WEST MIDLANDS POLICE

Force Policy Document

POLICY TITLE:	**External Supplier Management Policy**
POLICY REFERENCE NO:	**Inf/14**

Executive Summary.

In accordance with the HMG SPF Security Outcomes, West Midlands Police ensure that information risks in the Third Party supply chain are effectively managed so that wider information assurance requirements can be met and information assets are sufficiently protected from compromise.

***<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 0.3**	**21 July 14**
Business Area Owner	**Information Management Services**	
Department Responsible	**Information Management**	
Policy Contact	**Kate Jeffries – Head of Information Management**	
Policy Author	**Kate Jeffries – Head of Information Management**	
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. ABBREVIATIONS.

ACPO Association of Chief Police Officers

A/V Anti-Virus

ADS Accreditation Document Set (i.e. RMADS Risk Management Accreditation Document Set)

AO Accounting Officer (Chief Constable)

BC Basic Check

BCM Business Continuity Management

BCP Business Continuity Plan

BIA Business Impact Analysis

BS25999 Business Continuity Management - (BS 25999-1:2006) now ISO/IEC 22301:2012

CESG Communications-Electronics Security Group

CTC Counter Terrorism Check

CPU Central Processing Unit

DPA Data Protection Act 1998

DTI Department of Trade and Industry

HMG Her Majesty's Government

IAO Information Asset Owner

ICM Information Compliance Manager

InfoSec Information Security

ISF Information Security Forum

ISM Information Security Manager

ISO Information Security Officer (For the WMP Force)

ISO 22301 International Standards for Business Continuity Management - Requirements (ISO22301:2012)

ISO 27001 International Standard for Information Security Management System - Requirements (ISO27002:2005 contains the Implementation Guidance and Code of Practice)

IS Information Systems

ISP Information Security Policy

ISTU Information Systems Training Unit

ITIL Information Technology Infrastructure Library

LAN Local Area Network

NISCC National Infrastructure Security Co-ordination Centre

NPIRMT National Police Information Risk Management Team

PM Protectively Marked

RMADS Risk Management Accreditation Document Set

SC Security Check

SIRO Senior Information Risk Owner

SoA Statement of Applicability

SIIMN Strategic Information and Intelligence Management Board

SPF HMG Security Policy Framework

SyOPs Security Operating Procedures

SysOPs System Security Operating Procedures

System Information System

UNIRAS Unified Incident Reporting and Alerting Scheme.

UPS Uninterruptible Power

WMP West Midlands Police

2. TERMS AND DEFINITIONS.

Asset - An asset is something tangible or non-tangible which is of value to the organisation and needs to be protected, can be generally sub-divided into ‘Primary Assets’ and ‘Supporting Assets’. **Primary Assets** are ‘Processes’ and ‘Information Assets’ used by, stored or communicated by the organisation. **Supporting Assets** are all other Hardware, Software, Networks, Utilities, Physical Premises, People and Organisational Structures that are present to make the use of the ‘Primary Assets’ possible;

Availability - Ensuring that authorised users have access to information and associated assets when required;

Confidentiality - Ensuring that information is accessible only to those authorised to have access;

Identity and Access Management - In information systems, identity management is the management of the identity life cycle of entities (subjects or objects);

Information Asset - An Information Asset is a definable piece of information, stored in any manner which is recognised as 'valuable' to the organisation;

Information Security Policy - The set of laws, rules and practices that regulate how assets, including sensitive information, are managed, protected and distributed;

Integrity - Safeguarding the accuracy and completeness of information and processing methods;

Risk - The likelihood of a threat occurring and being successful in exploiting vulnerability, and causing a breach of security;

Security - A combination of confidentiality, integrity and availability considerations;

Evaluation - The assessment of an IS system or product against defined criteria;

Threat - The likelihood that an attacker will attempt, and has the capability, to exploit a vulnerability to breach security; and

Vulnerability - A feature of a system, which, if exploited by an attacker, would enable the attacker to breach security.

3. INTRODUCTION.

West Midlands Police has considerable exposure to external suppliers that deliver a range of services to support critical business and IT processes. An effective policy and framework of controls covering supplier selection, on-boarding, contract development, relationship management, compliance monitoring and assurance is required to protect critical business processes and information assets against known threats and reduce the overall risk to organisational value, brand and operations.

