CYBER GUIDELINE DOCUMENT

NCSP Guideline: INFORMATION TRANSFER

ABSTRACT:

Information transfer is the process of moving information from one location to another. Policies and processes are required to protection information during this process.

Any activity involving the movement of information from one place to another carries inherent risk whereby the confidentiality, integrity or availability of that information may be compromised. Appropriate and proportionate steps must be taken to ensure the security requirements of the information being transferred are protected against deliberate or inadvertent, authorised or unauthorised attack, damage or loss.

ANNEX A – Legacy NPIRMT Protection of OFFICIAL Police Data in Transit – Risks & contextual risk mitigation tables

ISSUED	February 2025
PLANNED REVIEW DATE	January 2026
DISTRIBUTION	Community Security Policy Framework Members

POLICY VALIDITY STATEMENT

This guideline is due for review on the date shown above. After this date, this document may become invalid.

Cyber guideline users should ensure that they are consulting the currently valid version of the documentation.

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 guideline in conjunction with the National Policing Community Security Policy Framework and associated documents sets out National Policing requirements supporting the Information Management standard requirements.

Introduction

Information transfer is the process of moving information from one location to another. Policies and processes are required to protection information during this process.

Any activity involving the movement of information from one place to another carries inherent risk whereby the confidentiality, integrity or availability of that information may be compromised. Appropriate and proportionate steps must be taken to ensure the security requirements of the information being transferred are protected against deliberate or inadvertent, authorised or unauthorised attack, damage or loss.

Information must be transferred using appropriate, secure, yet efficient means to support lawful purposes. Adherence to the Data Protection Act and other relevant legislation is paramount.

This guideline supports the NCSP Information Management standard. It provides guidance on how to securely transfer policing information between organisations.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this guideline is to:

- Provide advice on the secure transfer of information between individuals or organisations using a variety of methods including email.
- Ensure the confidentiality, integrity and availability of information is maintained while supporting operational requirements involving the transfer of information.
- Assist organisations to demonstrate compliance with the NCSP Information Management Standard.

Audience

All members of the policing community of trust as defined in the National Community Security Policy Framework.

This guidance is aimed at:

- Information Security Officers (ISOs), information security practitioners and any roles who may have responsibility for the protection of policing information.
- Member Senior Information Risk Owners (SIROs),Information Asset Owners (IAOs) and Platform Asset Owners (PAOs)
- Service providers and suppliers who in any way design, develop or supplier services for, or on behalf of policing.
- Auditors providing assurance services to members.
- All other staff working for, or on behalf of policing.

Scope

This guidance applies to:

1. Information or data assets that are being used for a policing purpose.
2. Information classified up to and including OFFICIAL - SENSITIVE

Guidelines

These guidelines provide details regarding appropriate mechanisms to transfer policing information to support lawful needs. They also help to ensure to protect against unauthorised disclosure.

Reference	Guidance	Reference(s)
1. Basis for safe sharing		
1.1.	Lawful transfer – the transfer of information must be legal in both the jurisdictions of the sender and receiver.	
1.2.	Data Protection – Where personal information is to be transferred, refer to appropriate data protection legislation and/or Data Protection Team or equivalent.	Data Protection Legislation Security and Privacy Controls for Information Systems and Organisations – NIST Special Publication 800-53
1.3.	Data Ownership – Where external solutions are required, ensure that data ownership is maintained. You may need to review services' Terms and Conditions, or Terms of Use to ensure ownership of the data is not claimed by the service provider.	Data Protection Legislation Security and Privacy Controls for Information Systems and Organisations – NIST Special Publication 800-53
1.4.	Classification – apply appropriate classification, protective marking and handling instructions in accordance with Police Classification Guideline	Government Security Classifications (GSC) Police Security Classification Guideline
1.5.	Consequences for loss – consider the implications of any loss, breach or unintentional disclosure. Perform a risk assessment for Confidentiality, Integrity and Availability security requirements and the impacts against these.	National Police Information Security Assessment Guidance Guide for Conducting Risk Assessments – Information Security – NIST Special Publication 800-30
1.6.	Data sharing agreements – where dealing with third parties or suppliers, consider whether appropriate data sharing agreements are in place	Vetting Requirement for Police systems Guidance NCSP TPAP Standard Cybersecurity Supply Chain Risk Management Practises for Systems and Organisations – NIST Special Publication 800-161
1.7.	Authorisation – where necessary, obtain authorisation for transfer from the information owner / controller.	Security Management Standard NCSP Identity and Access Management Standard NCSP System Access Standard

