Policy STRPOL14

APPENDIX A

Document Control

Description and Purpose

The Purpose of this Policy is to outline the Authority's approach to Protective Security

Active date	Review date	Author	Editor	Publisher
		Deb Appleton	Deb Appleton	

Permanent	X	Temporary		If temporary, review date must be 3 months or less.

Amendment History

Version	Date	Reasons for Change	Amended by

Risk Assessment (if applicable)

Date Completed	Review Date	Assessed by	Document location	Verified by(H&S)

Equalities Impact Assessment

Initial	Full	Date	Reviewed by	Document location

Civil Contingencies Impact Assessment (if applicable)

Date	Assessed by	Document location

Related Documents

Doc. Type	Ref. No.	Title	Document location
Service Instruction	SI0816	PROTECTIVE MARKING - GOVERNMENT SECURITY CLASSIFICATIONS AND GOVERNMENT PROTECTIVE MARKING SCHEME	
Service Instruction	SI0818	PERSONNEL SECURITY	
Policy	STRPOL09 and associated SIs	Information Governance and Security	

Contact

Department	Email	Telephone ext.
Strategy and Performance	debbieappleton@merseyfire.gov.uk	4402

arget audience

All MFrS	X	Ops Crews		Fire safety		Community FS			
Principal officers		Senior officers		Non uniformed					

Relevant legislation (if any)

DRAFT - PROTECTIVE SECURITY POLICY

STRPOL14

1. Policy Introduction and Background

Protective Security is the term used to describe the actions/policies required to meet the threats to an organisation and to protect its assets from compromise. Protective Security is important when considering the political climate and the technology that poses threats and risks to the Fire and Rescue Authority. Effective security is important in maintaining the confidence of the public, staff, stakeholders and partner agencies in efficient, effective and safe service delivery.

Protective Security is a holistic process that covers three related aspects of security; information (documents/data systems), personnel (staff/customers) and physical (buildings/estates/property).

2. Policy Explanation

This Policy outlines Merseyside Fire and Rescue Authority's (MFRA) approach to implementing protective security. Implementation of this policy and the supporting guidance reinforces the importance of Protective Security within every aspect of MFRA. This will be achieved by integrating a number of complementary security measures to create an approach that includes all three aspects. The aim of the policy is to achieve compliance, as far as practicable, with the relevant aspects of HMG Security Policy Framework, and as detailed within the DCLG Fire & Rescue Protective Security Strategy.

Underpinning the Policy are a number of complementary Service Instructions (SI) that provide guidance and detail in respect of the three protective security requirements. This policy and supporting policies and SIs reflect national policy, codes of practice and guidance. Protective Security is a collective responsibility for all staff and failure to comply with the requirements of this policy and associated SIs may result in disciplinary action.

3. Policy Implementation

Protective Security – Objectives

Appropriate personnel security, secure information systems, and practical but robust physical security measures are the core components of a secure working environment. The aim is to identify and value the assets of the Authority, understand the threat and vulnerability to these assets, determine any impact from loss or compromise, and ensure robust, proportionate controls are implemented through continuous security review.

In order to comply with the Fire and Rescue Services Protective Security Strategy MFRA will continue to implement secure methods of working. This will be supported and verified by internal audits and regular staff training in order to satisfy stakeholders of our security compliance.

Governance, Risk Management and Compliance

The implementation and management of Protective Security is led by the Deputy Chief Fire Officer who is responsible for taking an organisational lead on all aspects of protective security. He is supported by officers who fulfil the following roles designated in the Fire and Rescue Services Protective Security Strategy:

Service Security Officer (SSO) – Group Manager Operational Preparedness - Responsible for exercising day to day responsibility for all aspects of protective security; physical, personnel and information

Information Technology Security Officer (ITSO) – ICT Applications Manager - Responsible for the security of information held in MFRA,s ICT systems

Senior Information Risk Owner (SIRO) – Director of Strategy and Performance - Responsible for owning MFRA information risks

Information Asset Owners (IAO)- Senior individuals in each department responsible for the security of individual information assets (eg. records, databases ICT systems).

These officers (and others) and this policy, establish a framework by which we will deliver an effective approach to Protective Security.

Integrated Protective Security

Information Security

Information is a key asset and its correct processing is vital to the delivery of services and the integrity of the organisation. MFRA must strike the right balance between sharing and protecting information and manage the impact and risks associated with maintaining the confidentiality, integrity and availability of all information. This includes marking documents in line with The Government Protective Marking Scheme, ICT related security and information audit and governance. This includes potential disciplinary or criminal proceedings for users whose actions compromise protectively marked information

Personnel Security

The purpose of Personnel Security is to provide a level of assurance as to the trustworthiness, integrity and reliability of Service employees, volunteers and contractors. As a minimum requirement all staff will be subject to recruitment controls known as the Baseline Personnel Security Standard. For more sensitive posts there are a range of security controls referred to as 'National Security Vetting'; these are designed to ensure that such posts are filled by individuals who are unlikely to be susceptible, for whatever reason or motive, to influence or pressure which might cause them to abuse their position.

All Departments will employ a risk management approach to Personnel Security to comply with protective security principles, seeking to reduce the risk of damage, loss, or compromise of Authority assets by the application of personnel security controls before and during employment. These controls do not provide a guarantee of reliability and must be supported by continuous and effective line management.

Physical Security

Providing an appropriate and proportionate range of measures to protect the Authority's buildings, estate, vehicles, equipment and other property is a key requirement of this Policy. Physical Security involves a number of distinct security measures which form part of a Service-wide approach to security that takes account of the balance between prevention, protection and response.

Associated Service Instructions [included in the document control sheet]