WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Technical Security Infrastructure Policy**
POLICY REFERENCE NO:	**Inf/24**

Executive Summary.

In accordance with the HMG SPF Risk Management, West Midlands Police will ensure that Risk Assessments are carried out to identify, quantify and prioritise risks to all protectively marked information, information assets and personal data. Appropriate controls and proportionate measures will be selected and implemented to mitigate the risks identified.

***Any enquiries in relation to this policy should be made directly with the policy contact / department shown below.*

Intended Policy Audience.

This policy applies to every police officer, member of police staff, police community support officer, special constable, volunteer, contractor, and approved persons working for or on behalf of West Midlands Police.

Current Version And Effective Date.	**Version 0.2**	**14/01/2015**
Business Area Owner	**Information Management Services**	
Department Responsible	**Information Management**	
Policy Contact	**Kate Jeffries – Head of Information Management**	
Policy Author	**Tom King**	
Approved By	**DCC Thompson**	
Policy Initial Implementation Date	**17/03/2015**	
Review Date	**17/03/2017**	
Protective Marking	**Not Protectively Marked**	
Suitable For Publication – Freedom Of Information	**Yes**	

Supporting Documents

- HMG Security Policy Framework (SPF);
- CESG IA Standards (IAS) and Good Practice Guides (GPG's);
- BS ISO27001:2013 – Information Technology
- Security Assessment for Protectively Marked Assets (SAPMA)
- WMP Local Threat Assessment
- *Code of Ethics (http://www.college.police.uk/docs/Code_of_Ethics.pdf)*

Evidence Based Research

Full supporting documentation and evidence of consultation in relation to this policy including that of any version changes for implementation and review, are held with the Force Policy Co-ordinator including that of the authorised original Command Team papers.

Please Note.
PRINTED VERSIONS SHOULD NOT BE RELIED UPON. THE MOST UPTO DATE VERSION OF ANY POLICY OR DIRECTIVE CAN BE FOUND ON THE EQUIP DATABASE ON THE INTRANET.

Force Diversity Vision Statement and Values

"Eliminate unlawful discrimination, harassment and victimisation. Advance equality of opportunity and foster good relations by embedding a culture of equality and respect that puts all of our communities, officers and staff at the heart of everything we do. Working together as one we will strive to make a difference to our service delivery by mainstreaming our organisational values"

"All members of the public and communities we serve, all police officers, special constables and police staff members shall receive equal and fair treatment regardless of, age, disability, sex, race, gender reassignment, religion/belief, sexual orientation, marriage/civil partnership and pregnancy/maternity. If you consider this policy could be improved for any of these groups please raise with the author of the policy without delay."

Code of Ethics

West Midlands Police is committed to ensuring that the Code of Ethics is not simply another piece of paper, poster or laminate, but is at the heart of every policy, procedure, decision and action in policing.

The Code of Ethics is about self-awareness, ensuring that everyone in policing feels able to always do the right thing and is confident to challenge colleagues irrespective of their rank, role or position

Every single person working in West Midlands Police is expected to adopt and adhere to the principles and standards set out in the Code.

The main purpose of the Code of Ethics is to be a guide to "good" policing, not something to punish "poor" policing.

The Code describes nine principles and ten standards of behaviour that sets and defines the exemplary standards expected of everyone who works in policing.

Please see http://www.college.police.uk/docs/Code_of_Ethics.pdf for further details.

The policy contained in this document seeks to build upon the overarching principles within the Code to further support people in the organization to do the right thing.

CONTENTS

1. INTRODUCTION.

1.1 West Midlands Police applications and supporting infrastructure rely on technical security infrastructure to protect the underlying platform and enforce robust controls across trust boundaries. An effective policy and framework of controls is required to govern and manage the deployment of technical security infrastructure to protect critical applications and sensitive information against known threats and reduce overall risk to organisational value, and operations.

2. TECHNICAL SECURITY INFRASTRUCTURE POLICY

2.1 Security Architecture

2.1.1 Formal documented security architecture **must** be established and embedded within the overall enterprise IT architecture.

2.1.2 A formal documented risk assessment **must** be conducted to identify and evaluate potential security risks to business applications, supporting infrastructure and sensitive information. The security architecture, informed by the results of the risk assessment should determine the nature, degree and depth of protection required to defend against a broad range of security threats.