Reference	Guidance	Reference(s)
1.8.	Records Management – where possible, consider whether creating copies of information would introduce records management challenges e.g., asset record, destruction etc.	National Police Information Security Risk Management Framework Information Management Standard
1.9.	Handling instructions – where information has handling instructions applied, you MUST comply with these handling instructions e.g., FOR POLICE ONLY	Government Security Classifications (GSC)
1.10.	Ensure local information sharing agreements, policies and standards are adhered to.	Information Assurance Standard
1.11.	Information Asset Register – All information assets should be recorded within the organisational information asset register. Any sharing or transfer of information should also be recorded against that asset, to ensure the information asset owner knows exactly where their information asset is, and who has access to it.	Information Assurance Standard Cyber Security Architectural Principles
1.12.	System Configurations - Configuration of systems used in transfers of information are assured and appropriately penetration tested, and where vulnerabilities exist risk managed appropriately. Devices must be appropriately patched, maintained and supported, including end point devices.	Penetration testing and ITHC Guideline Information Assurance Standard Vulnerability Management Standard
1.13.	Consider implementing information transfer standard operating procedures (SOPS) which describe step by step approaches to regular exchanges that support regular business requirements. This is particularly important for transfers of large quantities of personal information (bulk transfers.) SOPS should also include exception processes to describe actions to be followed where required. See also Pattern: Safely Importing Data - NCSC.GOV.UK	Standard operating procedures in place for frequent and transfers of large sets (bulk) information. Documented exceptions.
2. Preparing information or data for transfer		
2.1.	Type of transfer – consider the most appropriate base of transfer for the type, classification, size or medium of information i.e., email, documentation, web-based file sharing etc.	Enterprise Impact of Information and Communications Technology Risk – NIST Special Publication 800-221
2.2.	Information Minimisation – remove unnecessary data from the set to be transferred. Transfer only information that is required. Use built in features and tools such as the document inspector in Word and Excel.	Cyber Security Architectural Principles

Reference	Guidance	Reference(s)
2.3.	Anonymisation / Pseudonymisation – Consider whether it is necessary to transfer personal information as part of the operational activity, or whether anonymised / pseudonymised information would suffice. Consult with local Data Protection teams for advice.	NCSP Cryptography Data Protection Legislation
2.4.	Transfer to Third Parties – where transfer of information to third parties or suppliers outside of the regular policing community of trust, consider what assurance has been conducted to assure of the security and appropriateness of that third party e.g., have they been assured via the TPAP? Has their physical site undergone a PASF assessment? Are their personnel vetted appropriately? etc.	Vetting Requirement for Police systems Guidance NCSP TPAP Standard
2.5.	Personnel security – consider whether users are required to have specific employment status or vetting. Determine whether recipients have a lawful requirement to receive the information.	Vetting Requirement for Police systems Guidance
2.6.	Time limiting – where information needs to be shared for a specific purpose or period, establish a process or technical control for ensuring this requirement is complied with e.g., at the end of an agreed period, ensuring unnecessary records are securely deleted.	Information Management Standard
2.7.	Backups – determine backup and storage requirements for exchanged information.	Cyber Security Architectural Principles NCSP Technical Security Management Standard
2.8.	Training and Awareness – consider training and coaching requirements for the safe handling and transfer of information and data. Does your organisation have specific requirements that need to be communicated e.g., legal or regulatory requirements. See also People Security Management Standard.	NCSP People Security Management Standard Vetting Requirement for Police systems Guideline
2.9.	Approved systems – **Do not** use unapproved, unsecured methods of communication or information transfer. If in any doubt consult your Information Security Officer (or equivalent) or contact PDSCyberServices@pds.police.uk for support.	

