WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Business Applications**
POLICY REFERENCE NO:	**Inf/22**

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 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. 5
2. BUSINESS APPLICATION POLICY 5
2.1 Application Protection 5
2.2 Browser-based Application Protection..... 7
3. UNDERPINNING POLICIES AND PROCEDURES 8
4. EQUALITY IMPACT ASSESSMENT (EQIA)..... 8
5. HUMAN RIGHTS. 8
6. FREEDOM OF INFORMATION (FOI)..... 9
7. TRAINING. 9
8. PROMOTION / DISTRIBUTION & MARKETING..... 9
9. REVIEW. 9
10. VERSION HISTORY..... 10

1. INTRODUCTION.

1.1 West Midlands Police (WMP) has a comprehensive portfolio of business applications that support a wide range of business processes. A robust policy is required to protect critical applications and the integrity of information stored in or processed by them against known security threats.

2. BUSINESS APPLICATION POLICY

2.1 Application Protection

2.1.1 A risk assessment **must** be conducted to identify and evaluate potential security risks with all business applications (including browser-based and mobile applications), consistent with the criticality of the processes 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 them.

2.1.2 A catalogue of all business applications **must** be maintained, capturing the following but not limited to, for each application, as appropriate:

- Business Data Owner(s)
- IT System Owner(s)
- External Supplier Contact(s)
- Nature, Volume and Classification of Information Stored or Processed
- Platform Information and Supporting Infrastructure Components
- Description of Internal and External Interfaces
- Legal and Regulatory Compliance Requirements
- Overall Application Criticality
- Description of Security Controls
- End-user and Administrative Connection Methods and Protocols
- History of Security Incidents and Breaches
- Known Flaws and Vulnerabilities and their Severity Levels
- Remediation Plans and Status
- Overall Policy Compliance

2.1.3 Formal documented standards should be in place defining baseline control requirements in line with the application security architecture and consistently applied to all business applications. Additional controls to meet specific business, regulatory and security requirements should be identified and agreed for implementation on relevant business applications.

2.1.4 The controls framework **must** protect business applications against invalid connections and attacks by:

- assuming all input from external or untrusted systems is insecure by default
- validating object access permissions when a request is made to access it
- repeat any client validation upon connection to the server

2.1.5 The controls framework should ensure business applications are protected against unauthorised access and disclosure of critical and sensitive business information by:

- hardening the operating system and database to minimise attack surface
- providing defence in depth to avoid reliance on a single control
- implementing secure defaults and ensuring key components fail securely
- running them with least privilege and enforcing separation of privilege
- preventing initiation of outbound connections to untrusted systems or networks
- filtering information that reveals the internal workings of applications

2.1.6 The controls framework should protect the integrity and availability of information stored or processed by business applications by:

- minimising manual intervention
- preventing unauthorised changes
- producing and reviewing error and exception reports
- providing adequate capacity and improving resilience
- eliminating or reducing single points of failure

2.1.7 Servers supporting critical business applications should be adequately segregated from untrusted networks and run on dedicated computers.

2.1.8 Connections between servers and back office systems should be:

- protected by firewalls or other robust filtering mechanisms
- restricted to only the services that are required by the business applications
- restricted to those originating from the servers
- based on documented, tested and approved application programming interfaces
- encrypted

2.1.9 The controls framework should ensure the integrity of information entered into, processed or output by business applications is checked and maintained by:

- implementing range, consistency and hash total checks
- comparison with control balances, original documentation and other external sources
- ensuring information cannot be overwritten accidentally and information processing is validated
- reviewing changes to key ‘static’ business information (i.e. master or standing data)
- detecting unauthorised or incorrect changes to information

2.1.10 A formal documented process **must** be established for regularly validating the security posture of critical applications. The process should cover on-going operational monitoring using metrics as well as periodic, focused audits, technical security assessments and independent vulnerability reviews, using black box and white box test approaches to provide holistic assurance.

2.2 Browser-based Application Protection

2.2.1 Information used by browser-based applications should be protected against unauthorised access or changes by locating them on separate partitions and restricting file permissions.

2.2.2 The controls framework should protect website content against unauthorised disclosure or changes by:

- storing it separately from the operating system and setting strict file permissions
- restricting updates to authorised individuals and using secure content management methods
- reviewing content to ensure that it is accurate, that hyperlinks are valid and functional, and that vulnerabilities have not been introduced by scripts or 'hidden' form fields
- performing regular checks to ensure that website content is not defamatory, offensive or in breach of legal and regulatory requirements

2.2.3 Sensitive information in transit **must** be protected against unauthorised access and disclosure by using an approved and reliable cryptographic mechanism.

2.2.4 The controls framework should prevent unauthorised access to or disclosure of information about system configuration by:

- suppressing or obfuscating the identity of the web server software and version
- ensuring directories of files on web servers are not index able
- preventing source code of server-side binaries and scripts from being viewed or downloaded
- ensuring that the source code does not contain unnecessary information

2.2.5 Web application sessions **must** be protected against interception or cloning by implementing robust session management and configuration mechanisms and encrypting traffic between the web browser and the web server.

2.2.6 Internet facing web servers hosting business applications **must** be configured to record all actions performed and log security related events generated by the website.

2.2.7 The controls framework should ensure that risks associated with our web presence are suitably managed by:

- maintaining a catalogue of Internet-facing web servers that captures their hosting location, IP addresses, domain names and digital certificates used
- renewing corporate domain name registrations periodically
- registering domain names that could be used to masquerade as the organisation
- monitoring websites to detect and respond to cybersquatting and domain hijacking threats
- maintaining service level agreements to cover relationships with service providers

2.3 Non Conformance and Exceptions

2.3.1 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 Business Applications 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 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