2.1.3 The process for defining security architecture should involve:

- an assessment of business requirements for information security
- definition of guiding principles that underpin the security architecture
- use of a layered security model for security architecture
- identification of security controls, services and technologies to be included in the security architecture
- supporting tools and resources required to manage the security architecture

2.1.4 The process for developing the security architecture should include:

- engagement of a security architect
- input from relevant functional areas and internal specialists
- communication and education of individuals who are required to use the security architecture

2.1.5 The security architecture should consider the design principles in the table below when defining and implementing architectural safeguards:

Security Architecture Principles	Description
Secure by Design	Considering the security requirements of a business application or information system as part of its overall requirements, to protect itself and the information it processes, and to resist attacks.
Defence in Depth	Using multiple layers of different types of protection to avoid reliance on one type or method of security control.
Secure by Default	Setting preselected options to limit the level of inherent vulnerability, such as providing least privilege or making only necessary services and features available.

Default Deny	Denying access to information systems by default to prevent unauthorised access.
Fail Secure	In the event of a system failure, information is not accessible to unauthorised individuals, remains available to authorised individuals and cannot be tampered with or modified.
Secure in Deployment	Providing complementary tools and guidance to help support system administrators and users, ensuring configuration is not difficult and software updates are simple to deploy.
Usability and Manageability	Security controls do not obstruct users in performing their work and are not difficult to manage.

2.1.6 The security architecture should support a consistent enterprise-wide process for implementing security services and establishing common user and application programming interfaces.

2.1.7 The security architecture should support achievement of the following outcomes across the organisation:

- minimise the diversity of hardware and software in use
- provide consistent security functionality across different hardware and software platforms
- standardise user provisioning and access control to internal and external business applications
- integrate security controls at application, computer and network levels
- apply consistent cryptographic techniques
- implement common naming conventions
- segregate environments with diverse security requirements and trust levels
- control the flow of information between different environments

2.1.8 The security architecture **must** be applied to:

- development or acquisition of secure and resilient business applications or services
- development or acquisition and deployment of a secure and resilient technical infrastructure
- review and refresh of existing business applications, services and technical infrastructure
- major IT projects involving system, service and platform transition and transformation activities
- deployment of information security products, technologies and services

2.1.9 The controls framework should ensure that security architecture documentation and related artefacts are classified as Restricted and managed accordingly.

2.1.10 A formal documented process **must** be established for governing the implementation of security architecture within West Midlands Police. The process should assess the security controls framework implementation and management practices, using metrics, project oversight, as well as periodic, focused reviews to provide holistic assurance.

2.1.11 A formal documented process **must** be established for periodically reviewing and updating the security architecture to ensure it remains current and relevant.

2.2 Identity and Access Management

2.2.1 The controls framework should ensure Identity and Access Management (IAM) arrangements:

- are based on an assessment of risk to business applications, supporting infrastructure and sensitive information
- meet legal, regulatory and contractual requirements
- are established for consistent organisation-wide user provisioning and access control
- are incorporated into an enterprise-wide solution and applied to development or acquisition of new business applications
- include a method for validating user identities prior to enabling user accounts
- minimise the number of sign-on's required by users to access IT systems and resources
- provide a consistent set of methods for user identification and authentication, sign-on process, authorisation and administration of user access privileges
- enable access rights to be quickly and easily granted, changed or removed for a large number of users using role based access control or other robust equivalent
- enable management of user access privileges to be performed by relevant system owners rather than by system administrators and IT Staff
- are periodically reviewed and updated to ensure their adequacy and operating effectiveness

2.2.2 IAM arrangements should improve the integrity of user information by:

- making this information readily available for users to validate and update in a controlled manner
- maintaining a limited number of identity stores
- using an automated provisioning system
- using a centralised change management system

2.2.3 Where deployed, Federated IAM (FIAM) arrangements should:

- build upon existing Identity and Access Management arrangements
- be subject to separate governance, planning, risk assessment, review and monitoring
- meet architectural requirements
- employ only approved FIAM protocols, services and connection software

2.2.4 A formal documented process and control standards should be established for managing FIAM connections that cover:

- gaining approval for each FIAM connection, by both the identity provider and service provider that includes connection protocols, software and configuration parameters to be used
- designing each FIAM connection including determining how user access rights are managed, agreeing the structure of identifiers and attributes for users and the approach for provisioning user accounts, and updating contractual requirements

