WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**Technical Vulnerability (Patching/Updating) Policy**
POLICY REFERENCE NO:	**Inf/08**

Executive Summary.

West Midlands Police's computers must be properly patched with the latest appropriate updates in order to reduce system vulnerability and to enhance and repair application functionality.

The purpose of this Policy is to establish standard Policy and procedures for the identification of vulnerabilities, potential areas of functionality enhancements as well as the safe and timely installation of patches.

***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 1.4**	**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*
- *WMP Information Security Policy (Currently in draft)*
- *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
COTS Commercial off the shelf
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.

3.1. This Policy applies to all software, servers, desktops, laptops, mobile devices and network infrastructure owned and operated by West Midlands Police.

4. PATCHING POLICY.

4.1. West Midlands Police use a variety of bespoke and COTS software however; all PC based applications are predominantly standard COTS (Commercial off the shelf) products from trusted sources.

4.2. All assets must be recorded and auditable as per the asset management policy.

4.3. Service Packs and Patches or IOS based updates identified as 'Critical' or 'important' by trusted suppliers must be implemented on the relevant devices. The Support team (ICT) will be responsible for reviewing the relevant updates, assessing the criticality of the patch or fix, through relevant change control procedures, and roll out the relevant patches. The support team will be required to ensure that all relevant devices (when connected to the network) are patched and up to date. Records of non-compliance to this policy must be maintained and available for audit. Remote devices or remote access users that are not patched or have a risk profile of not applying patches for over 1 month will not be allowed to connect to the force network.

4.4. All server, desktop, and laptop systems, including all hardware and software components, must be accurately listed in the West Midlands Police asset register to support patching and threat management.

4.5. Vulnerability assessments of assets or devices must be completed in intervals that are relevant to the criticality of the system device or server. Antivirus must be installed on all devices. AV signature files MUST be updated and implemented on release. Failure to comply must be reported and investigated. Devices with AV that are 1 month out of date will be subject to disconnection. . Any exception to this must be logged investigated and reported.

4.6. Each vulnerability alert and patch release must be checked against existing West Midlands Police systems and services prior to taking any action in order to avoid unnecessary patching. All alerts must be read carefully as not all patches will be relevant to actual system versions in use at West Midlands Police.

4.7. The decision to apply other, optional patches must be made by the ICT Manager after careful consideration as to the appropriateness of such patches or updates and in consultation with Information Security resources.

4.8. All patches must be downloaded from the relevant system vendor or other trusted sources. Each patch's source must be authenticated and the integrity of the patch verified. All patches must be submitted to an anti-virus scan upon download. All patch testing must take place in a segregated or sandbox environment. Testing must not include any live data.

4.9. All patches must be tested prior to full implementation since they may have unforeseen side effects. All changes must be implemented through a relevant change control procedure.

4.10. New servers and desktops must be fully patched and subject to a vulnerability assessment before coming online in order to limit the introduction of risk.

4.11. New software must be fully patched when installed on West Midlands Police resources to limit the introduction of risk.

4.12. Disaster Recovery (DR) must be considered in the process of applying patches to ensure there is no impact to current DR solutions. Prior to major patch updates or service packs, a 'restore point' must be set to allow safe restoration of systems to their pre-patch state in the event that the patch has unforeseen effects.

4.13. System Audits shall be performed on a regular basis to ensure that all appropriate patches have been applied and are functioning as expected. Exceptions MUST be reported and investigated with a full audit trail to support this process.

5. VULNERABILITY ASSESSMENT.

5.1. West Midlands Police use a variety of bespoke and COTS software however; all PC based applications are predominantly standard COTS (Commercial off the shelf) products from trusted sources.

5.2. All assets must be recorded and auditable as per the asset management policy.

5.3. Service Packs and Patches or IOS based updates identified as ‘Critical’ or ‘important’ by trusted suppliers must be implemented on the relevant devices. The Support team (ICT) will be responsible for reviewing the relevant updates, assessing the criticality of the patch or fix, through relevant change control procedures, and roll out the relevant patches. The support team will be required to ensure that all relevant devices (when connected to the network) are patched and up to date. Records of non-compliance to this policy must be maintained and available for audit. Remote devices or remote access users that are not patched or have a risk profile of not applying patches for over 1 month will not be allowed to connect to the force network.

5.4. All server, desktop, and laptop systems, including all hardware and software components, must be accurately listed in the West Midlands Police asset register to support patching and threat management.

5.5. Vulnerability assessments of assets or devices must be completed in intervals that are relevant to the criticality of the system device or server. Antivirus must be installed on all devices. AV signature files MUST be updated and implemented on release. Failure to comply must be reported and investigated. Devices with AV that are 1 month out of date will be subject to disconnection. Any exception to this must be logged investigated and reported.

5.6. Each vulnerability alert and patch release must be checked against existing West Midlands Police systems and services prior to taking any action in order to avoid unnecessary patching. All alerts must be read carefully as not all patches will be relevant to actual system versions in use at West Midlands Police.

5.7. The decision to apply other, optional patches must be made by the ICT Manager after careful consideration as to the appropriateness of such patches or updates and in consultation with Information Security resources.

5.8. All patches must be downloaded from the relevant system vendor or other trusted sources. Each patch’s source must be authenticated and the integrity of the patch verified. All patches must be submitted to an anti-virus scan upon download. All patch testing must take place in a segregated or sandbox environment. Testing must not include any live data.

5.9. All patches must be tested prior to full implementation since they may have unforeseen side effects. All changes must be implemented through a relevant change control procedure.

5.10. New servers and desktops must be fully patched and subject to a vulnerability assessment before coming online in order to limit the introduction of risk.

5.11. New software must be fully patched when installed on West Midlands Police resources to limit the introduction of risk.

5.12. Disaster Recovery (DR) must be considered in the process of applying patches to ensure there is no impact to current DR solutions. Prior to major patch updates or service packs, a ‘restore point’ must be set to allow safe restoration of systems to their pre-patch state in the event that the patch has unforeseen effects.

5.13. System Audits shall be performed on a regular basis to ensure that all appropriate patches have been applied and are functioning as expected. Exceptions MUST be reported and investigated with a full audit trail to support this process.

6. EQUALITY IMPACT ASSESSMENT (EQIA).

6.1. 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.

7. HUMAN RIGHTS.

7.1. 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.

8. FREEDOM OF INFORMATION (FOI).

8.1. Public disclosure of this policy document is determined by the Force Policy Co-ordinator on agreement with its owner. Version 1.4 of this policy has been GPMS marked as Not Protectively Marked.

8.2. 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

9. TRAINING.

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

10. PROMOTION / DISTRIBUTION & MARKETING.

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

- Newsbeat
- Intranet
- Posters
- Policy Portal

11. REVIEW.

11.1. 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.

11.2. 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.

11.3. 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.

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

11.5. 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

12. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
1.1	07/08/2014	Amended to new WMP format	Stephen Laishley/Paul Richards
1.2	12/08/2014	Policy/Procedure amendments	Stephen Laishley/Paul Richards
1.3	13/08/2014	Format amendment	Stephen Laishley/Paul Richards
1.3	12/09/2014	Formatted and included missing parts	56408 Couchman
1.4	14/10/2014	Minor amendment to list of abbreviations	Stephen Laishley
1.4	21/10/2014	Policy Published	56408 Couchman