WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**System Management**
POLICY REFERENCE NO:	**Inf/25**

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 Jan 15**
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 ISO 27001:20013 – 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 depend on supporting technical infrastructure to deliver a secure and reliable service, to meet internal and external stakeholder requirements. A robust policy is required to protect business information systems from control weaknesses in infrastructure components

2. SYSTEM MANAGEMENT POLICY

2.1 Technical Infrastructure Installations

2.1.1 A risk assessment must be conducted to identify and evaluate potential security risks with technical infrastructure installations, consistent with the criticality of the business applications and resources they support. The controls framework, informed by the results of the risk assessment should determine the degree and depth of security controls required for protecting these installations.

2.1.2 An inventory of all technical infrastructure installations must be maintained, kept current and periodically reviewed. The inventory should capture the following:

- Infrastructure Component Type, Function and Owner
- Component Nature (Physical/Virtual) and Criticality
- Environment and Hosting Information
- Key Management and Support Contact(s)
- Applications and Infrastructure Components Supported
- Platform information and Key interfaces
- Connection Methods and Protocols
- Description of Security Controls
- History of Security Incidents and Breaches
- Known Flaws and Vulnerabilities and their Severity Levels
- Remediation Plans and Status

2.1.3 Formal documented standards should be in place defining baseline control requirements for technical infrastructure installations in line with the infrastructure security architecture.

2.1.4 Technical infrastructure installation designs should:

- consider, security requirements and security architecture principles
- maintain compatibility with existing technical infrastructure installations
- address emerging requirements and foreseeable developments in the use of IT within the organisation

2.1.5 Technical infrastructure installations should:

- be managed from a central point
- minimise the requirement for manual intervention
- be set up to support remote configuration and automatic monitoring against pre-defined thresholds
- provide a secure means of access to administer infrastructure components

2.1.6 Technical infrastructure installations should be designed to incorporate security architecture principles through:

- building security into design of installations (security by design)
- using multiple layers of different types of protection (defence in depth)
- granting users the minimum level of access required (least privilege)
- incorporating a comprehensive set of technical standards
- supporting consistent naming conventions
- minimising single points of failure
- providing systems that fail securely

2.1.7 Technical infrastructure installations should have:

- sufficient capacity to cope with peak workloads
- expansion and upgrade capabilities to cope with projected demand
- control and monitoring capabilities to provide management reports

2.1.8 Information systems should be designed to:

- include malware protection on servers
- be built from pre-determined server images or standard builds
- reduce sign on requirements for authorised users to access multiple systems and platforms
- be administered from a central point

2.1.9 Networks should be designed to:

- incorporate use of security domains to segregate systems with specific security requirements
- employ firewalls that are configured to prevent them being by-passed
- isolate particular types of network traffic using dedicated networks to prevent impact on other network traffic
- prioritise network traffic to reduce latency
- restrict the number of entry points into networks
- validate entitlement and security posture of devices connecting to the network before granting them access to resources

2.1.10 The controls framework should ensure technical infrastructure components are protected by:

- segregating critical applications from all other applications and information, in agreement with system owners
- storing source code (or equivalent) in a secure location, away from the live environment and restricting access to authorised staff
- segregating storage of software and information into different storage locations
- permitting only execute access to executable software

2.1.11 Production environments should be segregated from activities undertaken within development, testing and user acceptance environments.

2.1.12 A formal documented process must be established for regularly validating the security posture of technical infrastructure installations. The process should cover ongoing operational monitoring of security controls and management practices using metrics, as well as periodic, focused audits and independent vulnerability reviews to provide holistic assurance.

2.2 Server Configuration

2.2.1 Formal documented standards and procedures should be in place for configuring servers.

2.2.2 Server firmware configuration should provide secure pre-configured BIOS settings and restrict access to the BIOS functions to authorised administrators.

2.2.3 Servers should be configured to disable or restrict:

- non-essential or redundant services and functions
- communication services, management services and protocols that are inherently insecure
- powerful system management tools and utilities
- sensitive scripts, run commands or command processors
- direct access to generic user accounts with administrative privileges

2.2.4 The controls framework should ensure access to powerful system utilities and configuration parameters is restricted to trusted staff for specific purposes and subject to authorisation and monitoring.

2.2.5 The controls framework should ensure that servers are configured to prevent unauthorised access by:

- disabling unnecessary or insecure user accounts (i.e. Guest accounts)
- changing insecure or default security related parameters provided by suppliers
- implementing time out and clear screen facilities after a set period of inactivity

2.2.6 The controls framework should define and enforce standard security management practices to protect servers that include:

- restricting physical and logical access to authorised staff
- keeping them up to date through approved change and patch management processes
- deploying malware protection software
- applying a set of approved management tools for maintenance, support and backup
- monitoring of servers to effectively detect and respond to adverse events
- reviewing them on a regular basis to verify configuration settings, evaluate security controls and assess activities performed on the server through server log reviews
- subject them to periodic independent security assessments and vulnerability reviews

2.3 Virtual Servers

2.3.1 Formal documented standards and procedures should be in place for configuring virtual servers that include protection of physical servers, hypervisors and virtual servers.

