NOT PROTECTIVELY MARKED

WEST MIDLANDS POLICE
Force Policy Document

POLICY TITLE:	**PROTECTIVE MONITORING POLICY (ISP)**
POLICY REFERENCE NO:	**Inf/23**

Executive Summary.

West Midlands Police, by virtue of Section 6, Human Rights Act 1998, is a public authority and is required to act in a manner that is compatible with the rights outlined in the Convention.

The Regulation of Investigatory Powers Act 2000 (RIPA) enables the Secretary of State to make regulations setting out those circumstances where it is lawful to intercept or monitor communications for the purposes of carrying on a business. These regulations apply equally to public authorities.

Various legislation and codes of practice including the Data Protection Act 1998, ISO 27001/2 Information Security Management Systems and ACPO Community Security Policy impose a positive duty on the Force to protect its information assets and provide the assurances that appropriate controls are in place.

The monitoring of staff activity is an established concept which includes the routine supervision of performance and staff behaviour. RIPA extends the principle of supervision to the use by staff of communications equipment provided by the organisation for business purposes.

Protective Monitoring is a lawful and ethical tool used to assist the Force in the protection of its staff, information and to assist in the investigation of misconduct or criminal activity. The audit system will monitor and record all computer based actions conducted using any West Midlands Police computer equipment.

This policy defines the monitoring and auditing of staff activity as a means of ensuring all staff comply with Force policy and procedures and with the standards of behaviour expected by West Midlands Police.

This policy does not over-ride any existing policies or negate any existing guidance regarding information security, data protection or acceptable use. It is intended that it will supplement such policies but with a specific focus on the protective monitoring of the force computer network and access to the data held within or transported by it. Main aims and objectives are:

- To ensure the data integrity of the information held by West Midlands Police and enhance operational security of criminal investigations. This will be achieved by way of a single force-wide network based facility that will audit computer and peripheral device usage independent of any specific application. The system will ensure that West Midlands Police complies with the ACPO Community Security Policy (CSP) requirement to carry out “Protective Monitoring”.

- To identify misuse, monitor exceptional usage and support intelligence led investigations. All users of West Midlands Police LAN accounts must note that the monitoring system will include any personal use staff make of Force equipment, even if undertaken in their own time and with Management agreement. Standard use of all West Midlands Police systems and information is identified to all users as for ‘Business Use Only’;

- To provide a forensic capability to the auditing process to ensure its evidential credibility;

- To protect the Force by providing the Counter-Corruption Unit (CCU) with the means by which they can effectively seek out those who abuse their position within the force for personal gain or benefit of others;

- To instil within the communities of West Midlands Police the confidence that those employed by West Midlands Police maintain the highest levels of honesty and integrity by enforcing the relevant Codes of Conduct in relation to unethical behaviour or gross misconduct;

- To protect the information and intelligence assets of the Force from malicious or accidental 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	**Paul Richards/Tom King - Information Security Officer**	
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

- **Information Security Policy**
- **ACPO – Community Security Policy (CSP)**
- **CESG Good Practice Guide 13 (Protective Monitoring)**
- **Statutory Instruments 2000 No.2699. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000**
- **Management of Police Information (MoPI) Codes of Practice 2010**
- **Information Security Management Systems (ISO 27001:2013)**
- **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. Protective monitoring is an essential component of risk treatment when accrediting ICT Networks and Services processing protectively marked information to HMG standards. Good Practice Guide 13 – Protective Monitoring for HMG Systems (GPG 13) defines protective monitoring and provides a set of protective monitoring controls. Therefore, in order to ensure that the protective monitoring requirements are correctly implemented the following implementation guidance has been produced.

2. PROTECTIVE MONITORING CONTROLS

2.1. The implementation of protective monitoring for the West Midlands Police network has been aligned to the baseline requirements of GPG 13 (Appendix A, Table A-3) and the Consolidated Risk Statement (CRS) for West Midlands Police. Therefore, all protective monitoring controls (PMC) will require implementation using the Deter segment requirements. Although where appropriate some requirements may not be fully implemented if not applicable or where it is impracticable to do so. Where this is the case justification is to be provided.

2.2. The PMCs are:

PMC No.	Description	PMC To CRS Mapping
1	Accurate time in logs	1, 2, 3, 4, 5, 6, 7, 8, 9, 12
2	Recording of business traffic crossing a boundary	1, 2, 8, 9
3	Recording relating to suspicious activity at the boundary	1, 2, 8, 9
4	Recording on internal workstation, server or device status	3, 4, 5, 6, 7, 8, 9, 10, 12
5	Recording relating to suspicious internal network activity	3, 5 ,6, 8, 9
6	Recording relating to network connections	1, 2, 3, 10
7	Recording on session activity by user and workstation	3, 9,
8	Recording on data backup status	1, 2, 3, 5, 6, 8, 9
9	Alerting critical events	1, 2, 3, 5, 6, 8, 9
10	Reporting on the status of the audit system	1, 2, 3, 5, 6, 8, 9
11	Production of sanitised and statistical management reports	1, 2, 3, 5, 6, 8, 9
12	Providing a legal framework for Protective Monitoring activities	11

2.3. The 12 tables included at Appendix 1 provide a description for how each control should be implemented. At the end of each PMC table there is also a section covering Accounting Recommendations which detail the recordable events (or logs) for each PMC and which items are to be reported and/or alerted for each recordable event.

3. LOG GATHERING

3.1. It should be noted that the protective monitoring requirements of GPG 13 are achievable using the tools or features intrinsic to many types of software (particularly Microsoft). However, there are also many auditing software products that provide the additional benefit of automating many event or log gathering requirements as well as enabling user workstations to be audited remotely. Any product that supports log management or Security Information and Event Management should be suitable.

