protocols or agreements that enable different police forces to share information and data.

- PDS:
  Responsible for co-ordinating, developing and delivering digital services and solutions that enable UK policing to harness technology.

- Information Commissioner's Office (ICO):
  Upholds information rights in the public interest.

- College of Policing (CoP):
  Provides forces with APP documentation. Please see the Information Management APP.

4.1.3 Both forces are required to demonstrate IA compliance and in doing so will provide reassurance to the PIAB and other relevant His Majesty's Government organisations that risk to information and assets is being managed at an acceptable level. Compliance includes:

- Timely annual submission of ongoing SyAP assessment, culminating in a Force level report that covers both forces to the Joint SIRO.

- Independent audits whose scope includes elements of the required IA standards described in this policy, undertaken by His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS), suitable accredited auditors and/or agents of the PIAB and PDS.

- Timely completion of the annual Information Technology Health Check (ITHC) and appropriate remediation.

4.2 ICT and physical security governance

To deliver the five areas within the SyAP (Identify, Protect, Detect, Respond, Recover), both forces will comply with a number of associated IA policies, guidance and procedures as detailed below.

4.2.1 Information systems acquisition, development, and maintenance:

- Both forces will ensure all new information systems, applications, cloud services and networks are robustly scrutinised prior to implementation. Due diligence will include support from business stakeholders, ICT Technical Security Team and the IA Team before certification is provided. If a new information system, application, cloud service or network is used for the handling of personal data, it must be formally assured prior to live operation and be subject to a Data Protection Impact Assessment (DPIA).

- Management of client devices infrastructure and networks must be controlled through standard documented procedures. This will include

procedures outlining anti-virus, boundary protection, identity protection, patching, and lockdown.

- An Artificial Intelligence (AI) policy to govern the responsible adoption, development, and use of AI technologies will be developed, covering both forces. This policy will ensure alignment with the PDS' national standards and promote compliance with recognised principles of data management, accountability, and ethical governance. The organisation will also integrate the National Police Chiefs' Council (NPCC) PROBabLE Futures Responsible AI Checklist into its due diligence implementation processes to assess risks, uphold ethical obligations, and support the deployment of AI systems in a consistent manner.

- Please refer to J-P-113 Artificial intelligence - acceptable use across the Alliance, IAG08 IA Requirements for iCloud Service Procurement and IAP05 New Projects and Systems.

- Remote Desktop Control (using tools such as Beyond Trust or Microsoft Teams) is provided for authorised ICT support purposes only. Access must be initiated in line with Service Desk procedures and only by members of the police workforce with the appropriate permissions/vetting. Permitted users must not attempt to bypass security controls, share sessions details with unauthorised parties, or use the tool for any activity outside the scope of their official duties. Where a device is already in use, the support technician must request and receive the active user's permission before taking remote control. All sessions are logged and monitored for audit and security purposes, and any misuse may result in disciplinary action in accordance with organisational policy.

4.2.2 System change control:

- Changes to existing systems, applications and networks will be submitted through the Change Co-Ordination Board (CCB) after the completion of necessary DPIA/IAG08 documentation.

- Development, test, and operational facilities shall be separated to reduce risks of unauthorised access or changes to the operational or corporate systems. When testing systems in a live or test environment, no operational or corporate data will be used. Instead, 'dummy' data, anonymised to the level that cannot lead to the identification of an individual, will be used.

- Please refer to IAG08 IA Requirements for iCloud Service Procurement.

4.2.3 Malware protection:

- Both forces via the Managed Service Contract will use and update software countermeasures to protect against malicious software in a timely manner and in line with PDS requirements. New software will not

be installed on Force networks or devices without being assessed and certified by the IA Team and both forces governance process.

- Please refer to IAG08 IA Requirements for iCloud Service Procurement.

- Both forces will engage with the National Management Centre (NMC) in respect of incident response, threat intelligence, and cyber threat assessment/remediation as part of its wider Security Information and Event Management (SIEM) response to centralised log management, analysis, and collation of security events from sources, including firewalls, servers, and applications.

4.2.4 Information risk assessment/incident management:

- The core principle of risk assessment and management requires the identification and quantification of information security risks in terms of the perceived value of the asset, the vulnerability and severity of the impact of an information breach and the likelihood of it occurring.

- All security events, incidents, data breaches, near misses and suspected vulnerabilities, both cyber and physical, must be reported to the IA Team via report a data breach/Incident.

- Once identified, information security risk shall be managed on a formal basis. Incidents will be recorded by the IA Team and action plans created to effectively manage identified risk. Any remediation or mitigation should be in proportion to the degree of risk posed. The IA Team will liaise with IAOs to conduct incident investigations and remediate future risk.

- Please refer to IAG09 Incident Management.

4.2.5 Major incident and incident recovery:

- A major incident is “an incident which causes, or is likely to cause, significant disruption to the customer and its operations.” A major incident would be deemed as causing significant disruption if it severely impaired the normal operations of either Force. This can also be a low impact, high volume incident.

- When an incident causes extreme impact to policing activity for either or both forces, this will be defined as a major critical incident.

- Both forces will employ existing incident management processes as part of their overarching Incident Response Plan (IRP) and will include stakeholders from Information Management, ICT, BT and impacted business areas.

- Please refer to IAG 09 Incident Management, ITIL009 Incident Management, and ITIL051 Local Security Management Process

4.2.6 Application access control

- Access to data, applications, network, cloud environments and system utilities, and program source libraries shall be controlled and restricted to those authorised users who have appropriate vetting, training, and a legitimate business need.

