INFORMATION RISK MANAGEMENT

Executive Summary

The purpose of this Information Risk Management Policy (IRMP - the Policy) document and supporting procedures is to set out the commitment of West Midlands Police (WMP) to protect WMP information, physical and personnel assets from all information risks. This policy outlines the governance requirements, the appropriate roles and responsibilities, and methodologies to be employed for ensuring the continued protection of National and Regional Information Systems and Assets. These will be achieved by the identification, review, escalation and treatment of risks, and how these risks will be proportionately and cost effectively managed.

Authorised Professional Practice (APP):

- This policy has been checked against APP. West Midlands Police has adopted the APP provisions, with supplementary information contained herein, which reflects local practice and the needs of the communities served by West Midlands Police.

Those provisions are shown in the links below and can be accessed via the home page of the APP website

APP CONTENT

Policy Statements:

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

- This is due to:
  - The increased reliance on National and Regional Information Systems and policing information by Forces, Agencies, Criminal Justice, local government partnerships and others;
  - The ever-changing threat landscape to and introduction of new technologies in UK Policing;
  - Collaborative working;
  - Changes in data handling requirements and legislation;
  - Increased personal, organisational liability and accountability; and
  - The need to protect this information and the assets used to deliver it is greater than in previous years.

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

INFORMATION ASSURANCE RISK MANAGEMENT

- There are three areas of Information Assurance (IA) risk management, defined as follows:

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Ensuring the information is accessible only to those authorised to have access	Safeguarding the accuracy and completeness of information and processing methods - this may include the ability to prove an action or event has taken place, such that it cannot be repudiated later	Ensuring that authorised users have access to information and associated IS when required.

- Confidentiality, integrity and availability are all equally important. Although integrity and availability have always been key considerations, policy has tended to focus on confidentiality.
- This policy ensures that all three are fully addressed and given equal importance.
- It recognises that many assets may have little or no requirement for confidentiality but availability and integrity may be vital.
- It also recognises that confidentiality extends beyond government protective markings to privacy and other sensitivities.

RISK APPETITE STATEMENT

- The Risk Appetite Statement is a separate document, reviewed and approved by the Senior Information Risk Officer (SIRO) annually.
- It sets the background against which the force manages its Information risks**.**
- In line with best practice, WMP's risk appetite is set in the context of confidentiality, integrity and availability.
- There are five categories of risk appetite and the descriptions of the associated behaviours are as follows:

Averse (Risk Avoidance)	Minimalist	Cautious	Open	Hungry (high risk, high reward)
Avoidance of risk and uncertainty is a key objective. Exceptional circumstances are required for any acceptance of risk	Preference for ultra-safe options that have a low degree of inherent risk and only have a potential for limited business benefit	Preference for safe options that have a low degree of residual risk and may only have limited potential for business benefit	Willing to consider all options and choose the one that is most likely to result in successful delivery minimizing residual risk as far as possible, while also providing an acceptable level of business benefit	Eager to realise business benefits and to choose options to achieve this despite greater residual risk.

RISK ASSESSMENT

- Any individual or group of individuals that wish to commission a change to an existing system or implement a new one will initially discuss this with the appropriate IAO to gain approval in principle.
- If a change is commissioned through a formal project gaining approval is the responsibility of the assigned project (or programme) manager.
- The IAO will, either personally or through an approved delegate, discuss this change with the Security and Information Risk Advisor (SIRA).

- The SIRA will be responsible for gathering sufficient information to articulate a clear risk assessment of the proposal.

- The risk assessment will be prepared based on the Security Policy Framework (SPF). This will generate a residual risk score after risk mitigation.

- Risks will be treated in a reasonable and cost-effective manner and will not be overly mitigated in excess of what is needed to reasonably meet the risk appetite.

RISK ACCEPTANCE

- Once residual risk has been assessed it will move into the acceptance process.

- Risk can be accepted by different roles within WMP's information assurance structure.

- In the event that the risk cannot be accepted by the IAO, the SIRA will prepare a risk assessment and present it to the accreditor for discussion.

- Dependant on the risk matrix the Force Accreditor may be in a position to accept the risk.

- If the risk acceptance decision sits at SIRO level, then the Force Accreditor will produce an executive summary, showing risk, mitigation and residual risk for the proposal and present this to the SIRO.

- The SIRO will accept or reject the proposal and inform the Force Accreditor of the decision.

- It is the responsibility of the Force Accreditor to update the national body of any significant change.

- Usually the SIRO is the final decision maker for accepting local risks, however, in extreme cases it is possible to escalate a conflict to the Accounting Officer.

TRAINING

- Every network user must complete the National Centre for Applied Learning Technologies (NCALT) on-line training modules entitled 'Managing Information' within 3 days of joining the Force and prior to gaining access to the corporate network.

- This training must be completed every other year thereafter.

- All details of training commenced, progress and completion are held centrally and accessible by the Force Data Protection Officer (DPO).

- Non-completion may result in the individual being denied access to the Force network and all systems until the training is completed.

- In this event, the individual's Line Managers and Supervisors must assess the risk of leaving the individual in any role with unsupervised access to personal data and take action accordingly.

- All Line Managers and Supervisors must encourage individuals within their areas of responsibility to increase their data protection knowledge and the obligations the Data Protection Act 2018 Act places upon them, at every opportunity.

- Individuals who leave and re-join the Force in a new role e.g. as a Special Constable, or who have had a break in service of more than 6 months or are returning from long term sick, are required to repeat the training.

- Information Asset Owners (IAOs) will receive bespoke training in addition to the above training packages.

Definitions/Acronyms:

WMP – West Midlands Police

IAO – Information Asset Owner

DPA 2018 – Data Protection Act 2018

DPO – Data Protection Officer

NCALT - National Centre for Applied Learning Technologies

SIRA - Security and Information Risk Advisor

SIRO – Senior Information Risk Officer

Procedural Guidance Documents List:

RISK APPETITE STATEMENT
COMPLIANCE, AUDIT AND ASSURANCE PROCEDURE
INFORMATION ASSET OWNERS PROCEDURE (HANDBOOK)
SENIOR INFORMATION RISK OWNER (SIRO) HANDBOOK
INFORMATION SHARING PROCEDURE
FORENSIC READINESS PROCEDURE
INFORMATION SECURITY INCIDENT MANAGEMENT PROCEDURE

Publication Instructions:

- Suitable for publication to public

Policy Ref: DCC/04

Version: 1.0

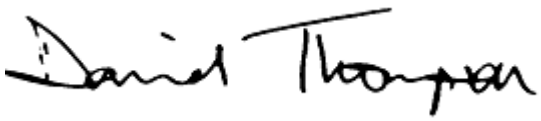
Date: 11/03/2022

Review Date: 11/03/2023

Policy Author: Kate Jeffries

Any enquiries in relation to this policy should be made directly with the policy author shown above.

Force Executive Approval:



CHIEF CONSTABLE

Monitoring and Review

Version	Date Reviewed	No change / Minor Changes / Major Changes *(detail)*	Amended / Agreed by	New review date