3.2. The following table provides a summary of potential intrinsic software features:

Class	Types	Logging Capabilities
Servers	• Network Servers • Database Servers • Application Servers	• Provide a source of information regarding access to network resources hosted by server • May conform to Controlled Access Protection Profile (CAPP) or better, if evaluated to EAL3 or above • Are essential for tracking privileges and monitoring file system based access control • May be supplemented by application level logging • Log collection and analysis tools tend to be primitive • Database and application servers may either use intrinsic server facilities or their own separate reporting mechanisms
Clients	• Workstations • Laptops • Thin-clients • Portable Electronic Devices (Smartphones, PDAs, etc)	• Often have similar capabilities to servers • Are more likely to be subject of manipulation by an attacker • Can generate logs while offline (especially for access to local resources) • May be of value for forensic analysis or local audit • Requirement for collection of local logs would be atypical • May provide logs and alerts relating to I/O attachments while connected to the network
Authentication Services	• Domain Controllers • Directory Servers • Authentication Servers (Kerberos, RADIUS, TACACS, etc)	• Provide source of records regarding network authentication attempts and failures • May also provide information regarding sessions, privileged assignments, directory information, remote access and token use
Network Components	• Routers • Switches • Network Management System	• Can track network attachments, IP address mapping, wireless access and network health • Typically have very low local log

	• DNS • DHCP • Wireless Access Points	retention and often reliant upon proprietary add-on or SNMP based management infrastructure • NMS output covers many events and requires filtering to select those that are security relevant
Security Services	• Network Firewalls • Application Firewalls • Proxy Servers • Content Scanners • Anti-Malware • Guard Processors	• There are many proprietary products with vendor specified logging characteristics • May support SNMP traps or other means of sending alerts • Are essential for tracking and enumerating information regarding alerts raised within DMZs and for tracking boundary operations • May support integration with NIDS
Storage Management	• RAID Controllers • SAN Controllers • Backup Servers • Cache Servers	• Provide disposition of storage health and information protection status • Can track movement of information between storage compartments and network boundaries • Are essential to support incident recovery

4. PROTECTIVE MONITORING RESPONSES

4.1. As well as defining the protective monitoring requirements for West Midlands Police there other requirements that need to be determined. These are addressed as follows:

- Audit periods – Logs should be reviewed at least once a week
- Retention periods – Logs should be retained for between 3 and 6 months
- Console manning – Where logs are sent to a monitoring console, the console should be monitored during core business hours
- Response times to critical alerts – A first response should be made within 4 hours of the alert and an investigation initiated within 2 days
- Accounting data capacity – The collection and retention of protective monitoring logs will require significant storage capacity which will need to be adequately catered for when implementing protective monitoring.

5. GLOSSARY

5.1. The following provides an explanation of terms and abbreviations used with this document:

Term	Description
Access Attempt	Typically: Open, Create, Read, Write, Rename or Delete
Business Criticality	The recording level on each device should be established according to its capabilities and its level of business criticality. Clearly, requirements for servers will usually be in excess of the requirements for workstations. Exact requirements need to be defined for each device as part of detailed system design

Event Alert	As Operating Systems and other software generate numerous reports and alerts. Some assign different senses of criticality to an event logged ("critical", "error", "warning", etc.). The true sense of event criticality should be reviewed on a case-by-case basis by the organisation, in order to determine each event's implications regarding security, as this may differ from the default vendor setting
Host	Generic name for a networked device, typically a server or workstation
IDS	Intrusion Detection System – A device or software application that monitors network and/or system activities for malicious activities or policy violations
IPS	Intrusion Prevention System – A network security appliance that monitors network and/or system activities for malicious activity. IPS is considered an extension of an IDS but is placed in-line and are able to actively prevent/block intrusions that are detected
Log Rotation System	Provides log files of manageable size and also facilitates protection and collection
MSSP	Managed Security Services Provider that specialises in the delivery of security based services such as protective monitoring
NBA	Network Behaviour Analysis – is a way to enhance the security of a proprietary network by monitoring traffic and noting unusual actions or departures from normal operation. NBA solutions watch what's happening inside the network, aggregating data from many points to support offline analysis. After establishing a benchmark for normal traffic, the NBA program passively monitors network activity and flags unknown, new or unusual patterns that might indicate the presence of a threat
Receiving Console	Organisations can send reports and alerts to an ICT system used for monitoring purposes. The system could be a dedicated ICT system within an Operations Centre or simply the PC used by a Security Manager configured to receive such reports/alerts
SIEM	Security Information and Event Management – SIEM provides real-time analysis of security alerts generated by network hardware and applications. SIEM solutions come as software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes

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 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.

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 West Midlands Police (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 0.1 of this policy has been GPMS marked as Not Protectively Marked.

8.2. 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		

9. TRAINING.

9.1. There is no specific training for West Midlands Police personnel; however those individuals with a specific involvement in Protective Monitoring will have the relevant training courses detailed within their job specifications.

10. PROMOTION / DISTRIBUTION & MARKETING.

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

- Newsbeat
- Intranet
- Posters
- Policy Portal

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

11. REVIEW.

11.1 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.

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.