- Implementing each FIAM connection including configuring agreed settings in FIAM software, updating IAM system and administration processes to support the FIAM connection, modifying the corresponding business applications to support the FIAM connection and subjecting the FIAM connection to standard IT management processes
- operating each FIAM connection including user account and privilege management, monitoring access to business applications, reporting user activity in FIAM business applications and monitoring the connection for actual or suspected security incidents
- regularly reviewing each FIAM connection, for planned and unplanned changes to connections

2.3 Critical Infrastructure

2.3.1 A risk assessment **must** be conducted to identify and evaluate potential security risks to critical infrastructure components, services and supporting information systems. The controls framework, informed by the results of the risk assessment should determine the nature, degree and depth of security controls required to protect them against a broad range of security threats.

2.3.2 Formal documented standards and procedures should be in place for the protection of critical infrastructure components and services that cover:

- identifying the organisation's critical infrastructure
- determining the information systems that support or enable the critical infrastructure
- establishing a framework of controls to help secure the critical infrastructure
- monitoring the security controls that protect the critical infrastructure
- performing periodic threat and vulnerability assessments of information systems that support or enable critical infrastructure

2.3.3 A formal documented process should be established to identify and document critical infrastructure components, services and supporting information systems in an inventory. The inventory should record:

- types and classification of information processed by each critical information system
- owner(s) of each critical information system
- location and function of each critical information system
- level of criticality of each information system
- interrelationship (and any dependencies) with other information system

2.3.4 The controls framework should include a range of security controls to protect information systems supporting critical infrastructure that include:

- monitoring and tracking critical infrastructure components and dependencies on information systems
- sharing information about threats and vulnerabilities with selected internal Staff and appropriate external parties
- regularly reviewing critical infrastructure and supporting information systems to confirm criticality
- storing spares onsite for critical or obtaining such spares at short notice
- decommissioning aging or costly information systems and replacing them with up-to-date and cost effective technology

2.3.5 Security controls applied to information systems that support or enable critical infrastructure should incorporate security architecture principles.

2.4 Cryptographic Solutions and Key Management

2.4.1 A risk assessment **must** be conducted to determine the nature and degree of cryptographic protection required, consistent with the nature and sensitivity of information and that takes into account the legal aspects of using cryptography.

2.4.2 The controls framework **must** implement cryptographic protection to:

- protect the confidentiality of sensitive information or information in accordance with legal and regulatory requirements
- protect the confidentiality and integrity of control mechanisms such as passwords and keys that underpin cryptographic protection
- determine if sensitive information has been altered using mechanisms such as hash functions or digital signatures
- provide strong authentication for users of critical business applications and systems using mechanisms such as digital certificates and smartcards
- enable the identity of the originator of critical and sensitive business transactions or communications to be proven using mechanisms such as digital signatures

2.4.3 Formal documented standards and procedures **must** be in place for implementation of cryptographic protection that covers:

- definition of circumstances where cryptographic protection is required to be used
- approving use of and maintaining an inventory of authorised cryptographic solutions
- responsibilities for defining, managing, operating and maintaining cryptographic solutions
- selection of approved and publicly proven cryptographic protocols and services with a long term protection outlook
- suitability of cryptographic protocols and mechanisms employed including algorithms for symmetric and asymmetric encryption, hashing, signing, key agreement and other cryptographic functions, key lengths, cryptographic strength and protection outlook
- precluding the development or use of proprietary cryptographic protocols and solutions
- addressing obsolete or insecure cryptographic protection mechanisms within business applications and technical infrastructure components
- laws and regulations relating to restrictions on the export and use of cryptographic solutions

2.4.4 The controls framework **must** implement the following minimum requirements for cryptographic protection of sensitive information:

Information Classification	Cryptographic Protection (Encryption/Hashing)		
	Storage*	Processing	Transmission
Strictly Confidential	Must	Must	Must
Restricted	Should	Should	Must
Not Sensitive	May	May	May

2.4.5 The controls framework **must** ensure that passwords or encryption keys associated with sensitive information are classified as Strictly Confidential and managed accordingly.

