WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Access Management**
POLICY REFERENCE NO:	**Inf/15**

Executive Summary.

In accordance with the HMG SPF West Midlands Police will ensure that appropriate security measures are implemented and managed to control access to information assets and reduce the risks associated with unauthorised system access and information disclosure.

***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 0.5**	**26/03/2014**
Business Area Owner	**Information Management Services**	
Department Responsible	**Information Management**	
Policy Contact	**Kate Jeffries – Head of Information Management**	
Policy Author	**Paul Richards – Information Security Officer**	
Approved By	**DCC Thompson**	
Policy Initial Implementation Date	**26/11/2014**	
Review Date	**26/11/2016**	
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 EN ISO27001 – 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.

This policy defines the guiding principles and requirements that apply to all applications and supporting infrastructure components that are within the direct control of West Midlands Police. These requirements should also be considered for inclusion within external supplier contracts, where relevant to the nature, criticality and sensitivity of services and associated risks.

2. ACCESS MANAGEMENT POLICY

A risk assessment must be conducted to identify and evaluate potential security risks involving access to sensitive applications and supporting infrastructure components, consistent with the nature and sensitivity of information processed by them. The controls framework, informed by the results of the risk assessment should determine the nature, degree and depth of access control mechanisms required to protect against unauthorised access and maintain individual accountability.

Application and supporting infrastructure inventories should capture access control arrangements established to safeguard their operational integrity and protect information stored, processed or transmitted by them from unauthorised access, modification or destruction.

Access control arrangements should be supported by formal documented standards and procedures which incorporate:

- Information Security Policy requirements
- Information Asset Classifications
- Agreements with Information Asset Owners
- Requirements set by owners
- Legal, Regulatory and Contractual Obligations
- The need to achieve individual accountability, apply additional control for users with privileged access or special capabilities and provide segregation of duties

Access control arrangements should cover access by all users and to all types of applications, business information and supporting infrastructure components.

Access control arrangements must be determined by the requirements; security classification of information processed and related risk exposures. This should include:

- limiting access in line with access requirements set by Information Asset owners
- approval of access privileges by business managers before they are granted
- restricting access to system capabilities by providing menus or access profiles to enable access to the capabilities required to fulfil a defined role
- identifying the location of computing devices in use and their security posture
- Supplementing password based authentication with stronger authentication where necessary, including long term third party external connections.
- minimising the need for privileged access or special capabilities

Before access privileges come into effect:

- authorisations should be checked to confirm access privileges are appropriate
- details of users should be recorded, including their true identity, associated identifier (e.g. User ID) and access privileges to be granted
- Users should be advised of, and be required to confirm understanding of their access privileges and associated conditions of use.
- User will have completed the “Lawful Handling of Information” training package (or subsequent NCALT package)

The controls framework must ensure sufficient protection for generic accounts, default user accounts and groups that includes documented requirements for approval, management authorisation, periodic re-certification, security event logging and activity monitoring.

The controls framework must provide enhanced controls for user accounts with privileged access that includes:

- specifying the purpose of privileged access
- restricting the use of privileged access to specific circumstances
- individual approval for the use of privileged access
- requiring sign-on using identification codes or tokens that differ from those used in normal circumstances before undertaking privileged activities
- clear audit trail and review of privileged access activity
- change of privileged passwords following staff changes such as resignation, dismissal, role change and functional moves

The controls framework should provide enhanced controls for user accounts with special capabilities that include:

- specifying the purpose of special capabilities
- restricting the access to functions with special capabilities
- providing additional approval and review of access to functions with special capabilities
- ensuring there is appropriate segregation of duty, dual control or logging of changes made through functions with special capability

Formal documented standards should be in place for timely termination of access privileges which ensures that:

- authentication details and access rights are revoked promptly and then subsequently deleted on all systems to which the user had access
- components dedicated to providing access, such as tokens, modems or virtual private networks (VPNs) are disabled or removed and returned
- access provided for third parties is disabled on completion of the services being performed

The controls framework should provide controls for inactive accounts so these are identified on a regular basis, reviewed, reasons for 30 days or more inactivity investigated and accounts de-activated or disabled where appropriate.

Access control arrangements must be formally reviewed on a periodic basis and upgraded in response to new threats, capabilities, business requirements or experience of incidents related to access management.

User Authorisation
The process for authorising users must:

- be formally documented, approved and applied to all users requesting access
- associate access privileges with unique user identifiers
- assign access based on the principle of least privilege and requirements of current role
- ensure that redundant user identifiers are not re-issued for use

All user access authorisation records should be logged and retained in line with the requirements of the WMP Asset Management Policy, but for not less than 24 months from the latest change.

A formal documented process for periodic review of authorised users must be established. The process should:

- ensure that access privileges remain appropriate for the role being performed
- check that redundant authorisations are deleted for staff who have changed role or left the organisation
- define responsibilities and schedule for reviews in line with the results of the risk assessment for the resource
- Maintain evidence of the review defined period in line with the risk assessment for the resource, but not for less than 24 months.

2.2 Access Control Mechanisms

All staff **must** be uniquely identified and positively authenticated before they gain access to WMP applications, business information and supporting infrastructure.

Access to WMP applications, business information and supporting infrastructure should be restricted to authorised individuals by use of access control mechanisms such as passwords, passphrases, tokens or biometrics.

Access control mechanism functionality should be subject to an evaluation to determine the degree to which they will meet access requirements. The evaluation should include:

- the strength of existing controls that influence the suitability of access control mechanisms such as identity and access management, physical security or system hardening
- special factors that may influence the choice of access control mechanism such as vendor capabilities, integration with physical security or specific regulatory requirements

Access control mechanisms should be provided using approved hardware and software such as physical tokens and biometric devices.