CHIEF CONSTABLE

12. VERSION HISTORY.

Version	Date	Reason for Change	Amended/Agreed by.
0.1	26/09/2014	Initial version	Paul Richards/Stephen Laishley
0.2	15/01/2015	Amended version	Tom King/Stephen Laishley
0.2	28/01/2015	Amended Formatting – included code of ethics section	Vicki Couchman
0.2	20/03/2015	Policy approved by CC – now live. Added policy ref & sig	56408 Couchman

Appendix 1 – PMC Descriptions and Requirements

PMC1 – Accurate Time in Logs

Control Description

Provide a means of providing accurate time in logs and synchronisation between system components with a view to facilitate collation of events between those components. This can be achieved by any or all of the following means.

- Providing a master clock system component which is synchronised to an atomic clock
- Updating device clocks from the master clock using the Network Time protocol (NTP)
- Record time in logs in a consistent format (Universal Co-ordinated Time (UTC) is recommended)
- As a fallback, checking and updating device clocks on a regular basis (e.g. weekly).

Projects should define the error margin for time accuracy according to business requirements. The following issues also need to be considered.

- Some devises may not support clock synchronisation and need to be manually maintained
- Although recording time in UTC, the human interface should also support local time
- Clocks drift on mobile devices (e.g. Portable Electronic Devices (PEDs) may require correction upon attachment.

Specific Requirements

- All events should be accurately time-stamped
- All log file collections should include a cryptographic checksum (eg. Hash Message Authentication Code that incorporates an accurate cryptographic time-stamp).

Recording & Accounting Requirements

Event ID	Recordable Event	Accounting Items	Potential Sources for Event Information
1	Every event record required by protective monitoring should be time-stamped	• The date and time for each event	N/A
2	All alert messages that relate to protective monitoring should also be time-stamped	• The date, time and event referenced by the alert message	N/A
3	All event log extracts should also have an accurate time-stamp that is digitally signed	• The date, time, event log extract hash and signature	N/A

Description of Control Process in Place

PMC2 – Recording Relating to Business Traffic Crossing a Boundary

Control Description

The objective of this control is to provide reports, monitoring, recording and analysis of business traffic crossing a boundary with a view to ensuring traffic exchanges are authorised, conform to security policy, transport of malicious content is prevented and alerted, and that other forms of attack by manipulation of business traffic are detected or prevented.

The main requirement is to provide an accountable record of imports and exports executed by internal users and to track cross-boundary information exchange operations and the utilisation of any externally visible interfaces. This includes all checking of cross-boundary movement of information, content checking and quarantining services.

Application based check can be applied to business traffic to accept legitimate transactions and reject and alert malformed exchanges.

Specific Requirements

- Malware detection and status of signature updates should be logged and reportable at the boundary
- User web browsing activity should be checked against an Acceptable Use Policy at the boundary and logged
- All imported content across the boundary should be subject to content checking
- Detected malware or blocked/dangerous imports should be quarantined and alerted to the System Manager
- If there are not means to check encrypted content at the boundary (e.g. decrypt-scan, decrypt-scan-encrypt of SSL traffic) then this should either be discarded or quarantined, and the event logged, reportable and audited.

Recording & Accounting Requirements

Event ID	Recordable Event	Accounting Items	Potential Sources for Event Information
1	Any malware detection at boundary	The following shall be reported and an alert sent to a receiving console: • The malware name • The application stream (eg. FTP, SMTP, HTTP) • The direction (in or out bound)	• Anti-malware software or anti-malware boundary checking
2	Every change in status of the boundary anti-malware signatures	The following shall be reported: • Changes (updates) to the anti-malware signature based library	• Anti-malware software or anti-malware boundary checking • SIEM, NBA, IDS, IPS or other Management Console System
3	Any blocked web browsing activity	The following shall be reported and an alert sent to a receiving console: • The username and identifier of the workstation used • The URL of the blocked website • The reason the activity was blocked (eg, blacklisted on proxy server)	• Operating Systems • Network Management System • Directory or Remote Access Server (eg. RADIUS) • Web Server • Domain Name Service • Web Proxy Server • Web Content Scanner
4	Blocked file import attempts across the boundary	The following shall be reported and an alert sent to a receiving console: • The username, workstation identifier or process used • The source URL of the blocked file • The reason the activity was blocked (eg, blacklisted on proxy server)	

5	Blocked file export attempts across the boundary	The following shall be reported and an alert sent to a receiving console: • The username, workstation identifier or process used • The intended URL of the blocked file • The reason the activity was blocked (eg, blacklisted on proxy server)	
Description of Control Process in Place			

PMC3 – Recording Relating to Suspicious Behaviour at a Boundary

Control Description

The objective of this control is to provide reports, monitoring, recording and analysis of network activity at the boundary with a view to detecting suspect activity that would be indicative of the actions of an attacker attempting to breach the system boundary or other deviation from normal business behaviour.

The main requirement is to receive information from firewalls and other network devices for traffic and traffic trend analysis. This will enable detection of common attacks such as port scanning, malformed packets and illicit protocol behaviours.

An intrusion detection service is a recommended defence at the boundary with any untrusted network (eg. the Internet). It may also be a mandated requirement in codes of connection for membership of community of interest networks (such as GSI).

