WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Information Risk Management Policy**
POLICY REFERENCE NO:	**Inf/18**

Executive Summary.

In accordance with the HMG SPF Risk Management 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 0.2**	**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. Information Assurance (IA) is the confidence that information assets will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.

1.2. Risk management is an iterative process throughout the lifecycle of the information systems (IS), from early planning, through development to in-service and eventually decommissioning and disposal. This will lead to improved IA and avoid costs often associated with late consideration of security requirements.

1.3. This document describes the process by which information assurance (IA) risks will be managed in force including the risk assessment and acceptance processes.

2. RISK APPETITE

2.1 The risk appetite statement is a separate document, reviewed and approved by the SIRO annually. It sets the background against which the force manages its Information risks.

2.2 In line with best practice WMP's risk appetite is set in the context of confidentiality, integrity and availability. There are five categories of risk appetite and the descriptions of the associated behaviours are as follows:

- **Averse (Risk Avoidance)**: Avoidance of risk and uncertainty is a key objective. Exceptional circumstances are required for any acceptance of risk.
- **Minimalist**: Preference for ultra-safe options that have a low degree of inherent risk and only have a potential for limited business benefit.
- **Cautious**: Preference for safe options that have a low degree of residual risk and may only have limited potential for business benefit.
- **Open**: Willing to consider all options and choose the one that is most likely to result in successful delivery minimizing residual risk as far as possible, while also providing an acceptable level of business benefit.
- **Hungry (high risk, high reward):** Eager to realise business benefits and to choose options to achieve this despite greater residual risk.

3. THREE AREAS OF IA RISK MANAGEMENT

Confidentiality – ensuring the information is accessible only to those authorised to have access;

Integrity – safeguarding the accuracy and completeness of information and processing methods - this may include the ability to prove an action or event has taken place, such that it cannot be repudiated later;

Availability – ensuring that authorised users have access to information and associated IS when required.

3.1 Confidentiality, integrity and availability are all equally important. Although integrity and availability have always been key considerations, policy has tended to focus on confidentiality. This process ensures that all three are fully addressed and given equal importance. It recognises that many assets may have little or no requirement for confidentiality but availability and integrity may be vital and also that confidentiality extends beyond government protective markings to privacy and other sensitivities.

4. IA KEY ROLES

4.1. Key roles involved in risk management include –

- Accounting Officer (AO);
- Senior Information Risk Owner (SIRO);
- Information Asset Owners (IAO);
- Security Information Risk Advisor (SIRA);
- IT Security Officer (ITSO); and
- Accreditor (A).

4.2. However it should be understood that IA risk management is everyone's business, hence all members of the force have some responsibility for information risk ownership of the specific IS with which they are associated. Different specific roles may be assigned to ensure effective acceptance of information risk ownership in terms of the governance of IA within the force.

5. RISK ASSESSMENT

5.1 Any individual or group of individuals that wish to commission a change to an existing system or implement a new one will initially discuss this with the appropriate IAO to gain approval in principle. If this change is commissioned through a formal project then this is the responsibility of the assigned project (or programme) manager.

5.2 The IAO will, either personally or through an approved delegate, discuss this change with the SIRA. The SIRA will be responsible for gathering sufficient information to articulate a clear risk assessment of the proposal.

5.3 The risk assessment will be prepared based on the Security Policy Framework, IS1 & 2 which will generate a residual risk score after mitigation. This score will be plotted onto the risk assessment matrix below to ensure that treatment is acceptable and proportionate to the risk appetite.

5.4 Risks will be treated in a reasonable and cost-effective manner and will not be overly mitigated in excess of what is needed to reasonably meet the risk appetite.

5.5 Risk Assessment Matrix -

IMPACT						
	5	C	O	O	H	H
	4	M	C	O	H	H
	3	M	C	O	O	O
	2	A	M	C	C	O
	1	A	A	M	M	C
		1	2	3	4	5
		Likelihood				

A = Risk Averse
M = Minimalist
C = Cautious
O = Open
H = Hungry

6. RISK ACCEPTANCE

6.1 Once residual risk has been assessed it will move into the acceptance process.

6.2 Risk can be accepted by different roles within the force's information assurance structure and the correct level of acceptance will be determined using the risk appetite statement, the residual risk score and the acceptance matrix below.

6.3 Risk Acceptance Matrix -

Residual Risk Level						
	16-25	SIRO	SIRO	SIRO	SIRO	SIRO
	9-15	SIRO	SIRO	SIRO	A	A
	5-8	SIRO	SIRO	SIRO	A	IAO
	3-4	SIRO	A	A	IAO	IAO
	1-2	SIRO	A	IAO	IAO	IAO
		Risk Averse	Minimalist	Cautious	Open	Hungry
		Risk Appetite				

6.4 In the event that the risk cannot be accepted by the IAO the SIRA will prepare a risk assessment and present it to the accreditor for discussion. Dependant on the risk matrix the accreditor may be in a position to accept the risk.

6.5 If the risk acceptance decision sits at SIRO level then the accreditor will produce an executive summary, showing risk, mitigation and residual risk for the proposal and present this to the SIRO.

6.6 The SIRO will accept or reject the proposal and inform the accreditor of the decision.

6.7 It is the responsibility of the accreditor to update the national body of any significant change.

6.8 Usually the SIRO is the final decision maker for accepting local risks however in extreme cases it is possible to escalate a conflict to the Accounting Officer.

7. UNDERPINNING POLICIES AND PROCEDURES

7.1 To support the overarching Change and Release Management 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;

8. EQUALITY IMPACT ASSESSMENT (EQIA).

8.1 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.

9. HUMAN RIGHTS.

9.1 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.

10. FREEDOM OF INFORMATION (FOI).

10.1 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.

10.2 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		

11. TRAINING.

11.1 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.

12. PROMOTION / DISTRIBUTION & MARKETING.

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

- Newsbeat
- Intranet
- Posters
- Policy Portal

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

13. REVIEW.

13.1 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.

13.2 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.

13.3 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.

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

13.5 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

14. 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 2014	Amended Version	Tom King/Stephen Laishley
0.2	10/02/2015	Policy approved – Added CC signature and policy ref no	56408 Couchman