WILTSHIRE POLICE
FORCE POLICY

Information Risk Management

Date of Publication: June 2021
Version: 4.0
Next Review Date: June 2023

TABLE OF CONTENTS

POLICY STATEMENT

1. Introduction

The ability of the Wiltshire Police to deliver its policing priorities including public protection, stewardship of resources and to protect its reputation is dependent, often critically dependent, on its ability to manage information and information risks.

The Wiltshire Police Executive Leadership Team has stated its commitment to managing information risks effectively and the standard of Information Risk Management (IRM) expected.

Implementation of the Wiltshire Police IRM Policy and the basic principles set out in the policy for identification, assessment, management and escalation are **mandatory** for all Police Officers, Police Staff, 3rd parties, other agency representatives and delivery chain partners.

The policy applies to all information risks and sets out accountabilities, how risks are to be managed and performance tracked.

What are 'Information Risks'?

Information is essential to policing operations and enabling services. It takes many forms – from data sets of sensitive personal data through to records of sensitive meetings, personnel records, policy recommendations, correspondence, case files, intelligence reports and historical records. It exists in many formats from databases through e-Mail, persistent and non persistent messaging, paper, video and digital / magnetic media.

Information is not the same as Information Technology (IT) – IT Infrastructure, Systems, Services and Applications are the assets / platforms on which information is stored, processed, manipulated, retrieved, output, communicated, exchanged and managed. Therefore, information risks are not necessarily the same as IT security risks although managing IT security risks is a fundamental / critical component of any strategy to manage information risks.

Risk management not only means mitigating risks but also taking considered risks where the rewards are expected to be greater than any short term losses. The risks of not managing information illustrate this. Information Risks have the same characteristics as other organisational risks and must be managed with the same degree of consideration.

A Risk Assessment (RA) is essential to prioritise the correct actions for each part of our business. Some information, for example web publications, rarely carries security risks associated with disclosure – the risks here are more likely to be about tampering with the published official record or failure to achieve sufficient dissemination of key information. This is in contrast with Classified or other sensitive information where risks are more likely to be around confidentiality, disclosure or integrity although there are cases which demonstrate that there are also risks in not sharing sensitive information and of not maintaining sufficiently accurate records.

What is Information Risk Management?

Information Risk Management (IRM) adapts the generic processes of Risk Management and applies it to the Confidentiality (the property that information is not made available or disclosed to unauthorised individuals), Integrity (the property of safeguarding the accuracy and completeness of information) and Availability (the property of being accessible and usable on demand by an authorised and authenticated entity) of information and the information environment.

Table of contents

Information Risks when realised are therefore threats to:

Confidentiality – resulting in unauthorised access or disclosure
Integrity – resulting in inaccurate, incomplete or corrupted information or data
Availability – resulting in authorised and authenticated users not being able to access information on demand

Information Risk Management must be incorporated into all decisions in day to day operations and when effectively used is a tool for managing information proactively rather than reactively.

2. Information Risk Management Policy

This policy sets out the Wiltshire Police Commitment to the management of information risk.

Responsibility & Accountability

Senior Information Risk Owner (SIRO) – Deputy Chief Constable with responsibilities as set out at Annex A including responsibility for advising the Accounting Officer (Chief Constable) on information risk exposure, accepting or rejecting residual information risks on behalf of the AO and setting this policy. The SIRO is the only person authorised to approve deviations to this policy.

Head of Information Management & Assurance (Deputy SIRO) – directly responsible to and accountable for the provision of information management and governance advice and guidance to the SIRO, presenting and promoting Information Management, Records Management, Data Protection, Information Security and Risk Management policy to the Executive Leadership Team, ensuring that Information Management & Assurance strategies, plans, policies and initiatives are linked to and consistent with national strategic aims and objectives for information, undertaking quarterly and annual Information Management & Assurance reviews and ensuring that any significant control weaknesses are reflected in Statements of Residual Risk / Statements of Internal Control, publishing and maintaining this and complementary policies, the provision of threat assessments and warning advice, commissioning independent assurance of the Wiltshire Police Information Security Management System including the implementation of this and complementary security policies in accordance with Statutory and Regulatory body requirements & expectations

Records Manager – operationally responsible for the effective and appropriate management of Wiltshire Police operational and business records from their creation through to their eventual disposal, providing access to accurate records for a range of operational and business purposes and ensuring that legal and regulatory obligations are met (this includes controlling the number of records created and stored, identifying which records are to be preserved for business, historical and research purposes and which records should be destroyed).

Information Asset Owners (IAO) – responsibility, including that attendant with implementing this policy as set out at Annex B.