- Passwords must be protected to avoid unauthorised use and must have a strong construction.

- Please refer to IAG09 Incident Management.

4.2.7 Asset management

- Force assets (hardware, software, applications, or data) must be asset tracked (including through the relevant Information Asset Register, where applicable), encompassing the entire lifecycle of an asset including acquisition, operation to disposal/archive.

- Please refer to IAG02 Information Asset Management and IAP08 Asset Management policy.

4.2.8 Physical and environmental security:

- All members of the police workforce are responsible for physical security of estate assets, ensuring unauthorised physical access, damage or interference with premises and assets is prevented or minimised to include:
  - Windows, doors, and access points are secured.
  - All members of the police workforce must wear visible identification when on Force premises.
  - Check and challenge individuals on Force premises not displaying visible identification.
  - Visitors are signed in and provided with suitable identification.
  - Visitors have an organisational sponsor, are vetted to the correct level, and are chaperoned if necessary.

4.2.9 Clear desk and clear screen:

- Where practical, paper and computer media must be stored in cabinets or furniture when not in use; sensitive or critical business information must be locked away when not required; stand-alone computers and network terminals must be logged off or locked when unattended; and multi-functional devices will be protected from unauthorised use.

- It is recognised that some members of the police workforce do not have exclusive use of office and desk facilities so where there is shared use of facilities, line managers and supervisors are responsible for ensuring

reasonable care is taken to protect sensitive information from unauthorised access.

- Please refer to IAG12 Remote Working.

4.2.10 Protective marking

- All members of the police workforce have a responsibility to protect the data they access, use or manage; to comply with IA policy IAP01 Personal Security, and to report data breaches/security incidents using the report a data breach/security incident process.

- Protective markings are used to label documents with a GSC, handling instructions and FOIA status to ensure information is managed securely, accessed properly, and retained or disposed in line with legal and regulatory requirements. See the Alliance FOI Team for FOIA guidance.

- Please refer to GSC, M365 sensitivity labels, Handling instructions, FOIA - marking of documents, and Joint Policy J-P-011 Joint records management.

4.2.11 Education and culture

- Information Management training will include Data Protection, FOI, IA and Data Quality. Information security training aims to educate users about cyber threats and security best practices to safeguard both forces systems and data by raising awareness of the importance of security and how attacks happen, ‘phishing’ exercises, and how to react to security incidents.

- A series of specific IA local policies, procedures, and guidance sits underneath this Joint Force policy which provide more detailed instructions on how this policy will be implemented. These additional documents will align to ISO/IIEC27001, and the requirements set by the National Policing Information Risk Management Team.

- The intended outcome of this policy and its associated procedure is to:
  - Enable both forces to use and share information with confidence.
  - Employ suitable safeguards to protect the confidentiality, integrity, and availability of both forces information systems.
  - Deliver both forces statutory, regulatory, and contractual information security obligations.

- The specific objective of the controls and related procedures is to enable both forces to conduct business (corporate and operational), making best use of systems and information, whilst preventing and minimising the impact of information security incidents and their associated risk.

- When creating training content, no operational or corporate data will be used (i.e. NICHE records, Body Worn Video, MG series documents). Instead, ‘dummy’ data, anonymised to the level that cannot lead to the identification of an individual, will be used.

5. Monitoring and review

5.1 Review and amendments will be coordinated by the Policy Unit.

5.2 The policy owner has overall responsibility for ensuring the content of the policy is appropriate and up to date.

5.3 This policy will be reviewed every 2 years subject to legislation/process changes.

5.4 In order to review the success of this policy the Alliance IA Team will continually monitor the number of IA incidents reported to IA via IAG09 Incident Management Process.

6. Associated documents

Polices and procedures

- Force Policies and Procedures
- J-Pr-005 Information security
- J-P-011 Joint records management
- J-P-013 Alliance data protection
- J-P-071 Information sharing
- J-P-073 Use of Force computers by outside agencies
- J-P-113 Artificial intelligence - acceptable use across the Alliance

SharePoint

- Force Purpose and Objectives (DCP)
- Priorities and Ethics (DP)
- IA Team
- IA policies, procedures and guidance
- Information Management: Data Protection, Freedom of Information, Records Management, Government Security Classification, Information Assurance, Information Sharing, Disclosure, Disclosure & Barring Service and Data Quality

College of Policing

- Code of Ethics
- Authorised Professional Practice (APP)

Other

- Human Rights Legislation

- Computer Misuse Act 1990

7. Document history

Present portfolio holder: Director of Legal, Reputation, and Risk
Present document owner: Head of Alliance Information Management
Present owning department: Alliance Information Management, IA Team

Below details required for new documents, major amendments (Dorset only) or novel/contentious amendments (Devon & Cornwall only)
Name of Board and/or Chief Officer approving: N/A
Date approved: N/A
Business Board member approving (Devon & Cornwall only when not contentious or novel): Head of Alliance Information Management
Date approved: 11/05/2026

8. Version history

Version: 2.1
Date: 11/05/2026
Reason for amendments: Amendments to 4.2.2 and additional bullet point at 4.2.11. Review date unchanged.
Amended by: Alliance Information Security Manager

Version: 2.0
Date: 20/01/2026
Reason for amendments: Significant review and rewrite to update to current practice.
Amended by: Alliance Information Security Manager

We welcome any comments or suggestions you wish to share about the content or implementation of this procedure. If you would like to make contact to discuss further, please email: Forcepolicyandprocedures@devonandcornwall.pnn.police.uk