# WEST MIDLANDS POLICE
## Force Policy Document

| | |
|---|---|
| POLICY TITLE: | Information Security Incident Management |
| POLICY REFERENCE NO: | Inf/09 |

### Executive Summary.

In accordance with the HMG Security Policy Framework, West Midlands Police will implement an effective policy and supporting procedures for the identification, management of and recovery from information security incidents. This policy document sets out the high level requirements of incident management within West Midlands Police.

***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 0.4 | 14/10/2014 |
| Business Area Owner | Intelligence | |
| 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 | 17/10/2014 | |
| Review Date | 17/10/2016 | |
| 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.

1.1. West Midlands Police Policies consolidate legal, regulatory obligations into a set of objectives and minimum requirements that enable the First Line of Defence to construct a robust control framework. The specific purpose of this policy is to minimise the impact of information security incidents by ensuring incidents are correctly identified, responded to, recovered from, communicated and reported.

## 2. INFORMATION SECURITY AND INCIDENT MANAGEMENT.

2.1. A formal capability for governing the management of information security incidents end-to-end **must** be established and supported by documented standards and procedures.

2.2. The information security incident management capability should include:

- resources with defined roles and responsibilities
- sufficient skills and experience in information security incident management
- authority to make critical business decisions and escalate information security incidents
- agreed methods for engaging relevant internal and external stakeholders
- ensuring external suppliers' compliance with the policy or verifying that equivalent information security incident management procedures are in place
- periodic testing and exercising to provide assurance over adequacy and operating effectiveness

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

- incident identification that covers receiving incident reports, business impact assessment, classification and categorisation of incidents, and recording of incidents
- incident response that covers escalation to incident management team, investigation, containment and eradication of the cause of the incident
- incident recovery that covers rebuilding systems, restoring data, and incident closure
- incident follow-up that covers root cause analysis, forensic investigations, reporting to business areas and notifying statutory and regulatory authorities

2.4. The process for reporting information security events to predetermined contacts **must** be defined, documented and communicated.

2.5. The touch points in the information security infrastructure where information security events are likely to occur should be identified, documented and specific incident reporting procedures defined and documented.

2.6. Information security incidents **must** be recorded in a log and categorised and classified according to a documented framework.

2.7. The response to information security incident management should cover:

- analysing all the available and relevant information from reliable and authentic sources
- collecting, handling and securing necessary evidence
- investigating the cause of information security incidents
- containing and eradicating the information security incident using agreed response procedures

2.8. The recovery from information security incidents should cover:

- rebuilding systems and supporting IT infrastructure to a secure state
- restoring information from uncompromised and reliable sources
- formal closure of the information security incident

2.9. Details about information security incidents experienced should be recorded and maintained in an incident record on a continuous basis using a consistent approach and be regularly reviewed to:

- determine anomalous patterns and trends of information security incidents
- understand the costs and impacts associated with information security incidents
- identify common factors influencing or triggering information security incidents
- evaluate and validate the effectiveness of preventive, detective and reactive controls
- support on-going monitoring of incident management processes using metrics and other mechanisms
- provide a comparison of internal and external information security incident information

2.10. Management information in relation to information security incidents **must** be produced and reviewed on a regular basis

2.11. Disclosures of information security incidents to external stakeholders such as regulators or national Certs (GovCERT and CINRAS) **must** follow a formal documented process with clearly defined responsibilities.

**Incident Management Team Procedures**

2.12. Incident management team procedures **must** be invoked for significant incidents as defined in the incident management procedures.

2.13. Significant incidents **must**:

- be documented in an incident report and kept up to date throughout the incident lifecycle
- be reported to the Force Information Security Officer
- be subject to incident de-brief and root cause analysis prior to closure. For impartiality, this should not involve Staff who directly managed the information security incident

2.14. Information relevant to managing information security incidents **must** be made available to the incident management team on a need to know and need to do basis.

2.15. Information and documentation relevant to managing the incident **must** be secured and protected from unauthorised access, tampering or destruction.

### Cyber Attacks

2.16. The information security incident management capability should include formal documented standards and procedures for responding to cyber attacks.

2.17. A formal documented process should be established for regularly assessing the organisation’s vulnerability to and effectiveness of the controls framework in addressing known security threats associated with cyber attacks.

2.18. Information security incident management processes should be augmented by response procedures that include additional measures to respond to cybercrime attacks.

2.19. Formal documented standards and procedures should be developed to address cybercrime attacks that include:

- Staff awareness programmes with targeted briefings for vulnerable or high exposure individuals
- obtaining and monitoring cyber intelligence from a range of sources
- liaison with internal and external groups providing attack intelligence
- establishing and maintaining a formal relationship with relevant external groups typically involved during preparation and response to cyber related attacks
- performing attack simulations and tests of response plans to validate the effectiveness of the controls framework and the information security incident management process
- sharing intelligence with interested parties including customers, third party providers, industry bodies and law enforcement

### Emergency Fixes

2.20. A formal documented process **must** be established for applying emergency fixes to business information, business applications and technical infrastructure.