Data Protection Officer (DPO) - inform and advise the AO and the employees (who carry out his Processing) of their obligations, to monitor compliance with GDPR / LED, to provide advice in relation to a data protection impact assessment (including monitoring compliance), to co-operate with the Supervisory Authority (Information Commissioner's Office) and to act as the principal contact point for the Supervisory Authority and Data Subjects

Table of contents

Competence

Training – SIRO, H IM & A and IAO will receive specific formal IRM training from an approved commercial provider.

Authorised Users – will receive Information Management and Data Protection training as part of the induction and development process and through managed learning environment training. Security Operating Procedures (SyOPs) / practice directions are available for reference through 'firstpoint'.

Behaviour & Culture – all leaders, managers and supervisors will model the behaviours and culture that ensures information is valued, protected and used for the public good. All staff and stakeholders are encouraged to identify risks which may be reported anonymously if necessary through the Professional Standards Department (PSD) confidential reporting line.

Management

A threat assessment may be issued by the H IM & A to the SIRO and disseminated to IAO.

Control of information risk will be carried out using an Information Security Management System (ISMS) in accordance with applicable standards and community of trust governance and information risk baseline requirements. IAO will have some discretion over how to demonstrate compliance although in the majority of areas, a specific approach will be mandated. Security Classification, Personnel Security, Physical Security and Business Continuity are governed by separate policies and guidance as outlined in Chapter 3.

Business models and business plans will take account of information risk assessments.

Measuring performance and providing assurance – Wiltshire Police will:

- Measure and improve information risk management culture using the Community of Trust GIRR
- Report risks quarterly in response to legislative and regulatory body requirements
- Audit the implementation of this and complementary security policies at least annually and make a public statement about the quality of our system of internal control
- Report incidents in accordance with Cabinet Office, Home Office and local requirements as outlined at Annex E
- Ensure that all mission critical Information Systems (IS) handling Classified or otherwise sensitive information (personal data for example) will be 'Assured' in accordance with applicable HMG Standards and 'Reassured' when the threats and or risks change or when the system undergoes significant change or at least every 5 years for Official, every 3 years for Official-Sensitive and annually for Secret. Supporting infrastructure will be subject to bi-annual Assurance

Non compliance – will result in performance / misconduct considerations and, in some cases criminal investigation unless the SIRO has explicitly authorised a compliance expectation waiver.

Business Risk Environment Overview

Risk management is seen as the key to successful delivery of policing whilst protecting stakeholder interests. This allows Wiltshire Police to have increased confidence in achieving its desired outcomes, effectively constrain threats to acceptable levels and reach informed decisions about exploiting opportunities.

Table of contents

Information Risk Appetite

National – Cautious

Force

Official – Open (Willing to consider all options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward).

Official-Sensitive – Cautious (Preference for safe options that have a low degree of residual risk and may only have limited potential for reward).

Secret – Minimalist (Preference for ultra safe options that have a low degree of inherent risk and only have a potential for limited reward).

Risk Tolerance

Official – Medium
Official-Sensitive – Low
Secret – Very Low

Reason for Variance (if any)

National
Classification change

NB. The SIRO will be given every possible option for managing risk above set risk tolerance level.

Governance

The Wiltshire Police Information Risk Appetite is owned by the SIRO and approved by the AO. It is reviewed and updated on an inherent and residual basis and at least annually and or when triggered by a major security incident or identified very high risk.

Delegation and Escalation

- The roles authorized to accept information risk are as follows:
- Risks assessed as very low or low can be accepted by IAO provided there is a documented security case for acceptance
- Risks assessed as medium must be escalated to H IM& A who can accept provided there is a documented security case for acceptance
- Risks assessed as medium-high must be escalated to H IM& A who can accept provided there is a documented security case for acceptance accompanied by a specific Risk Balance / Escalation Case describing the risk management decision
- Risks assessed as high must be escalated to the SIRO who can accept provided there is a documented security case for acceptance accompanied by a Risk Balance / Escalation Case document describing the risk management decision.
- Risks assessed as very high cannot be accepted under the current risk appetite. Any identified very high risks should be escalated immediately through the SIRO to the AO and, if applicable, the PIAB through NPIRMT.

Top Level Business Risks Overview

Compliance, legal and regulatory risk: Wiltshire Police has an Averse approach to this category of risk. Legal compliance is of primary importance for the organisation. Avoidance, wherever possible, of risk and uncertainty is a key objective.

Table of contents

Financial risk: Wiltshire Police has a Minimalist approach to this category of risk. It must operate within strict and tight budgets with little contingency and few opportunities for flexibility. There is a preference for ultra safe options that have a low degree of inherent risk and only have a potential for limited reward.

Operational and policy delivery risk: Wiltshire Police has an Open approach to this category of risk. Its operational activities involve a high degree of inherent risk. Wiltshire Police is willing to consider all options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward.

Information risk: Wiltshire Police has (currently – June 21) a Cautious approach to this category of risk. There is a preference for safe options with low degrees of residual risk which may have only limited potential for business benefit delivery risk appetite. IAO must take into account the nature of any benefits and the different risk appetite categories when making information risk management decisions.

Reputation and credibility risk: Wiltshire Police has a high profile and a Cautious approach to this category of risk. There is a preference for safe options with low degrees of residual risk which may only have limited potential for reward. Wiltshire Police intends to review this posture and, if possible, move to an Open posture (understanding that this risk approach introduces a level of inherent reputational risk and requires controlled, accountable and externally audited risk management processes to reduce the associated level of residual risk).

Business Impact Assessment Overview

Public Order, Public Safety & Law Enforcement

Official: Consequence of Compromise

Impact on Life & Safety – Risk to an individuals personal safety or liberty.

Impact on the Provision of Policing Services – A disruption to policing services and operations requiring a reprioritisation at force level in order to meet expected levels of service.

Impact on Crime Fighting – Hinder the detection, impede the investigation or facilitate the commission of low level crime (that is crime not defined in legislation as serious crime) or hinder the detection of serious crime.

Judicial Proceedings – Cause a low level criminal prosecution to collapse, cause a conviction for a low level criminal offence to be declared unsafe or referred for appeal.

Official-Sensitive: Consequence of Compromise
Impact on Life & Safety – Risk to a group of individuals safety or liberty.

Impact on the Provision of Policing Services – A disruption to policing services and operations requiring reprioritisation at a national level (Cross Border Mutual Aid for example) to meet expected levels of service.

Impact on Crime Fighting – Impede the investigation of or facilitate the commission of serious crime as defined in legislation.

Judicial Proceedings – Cause a serious crime prosecution to collapse, cause a conviction for a serious criminal offence to be declared unsafe or referred for appeal.

Table of contents

Secret: Consequence of Compromise

Impact on Life & Safety – Threaten life directly leading to limited loss of life.

Impact on the Provision of Policing Services – A disruption to policing services and operations requiring emergency powers (MACP for example) to be invoked to meet expected levels of service

Impact on Crime Fighting – Cause major, long term impairment to the ability to investigate serious crime as defined in legislation.

Judicial Proceedings – Cause a number of criminal convictions to be declared unsafe or referred for appeal (persistent and undetected compromise of the evidence handling chain for example).

3. Landscape

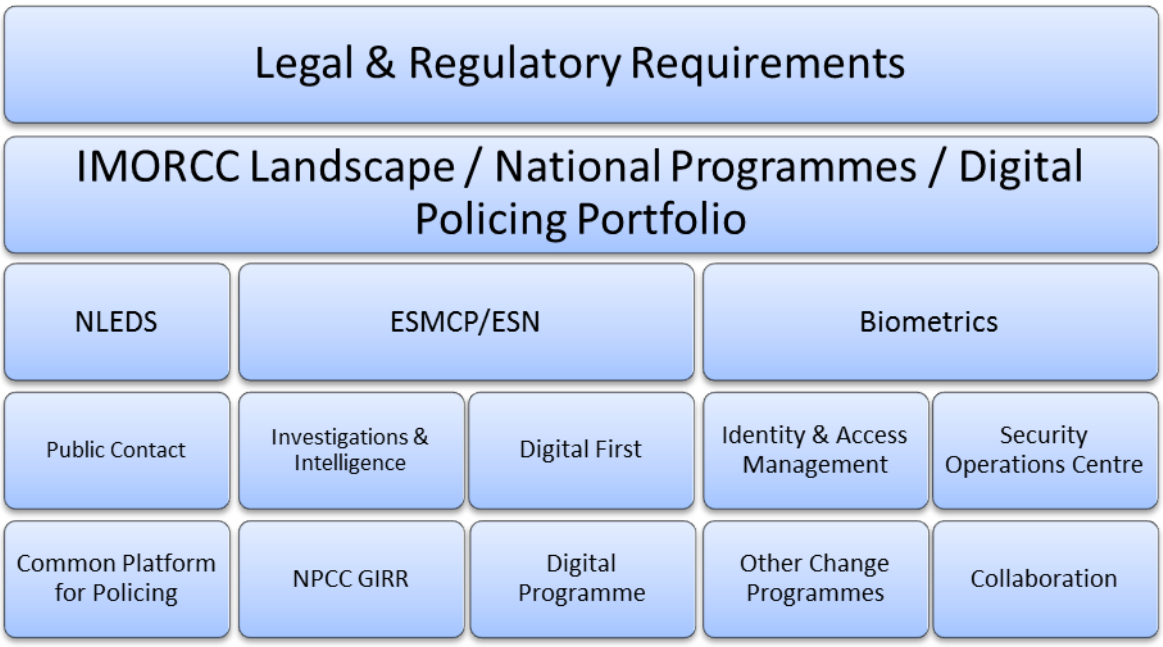

Table of contents

4. Key Areas of Information Risk

Risk Category	Example of Risk
Governance & Culture	Lack of comprehensive oversight and control (anything can go wrong) When something goes wrong, handling it badly and not learning (so it happens again) Third party mistakes (reputation suffers) New business processes don't take information and privacy risk into account (with potentially serious consequences)
Information Management & Integrity	Critical information is wrongly disposed of / destroyed, not kept or can't be found when needed (leading to reputational damage or financial penalties) Lack of basic records management disciplines (which can have wide ranging consequences) Inaccurate information (causing the wrong decision to be made or the wrong action to be taken) Critical electronic information becomes useless due to technical obsolescence (legal, reputational and financial consequences) Critical information is lost (legal, reputational and financial consequences)
The Human Dimension	Notwithstanding published rules (policies and procedures), staff, acting in error do the wrong thing (and things go badly wrong) Despite having rules, staff (the insider threat attack agent), acting deliberately, do the wrong thing (and things go badly wrong) 3rd parties obtain our information illegally or inappropriately (exposing it or act maliciously)
Information Availability & Use	Inappropriate disclosure of Classified or other sensitive information (causing reputational damage or worse) Failure to disclose critical information for public safety, public order or law enforcement purposes (leading at worst to loss of life) Failure to utilise the value of the information asset (leading to a waste of public money) Failure to allow information to be disseminated / communicated to the right people at the right time (leading to service delivery failure)

POLICY AIM

The aim of this policy is to set out the Wiltshire Police Commitment to the management of information risk allowing Wiltshire Police to deliver its policing priorities including public protection, stewardship of resources and to protect its reputation.

APPLICABILITY

This policy applies to all Police Officers, Police Staff, Special Constables, Volunteers and all contracted third parties. The policy applies to all information risks and sets out accountabilities, how risks are to be managed and performance tracked.

LEGAL BASIS AND DRIVING FORCE

HMG Security Policy Framework
Applicable HMG IA Standards No 6
ISO 27001 Part 3
Freedom of Information Act 2000
Data Protection Act 2018

RELATED POLICIES, PROCEDURES and OTHER DOCUMENTS

HMG Security Policy Framework
NPCC Community Security Policy
Business Continuity Management Systems (BCMS) Policy
Information Management Policy
Force Information Security Policy
Risk Management Policy
Vetting Policy and Procedure

AUTHORISED PROFESSIONAL PRACTICE

Information Management
Risk

DATA PROTECTION

Any information relating to an identified or identifiable living individual recorded as a consequence of this policy will be processed in accordance with the Data Protection Act 2018, General Data Protection Regulations (UK-GDPR) and the Force Data Protection Policy.

FREEDOM OF INFORMATION ACT 2000

This document has been assessed as suitable for public release.

MONITORING AND REVIEW

This policy will be reviewed bi-annually taking into account any newly published HMG policy and NPCC policy and guidelines.

WHO TO CONTACT ABOUT THIS POLICY

The Head of Information Management & Assurance is responsible for this policy. All queries relating to this policy should be directed to the Head of Information Management & Assurance.

Table of contents

Annex A

Terms of Reference – SIRO

The WP SIRO (DCC) is responsible for ensuring that information risks are effectively managed. The SIRO is accountable to the Accounting Officer (AO) (Chief Constable) and provides an annual report of the assessment and treatment of risks.

Responsibilities include but are not necessarily limited to:

Leading and fostering a culture that values, protects and uses information for the public good:

- Ensuring WP has a plan to achieve and monitor the right culture across the force, our partners and those involved in the service delivery chain
- Taking visible steps to support and participate in that plan
- Ensuring that WP has Information Security & Assurance specialist capability and Information Asset Owners who are skilled and focused on the issues

Ownership of the information risk management policy and risk assessment process:

- Testing outcome and ensuring it is used
- Ensuring risk policy is complete including how WP implements minimum mandatory measures in its own activity and that of partners and how compliance will be monitored
- Ensuring that risk assessments are completed every quarter taking into account extant legislative and regulatory body expectations and guidance
- Understanding (based of risk assessments) what information risks there are to WP through the service delivery chain and ensuring that they are addressed and that they inform investment decisions
- Ensuring that risk assessments and action taken benefit from adequate levels of independent scrutiny
- Considering all requests to deviate from policy

Advising the AO on information risk aspects of the statement of internal control:

- Receiving annual assessments of performance, including material from Information Security & Assurance specialists, independent assessors and IAO covering minimum mandatory measures as well as actions planned for WP specific circumstances
- Providing advice to the AO on the information risk parts of statements on internal control
- Sharing assessments and supporting material with the Home Office and Cabinet Office in support of pan government work in this area

Table of contents

Annex B

Terms of Reference – Information Asset Owners

Information Asset Owners are senior police officer and police staff colleagues involved in running an operational or business area which uses registered WP Information Systems (IS) and Information Assets. Their role is to understand what information is held, what is added, what is removed, how information is moved, who has access and why. As a result, they are able to understand and address risks to the information, ensure it is fully used within the law for public good and provide written input to the Protective Security Manager at least annually on the security and use of the Asset under their control.

Responsibilities:

Leading and fostering a culture that values, protects and uses information for the public good:

- Understanding WP plans to achieve and monitor the right culture across the force and our partners
- Taking visible steps to support and participate in that plan
- Participating in and contributing to the activities of the IAO community, identifying best practice and opportunities for continuous improvement

Knowing what information is held, what is added, what is removed and how:

- Maintaining an understanding of the Asset and how it is used
- Approving and minimizing information transfers whilst simultaneously achieving the business purpose
- Approving arrangements so that information placed onto removable media for example flash memory devices, CD-Rom and Laptop computers is the minimum necessary and appropriately protected with approved encryption methods when required
- Approving disposal schedules and mechanisms for paper and electronic records from the Asset

Knowing who has access to an Information Asset and why and ensuring use of it is monitored:

- Understanding WP policy on information use
- Being aware of and understanding relevant statutory requirements with regard to handling information
- Checking that access provided is the minimum necessary for the efficient conduct of business, considering requests for access from other business area / partner agency users and maintaining records of requests for access and decisions reached
- Undertaking / commissioning checks of Information Asset use
- Reporting security breaches promptly

Understanding, identifying and controlling risks in relation to their Information Asset and providing assurances to the Protective Security Manager (PSM):

- Contributing to the implementation of the Information Risk Management Policy in their operational / business area

- Contributing to risk assessments
- Providing (at least annually) written assessments to the PSM on the use and security of the Information Asset they are responsible for and the information they hold
- Making the case where necessary for new investment to secure the Information Asset

Ensuring the Information Asset is fully used for the public good including responding to requests from others:

- Considering whether better use of the Information Asset could be made
- Receiving and logging requests for access from others
- Ensuring decisions on access are taken accordingly

Table of contents

Annex C

Information Security Risks

Assets

An Asset is something assigned value by WP. By definition, Assets require protection. The proper management of and accountability for Assets is vital in order to maintain appropriate protection and these two aspects are prioritized responsibilities for all staff. An inventory of Information Assets associated with the Information Security Management System (ISMS) will be maintained with each Asset clearly identified, appropriately valued with ownership and security classification agreed and documented. Examples of Assets include but are not limited to:

- Information Assets – databases, data files, voice records, image files, system documentation, user manuals, training material, operational and support procedures, business continuity plans, fallback arrangements
- Paper Documents – contracts, guidelines, corporate documentation, documents containing important performance data
- Software Assets – application software, system software, development tools and utilities
- Physical Assets – computer (including laptop computers, PDA, Blackberry, flash memory devices) and communications equipment
- Corporate Assets – organisational image and reputation
- Services / Infrastructure – computing and communications services, utilities including heating, lighting, power, air-conditioning

Asset Values & Potential Impacts

In order to identify the appropriate protection for Assets, they will be valued in terms of implications to operations and business. These values will be expressed in terms of the potential impacts of unwanted incidents from Confidentiality, Integrity and / or Availability loss perspectives. In order to assess these potential losses consistently, a value scale for Assets will be applied. For each Asset and each of the possible losses, a value will be assigned.

Threats

Assets are subject to many threats. Threats have the potential to cause unwanted incidents resulting in harm to a system and or Assets. This harm can occur from a direct or indirect attack against information for example unauthorized disposal, destruction, disclosure, modification, corruption and availability or loss of Assets.

Threats can originate from accidental or deliberate sources or events but need to exploit system, application or service vulnerabilities in order to successfully cause harm to assets. (Threat type examples appear at Annex F).

Vulnerabilities

These are weaknesses associated with Assets which may be exploited by a threat causing unwanted incidents resulting in loss, harm or damage to Assets. Vulnerabilities in and of themselves do not cause harm – they are conditions or sets of conditions allowing a threat to adversely affect an Asset.

Table of contents

Security Risks

A security risk is the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of Assets. Measures of risk are determined from the combination of Asset value and assessed levels of related threats and associated vulnerabilities (threat x vulnerability x impact / value).

Security Requirements

There are three (3) main sources of security requirements to be documented in the ISMS:

- Unique security risks which could lead to significant losses in operational / enabling service capability if they are realised
- Statutory, regulatory and contractual obligations which must be satisfied by WP and trusted third parties
- Unique principles, objectives and obligations that WP has developed to support operations and business processes and which apply to our IS

Once these security requirements have been identified, they will be formulated in terms of requirements for **Confidentiality**, **Integrity** and **Availability**.

Security Issues

When determining security requirements, it is important to understand what damage risks can do to operations and business. When establishing the context, identifying potential risks and valuing assets the following questions will be asked:

- What are the most important parts of the business, how are they supported by using or processing information and how essential is this support
- What essential decisions depend on the accuracy, completeness and currency of information and its availability
- What sensitive or classified information needs to be protected and why
- What are the implications of information related security incidents

Legal, Regulatory & Contractual Requirements

The security requirements specifying statutory, regulatory and contractual obligations that WP, trusted third parties and service providers / suppliers have to satisfy will be documented in the ISMS. It is important, for example controlling proprietary software copying, safeguarding organizational records and satisfying the Data Protection Act that the ISMS supports these requirements and that the implementation of, or absence of security controls in each IS does not breach statutory obligations or commercial contracts.

Organizational Principle, Objectives & Requirements

The security requirements relating to force wide principles, objectives and requirements for information processing to support operations and business will be documented in the ISMS. It is important that the ISMS supports these requirements and vital that the implementation of or absence of security controls in each IS does not impede efficient operations and business. Each security requirement will be translated in terms of the Confidentiality, Integrity and or Availability of the information encompassed by the ISMS.

Table of contents

Information Security Controls

Security controls are practices, procedures and mechanisms which are designed to protect against threats, reduce vulnerabilities, limit the impact of an incident or protect against risks in any other way. Effective security requires a combination of controls that perform one or more of the following functions:

- Detection
- Deterrence
- Prevention
- Limitation
- Correction
- Recovery
- Monitoring
- Awareness

Expenditure on information security controls will be balanced against and appropriate to the value of the information and other Assets at risk and the operational or business harm likely to result from security failures.

Table of contents

Annex D

Policy: Transmitting Personal Data beyond the Secure Boundary

These mandatory instructions apply whenever there is a requirement to transmit (send or receive) personal data / information beyond the secure boundary of the WP. In relation to e-Mail, the secure boundary encompasses the Public Services Network (PSN) and the Government Secure Intranet (GSI).

Circumstances in Which Personal Data / Information may be Transmitted

Wherever there is an approved operational / business requirement to transmit personal information / data belonging to the WP or our delivery partners / trusted third parties across the boundaries of our secure premises:

a) The approval of the IAO for the information must be obtained before such information is transmitted

b) Before giving approval, the IAO must be satisfied that:
   - The data to be transmitted cannot be stripped of personal information without undermining the purpose of the transmission
   - There is an operational / business need to transmit the personal information which cannot be met by alternative means not involving the movement of the information outside the secure boundary
   - The proposed means of transmitting the information accords with the guidance below and the reasons have been recorded (for example in an Information Transfer Register - ITR)
   - There is evidence that the security measures applied by the receiving party to protect the information are appropriate having regard to the nature of the data and covering technical, physical, procedural and personnel security requirements
   - A risk assessment has been carried out and mitigating measure have been applied – the risk assessment must include the arrangements for the transmission of information and the security arrangements applied by the receiving party
   - The measures set out in this policy are in place and fully complied with

c) Personal information will, wherever possible be transmitted to a remote computer on a secure site – both the communication link and the data at rest being protected to an agreed standard. Where this is not possible and it is necessary to use removable media, the reason will be recorded in the ITR.

d) Where it is necessary to use removable media to transfer personal information / data:
   - The information transferred to the removable media must be the minimum necessary to achieve the business purpose in terms of the numbers of people covered by the information and the scope of information held – where possible, only anonymised information should be held
   - The removable media must be encrypted to an agreed standard
   - Each individual transfer of data will be recorded in the ITR together with other information described below

Table of contents

e) The ITR will record:

- The date and time on which the information is transmitted
- Sender and recipient details
- The means by which the information is transmitted
- A description of the information
- The name of the person who prepared the information for despatch
- The despatching business area reference number for the transmission
- The reasons for transmitting the information including reference to the risk assessment
- Confirmation that the information has been received with the date and time of receipt
- The name of the IAO and confirmation that the transfer was authorised

Table of contents

Annex E

Incident Reporting Requirements

Reporting of an Incident Involving WP IT Equipment and Information

Please use this report to notify any loss or theft of WP Information Assets, unauthorised disclosure of information or misuse of equipment of identification & authentication privileges. This report may be completed electronically or by hand. Once completed, you can either e-Mail the completed report to (enter Group Mailbox address) or send the hand completed report to (enter Internal Postal Address).

Table of contents

SECURITY INCIDENT REPORT

Reporting Officer's Details					
Name					
Department / Command					
e-Mail					
Telephone Number					
Date Reported					
Details of Asset					
1	Type of Asset?				
2	If loss of a remote access laptop, was the Secure Id token also lost?	Yes		No	
3	Classification	Official		Official-Sensitive	
4	Asset /Serial Numbers?				
5	Date incident happened or when 1st identified?				
6	Type of incident?				
	Theft				
	Loss				
	Damage	Accidental		Deliberate	
	Unauthorised Information Disclosure	Accidental		Deliberate	
	Asset misuse				
	Other (please state)				
7	Cost of replacement (if known)?				
8	Incident description				

9	What action was taken when the incident occurred?	
10	Crime reference number (if applicable)	
Subsequent Actions		
11	Who has been notified of this incident?	
12	What action is planned to prevent or reduce the risk of any re-occurrence?	
13	What actions, if any, are outstanding?	
14	Any other relevant information?	
15	Do you have any recommendations for preventing this type of incident?	
16	Is there any advice you would like concerning this incident?	

Table of contents

Annex F

Examples of Possible Threat Types

The table gives examples of typical threats that might be considered during the threat assessment process. Threats can be caused by one or more events of a deliberate, accidental or environmental nature.

Checklist 1: Potential Threat Types to Consider

Threat types = **D** (Deliberate), **A** (Accidental) and **E** (Environmental). **D** is used for all deliberate actions aimed at information assets, **A** is used for all human actions which can accidentally damage information assets and **E** is used for all incidents which are not human based.

Earthquake	E
Flooding	A, D, E
Hurricane	E
Lightning	E
Industrial Action	A, D
Bomb Attack	D
Use of Arms	D
Fire	A, D
Wilful Damage	D
Power Supply Failure	A
Water Supply Failure	A
Air Conditioning Failure	A, D
Hardware Failure	A, D
Power Fluctuation	A, E
Temperature / Humidity Extremes	A, D ,E
Dust	E
Electromagnetic Radiation	A, D, E
Electrostatic Charging	E
Theft	D
Unauthorized Use of Storage / Exchange Media	A, D
Deterioration of Storage Media	E
Human Error	A, D
Software Failure	A, D
Unauthorized Software Use	A, D
Masquerading of User Identity	D
Illegal Software Use	A, D
Malicious Software	A, D
Illegal Import or Export of Software	D

Maintenance Error	A, D
Unauthorized Network Access	D
Unauthorized use of Network Facilities	D
Technical Failure of Network Components	A
Transmission Errors	A, D
Damage to Communications Lines	A, D
Traffic Overloading	A, D
Eavesdropping of Communications	D
Communication Infiltration	D
Traffic Analysis	D
Message Misrouting	A, D
Message Rerouting	D
Repudiation	D
Communications Service Failure (Network Services)	A, D
Staff Shortages	A, D
User Errors	A, D
Resources Misuse	A,D

Checklist 2: Common Vulnerabilities to Consider

This can provide help during vulnerability assessments. It is emphasized that this list is not exhaustive in any way and in some cases, other threats may also exploit these vulnerabilities.

Environment & Infrastructure	
1	Lack of physical protection of the building, doors and windows – could be exploited by for example threat of theft
2	Inadequate or careless use of physical access control to buildings, areas and rooms – could be exploited by, for example, the threat of wilful damage
3	Unstable power grid – could be exploited by, for example, the threat of power fluctuation
4	Location in an area susceptible to flood – could be exploited by, for example, the threat of flooding
Hardware	
5	Lack of periodic replacement schemes – could be exploited by, for example, the threat of deterioration of storage media
6	Susceptibility to voltage variations - could be exploited by, for example, the threat of power fluctuation
7	Susceptibility to temperature variations - could be exploited by, for example, the threat of temperature extremes
8	Susceptibility to humidity, dust, soiling - could be exploited by, for example, the threat of dust

9	Sensitivity to electromagnetic radiation - could be exploited by, for example, the threat of tempest radiation
10	Insufficient maintenance / faulty installation of storage media - could be exploited by, for example, the threat of staff error
11	Lack of efficient and effective configuration control - could be exploited by, for example, the threat of staff error
Software	
12	Unclear or incomplete development specifications - could be exploited by, for example, the threat of software failure
13	No or insufficient software testing - could be exploited by, for example, the threat of unauthorized use of software or use of software by unauthorized users
14	Complicated user interface - could be exploited by, for example, the threat of staff error
15	Lack of identification and authentication mechanisms - could be exploited by, for example, the threat of masquerading user identities
16	Lack of audit and accounting - could be exploited by, for example, the threat of use of software in an unauthorized way of repudiation of action
17	Well known flaws in software - could be exploited by, for example, the threat of the use of software by unauthorized users
18	Unprotected password tables - could be exploited by, for example, the threat of masquerading user identities
19	Poor password management (easily guessable passwords, storing passwords in clear view, insufficient frequency of password change) - could be exploited by, for example, the threat of masquerading user identities
20	Inappropriate allocation of user privileges / access rights - could be exploited by, for example, the threat of inappropriate access to information breaching the need to know principle
21	Uncontrolled downloading and use of software - could be exploited by, for example, the threat of malicious software
22	Lack of system and other documentation - could be exploited by, for example, the threat of staff error
23	Lack of back-up copies - could be exploited by, for example, the threat of malicious software or the threat of loss through fire or flooding
24	Lack of effective change control - could be exploited by, for example, the threat of software / hardware failure
25	No logout when leaving work stations / client devices - could be exploited by, for example, the threat of unauthorized access to information assets
26	Disposal or reuse of storage media without proper erasure - could be exploited by, for example, the threat of unauthorized access to information of unauthorized use of software
Communications	
27	Unprotected communications lines - could be exploited by, for example, the threat of eavesdropping
28	Poor cabling controls - could be exploited by, for example, the threat of communications infiltration
29	Lack of identification and authentication of sender and receiver - could be exploited by, for example, the threat of masquerading user identities

30	Transfer of passwords in clear view - could be exploited by, for example, the threat of unauthorized network and other information asset access
31	Lack of proof of sending / receiving messages - could be exploited by, for example, the threat of repudiation
32	Dial up lines - could be exploited by, for example, the threat of network access by unauthorized users
33	Unprotected (unencrypted) sensitive traffic - could be exploited by, for example, the threat of eavesdropping
34	Inadequate network management (routing resilience) - could be exploited by, for example, the threat of traffic overloading
35	Unprotected public network communications - could be exploited by, for example, the threat of unauthorized access to information assets
Documents	
36	Unprotected storage - could be exploited by, for example, the threat of theft
37	Lack of care during disposal - could be exploited by, for example, the threat of theft or unauthorized access to information
38	Uncontrolled copying - could be exploited by, for example, the threat of theft
39	Lack of compliance with protective marking precautions - could be exploited by, for example, the threat of theft, unauthorized / uncontrolled access, loss of documents
Personnel	
40	Absence of personnel - could be exploited by, for example, the threat of staff shortage
41	Unsupervised work by third parties - could be exploited by, for example, the threat of theft or unauthorized access
42	Insufficient security education, training and awareness - could be exploited by, for example, the threat of staff error
43	Incorrect use of software and hardware - could be exploited by, for example, the threat of staff error
44	Lack of monitoring mechanisms - could be exploited by, for example, the threat of repudiation of action or the use of software in an unauthorized way
45	Lack of effective policies and procedures - could be exploited by, for example, the threat of staff error
46	Inadequate recruitment and vetting procedures - could be exploited by, for example, the threat of infiltration, theft, wilful damage

Table of contents

DOCUMENT ADMINISTRATION

Ownership:

Department Responsible: Information Management & Assurance
Policy Owner/Author: Keith LEWIS (Head of Information Management & Assurance)
Technical Author:
Senior Officer/Manager Sponsor: Deputy Chief Constable

Revision History:

Revision Date	Version	Summary of Changes
June 2017	2.0	Bi-annual review - non substantive (phraseology / abbreviation and acronym amendments)
June 2019	3.0	Bi-annual review – changes to Responsibility & Accountability (inclusion of DPO and Records Manager) slight changes to top level business risks overview
June 2021	4.0	Non substantive narrative.

Approvals:

This document requires the following approvals:

Name & Title	Date of Approval	Version
Continuous Improvement Team	June 2019	3.0
Head of Information Management & Assurance	June 2019	3.0
JNCC	N/A	

Distribution:

This document has been distributed via:

Name & Title	Date of Issue	Version
E-Brief		
Email to relevant affected Staff/Officers		
Other: (state method here)		

Diversity Impact Assessment:

Has a DIA been completed? If no, please indicate the date by which it will be completed. If yes, please send a copy of the DIA with the policy.	☐ **Yes** ☐ **No** **Date**:

Consultation:

List below who you have consulted with on this policy (incl. committees, groups, etc):

Name & Title	Date Consulted	Version
N/A		

Implications of the Policy:

Training Requirements

No additional training requirements.

IT Infrastructure

No additional IT infrastructure required.