2.4.6 Formal documented standards and procedures **must** be established for managing cryptographic keys. The process should cover:

- generation of cryptographic keys using approved key lengths
- centralised distribution, activation, storage, recovery, replacement or update of cryptographic keys
- timely revocation or deactivation of cryptographic keys in response to specific events such as key compromise or changes to key ownership
- recovery of cryptographic keys that are lost, corrupted or have expired
- management of compromised cryptographic keys
- backup and archiving of cryptographic keys and the maintenance of key history
- allocation of defined activation and deactivation dates
- restriction of access to cryptographic keys to authorised individuals
- sharing of cryptographic keys using split key generation or equivalent required for protecting sensitive information and critical systems
- internal investigations or legal requests for access to encryption keys in the event encrypted information is needed in unencrypted form as evidence

2.4.7 Awareness programmes should ensure that Staff are aware of the standard operating procedures for the use of approved cryptographic solutions and consistently comply with the requirements for processing and handling sensitive data.

2.4.8 A formal documented process should be established for regularly reviewing the adequacy and effectiveness of cryptographic protocols and mechanisms within business applications and supporting infrastructure components, to ensure they continue to provide the required level of protection in line with the level of risk and relevant legal, regulatory and contractual requirements.

2.5 Public Key Infrastructure

2.5.1 Formal documented standards and procedures should be in place for public key infrastructure that covers:

- establishment of a root Certification Authority (CA) and one or more subsidiary CAs (sub-CAs) for managing digital certificates
- methods of protecting important internal Certification Authorities (and related sub-CAs)
- integration of the public key infrastructure with business applications and technical infrastructure that will use it
- establishment of one or more Registration Authorities (RAs)
- actions to be taken in the event of loss or compromise of the public key infrastructure

2.5.2 The controls framework **must** ensure that internal Certification Authorities are protected by:

- restricting access to a limited number of authorised individuals using strict access control mechanisms and strong authentication
- issuing separate cryptographic key pairs for encrypting and decrypting information, and producing and validating digital signatures

- formal documented and tested contingency plans to deal with loss of the public key infrastructure or a potential security incident that results in a compromise of the public key infrastructure

2.5.3 The private keys of internal Certification Authorities should be protected by:

- storing them on approved hardware subject to strong logical and physical controls
- sharing them across two or more authorised individuals (referred to as secret splitting or key sharing) to avoid misuse of the CA and related sub-CAs

2.5.4 The public key infrastructure should be integrated with the organisation's user identity store to ensure digital certificates are available to all authorised users and applications.

2.5.5 The public key infrastructure **must** use a consistent, trusted date and time source to ensure the Certification Authority provides accurate timestamps.

2.5.6 The public key infrastructure should be supported by Certification Practice Statement and Certificate Policies for each type of digital certificate issued by the Certification Authority.

2.5.7 A Registration Authority (RA) should be established to:

- verify the identity of individuals requiring the use of the PKI
- issue authentication hardware relating to the PKI
- oversee cryptographic key generation
- generate and submit requests for the issuance of PKI certificates

2.5.8 Awareness programmes should ensure that relevant Staff understand the purpose and function of PKI components and aware of their security responsibilities to ensure safe handling and usage.

2.6 Information Leakage Protection

2.6.1 The controls framework **must** employ information leakage protection mechanisms for systems, networks and endpoints that store, process or transmit sensitive information commensurate with the level of risk associated with them.

2.6.2 Formal documented standards and procedures should be in place for information leakage protection that covers:

- registering types of sensitive information to be monitored
- methods of discovering sensitive information at risk of unauthorised disclosure
- techniques for detecting sensitive information when disclosed during processing or transmission
- methods of blocking user actions or network transmissions that expose sensitive information
- management of information leakage protection software
- monitoring, alerting and reporting of security incidents

2.6.3 The controls framework should ensure that information leakage protection mechanisms are:

- pre-registered with specific types of sensitive information that need to be protected from unauthorised disclosure
- capable of taking into account the context of information such as time, sender, receiver, subject
- heading, message content and file attachments before identifying information as being at risk of disclosure or detected as being disclosed to unauthorised individuals
- regularly updated and optimised to ensure their configuration reflects the sensitive information that needs to be protected
- managed centrally and reviewed to reduce false positives and false negatives
- configured to raise an alert when unauthorised disclosure activity is detected
- configured to aggregate the results of discovery and detection to determine the potential business impact over a period of time

2.6.4 Information leakage protection mechanisms **must** be configured to perform specific enforcement actions to protect sensitive information at risk of disclosure or is being disclosed to unauthorised individuals. These actions should include:

- removing sensitive information from inadequately controlled hosts or network locations
- warning users and notifying business managers of potential unauthorised disclosure of pre-registered sensitive information
- blocking unauthorised user actions
- preventing the transmission of pre-registered sensitive information
- quarantining information for further analysis

2.6.5 The Information Leakage Protection system should be subject to standard security management practices as outlined in the System Management Policy.

