



This is an unpublished work, the Copyright in which vests in Merseyside Fire & Rescue Service. All rights reserved. The information contained herein is the property of Merseyside Fire & Rescue Service, and is supplied without liability for errors or omissions. No part may be reproduced or used except as authorised by Contract or other written permission. The Copyright and the foregoing restriction on reproduction and use extend to all media in which information may be embodied ©

**Document Control:**

Active date	Review date	Author	Editor	Publisher
April 2014	April 2028			

**Amendment History:**

Version	Date	Author	Reasons for Change
1.2	01/04/15	Annual Review	
1.3	4/7/16	Annual review (no changes)	
1.4	13/6/17	Annual Review (no changes)	
1.5	01/04/18	Annual Review (no changes)	
1.6	01/04/19	Annual review (no changes)	
1.7	01/04/20	Annual review (no changes)	
1.8	01/04/21	Annual review (no changes)	
1.9	01/04/23	Minor changes to titles	
1.10	April 2024	Annual review and procedural changes	
1.11	10/03/25	Annual review	
1.12	March 2026	Annual review	

**Equalities Impact Assessment:**

Initial	Full	Date	Reviewed by	Comments
	X		ED&I TEAM	LOCATED ON PORTAL

**Civil Contingencies Impact Assessment:**

Date	Reviewed by	Comments

**Related Documents:**

Doc. Type	Ref No.	Title	Location
Service Instruction	SI 0816	Protective Marking – Government Security classifications & Government Protective Marking Scheme	
Service Instruction	SI0818	Security Vetting	
	STRPOL09	Information Governance and Security	

**Distribution List:**

Name	Position	Department
ALL MFRS		

**Sign-Off List:**

Name	Position
SMG	All members

**Target Audience:**

All MFRS	Principal Officers	Senior Officers	Operational Crews	Fire Safety	Community Fire Safety	Support Staff
X						

**Ownership:**

FOI exemption	Yes	URL

required?	No	X	Reason	
-----------	----	---	--------	--

**Legislation:**

Title	Government Security Classifications Policy 2014
-------	---

**Contact:**

Department	Email	Telephone ext.
STRATEGY & PERFORMANCE		

## STRATPOL14 Protective Security Policy

### 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, The NFCC Joint Guidance of DBS eligibility checks from FRA roles, and as detailed within the Government's 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 Data Protection Officer (Director of Strategy and Performance) who is responsible for taking an organisational lead on all aspects of protective security. This officer 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. This is delivered via our Security Vetting Process.

Under security vetting as a minimum requirement all staff will be subject to recruitment controls known as the Baseline Personnel Security Standard. The Baseline Personnel Security Standard comprises verification of four main elements:

- Identity
- Employment history
- Nationality and immigration status
- Criminal record Check

Disclosure and Barring Service (DBS) Criminal Records checks are completed as part of the BPSS. DBS applications are processed by MFRA using an online application Service provided by Atlantic Data who are a registered Umbrella Body with the DBS.

The DBS service helps employers make safer recruitment decisions by processing and issuing DBS checks for England and Wales. DBS also maintains the Adults' and Children's Barred Lists and makes considered decisions as to whether an individual should be included on one or both of these lists and barred from engaging in "regulated activity". From a DBS and eligibility point of view, the role is not important; it is the activity being carried out which should be used to determine eligibility for DBS checks.

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.

As MFRA co-locate with Merseyside Police some staff will require Non-Police Personnel Vetting Level Two Abbreviated (NPPV2a) to access certain parts of our estate.

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]

All policies can be found on the [Website](#)

POLICY