2.3 Access Control Mechanisms - Passwords

Awareness programmes should ensure staff are aware of their responsibilities to:

- keep passwords confidential
- promptly report an incident if passwords have been or are suspected of being compromised
- change passwords that may have been compromised
- not perform activities with access credentials belonging to others
- encourage users to construct strong passwords or passphrases

Formal documented standards and procedures should be in place for access control mechanisms based on passwords, consistent with the sensitivity of information and results of a risk assessment. These should:

- ensure identifiers are unique
- require users to choose a new password on first logon
- force new passwords to be verified before the change is accepted
- ensure users set their own passwords
- automate the process of password recovery using self-service
- restrict the re-use of passwords so they cannot be used again within a set period or number of changes
- ensure passwords are not displayed or are obfuscated on screen and in printed materials
- require secure storage and transfer of passwords

Access control mechanisms based on passwords should provide automated controls for password parameters that ensure passwords comply with specified WMP requirements as per Password management standard

A formal documented process should be defined for issuing new and changed passwords, including password resets that:

- ensures that passwords are not transmitted in clear text or communicated insecurely
- directly involves the person to whom the password uniquely applies
- verifies the identity of the user
- required temporary passwords to be changed on first use
- where possible, notifies users when passwords are due to expire shortly

Passphrases may be used where strong passphrase composition rules are supported in access control mechanisms for business applications and supporting infrastructure components.

2.4 Access Control Mechanisms - Token

A formal documented process should be defined for registering new token users and issuing tokens that:

- ensures that passwords required for tokens are not transmitted in clear text
- directly involves the person to whom the token uniquely applies
- verifies the identity of the person to whom the token uniquely applies
- ensures access to the token's PIN/Password database is only available to authorised users
- ensures inactive tokens are identified and deactivated or disabled after a defined period of inactivity

Awareness programmes should advise staff that use token authentication to:

- keep passwords and PINs for access to tokens confidential
- protect tokens against loss, theft and misuse
- promptly report an incident if tokens, passwords or PINs have been or are suspected of being compromised

The controls framework should support a secure process to enable authentication when token authentication fails.

Where passwords are used to supplement token authentication, they should conform to the requirements outlined in the Access Control Mechanisms – Passwords section of this policy.

2.5 Access Control Mechanisms – Biometric

A formal documented process should be defined for staff biometric enrolment that:

- directly involves the person to whom the biometric uniquely applies
- verifies the identity of the person to whom the biometric uniquely applies
- ensures that biometric information is only made available to authorised individuals and retained in accordance with the WMP Asset Management Policy.

Awareness programmes should advise staff that use biometric authentication to:

- keep passwords for access to biometric equipment confidential
- protect equipment used for biometric authentication against loss, theft and misuse
- report an incident if biometric equipment is or is suspected of being compromised

The controls framework should ensure that biometric authentication is configured to:

- support a secure process to enable user authentication when biometric authentication fails
- reduce the likelihood of errors through reduction of false positives and false negatives

Where passwords are used to supplement biometric authentication, they should conform to the requirements outlined in the Access Control Mechanisms – Passwords section of this policy.

2.6 Sign-On Process

The controls framework must define and enforce a secure sign-on process for gaining access to WMP information, applications and supporting infrastructure components, based on a formal risk assessment.

The controls framework should ensure that sign-on mechanisms are configured to:

- enable individual users to be uniquely identified
- prevent the sign-on process from being bypassed, disabled or changed without authorisation
- validate sign-on information only after it has all been entered
- limit the number of consecutive unsuccessful sign-on attempts which are permitted
- de-activate signed on sessions after a defined period of inactivity
- be invoked automatically after interruption following a session disconnection or termination

The controls framework should ensure that sign-on mechanisms are configured to:

- not display any identifying details until after sign-on is completed successfully
- visibly warn that only authorised users are permitted access
- not provide help or informational error messages that would aid an unauthorised user
- record all successful and unsuccessful sign-on attempts
- advise users (on successful sign-on) of the date and time of their last successful sign-on and all unsuccessful sign-on attempts since their most recent successful sign-on

Sign-on mechanisms should be configured so that they do not:

- reveal authentication details as clear text in automated routines such as scripts, macros, cache memory, batch services and started tasks
- store or transmit authentication credentials without adequate cryptographic protection

2.7 Non Conformance and Exceptions

Non conformance to this policy must be reported to the Information Security Officer who must approve, track and report all exceptions to this policy. 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

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

1. Physical security policy;
2. Vetting\personnel policy;
3. Force Information Security Policy;
4. Information Management Policy;
5. Password management standard;
6. Information Security Incident Management Policy;
7. Clear Desk & Screen Policy;
8. Information Services Risk Register;
9. West Midlands Police Risk Appetite Statement;

4. EQUALITY IMPACT ASSESSMENT (EQIA).

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.

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).

Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 0.5 of this policy has been GPMS marked as Not Protectively Marked.

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		

9. TRAINING.

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

10. PROMOTION / DISTRIBUTION & MARKETING.

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

- Newsbeat
- Intranet
- Posters
- Policy Portal

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

11. REVIEW.

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.

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.

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.

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

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

12. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
0.1	21st March 2014	Initial Draft	Del Brazil, Advent-IM
0.2	21st July 2014	Amended Draft	Paul Richards
0.3	15th October 2014	Amended Draft	Stephen Laishley
0.4	16th October 2014	Formatted Draft	56408 Couchman
0.4	27/11/2014	Policy approved & implemented	56408 Couchman
0.5	26th March 2015	"Password Management Policy" changed to "Password Management Standard"	Stephen Laishley