Specific Requirements

- It should be possible to interrogate and review firewall logs to determine current boundary conditions
- There should be an integrated firewall reporting solution that permits attack trend analysis to be conducted at all boundary points
- There should be intrusion detection services that cover all boundary servers, firewalls and routers

Recording & Accounting Requirements

Event ID	Recordable Event	Accounting Items	Potential Sources for Event Information
1	Packets being dropped by boundary firewalls	The following shall be reported: • The name and size of the IP packet header • The name of the firewall • The network interface identifier • The relevant firewall rule	• Firewall/Firewall Console or Router/Switch • Host Network Interface • Packet Sniffer
2	All boundary monitoring system consoles considered CRITICAL messages.	The following shall be reported and an alert sent to a receiving console: • The criticality and message content	• Operating Systems • Anti-malware software or anti-malware boundary checking • Anti-malware software or anti-malware boundary checking • Other device logs • SNMP traps • Firewall/Firewall Console • SIEM, NBA, IDS or IPS • Network Management System or other Management Console System
3	User logon authentication failures on boundary devices and systems	The following shall be reported and an alert sent to a receiving console: • The username • The network device identifier • The reason for the failure	• Operating Systems • Domain Controller • Directory or Remote access Server • Name Service (eg. DNS) or DHCP Server • Web Proxy Server • Web Content Scanner
4	The detection of all suspected attacks at the boundary	The following shall be reported and an alert sent to a receiving console:	• SIEM, NBA, IDS or IPS • Name Service or DCHP

		• Details concerning the type, source & target of the attack • If relevant, the identifier for the detecting IDS/IPS probe or host identifier on which a SIEM, NBA, IDS or IPS agent is installed	Server
5	All boundary monitoring system console Error (non-critical) messages	The following shall be reported: • The message criticality and • The message content	• Operating Systems • Anti-malware software or anti-malware boundary checking • Other device logs • SNMP traps • Firewall/Firewall Console • SIEM, NBA, IDS or IPS • Network Management System or other Management Console System
6	User sessions on boundary devices and consoles of boundary management systems	The following shall be reported: • The username • The network device identifier • The session status (eg. login/logout, disconnected, timed-out, etc)	• Operating Systems • Domain Controller • Directory Service or Remote access Server • Name Service or DCHP Server
7	All changes to the boundary firewall and other relevant device rule-bases	The following shall be reported: • The username of the person making the change • The network device identifier • The rule being changed including the details of the change	• Operating Systems • Domain Controller • Directory or Remote access Server • Name Service or DCHP Server • Firewall/Firewall Console • Web Proxy Server • DMZ Server • Email Server • SIEM, NBA, IDS or IPS
8	All actions invoked by users in response to an external attack notification	The following shall be reported: • The username of the person responding • The network device identifier • The session identifier associated with the actions and a description of the manual or automatic action(s) being taken	
9	Every change in status of external attack recognition software (eg. SIEM, NBA or IDS/IPS)	The following shall be reported: • Changes to the signature base of the software for the IDS/IPS probe or host identifier on which a SIEM, NBA, IDS or IPS agent is installed shall be reported	• Anti-malware software or anti-malware boundary checking • SIEM, NBA, IDS or IPS • Network Management System or other Management Console System • Name Service or DCHP Server
Description of Control Process in Place			

PMC4 – Recording of Workstation, Server or Device Status

Control Description

The objective of this control is to detect changes to device status and configuration. Changes may occur through accidental or deliberate acts by a user or by subversion of a device by malware (e.g. installation of Trojan software or so called "rootkits"). It will also record indications that are typical of the behaviours of such events (including unexpected and repeated system restarts or addition of unidentified system processes).

It also attempts to detect other unauthorised actions in tightly controlled environments (e.g. attachment of USB storage devices). This includes extension monitoring of any business critical file areas.

Specific Requirements

- It should be possible to check the status of anti-malware software updates and receive alerts of malware detection
- File, Input/Output and other system errors should be logged and reportable and alerted to a network management system
- System start-up and shutdown events should be logged and reportable for all Servers, Workstations and Network Devices
- All file system access violation messages should be logged, reportable and alerted
- File system monitoring should be active at the storage device or partition/volume level and the attachment of Input/Output devices (eg USB devices) and volume activity logged on business critical devices (ie. Servers).

Recording & Accounting Requirements

Event ID	Recordable Event	Accounting Items	Potential Sources for Event Information
1	All CRITICAL messages for servers and selected workstations if deemed business critical	The following shall be reported and an alert sent to a receiving console: • The criticality and message content • The details of the effected host	• Operating Systems • Anti-malware software or anti-malware boundary checking • Other device logs • SNMP traps • Firewall/Firewall Console • SIEM, NBA, IDS or IPS • Network Management System or other Management Console System • Name Service or DCHP Server • Domain Controller • Directory Server
2	All malware detection incidents on servers and workstations	The following shall be reported and an alert sent to a receiving console: • The malware name • Details of the host on which it is detected	• Anti-malware software or anti-malware boundary checking • Name Service or DCHP Server • Domain Controller • Directory Server
3	All ERROR messages for servers and selected workstations if deemed business critical	The following shall be reported: • The criticality and message content • The details of the effected host	• Operating Systems • Anti-malware software or anti-malware boundary checking • Other device logs • SNMP traps • Firewall/Firewall Console • SIEM, NBA, IDS or IPS