4. THIRD PARTY MANAGEMENT POLICY

An external supplier security management process must be defined with specific activities and responsibilities for delivery. The following areas should be covered:

- external supplier due diligence
- contract definition and safeguards
- contractual compliance monitoring and reporting
- supplier audit and assurance
- supplier termination activities

Depending upon the supplier, context and nature of services involved, the external supplier management process should involve representatives from the following areas to fulfil the key obligations of this policy:

- Business Area – Head/Contract Owner, Contract Manager, Commercial Management and Risk Coordinator
- Strategic Sourcing Partner
- IT – Supplier Relationship Management, Security Architecture
- IA – Information Security

The external supplier security management process must capture and maintain the following but not limited to, in the centralised external supplier database, for each relationship, where relevant:

- Business Contract Owner and Contract Manager
- Strategic Sourcing Contact(s)
- Commercial Management Contact(s)
- Relevant First Line of Defence Contact(s)
- Relevant External Supplier Contact(s)
- Nature, Volume and Classification of Information Stored or Processed
- Relevant Systems and Platforms Used
- Legal and Regulatory Compliance Requirements
- Overall Supplier Criticality
- External Supplier Rating from an Information Security Standpoint
- Known Incidents and Breaches
- Known Issues and Risks
- Audit/Assurance Snapshot and History
- Remediation Plans and Status

The external supplier security management process must ensure an initial risk assessment is undertaken to determine the nature, criticality/sensitivity and implications of the service(s) provided. The controls framework, driven by the level of risk, should require the following, before contract execution:

- a due diligence review to identify and assess supplier risk exposures and implications of the services provided, contractual requirements, their controls environment and demonstrable commitment to information security, before supplier on-boarding
- a supplementary physical site review, using the Police Assured Secure Facility standard where relevant, to evaluate and validate the adequacy and effectiveness of their information security arrangements

- a supplementary vulnerability assessment and penetration test where necessary to validate the adequacy and effectiveness of their technical security controls

A baseline set of controls should be documented and consistently used for agreeing information security arrangements with external suppliers. Additional controls to meet specific business and security requirements should be identified and agreed for inclusion within a contract.

A contract or other appropriate legally binding agreement must be established with agreed information security arrangements to govern the external supplier relationship. Any contractual requirement deemed unacceptable by an external supplier must be risk assessed and suitably mitigated or formally accepted, before contract execution.

A formal documented process must be established for regularly validating external supplier conformance to agreed contractual requirements for information security. The process should cover on-going operational monitoring of their security controls and practices using metrics, as well as periodic, focused audits and independent reviews to provide holistic assurance.

A method for secure termination of external supplier relationships must be established and agreed that includes the following but not limited to:

- defining ownership and responsibilities for managing termination activities
- revocation of physical and logical access to premises and information
- return, transfer or destruction of assets
- coverage of license agreements and intellectual property rights
- review and refinement of termination activities
- Hardware and Software Acquisition

Formal documented standards and procedures should be in place for organisation-wide acquisition of all hardware and software that cover the following:

- criteria for hardware and software selection
- security assessment of hardware and software to be acquired
- software licensing requirements
- process for review and approval of hardware and software

Corporate hardware and software must be acquired only from approved suppliers, tested prior to deployment, and supported by maintenance arrangements.

The risk of potential security vulnerabilities in hardware and software to be acquired should be reduced by defining security requirements, obtaining independent assessments from trusted sources, identifying security flaws and deficiencies and considering alternative methods of achieving security.

Outsourcing

A formal documented process must be in place to govern the selection of outsourcing service providers and transfer of business activity to them, with documented agreements that specify information security requirements to be met.

When determining the requirements for outsourcing, a risk assessment must be conducted to evaluate potential security risks associated with the outsourcing arrangements, in light of the particular business functions being outsourced. The controls framework, informed by the results of the risk assessment, should determine the degree and depth of contractual protection and controls required, before the activities are transferred.

Contracts must be established with agreed information security controls and approvals from relevant business owners obtained, before the management of a particular environment is transferred. The contracts must be reviewed by all relevant stakeholders, approved by senior management, agreed and signed by both parties and kept up-to-date.

