WEST MIDLANDS POLICE

Force Policy Document

POLICY TITLE:	Compliance, Audit Assurance and Accreditation
POLICY REFERENCE NO:	Inf/17

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.

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

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 – Information Security Officer	
Approved By	DCC Thompson	
Policy Initial Implementation Date	10/02/2015	
Review Date	10/02/2017	
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. This is the Compliance, Audit Assurance and Accreditation policy which sets out the expectations of West Midlands Police (WMP) in relation to accreditation and ensuring on-going compliance. It will be agreed between the Senior Information Risk Owner, the force Accreditor, the Head of Change and the Head of ICT. Audit & Accreditation does not purely cover ICT systems, this assurance will cover all supporting systems processes and procedures across the force which supports or governs a requirement or control which is relevant to the information, physical or logical requirement for the force accreditation.

2. COMPLIANCE, AUDIT ASSURANCE AND ACCREDITATION POLICY

Accreditation Principles

2.1. The WMP RESTRICTED infrastructure will be accredited on an annual, risk managed basis unless significant change is introduced which makes interim accreditation necessary. All changes will include Information security to ensure that changes do not impact the current accreditation documentation set.

2.2. The approach to accreditation will be flexible, balanced and proportionate to the specific requirements of any change, supporting the business whilst not compromising the accreditation of the environment.

2.3. All systems require review and accreditation when they are introduced, changes to current systems must follow the relevant change control procedure and supporting documentation must be updated to show the relevant changes. All new or changed environments are subject to a vulnerability assessment to ensure that there is no impact to the accredited environment. The level of accreditation required will depend on the solution and the data being processed or managed.

2.4. Changes to systems may generate a re-accreditation process but at the very least will require documentation to be updated to reflect the changes made. This Information Security Team will be the only authority which can determine if a full, partial or no re-accreditation process is required. The full change process is documented separately. Systems that are not changed will be re-accredited on a 3 year cycle.

2.5. Change is not limited to ICT systems and would include processes and procedures e.g. a change in supplier, maintainer or how we handle our assets, such as confidential waste or visitor handling.

2.6. Change can also occur nationally from policy, guidance or from a change in the threat landscape.

2.7. Systems that are due to be retired within 6 months of their re-accreditation date will not be subject to re-accreditation.

2.8. Minor change such as routine maintenance or patching is outside the change process and will not require additional accreditation. Significant upgrades or widening of scope (e.g. extending access from all Ch. Supts to all officers) will require re-accreditation.

2.9. Accreditation will be based on standard issue government guidance. (HMG IA Standards 1 & 2). It will be managed by exception and only when a residual risk score falls outside the tolerance of the Security and Information Risk Advisor (SIRA) will a report be prepared for the Accreditor. In the cases where it exceeds the tolerance of the Accreditor an executive summary will be produced for the SIRO for discussion and final decision.

2.10. The SIRA is responsible for producing and maintaining the accreditation schedule over a three year rolling period.

2.11. The project office will ensure that the SIRA is included in all project work at initiation stage. At that time the on-going level of involvement that will be needed will be discussed and agreed using a triage process.

2.12. Whatever the level of involvement during the project development, the SIRA will be included in discussions prior to transition to BAU.

2.13. The SIRA, IT Security Officer (ITSO) and Accreditor and their associated work are considered as resources that need to be scheduled by the project. The project manager is responsible for ensuring that the time and costs of accreditation work are included in the project plan.

2.14. The Accreditor will update the SIRO on a monthly basis by way of an executive summary of recent accreditation activity.

2.15. The quarterly Strategic Information Management Board (SIMB) will monitor the annual infrastructure accreditation process.

2.16. HMG ICT systems and services must be reviewed annually and those storing, processing and handling PROTECT PERSONAL information must be re-accredited annually.

3. UNDERPINNING POLICIES AND PROCEDURES

3.1. To support the overarching Compliance, Audit Assurance and Accreditation policy the following policies will be maintained by the force –

1. Force Information Security Policy;
2. Information Services Risk Register;
3. 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 0.3 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 Compliance and Audit 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	29 Dec 2014	Initial Draft	Tom King/Stephen Laishley
0.2	14 Jan 2015	Amended Version	Tom King/Stephen Laishley
0.2	10/02/2015	Policy approved – CC signature and Policy Ref No Added	56408 Couchman