2.21. Formal documented standards and procedures should be established for applying emergency fixes that cover the following:

- applying emergency fixes to business application software, systems software, parameter settings and business and system information within the live environment
- emergency access for business and IT Staff as well as third parties
- logging and authorisation by business owner
- subjecting emergency fixes to established change management procedures and reviews
- implementing adequate oversight, technical safeguards and monitoring mechanisms to manage any potential incident resulting from an inappropriate emergency fix
- implementing technical safeguards to correct or roll-back inappropriate emergency fixes

- revoking authorisation for emergency access when access is no longer required
- ensuring emergency fixes are not left permanently in place
- conducting a review after the emergency to identify and address any flaws or defects that required the application of an emergency fix
- operational monitoring of security controls and practices relating to emergency fixes using metrics and other assurance mechanisms
- production and review of management information

2.22. Emergency access procedures should employ an on-demand access model to reduce the risk resulting from perpetual allocation of privileged access for making emergency fixes.

### Forensic Investigations

2.23. A formal documented process **must** be established for dealing with information security incidents that require forensic investigations.

2.24. Formal documented standards and procedures should be established for dealing with information security incidents requiring forensic investigations that cover:

- adequate management and technical oversight during the forensic investigation process
- planning the acquisition of evidence from relevant IT and non-IT sources with the intention of and in preparation for legal action
- collection of relevant passwords and encryption keys to access protected systems and storage areas containing electronic evidence
- immediate preservation of evidence on discovery of an information security incident
- conformance to a published and agreed standard or code of practice at every step of the forensic investigation to preserve evidence and ensure legal admissibility
- documentation requirements and maintenance of a log of evidence recovered and the investigation processes undertaken
- the need to seek legal advice where evidence is recovered
- monitoring requirements during the investigation
- reporting the results of a forensic investigation to relevant internal parties and appropriate external parties by approved individuals

2.25. All targeted investigations of Staff activities **must** be authorised by the Professional Standards Department and in consultation with Human Resources.

2.26. Forensic investigations **must** be conducted in accordance with legal constraints that include appropriate laws, privacy and employment legislation, human rights and any applicable policy and contractual requirements.

2.27. The controls framework should define and enforce adequate and effective safeguards to protect the sources of forensic information that include the following but not limited to:

- restricting physical and logical access to target IT systems and non-IT sources, to a limited number of authorised individuals
- preventing individuals from attempting to tamper or destroy possible evidence
- activating litigation hold to prevent deletion of documents and record archives that may contain electronic evidence

2.28. The forensic investigations process should safeguard the integrity of evidence by:

- demonstrating appropriate evidence has been collected, preserved and has not been modified
- analysing evidence in a controlled environment using clearly documented procedures
- having evidence reviewed by an independent expert to ensure conformance to legal requirements
- ensuring processes used to create and preserve evidence are consistent, repeatable and meet re-performance standards
- limiting information about an investigation to nominated individuals and ensuring it is kept confidential

### Non-Conformance and Exceptions

2.29. Non-conformance to this policy must be reported to the Force Information Security Officer. The Information Security Team 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 SIMB 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. Force Information Security Policy;
2. Information Management Policy;
3. Information Services Risk Register;
4. West Midlands Police Risk Appetite Statement;
5. (ICT Incident Procedures…..IM Incident Procedures)

## 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 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.*

## 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 WMP (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 |
|---|---|---|
| | | |

## 7. TRAINING.

7.1. This policy supports the core activities of the Information Security team and no additional or specific training needs to be provided.

## 8. PROMOTION / DISTRIBUTION & MARKETING.

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

- Newsbeat
- Intranet
- Posters
- Policy Portal

## 9. REVIEW.

9.1. 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.

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 by the date shown 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.

M. D. Thompson.

**CHIEF CONSTABLE**

## 10. VERSION HISTORY.

| Version | Date | Reason for Change | Amended/Agreed by. |
|---|---|---|---|
| 0.1 | 21 Mar 14 | Initial Draft | Del Brazil, Advent-IM |
| 0.2 | 11 Sep 14 | Amended Draft | Paul Richards/Stephen Laishley |
| 0.2 | 11/09/2014 | Formatted Document & added missing entries | 56408 Couchman |
| 0.3 | 14/10/2014 | Minor amendment to section 2 | Stephen Laishley |
| 0.3 | 21/10/2014 | Policy Published | 56408 Couchman |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |