MERSEYSIDE FIRE AND RESCUE AUTHORITY			
MEETING OF THE:	**POLICY AND RESOURCES COMMITTEE**		
DATE:	**1 APRIL 2014**	**REPORT NO:**	**CFO/012/14**
PRESENTING OFFICER	**DEPUTY CHIEF FIRE OFFICER**		
RESPONSIBLE OFFICER:	**DEB APPLETON**	**REPORT AUTHOR:**	**DEB APPLETON**
OFFICERS CONSULTED:	**PROTECTIVE SECURITY GROUP**		
TITLE OF REPORT:	**PROTECTIVE SECURITY POLICY AND RELATED SERVICE INSTRUCTIONS**		

APPENDICES:	**APPENDIX A:**	**DRAFT PROTECTIVE SECURITY POLICY**
	APPENDIX B:	**DRAFT PROTECTIVE MARKING SERVICE INSTRUCTION**
	APPENDIX C:	**DRAFT PERSONNEL SECURITY SERVICE INSTRUCTION**
	APPENDIX D:	**EQUALITY IMPACT ASSESSMENT**

Purpose of Report

1. To request that Members consider and approve the attached Policy and Service Instructions that have been developed to enable the Authority to implement the requirements of the Government's Protective Security Strategy.

Recommendation

2. That Members approve the Protective Security Policy, Protective Marking Service Instruction and Personnel Security Service Instruction attached as appendices A, B and C respectively. All of these documents have been through the Authority's consultation process with some minor changes being made as a result.

Introduction and Background

3. 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).

4. The Authority's aim 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. There are close links with Information Security and Governance, resilience, ICT security and building management. A working group with representatives from all related areas has been set up to implement the requirements of the Fire and Rescue Service Protective Security Strategy and Protective Security related roles, as set out in the FRS Strategy, have been allocated to staff as outlined below:

   Protective Security Lead - Deputy Chief Fire Officer
   Service Security Officer (SSO) – Group Manager – Operational Preparedness
   Information Technology Security Officer (ITSO) - ICT Applications Manager
   Senior Information Risk Owner (SIRO) - Director of Strategy and Performance
   Information Asset Owners (IAO) – at least one employee has been allocated this role in each department

5. The working group has produced the draft Protective Security Policy (Appendix A) which sets out how MFRA intends to comply with these requirements in general terms. In addition two new draft Service Instructions (attached at Appendices B and C) set out in more detail how new processes will be implemented to deliver against two important aspects of Protective Security; protective marking of information assets and personnel related security. Information Asset Owners are currently being given guidance as to their role and other Service Instructions will be developed as required to either enhance existing arrangements or introduce any new processes that are identified by the working group.

Protective Marking

6. Protective marking of information assets is an important element of Protective Security as it allows for a co-ordinated way of implementing an appropriate level of protective controls against the likely threat to sensitive information. The current scheme used is the Government Protective Marking Scheme, but this will change to the Government Security Classifications (GSC) on 2nd April 2014. As a result, it is proposed that MFRA starts to mark its information assets using the new GSC system and this is reflected in the Service Instruction. As this is a major piece of work the Authority will take a risk based approach with the Protective Security lead officers working with the Information Asset Owners to identify when information assets should be marked.

Personnel Security

7. 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. The draft Service Instruction sets out that as a minimum requirement all staff will be subject to recruitment controls known as the Baseline Personnel Security Standard. This consists of the verification of unspent criminal records. This will however be phased in, beginning with new recruits. Information Asset Owners will then work with the Protective Security

lead officers to identify in which order departments or staff require the checks to be carried out according to the Protective Security risk associated with each department. The other enhanced vetting processes referred to within this Service Instruction apply to a very small number of senior staff and are already in place.

Equality and Diversity Implications

8. An Equality Impact Assessment has been carried out and the initial findings are attached. The EIA will be reviewed and updated as the implementation of Protective Security progresses.

Staff Implications

9. There are implications associated with the implementation of the Baseline Personnel Security Standard as this involves the use of a new security check. However, enhancing Personnel Security is essential for compliance with the requirements of the Protective Security Strategy and these implications are currently being considered by People and Organisational Development.

Legal Implications

10. The Authority is a Category 1 responder under the Civil Contingencies Act 2004 and as such has a duty to assess, plan and advise in relation to certain emergencies. The Authority has a duty to keep information it holds in relation to this duty secure and this policy seeks to ensure the security of such information.

11. The Authority has duties under the Data Protection Act 1998 to keep personal information secure and should take steps to ensure such data is protected against loss or theft. This policy is one of a number of measures in place to protect personal information ensuring compliance with these statutory obligations.

Financial Implications & Value for Money

12. There are financial implications associated with the implementation of the Baseline Personnel Security Standard across the Service. Initially this will be limited to new recruits. This will however extend to all other staff through the risk based approach, which will take some time. Each check costs £25 and the current budget is £1,500 which limits the rate at which the process can be implemented.

Risk Management, Health & Safety, and Environmental Implications

13. Protective Security is a strategy to reduce risk, so all parts of the Strategy will help to improve Merseyside Fire and Rescue Authority's resilience.

14. There are some risk implications in relation to storing RESTRICTED and potentially OFFICIAL-SENSITIVE information on the MFRA network, but it is considered that it is operationally important to do so and systems will be put in place to ensure that information is kept as securely as possible.

15. There are no health, safety or environmental implications.

Contribution to Our Mission: *Safer Stronger Communities – Safe Effective Firefighters*

16. Implementation of the Protective Security Strategy will help improve security within all areas of Merseyside Fire and Rescue Authority.

BACKGROUND PAPERS

GLOSSARY OF TERMS