			• Network Management System or other Management Console System • Name Service or DCHP Server • Domain Controller • Directory Server
4	Every change in status of the anti-malware software signature base	The following shall be reported: • The new signature-base version • The details of the host on which it has been updated	• Anti-malware software or anti-malware boundary checking • SIEM, NBA, IDS, or IPS • Name Service or DCHP Server • Domain Controller • Directory Server
5	Every failed access attempt to the file system for the servers and workstations should be logged and reportable	The following shall be reported: • The file or path of the attempt • Details of the effected host • The username or process making the attempt • The type of access attempt and the reason for the failure	• Operating Systems • Name Service or DCHP Server • Domain Controller • Directory Servers or Remote Access Server • Web Proxy Server • Web Content Scanner
6	Changes to file or path access rights with system folders	The following shall be reported: • The username or process initiating the change • Details of the effected host, the file or path and access rights or access control list	• Operating Systems • Domain Controller • Directory Server or Remote Access Server
7	Change in status of all network servers, workstations and devices	The following shall be reported and an alert sent to a receiving console: • Details of the host and details of the change (start-up or shutdown)	• Operating Systems • Name Service or DCHP Server • Domain Controller • Directory Server or Remote Access Server • Network Management System • Port Control Software
8	Change in attachment status of devices attached to controlled servers and workstations	The following shall be reported: • The username or process initiating the change • The effected device, interface & host • Status of the attached device (attached, detached, disabled, etc)	• Operating Systems • Name Service or DCHP Server • Domain Controller • Directory Server or Remote Access Server • Port Control Software
9	Change in status of storage volumes of monitored servers and workstations	The following shall be reported and an alert sent to a receiving console: • The username or process initiating the change • Details of the effected host and the storage volume • The status of the change	• Operating Systems • Name Service or DCHP Server • Domain Controller • Directory Server or Remote Access Server • SIEM, NBA, IDS, or IPS
10	Change in software configuration status on servers, workstations and	The following shall be reported:	• Operating Systems • Name Service or DCHP

	devices	• The username or process initiating the change • Details of the effected host, • Details of the software package or patch identifier and the version identifier • Change details for the software package/patch configuration status	Server • Domain Controller • Directory Server or Remote Access Server • Configuration/Change Control Process
Description of Control Process in Place			

PMC5 – Recording Relating to Suspicious Internal Network Activity

Control Description

The objective of this control is to monitor critical internal boundaries and resources within internal networks to detect suspicious activity that may indicate attacks either by internal users or by external attackers who have penetrated to the internal network.

Likely targets for heightened internal monitoring include:

- Core electronic messaging infrastructure (e.g. email servers and directory servers)
- Sensitive databases (e.g. HR databases, finance, procurement/contracts, etc)
- Information exchanges with third parties.

Project servers and file stores with strict "need to know" requirements

Specific Requirements

- Consider implementation of firewalls in front of business critical servers or internal network zones
- If so, it should be possible to interrogate and review the firewall logs to determine current internal conditions
- There should be an integrated firewall reporting solution that permits attack trend analysis to be conducted at internal boundaries (this may be in common with PMC 3).

Recording & Accounting Requirements

Event ID	Recordable Event	Accounting Items	Potential Sources for Event Information
1	Packets dropped by internal firewalls	The following shall be reported: • The name & size of the IP packet header • The name of the firewall, its network interface identifier & the firewall rule	• Firewall/Firewall Console or Router/Switch • Host Network Interface • Packet Sniffer
2	All internal monitoring system console messages at CRITICAL status	The following shall be reported and an alert sent to a receiving console: • The criticality and message content	• Operating Systems • Anti-malware software or anti-malware boundary checking • Other device logs • SNMP traps • Firewall/Firewall Console • SIEM, NBA, IDS or IPS • Network Management System or other Management Console System • Name Service or DCHP Server • Domain Controller • Directory Server
3	User logon authentication failures on internal network devices and monitoring consoles	The following shall be reported and an alert sent to a receiving console: • The username • The network device identifier • Reason for the failure	• Operating Systems • Name Service or DCHP Server • Domain Controller • Directory Server or Remote Access Server
4	All internal monitoring system console messages at Error status	The following shall be reported: • The criticality and message content	• Operating Systems • Anti-malware software or anti-malware

			boundary checking • Other device logs • SNMP traps • Firewall/Firewall Console • SIEM, NBA, IDS or IPS • Network Management System or other Management Console System • Name Service or DCHP Server • Domain Controller • Directory Server
5	User sessions on internal network devices and monitoring consoles	The following shall be reported: • The username • The network device identifier • Session status (eg. login/logout, disconnected, timed-out, etc)	• Operating Systems • Name Service or DCHP Server • Domain Controller • Directory Service or Remote Access Server
6	All changes to internal firewall and other relevant device rule-bases	The following shall be reported and an alert sent to a receiving console: • The username of the person making the change • The network device identifier • The rule being changed including the details of the change	• Operating Systems • Name Service or DCHP Server • Domain Controller • Directory Server or Remote Access Server • Firewall/Firewall Console or Router/Switch • Proxy Server • DMZ Server
Description of Control Process in Place			

PMC6 – Recording Relating to Network Connections

Control Description

The objective of this control is to monitor temporary connections to the network either made by remote access, virtual private networking, wireless or any other transient means of network connection.

This includes:

- Environments which are permissive and that support Wireless LANs (WLANs), mobile users and remote working and it includes more restrictive environments in which the attachment of modems and wireless access points are prohibited
- More restrictive environments in which the attachment of modems and wireless access points are prohibited.

Specific Requirements

- Provide scope for resolving workstation addresses from dynamic IP to physical address (eg. resolving to Media Access Control (MAC) address by consultation of Dynamic Host Configuration Protocol (DHCP) or Address Resolution Protocol (ARP) logs)
- Also provide scope for resolving remotely attached workstations and workstations attached via wireless connections (e.g. by inspection of Remote Dial In User Service (RADIUS), wireless access point or remote access server logs)
- Log and alert unauthorised connections (including non-standard workstations and wireless access points)
- Capture all remote access authentication exchanges. Apply IDS to remote access and virtual private networking DMZs.