Reference	Guidance	Reference(s)
2.10.	Secure Electronic methods of information sharing are preferred over manual methods such as; • USB Memory sticks • Portable hard drives • CD / DVD disks • Paper Passphrases / keys are to be disclosed to named recipients using separate / alternative electronic means or medium, separate to the information being encrypted. See Electronic Communications Standard. Any movement of assets by hand such as courier are to be risk assessed and apply Accountable Security (AccSec) measures such as; • Escorted transport, • Local management approval • Document removal / movement register • Containers sealed with tamper evident seals • Not left unattended or accessible in public. A 'Chain of Custody' to track the movement and handling of information assets should be maintained. All digital media exchanges shall be inventoried and sent to recipients using a tracked courier service with tamper evident seals. You may also consider the use of tamper evident seals etc. Recipients are to be given handling instructions including securely returning the media or using secure methods of destruction. Paper based sharing shall be protected in accordance with Government Security Classification Policy and specific handling instructions. See NCSP Police Security Classification Guideline.	NCSP Police Security Classification Guideline NCSP Password Standard NCSP Cryptography

Reference	Guidance	Reference(s)
2.11.	Cloud / As-A-Service based information sharing solutions File sharing providers are to be subject to 3rd party assurance as any other supplier that handles policing information. **See NCSP Third Party Assurance in Policing (TPAP) standard.** Suitable sharing services will comply with the Cloud Security Alliance CSA Cloud Controls Matrix (CCM) and the NCSC Cloud Security Principles. A register should be kept of assured, suitable sharing services. It is recommended that sharing services should not be used as static file repositories and therefore used only to transfer information between organisations. Once information is shared it is considered good practice to remove it from the platform. Consider auto-delete rules to delete files in download folders. Good access management shall be in place to ensure that only authorised individuals have access as part of a lawful purpose. **See NCSP System Access standard**	NCSP TPAP Standard NCSP System Access Standard
2.12.	Consideration must be given to the management of information assets throughout the lifecycle of sharing, including; • Protection of assets / data before, during and after sharing, • Deletion of temporary / staged versions.	

3. Considerations for safe transfer of non-bulk datasets Data sets that are not large quantities of personal information or sensitive data.		
3.1.	Encryption in transit – encrypt the information for transfer (in transit) using sufficient and appropriate encryption (currently TLS.1.2 or greater). Maintain a register of trusted partners who you exchange information with. Review TLS connectors to ensure that they are still required and meet encryption requirements. See also RFC 526, NCSC Guidance on TLS profiles.	NCSP Cryptography NCSC – Using TLS to protect data
3.2.	Authentication – require mutual authentication to ensure the sender and recipient can confirm their identity	NCSP Identity and Access Management Standard
3.3.	Encryption at rest – encrypt information stored on systems to an appropriate level prior and post transfer.	NCSP Cryptography
3.4.	Recipient review – review the recipient and consider their appropriateness. Ensure that there is a reason for the intended recipient to have the information being transferred. Check distribution lists and plan the appropriate sending method.	Vetting Requirement for Police systems Guideline
3.5.	Sharing termination – where information sharing is no longer required, terminate the sharing mechanism e.g., revoke permissions to sharing platforms, remove users, or delete information.	
3.6.	Persistent sharing – where sharing of information is required on an ongoing or continuous basis, ensure that the appropriate business justification is approved by the appropriate owner of the risk (IAO / PAO) and recorded e.g., in a business case.	System Development Standard
3.7.	Impact on existing infrastructure – consider the impact on existing network infrastructure and systems and whether this is sufficient to support the information transfer e.g., a dedicated system interconnection and its impact on network traffic.	System Development Standard
3.8.	Email Transfer – when utilising email to transfer information, consider whether additional security controls are required e.g., password protect files, additional encryption (enforced rather than opportunistic) etc. The NCSC Email security check tool can assist in providing information about email domains – see NCSC web site.	NCSP Electronic Communication Standard NCSC Mailcheck Service
3.9.	Personal Accounts – Policing data that is not classified and not protected by legal instrument or contract can be emailed to or from personal accounts. For example personal payslip.	