2.6.6 Actual or suspected incidents of information leakage **must** be reported and handled in accordance with the requirements of the Information Security Incident Management Policy.

2.7 Non Conformance and Exceptions

2.7.1 Non-conformance to this policy must be reported to the relevant team. Information Security, Risk and Privacy must approve, track and report all exceptions to this policy in accordance with a formal documented process. The process should include a method for escalating significant exceptions that may breach a documented level of business risk tolerance, to appropriate boards and committees in accordance with established governance procedures for review and mitigation or formal risk acceptance

3. UNDERPINNING POLICIES AND PROCEDURES

3.1 To support the overarching IA Risk Management policy the following policies will be maintained by the force –

1. Physical Security policy;
2. Force Information Security Policy;
3. Systems Management Policy;
4. Information Security Incident Management Policy;
5. Information Services Risk Register;
6. West Midlands Police Risk Appetite Statement;

4. EQUALITY IMPACT ASSESSMENT (EQIA).

4.1 The policy has been reviewed and drafted against all protected characteristics in accordance with the Public Sector Equality Duty embodied in the Equality Act 2010. The policy has therefore been Equality Impact Assessed to show how West Midlands Police has evidenced 'due regard' to the need to:

- Eliminate discrimination, harassment, and victimisation.
- Advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it.
- Foster good relations between persons who share a relevant protected characteristic and persons who do not share it.

Supporting documentation in the form of an EQIA has been completed and is available for viewing in conjunction with this policy.

5. HUMAN RIGHTS.

5.1 This policy has been implemented and reviewed in accordance with the European Convention and principles provided by the Human Rights Act 1998. The application of this policy has no differential impact on any of the articles within the Act. However, failure as to its implementation would impact on the core duties and values of West Midlands Police (and its partners), to uphold the law and serve/protect all members of its community (and beyond) from harm.

6. FREEDOM OF INFORMATION (FOI).

6.1 Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 0.2 of this policy has been GPMS marked as Not Protectively Marked.

6.2 Public disclosure <u>does not</u> automatically apply to supporting force policies, directives and associated guidance documents, and in all cases the necessary advice should be sought prior to disclosure to any one of these associated documents.

Which exemptions apply and to which section of the document?	Whole document	Section number
N/A		

7. TRAINING.

7.1 There is no specific training for West Midlands Police personnel; however those individuals with a specific involvement in technical security infrastructure management will have the relevant training courses detailed within their job specifications.

8. PROMOTION / DISTRIBUTION & MARKETING.

8.1 The following methods will be adopted to ensure full knowledge of the Policy:

- Newsbeat
- Intranet
- Posters
- Policy Portal

8.2 No uncontrolled printed versions of this document are to be made without the authorisation of the document owner.

9. REVIEW.

9.1 The policy business owner – Head of Information Management – maintains outright ownership of the policy and any other associated documents and in-turn delegate responsibility to the department/unit responsible for its continued monitoring.

9.2 The policy should be considered a 'living document' and subject to regular review to reflect upon any Force, Home Office/ACPO, legislative changes, good practice (learning the lessons) both locally and nationally, etc.

9.3 A formal review of the policy document, including that of any other potential impacts i.e. EQIA, will be conducted annually as indicated on the first page.

9.4 Any amendments to the policy will be conducted and evidenced through the Force Policy Co-ordinator and set out within the version control template.

9.5 Feedback is always welcomed by the author/owner and/or Force Policy Co-ordinator as to the content and layout of the policy document and any potential improvements.

CHIEF CONSTABLE

10. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
0.1	24 Dec 14	Initial Draft	Tom King/Stephen Laishley
0.2	14 Jan 15	Amended Draft	Tom King/Stephen Laishley
0.2	22 Jan 15	Amended Formatting	56408 Couchman
0.2	20/03/2015	Policy approved by CC – now live. Added policy ref & sig	56408 Couchman