Recording & Accounting Requirements

Event ID	Recordable Event	Accounting Items	Potential Sources for Event Information
1	User authentication failures for remote access	The following shall be reported and an alert sent to a receiving console: • The username • User remote access credential identifier and host • The reason for the failure	• Operating Systems • Domain Controller • Directory or Remote access Server • Remote Access Server (eg. RADIUS)
2	All unsuccessful VPN node registrations	The following shall be reported and an alert sent to a receiving console: • Details of the node (identifier of the remote attached VPN subnet) • The VPN (identifier and characteristics of the VPN net) • The reason for the failure shall be reported and an alert sent to the receiving console	• VPN Router or Controller • Operating Systems
3	Changes of status of dynamic IP address assignments	The following shall be reported: • Details of the MAC address of the communicating device, • The IP Address and other relevant details of the assignment	• DHCP Server • Address Resolution Protocol • Operating Systems • Network Equipment or Network Management System • SIEM, NBA, IDS, or IPS
4	User sessions via remote access	The following shall be reported: • The username and the user remote	• Operating Systems • Domain Controller • Directory or Remote

		access credential identifier • The host used • The session identifier (associated with the user or process) • The session status (eg. logged-in, logged-out, timed-out, etc)	access Server
5	Changes in status of VPN node registration	The following shall be reported: • Details of the node (identifier of the remote attached VPN subnet) • The VPN (identifier and characteristics of the VPN net) • The VPN node connection status (eg. attached, detached, timed-out, etc)	• VPN Router or Controller • Operating Systems • Network Management System
6	All rejected attempts to connect equipment to protected network attachment points	The following shall be reported and an alert sent to a receiving console: • The physical network access point identifier • The MAC addresses of the communicating device • The reason for the rejection	• Network Equipment or Network Management System • DHCP Server • Address Resolution Protocol • Operating Systems
7	All network connection console messages at CRITICAL status	The following shall be reported and an alert sent to a receiving console: • The criticality and message content	• Operating Systems • Anti-malware software or anti-malware boundary checking • Other device logs • SNMP traps • Firewall/Firewall Console • SIEM, NBA, IDS or IPS • Network Management System or other Management Console System • Name Service or DCHP Server • Domain Controller • Directory Server
8	User authentication failures on network connection consoles	The following shall be reported and an alert sent to a receiving console: • The username • The network device identifier • The reason for the failure	• Operating Systems • Name Service or DCHP Server • Domain Controller • Directory Server or Remote Access Server
9	All network connection console messages at Error status.	The following shall be reported: • The criticality and message content	• Operating Systems • Anti-malware software or anti-malware boundary checking • Other device logs • SNMP traps • Firewall/Firewall Console • SIEM, NBA, IDS or IPS • Network Management System or other Management Console

			System • Name Service or DCHP Server • Domain Controller • Directory Server
10	All cases of attachment attempts of wireless devices to legitimate wireless access points	The following shall be reported: • The WLAN identifier • The MAC address of the communicating device • The status of the wireless node (eg. attached, detached, timed-out, etc)	• Wireless Access Point Controller • Operating System or Network Management System • DHCP Server • Address Resolution Protocol
11	User sessions on network connection consoles	The following shall be reported: • The username • The network device identifier • The session identifier and session status (eg. logged-in, logged-out, timed-out, etc)	• Operating Systems • Name Service or DCHP Server • Domain Controller • Directory Service or Remote Access Server
Description of Control Process in Place			

PMC7 – Recording of Session Activity by User and Workstation

Control Description

To monitor user activity and access to ensure they can be made accountable for their actions and to detect unauthorised activity and access that is either suspicious or is in violation of security policy requirements.

This is intended to support accountability requirements such that users can be held to account for actions they perform on ICT systems

Specific Requirements

- The following shall be logged and reportable on servers:
  - All log-on attempts to the network by all users (normal & privileged) whether successful or not
  - All log-offs
  - The creation, deletion or all user (normal & privileged) network privileges
  - The creation, deletion or change of network account passwords
  - The use of application and database server administrative facilities/accounts
- Alert on multiple log-on failures resulting in user account lock-outs
- Logging and capture of all accountable transaction summaries

Recording & Accounting Requirements

Event ID	Recordable Event	Accounting Items	Potential Sources for Event Information
1	User network sessions	The following shall be reported: • The username and user logon domain identifier • The host device used • The session identifier for the user or process and session status (eg. logged-in, logged-out, disconnected, timed-out, etc)	• Operating Systems • Domain Controller • Directory or Remote Access Server • Name or Directory Service
2	User network account status change	The following shall be reported: • The username and user logon domain identifier • The user account status (eg. logged-on, logged-off, timed-out, enabled, disabled, etc)	• Operating Systems • Domain Controller • Directory Server
3	Changes to network user privileges and user group status and membership	The following shall be reported: • The effected username(s) and user logon domain identifier • The host device used • The user identifier for the administrator or the software process identifier (carrying out the change) • The session identifier for the user or process and session status (eg. logged-in, logged-out disconnected, timed-out, etc)	• Operating Systems • Domain Controller • Directory Server • Name Service • DHCP Server • Network Equipment or Network Management Console
4	Use of any application or database administrative facility	The following shall be reported: • The host device used and user logon domain identifier	• Operating Systems • Domain Controller • Directory Server • Name Service