4. Considerations for safe transfer of bulk information Bulk means large quantities of personal information or sensitive information.		
4.1.	Bulk Information Protection – Ensure that bulk data sharing follows NCSC principles Consider classification where aggregation of data.	NCSC – Protecting bulk personal data
4.2.	Full System Interconnection – refer to Secure by Design standards and methodology for where interconnections between systems may be required.	Cyber Security Architectural Principles System Development Standard Secure by Design SbD Guideline
4.3.	Dedicated circuit or VPN – Consider Secure by Design standards and methodology for the development and deployment of dedicated or continuous circuits. See NCSP Electronic Communications & Networks standards	Cyber Security Architectural Principles System Development standard Secure by Design SbD Guideline
4.4.	Dedicated Cloud Systems – There are products available to enable the secure bulk transfer of information. Consult your Information Security Officer (or equivalent) for guidance. Information Security Officers can consult their peer support network such as Police Information Assurance Group (PIAG) or regional ISO networks.	
4.5.	Emailing of large files – Many organisations place size limits on emails e.g., for attachments. Consider the best method for transfer if needing to send a large file or large set of information. Ensure secure protocols are used.	NCSP Electronic Communication Standard
4.6.	Removable Media – Where removable storage media must be used, ensure that additional security controls are implemented e.g., device encryption, process and procedure controls, movement record etc.	
4.7.	Phone Calls – Phone calls might be monitored, overheard or intercepted. Consider the requirement for transfer of information over telephone, and whether alternative, more controlled methods can be used. For Voice Over IP (VoIP) consider implementing TLS of the SIP messages and use of SRTP to encrypt calls.	Vetting Requirement for Police systems Guideline NCSP Electronic Communication 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.

Measurables generated by adopting this guideline 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 guideline 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.)

Document Information

Document Location

https://knowledgehub.group/web/national-standards/policing-standards

Revision History

Version	Author	Description	Date
0.1	PDS Cyber Audit, Risk & Compliance	Initial version	17/12/24

Approvals

Version	Name	Role	Date
1.0	NCPSWG	National Cyber Policy & Standards Working Group	05/02/25

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	v2024	03/2024
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
CSA Cloud Controls Matrix	v4	01/2021

10 Steps to Cyber Security - NCSC.GOV.UK	Web Page	05/2021

ANNEX A - FOR REFERENCE ONLY - Protection of OFFICIAL Police Data in Transit legacy guidance

Published by NPIRMT (National Police Information Risk Management Team)– Risks & contextual risk mitigation tables – circa 2018

"The ticks and crosses in the tables, reflect the fact that to enable the transmission of OFFICIAL data classified as having a HIGH value, is generally build on the principle that at least 2 elements of security enforcing configuration (VPN and TLS 1.2) must be compromised before the data could be intercepted. Where there is a single security enforcing control, data could be compromised more easily or lost as a result of a misconfiguration, as a result only lower levels of data should be transmitted across the chosen Network.

The tables enables Forces to determine the appropriate controls to protect their data in each network type, the controls should be considered to be the minimum required where a Force is transporting data from National systems or belonging to other data controllers in common from the Policing community of trust.

The scope is limited to the protection of police data in transit, and does not replace the need for formal risk assessment to ensure the data is appropriately assessed and that the correct network and other security controls are implemented to provide appropriate assurance."

MPLS network

Additional Network Controls / Virtual Private Network	Client - Server cryptography	HIGH BULK	HIGH	MEDIUM BULK	MEDIUM	LOW BULK	LOW
Hardware to Hardware IPSEC VPN	Minimum TLS v1.2	✓	✓	✓	✓	✓	✓
		✓	✓	✓	✓	✓	✓
Hardware to Software IPSEC VPN	Minimum TLS v1.2	✓	✓	✓	✓	✓	✓
		✗	✓	✓	✓	✓	✓
None	Minimum TLS v1.2	✗	✗	✓	✓	✓	✓
		✗	✗	✗	✗	✓	✓

Optical Fibre, Single Customer

Additional Network Controls / Virtual Private Network	Client - Server cryptography	HIGH BULK	HIGH	MEDIUM BULK	MEDIUM	LOW BULK	LOW
Hardware to Hardware IPSEC VPN	Minimum TLS v1.2	✓	✓	✓	✓	✓	✓
		✓	✓	✓	✓	✓	✓
Hardware to Software IPSEC VPN	Minimum TLS v1.2	✓	✓	✓	✓	✓	✓
		✗	✓	✓	✓	✓	✓
None	Minimum TLS v1.2	✗	✗	✓	✓	✓	✓
		✗	✗	✗	✗	✓	✓

Copper wire / leased line

Additional Network Controls / Virtual Private Network	Client - Server cryptography	HIGH BULK	HIGH	MEDIUM BULK	MEDIUM	LOW BULK	LOW
Hardware to Hardware IPSEC VPN	Minimum TLS v1.2	✓	✓	✓	✓	✓	✓
		✗	✗	✓	✓	✓	✓
Hardware to Software IPSEC VPN	Minimum TLS v1.2	✗	✓	✓	✓	✓	✓
		✗	✗	✓	✓	✓	✓
None	Minimum TLS v1.2	✗	✗	✓	✓	✓	✓
		✗	✗	✗	✗	✓	✓

Microwave link

Additional Network Controls / Virtual Private Network	Client - Server cryptography	HIGH BULK	HIGH	MEDIUM BULK	MEDIUM	LOW BULK	LOW
Hardware to Hardware IPSEC VPN	Minimum TLS v1.2	✓	✓	✓	✓	✓	✓
		✗	✗	✓	✓	✓	✓
Hardware to Software IPSEC VPN	Minimum TLS v1.2	✗	✓	✓	✓	✓	✓
		✗	✗	✓	✓	✓	✓
None	Minimum TLS v1.2	✗	✗	✓	✓	✓	✓
		✗	✗	✗	✗	✗	✓

Laser link

Additional Network Controls / Virtual Private Network	Client - Server cryptography	HIGH BULK	HIGH	MEDIUM BULK	MEDIUM	LOW BULK	LOW
Hardware to Hardware IPSEC VPN	Minimum TLS v1.2	✓	✓	✓	✓	✓	✓
		✗	✗	✓	✓	✓	✓
Hardware to Software IPSEC VPN	Minimum TLS v1.2	✗	✓	✓	✓	✓	✓
		✗	✗	✓	✓	✓	✓
None	Minimum TLS v1.2	✗	✗	✓	✓	✓	✓
		✗	✗	✗	✗	✗	✓

Wifi link Assumes WPA2 + AES							
Additional Network Controls / Virtual Private Network	Client - Server cryptography	HIGH BULK	HIGH	MEDIUM BULK	MEDIUM	LOW BULK	LOW
Hardware to Hardware IPSEC VPN	Minimum TLS v1.2	✓	✓	✓	✓	✓	✓
		✗	✗	✓	✓	✓	✓
Hardware to Software IPSEC VPN	Minimum TLS v1.2	✗	✓	✓	✓	✓	✓
		✗	✗	✓	✓	✓	✓
None	Minimum TLS v1.2	✗	✗	✓	✓	✓	✓
		✗	✗	✗	✗	✗	✓

Internet connection							
Additional Network Controls / Virtual Private Network	Client - Server cryptography	HIGH BULK	HIGH	MEDIUM BULK	MEDIUM	LOW BULK	LOW
Hardware to Hardware IPSEC VPN	Minimum TLS v1.2	✓	✓	✓	✓	✓	✓
		✗	✗	✓	✓	✓	✓
Hardware to Software IPSEC VPN	Minimum TLS v1.2	✗	✓	✓	✓	✓	✓
		✗	✗	✓	✓	✓	✓
None	Minimum TLS v1.2	✗	✗	✓	✓	✓	✓
		✗	✗	✗	✗	✗	✓