INFORMATION SECURITY

Executive Summary

The purpose of this Information Security Policy (ISP - 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 threats, whether internal, external, deliberate or accidental.

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

https://www.app.college.police.uk/app-content/information-management/information-assurance/

Policy Statements:

- This Policy is a key component of WMP overall information security management framework.
- This policy must be read and considered alongside more detailed information security documentation including relevant security guidance and procedures relating to Information Security and Assurance.
- It is the policy of WMP to ensure that:

Information and physical assets will be protected against unauthorised access
Confidentiality of all assets will be assured
Integrity of information will be maintained
Regulatory and legislative requirements will be met
Information Security training will be provided
All breaches of Information Security, actual or suspected, will be reported and investigated
Business requirements for the availability of information and information systems will be met
All Managers are directly responsible for implementing the Policy within their business area, and for the adherence by their staff

- We must establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by WMP.
- We can do this by:

Identifying through appropriate risk assessment, the value of information assets, to understand their vulnerabilities and the threats that may expose them to risk
Managing the risks to an acceptable level through the design, implementation and maintenance of a formal Information Security Management System (ISMS)

Compliance with any third party or delivery partner contract/agreement conditions relating to information security
Commitment to comply with HMG's Security Policy Framework (SPF)
Commitment to achieve and maintain accreditation under the National Police Chief's Council Information Systems Community Security Policy
Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies
Describing the principles of security and explaining how they shall be implemented in the Force
Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities
Creating and maintaining within the Force a level of awareness of the need for information security as an integral part of our day to day business
Protecting information assets under the control of the Force

- It is the responsibility of each employee or third-party representative to adhere to this Policy.
- Information security is a responsibility shared by all members of the Force but ultimate responsibility rests with the Chief Constable.
- The "user" logging onto authorised systems implicitly agrees to be bound by the rules of the Information Security Policy and associated procedures.
- WMP recognise the importance of Force information assets and supports the goals and principles of effective security management to safeguard the confidentiality, integrity and availability of all information held.
- Therefore, it is important that there be in place sufficient and adequate information security safeguards and countermeasures.
- This is to be able to provide the continued availability of Force information and information systems both internally and to policing partners.
- Only current and vetted officers and staff will be granted access to WMP equipment, data and information systems.
- Access is granted to the information system on employment if a network account is required for the role.

NON-COMPLIANCE

- You are expected to handle information in accordance with policy and legislation at all times.
- If you suspect anyone is accessing information for a non-policing purpose or mishandling information you must report it to your supervisor.
- The supervisor must bring it to the attention of the local Appropriate Authority so that any available evidence is secured.

- If the Standards of Professional Behaviour, Codes of Ethics or criminal offences have been committed the Appropriate Authority must refer the conduct to the Professional Standards Department who may progress to criminal or disciplinary proceedings.

TRAINING

- Appropriate training shall take place for each group of responsible persons.
- Training will include induction training on appointment or transfer and further specialist training as required and as appropriate.
- Specialist training shall take place in particular for the roles of DPO, SIRA, ISM, Force Accreditor, IAO.
- Induction training and update training/briefings shall take place for all other officers and staff, such as Line Managers and general users of systems.

Definitions/Acronyms:

- DCC – Deputy Chief Constable
- DPO – Data Protection Officer
- IAO – Information Asset Owner
- ISM – Information Security Manager
- ISMS – Information Security Management System
- ISAO – Information Security Assurance Officer
- SIMB – Strategic Information Management Board
- SIRO – Senior Information Risk Owner
- SIRA – Security and Information Risk Advisor
- SPF – Security Policy Framework
- SSO – Senior System Owner
- SyOPs – Security Operating Procedures

Procedural Guidance Documents List:

Acceptable Use Procedure
Bluetooth Procedure
Clear Desk Procedure
Cryptographic Procedure
Data Breach Procedure
Government Security Classification Procedure.
Information Security Incident Management Procedure
Mobile/Remote Working Procedure
Password Procedure
Physical Security Procedure
Protective Monitoring Procedure
Subject Access Requests Procedure

Publication Instructions:

- Suitable for publication to public

Policy Ref: DCC/03

Version: 1.0

Policy Implementation Date: 11/03/2022

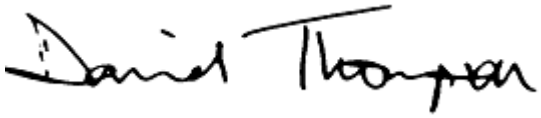
Version Date: 11/03/2022

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