		• The user identifier for the administrator or the software process identifier • The session identifier • The name of the transaction based application, application server or database server • A description of the action taken in respect of accountable transactions at the application layer • Outcome of transaction or command request (ie, success or failure, with any extended result code)	• DHCP Server • Application, Database, EMail Servers
5	User network account status changes to locked-out state should be alerted	The following shall be reported and an alert sent to a receiving console: • The username and user logon domain identifier	• Operating Systems • Domain Controller • Directory Server • Name Service • DHCP Server • Network Equipment or Network Management Console
6	Change in privilege level status of a user on a server or critical workstation	The following shall be reported: • The username and user logon domain identifier • The host device used • The session identifier for the user or process • The privilege level status (eg. normal, superuser, etc) of the user	• Operating Systems • Domain Controller • Directory Serve • Name or Directory Service
7	Invocation of any accountable user transaction (including interactions with applications and database servers)	The following shall be reported; • The host device used and user logon domain identifier • The user identifier for the administrator or the software process identifier • The session identifier • The name of the transaction based application, application server or database server • A description of the action taken in respect of accountable transactions at the application layer • A description of the outcome of the transaction or command request (eg. success, failure)	• Operating Systems • Domain Controller • Directory Server • Name or Directory Service • Application, Database, EMail Servers
Description of Control Process in Place			

PMC8 – Recording of Data Backup Status

Control Description

To provide a means by which previous known working states of information assets can be identified and recovered from in the event that either their integrity or available is compromised.

Providing and audit trail of backup and recovery operations is essential part of the backup process and will enable identification of the most reliable source of the prior know good states of the information assets to be recovered in the event of data corruption, deletion or loss.

The need for more sophisticated backup and recovery facilities are generally driven by higher levels of risk to Integrity and Availability properties.

There is a complimentary requirement for online storage failure events to be alerted, this is met by PMC4 Recordable Event 1 (the detection of any server storage failure should be classed as an alertable Critical event).

Specific Requirements

- All backup, test (verify) and recovery operations should be logged and reportable including completion status
- Failure of operation completion should be an alertable event

Recording & Accounting Requirements

Event ID	Recordable Event	Accounting Items	Potential Sources for Event Information
1	Backup, test and recovery operations	The following shall be reported: • The operation and parameters used for backup, test or recovery • The identification of the media or other storage method used for the backup (or archive) function • The result of the operation (success or fail)	• Operating Systems • Backup Management System • Media Library System
2	Backup, test and recovery operation failures should be alerted	The following shall be alerted: • The log entry for the failure should be referenced to the above corresponding report items	

Description of Control Process in Place

PMC9 – Alerting Critical Events

Control Description

To allow critical classes of events to be notified in a close to real-time as is achievable. The aware level requirement is for console based alerts that can be watched for by duty Security Managers.
It would be expected that extensive projects (with continuous monitoring requirement) would require a Security Operations Centre with summary wall displays (with the most complex scenario implementing redundant monitoring centres).

It should be noted that alerts themselves are recordable events.

Smaller projects can have a solution to fit their size and would typically only require a profile A solution with simple monitoring facilities (e.g. security and network management) provided this does not conflict with segregation requirements.

Secondary alerting channels may also be supported for projects that cannot provide continuous console manning (e.g. SNMP, email, SMS etc) via either in hours or out of hour's services.

Specific Requirements

- A summary alert message can be displayed on dedicated Security Manager console(s) that reflects all or part of the associated log message(s)
- Display of alerts of the same type occurring closely in time and consecutively should be throttled and aggregated into grouped alerts
- Any secondary alert channel should not contain information useful to an attacker and should provide a reference to corresponding log entries
- All alerts should be configurable and tuneable items

Recording & Accounting Requirements

Event ID	Recordable Event	Accounting Items	Potential Sources for Event Information
1	Alert messages routed to Security Manager console(s)	The following shall be reported and alerted: • The alert message contents • The log reference • The criticality of the alert • The count of records within individual log segments for aggregated logs passing along the log handling chain • Details of the receiving console	• Operating Systems • Other device logs • SNMP traps • Firewall/Firewall Console • SIEM, NBA, IDS or IPS • Network Management System or other Management Console System
2	Simple alert notifications sent via secondary channels (eg. emails, SMS, pager, etc)	The following shall be reported and alerted: • The log reference • The criticality of the alert • The channel identifier on which the secondary alerts are sent across (eg. emails, SMS, pager, etc)	• Network Management System • SIEM, NBA, IDS, IPS or other Management Console Systems
3	Configuration changes of alerts and secondary alerts	The following shall be reported: • The user identifier for the administrator or the software process identifier • The session identifier • User logon domain identifier • Message class	• Operating Systems • Domain Controller • Directory Server • Network Equipment or Network Management Console System • SIEM, NBA, IDS or IPS • Log Relay or Log

		• Alert options following change • Status of logging function	Collector System
Description of Control Process in Place			

PMC10 – Reporting on the Status of the Audit System

Control Description

To support means by which the integrity status of the collected accounting data can be verified.

The Aware segment requirements comprise the need to inspect log status on end devises and alerting of log error or other security relevant conditions.

Upper segment requirements expand to include the requirement for log collection and query systems (ultimately served as a resilient solution).

Smaller (especially single location) projects can have a solution to fit their size and would typically only require a profile level A solution without log collection facilities (perhaps assisted by COTS log analysis tools).

Specific Requirements

- Provide information on devise log status
- Alert log resets, error conditions, failures and threshold exceptions
- Provide a log collection facility with filtering capability
- Record automated log file rotation and collection actions
- Provide statistics on each log file collection within the accounting database.