The controls framework should define a set of standard elements and model clauses that are consistent with HMG GPG5 – Outsourcing and Offshoring, and be consistently embedded within all outsourcing contracts. These should cover:

- following good practices for information security
- safeguarding the confidentiality, integrity and availability of information and systems transferred
- timely reporting of security incidents
- limiting physical and logical access to assets, premises and information
- protection of individually identifiable information
- compliance with relevant legal and regulatory requirements
- following protocols for sub-contracting to other outsourcing service providers and third parties
- secure return, transfer or destruction of hardware, software and information
- quality and accuracy of work performed
- effective business continuity arrangements
- licensing requirements and ownership of intellectual property rights
- cover right to audit and alternative assurance procedures (e.g. independent attestation)

A formal documented process must be in place for responding to any security issues or incidents via the outsourcing service provider’s agreed point of contact.

Cloud Services and Contracts

A formal documented process must be established in line with the controls framework and applied throughout the organisation to support the acquisition or use of cloud services.

Awareness programmes should ensure Staff are aware of the organisation’s position on the use of cloud based services, understand the risks of using unapproved cloud services and consistently comply with corporate requirements for the purchase and use of external services.

A risk assessment must be undertaken prior to purchase or use of cloud services. It should take into account the nature and criticality/sensitivity of information that may be handled on the cloud and associated legal/regulatory risks, throughout the information lifecycle.

The control framework should define requirements pertaining to data storage, encryption and processing in particular jurisdictions, based on the level of risk and the classification of information to be processed on the cloud.

The control framework should ensure the security and availability of sensitive information stored or processed in the cloud by:

- protecting information against co-mingling using adequate physical and logical safeguards
- developing a technical security infrastructure that is compatible with the cloud service provider's architecture and infrastructure
- maintaining compatibility and security posture of client systems used to access cloud services
- using secure communication mechanisms to access cloud services
- provisioning resilient network links, multiple connection methods and adequate bandwidth

Cloud service contracts must be established with clauses that apply to standard external supplier contracts and include other relevant security controls, before contract execution.

The controls framework for protecting data processed on the cloud should cover the following:

- providing a secure authentication service to meet corporate identity and access requirements
- restricting access to authorised users only
- controlling access to cloud services for connections originating outside the corporate firewall
- managing access controls of the cloud service
- implementing malware protection mechanisms
- implementing secure destruction of data according to corporate records retention requirements
- requiring cloud service providers to share data on anomalous or malicious activity
- protecting individually identifiable information and locating it within approved locations or in a particular jurisdiction that safeguards business position and interests
- meeting corporate data availability requirements by providing dedicated support in the event of a security incident or legal action (e.g. e-discovery requests and forensic investigations) and providing an escrow facility using a trusted third party, where appropriate
- providing advance notification to any changes being made to the service that includes infrastructure, major reconfiguration of cloud service delivery or security, data processing in a new geographical or legal jurisdiction, and the use of sub-contractors

Data Transfers to External Suppliers

The controls framework must define and enforce relevant and adequate controls over data/information transfers (physical or electronic) to external suppliers, based on the results of a risk assessment and security requirements for sensitive information.

An inventory of data transfers to external suppliers must be maintained by all business areas, kept current and regularly reviewed, in accordance with a formal documented process.

Awareness programmes must ensure Staff are aware of the standard operating procedures and controls instituted to protect data/information sent to or received from external suppliers.

Controls over data transfers to external suppliers, including supporting infrastructure components, must be regularly reviewed to assure compliance with the policy requirements.

Non Conformance and Exceptions

Non-conformance with this policy must be reported to the Information Security Officer (ISO). The ISO 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

5. UNDERPINNING POLICIES AND PROCEDURES

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

1. Force Information Security Policy;
2. Information Management Policy;
3. Information Security Incident Management Policy;

6. 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 WMP 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.

7. 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 WMP (and its partners), to uphold the law and serve/protect all members of its community (and beyond) from harm.

8. FREEDOM OF INFORMATION (FOI).

Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 0.3 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.

This policy reflects best practice within ICT and IM and does not require a training element

10. PROMOTION / DISTRIBUTION & MARKETING.

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

- Newsbeat
- Intranet
- Posters
- Policy Portal

11. REVIEW.

The policy business owner Information Management, maintain 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 by the date shown 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.

M. D. Thompson.

CHIEF CONSTABLE

12. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
0.1	21 Mar 14	Initial Draft	Del Brazil, Advent-IM
0.2	21 Jul 14	Amended Draft	Paul Richards
0.3	15 Oct 2014	Amended Draft	Stephen Laishley
0.3	16 Oct 2014	Formatted Draft	56408 Couchman
0.3	27/11/2014	Policy approved & implemented	56408 Couchman