2.3.2 The controls framework should ensure physical servers used to host virtual servers are protected by:

- locating them in physically secure environments
- restricting physical and logical access to authorised staff
- providing access only when access is needed
- preventing unmanaged or ad-hoc deployment
- avoiding resource overload

2.3.3 Hypervisors should be configured to:

- segregate virtual servers consistent with the sensitivity of information they process and associated risks
- logically separate each virtual server to prevent information leakage between discrete environments and virtual components
- restrict access to a limited number of hypervisor administrators
- segregate the roles of hypervisor administrators
- separate administrative responsibilities of hypervisor administrators from virtual server from virtual server administrators
- secure communication between virtual servers

2.3.4 The controls framework should protect virtual servers by subjecting hypervisors to standard security management practices that include:

- enforcing a change management processes to ensure the hypervisor remains up to date
- monitoring, reporting and reviewing administrative activities
- restricting access to the virtual server management console
- monitoring network traffic between different virtual servers and between virtual and physical servers to detect malicious or unusual activity

2.3.5 The controls framework should define and enforce to standard security management practices and network-based security controls to protect virtual servers.

2.4 Network Storage Systems

2.4.1 Formal documented standards and procedures should be in place for network storage systems such as storage area networks and network attached storage that cover:

- design and configuration of network storage systems
- protection of network storage management consoles and administration interfaces
- security of information stored on network storage systems
- security controls specific to network storage system components

2.4.2 Network storage systems should be designed and configured to:

- use standardised components
- be managed from a central point using a minimum number of management consoles
- restrict access to particular areas of storage
- enable authorised users to access multiple servers / resources via a single sign on

2.4.3 The controls framework should define and enforce standard security management practices to protect network storage systems.

2.4.4 Network storage system components should be protected by:

- restricting administrative access to a limited number of authorised staff
- using access controls that support individual accountability and protect against unauthorised access
- restricting management functions including SAN management consoles and NAS device utilities
- restricting access to NAS devices to authorised network devices and enabling file locking
- using cryptographically secure protocols and services for access to management consoles and running terminal sessions

2.5 Backup

2.5.1 Essential information and software **must** be backed up and stored at a secondary location for the period specified by the business in the record retention schedule.

2.5.2 Formal documented standards and procedures should be established for performing backups, including:

- types of information to be backed up
- back up schedules and cycles
- methods for performing back up including validation, labelling and storage

2.5.3 Backups should be:

- performed using specially designed backup management software
- documented in a log which contains details of the data backed up, the date and time of the back-up, the media used and its physical location
- verified to ensure the backed up information can be restored successfully
- related to control points in live processes
- reconciled to the live version when copies are made
- clearly and accurately labelled
- protected from accidental overwriting
- subject to an equivalent level of protection as live information
- performed within critical timescales

2.5.4 Backup arrangements should enable software and information to be restored within critical timescales using an appropriate back-up solution.

2.5.5 Backups should be protected against loss, damage and unauthorised access by:

- storing back up media in accordance with manufacturer specifications
- locating on-site backups in locked, computer media fireproof safes
- locating off-site backup copies in secure facilities with secure transit arrangements
- restricting access to backups to authorised staff

2.5.6 All backup media containing Strictly Confidential or Restricted information including customer or personal data **must** be encrypted. Backup media holding data which is classified as Non Sensitive should also be encrypted.

2.6 Change Management

2.6.1 A formal change management process **must** be in place to manage and document all types of change to business applications and supporting technical infrastructure.

2.6.2 The controls framework **must** define adequate controls within the change management process to reduce adverse impacts, prior to applying changes to the production environment that ensure:

- change requests are documented
- changes are accepted and authorised by pre-approved individuals
- potential business and technical impacts of change are assessed
- changes are tested to help confirm the expected results
- changes are reviewed to ensure they do not compromise security controls
- back-out positions are established to facilitate recovery from failed changes or unexpected results

2.6.3 Changes to business applications and technical infrastructure should be performed by skilled individuals who are capable of making the changes correctly and securely, supervised by an IT specialist and signed off by an appropriate business representative.

2.6.4 Once changes have been applied to the live environment, processes should ensure that:

- version control is maintained
- a complete and accurate record of the change is maintained
- details of changes are communicated to relevant individuals
- checks are performed to confirm that only intended changes have been made
- business application and technical infrastructure documentation is updated
- classification of information for information assets associated with the change is reviewed

2.7 Service Level Agreements

2.7.1 Technical infrastructure services that support critical business applications and processes should be defined in documented service agreements.

2.7.2 Service agreements should specify:

- ownership and accountability for provision of technical infrastructure services
- ownership and accountability for delivery of the required service
- the level of criticality of the service
- dates/times when the service is required
- the capacity requirements of technical infrastructure components
- maximum permissible down time
- critical timescales
- penalties to be imposed when the service provider fails to deliver the pre-agreed service levels

2.7.3 The controls framework must ensure a baseline set of control requirements are defined for inclusion within service agreements. These should include the following:

- access control restrictions
- authentication methods
- restrictions on methods and allowable services
- segregating technical infrastructure components
- segregation of duties and facilities
- protection against malware
- protecting sensitive information in transit
- installation and maintenance of hardware and software
- change and patch management
- information security incident management
- detecting and recovering from service interruptions
- ensuring business and system continuity of service
- restricting the use of services to those provided by approved suppliers
- obtain assurance of the security controls applied by the service provider
- provide a single point of contact with authority and competence to handle security issues

2.7.4 Service agreements should be:

- assessed by an information security specialist
- signed off by the business process owner and the service provider
- regularly reviewed to ensure service targets and security requirements are being met

2.8 Non Conformance and Exceptions

2.8.1 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. Information 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 does not 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 systems 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.

Ch S

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 Version	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