Recording & Accounting Requirements

Event ID	Recordable Event	Accounting Items	Potential Sources for Event Information
1	Log resets, error conditions, failures and threshold exceptions	The following shall be reported and alerted: • Identifier for network device on which operation has occurred • Filename of active log file • Status of logging function	• Name Service or DHCP Server • Operating Systems • Log Relay or Log Collector System
2	Query status of active log storage on all devices on which logs are kept either locally or centrally plus log rotation information	The following shall be reported and alerted: • Identifier for network device being queried • Amount of space allocated for active log • Space used for active log and remaining free space • Number of records within active log • Log segment file produced by the log rotation system (each file holds a number of log messages) • Size of log segment file	• Name Service or DHCP Server • Operating Systems • Network Management System or other Management Console System • Log Relay or Log Collector System
3	Optionally, provide a time record of Event 2 information displaying trends	The following shall be reported: • Graphically representation of Event 2	N/A
4	Movement of segments and messages along the collection chain (message time-stamps should not be superseded	Each part of the chain requires the following to be reported: • Source of original log message • Device identifier for the log handler (within the log collection system) for the relevant part of the chain • Details of the produced segment or	• Name Service or DHCP Server • Operating Systems • Network Management System or other Management Console System • Log Relay or Log

		message files • The total number of segment or message files produced • Details of cryptographic has for the produced files	Collector System
5	Query at central collector(s) to provide a report of log sources	The following shall be reported (over a given time window): • List of all log sources • The transmission chain for the log files along to the ultimate log collector. • The number of messages with the time window and the log segment size	• SIEM, NBA, IDS or IPS • Log Relay or Log Collector System • Operating Systems • Device Logs
6	Optionally, provide a time record of Event 4 in graphical form, displaying trends over time	The following shall be reported: Graphically representation of Event 4	N/A
Description of Control Process in Place			

PMC11 – Production of Sanitised and Statistical Management Reports

Control Description

To provide management feedback on the performance of the protective monitoring system in regard of audit, detection and investigation of information security incidents.

Specific Requirements

- Management reports will typically be prepared outside of framework using office automation tools and rely on manually updated statistics
- Reports which include log extracts (etc) must be sanitised and have identifying and sensitive information removed (including, but not limited to, User identifiers, workstation identifiers and IP addresses)
- Some devises may be capable of producing web reports. These will also need to be sanitised if used for management reporting purposes
- If external MSSP services are used they may include customer made tailored reports, which can be directly used for management purposes. Assuming the content of these messages can negotiated or configured, they may be used directly
- One benefit of MSSP reports is that it may be possible to compare experiences against their pan-customer profile of security events (etc) to provide a broader perspective of events and trends.

Recording & Accounting Requirements

Exact report content requirement needs to be agreed with management and it needs to be ensured that the contents are readily digestible by the target community. The objectives of such reporting are to:

- Promulgate awareness of the current information security situation to management and staff
- Demonstrate the ongoing contribution and return on investment of Protective Monitoring services deployed on a project
- Support business cases for improvement
- Provide evidence for IA capability maturity assessment.

All reports need to be designed with this in mind, examples of appropriate content for management reports includes:

- Trends of attacks over current period plus history
- Performance of detection and defence mechanisms (including percentage ratio of: real alerts / (real + false alerts))
- Rolling "top 10" attacks experienced
- Geographic representation of where the attacks are coming from
- Statistics on internal violations
- Sanitised summaries of significant ongoing events or investigations
- Summary of current audit and compliance check results.

These will be combined with information from other sources (e.g. SIEM system) to provide a complete information security status report.

Due to the broad range of outputs possible no Accounting Recommendations table is provided for this risk treatment.

Requirements for management reports will largely dictated by the technology adopted for any given project.

The more advanced log management and SIEMs can be expected to provide report tem-plating as well as a series of proforma reports.

It is possible that some tools will support multiple purposes and can provide support for:

- Information security incident management
- Computer forensic investigations.

In these cases they should be able to provide complete information security status reports.

Description of Control Process in Place

PMC12 – Provide a Legal Framework for Protective Monitoring Activities

Control Description

To ensure that all monitoring and interception of communications is conducted lawfully and that accounting data collected by the system is treated as a sensitive information asset in its own right.

The most significant aspect of ensuring Protective Monitoring is lawful is ensuring that it is justified. A major part of the evidence for that justification is that the risk management process ensures there is neither too much nor too little.

There are certain aspects of user consent that need to be recorded as part of the system implementation. As for the other treatments the degree of rigour and trust in these increased along the scale of increasing segment. It is important to seek legal advice on compliance with the law and wording of all related screen messages and comments. Online electronic sign up may also be supplemented, or alternatively replaced, by manual records of user agreements and monitoring policies.

Specific Requirements

- At this level the recording of user logon captured by risk treatment PMC7 Recordable Event 1 satisfies the requirement
- This predicts that the system includes a logon warning screen that requires acknowledgment and / or consent of monitoring
- Can be augmented by specific electronic signup to a terms and conditions document (SyOPs) presented before and after first user logon (and repeated following every update to the terms and conditions). This can provide a more detailed approach and include more specific information regarding monitoring activities
- For this segment the user would be expected to click on buttons marked **[I Accept]** or **[I Decline]** or similar. A positive action is required to record consent.

Recording & Accounting Requirements

Event ID	Recordable Event	Accounting Items	Potential Sources for Event Information
1	User signup operations	The following shall be reported: • The username and workstation identifier on which signup occurred • Version number of signup terms and conditions • Recorded user reply (ie. Accept or Decline)	• Operating Systems • Domain Controller • Directory Server • Name Service • DHCP Server • Logon Scripting or E-Signing Application
2	It should be possible to configure alerts for user sign refusals (refusals may also prevent the user completing logon or suspend their account)	The following shall be alerted: • Log reference to corresponding to Event 1 for users who decline/refuse the signup requirement	

Description of Control Process in Place