London Ambulance Service NHS Trust

Security Management Policy

DOCUMENT PROFILE and CONTROL

Purpose of the document: This policy details the processes by which the London Ambulance Service will effectively manage security across its activities

Sponsor Department: Health, Safety and Risk

Author/Reviewer: Local Security Management Specialist. To be reviewed by April 2018.

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
24/11/2015	1.4	IG Manager	Document Profile & Control update and minor change
28/04/2015	1.3	Local Security Management Specialist	Reviewed and minor amendments: To SMD; references to the Internal Security Review Group removed; Added references to Senior Managers and Managers replacing ADOs, AOMs, DSOs and Team Leaders
03/08/2012	1.2	IG Manager	Document Profile & Control update
04/07/2012	1.1	Local Security Management Specialist	Minor amendments – including updated monitoring section
31/05/2011	0.1	Local Security Management Specialist	New policy development

***Version Control Note:** All documents in development are indicated by minor versions i.e. 0.1; 0.2 etc. The first version of a document to be approved for release is given major version 1.0. Upon review the first version of a revised document is given the designation 1.1, the second 1.2 etc. until the revised version is approved, whereupon it becomes version 2.0. The system continues in numerical order each time a document is reviewed and approved.

For Approval By:	**Date Approved**	**Version**
ADG	24/02/12	1.0
Ratified by (If appropriate):		
SMG	11/07/12	1.1

Published on:	**Date**	**By**	**Dept**
The Pulse	25/11/15	Governance Administrator	G&A
The Pulse	06/08/12	Governance Co-ordinator	GCT
LAS Website	25/11/15	Governance Administrator	G&A
LAS Website	06/08/12	Governance Co-ordinator	GCT
Announced on:	**Date**	**By**	**Dept**
The RIB	07/08/12	IG Manager	GCT

Equality Analysis completed on	By
20th September 2011	Local Security Management Specialist
Staffside reviewed on	**By**
13th September 2011	Staffside Representative

Links to Related documents or references providing additional information		
Ref. No.	**Title**	**Version**
TP/005	Risk Management Policy	**v.7.1**
TP/035	Risk Assessment and Reporting Procedure	
TP/048	Information Security Policy	**v.2.1**
HS/001	Health & Safety Organisation – Policy Statement	
HS/012	Violence Avoidance and Reduction Procedure	**v.3.2**
OP/001	Uniform Work Wear Policy	**v.4.1**
OP/018	Procedure on Station Duties	
SA20 NHS Protect	Counter Terrorism Guidance	
	Olympic and Paralympic Games Counter Terrorism Security Guidance (Ambulance Sector)	**2012**

Document Status: This is a controlled record as are the document(s) to which it relates. Whilst all or any part of it may be printed, the electronic version maintained in P&P-File remains the controlled master copy. Any printed copies are not controlled nor substantive.

1. Introduction

The London Ambulance Service (LAS) is committed to ensuring the safety and security of its employees and any other persons affected by its activities and the assets of the organisation. The LAS seeks to control and manage security effectively through compliance with the requirements of this policy document. However, it must be realised that, by the nature of the work that the LAS carries out, it is not possible to be able to control the environment in which staff operate when away from LAS premises.

Working closely with NHS Protect (formerly the NHS Counter Fraud and Security Management Service – CFSMS) and together with staff, the LAS is committed to addressing safety and security issues in a proactive way. This process will involve employing good safety and security systems including risk assessment, planning, quarterly inspections and compliance auditing.

2. Scope

The Trust will ensure, so far as is reasonably practicable, the health, safety and welfare of employees and those affected by Trust actions. People are the most important asset of the Trust, and the Trust recognises that their security, safety and welfare and that of others affected by its activities is paramount. The Trust also recognises how information governance / security is a crucial part of security management.

2.1 The overriding principle of this policy is that the Trust will adopt measures to protect employees together with those working on our behalf and property against incidents of breaches of security from criminality (which, within this document will include all acts of terrorism and espionage). In addition, where possible, the Trust will pursue appropriate sanctions against those who have abused its employees and others working on behalf of the Trust through incidents of assault, verbal abuse or other criminality.

2.1.1 In addition the Trust will strive to ensure that physical assets, whether they are premises, equipment or vehicles are kept secure and the potential for theft or criminal damage is minimised.

2.1.2 The Trust will achieve these objectives by adopting the seven principles published by NHS Protect (NHSP):

- Creating a “pro-security“ culture amongst staff and the public; a culture where the responsibility for security is accepted by all, ensuring that security procedures and systems are adhered to. Where a culture of challenge is engendered and where the actions of those who breach security will not be tolerated.

- Deterring those who may be minded to breach security, using publicity to raise awareness of what the consequences of their intended actions could be personally and to the NHS.

- Preventing security incidents or breaches from occurring, wherever possible, or minimising the risk of them occurring, learning from operational experience and sharing best practice.

- Detecting security incidents or breaches and ensuring these are reported in a simple, consistent manner to NHSP.

- Investigating security incidents in a fair, objective and professional manner, to ensure those responsible for such incidents are held to account for their actions.

- Applying a wide range of sanctions against those responsible for security incidents, involving a combination of procedural, disciplinary, civil and criminal action as appropriate.

- Seeking redress through the criminal and civil justice systems against those who commit security incidents or breaches, whose actions lead to loss of NHS resources and to ensure that victims are fully supported.

3. Objectives

3.1 The aim of this document is to help achieve the vision of the LAS by facilitating the delivery of an environment which is properly secure for those who work for or use the Trust, so that the highest possible standard of clinical care can be made available.

3.2 The Security Management Policy is intended as an over-arching policy to enable a local framework for the management of security within the LAS. This policy links to a series of policies and procedures which cover violence and aggression, property, uniform and assets and any other relevant security polices and/or procedures designed to meet the security needs of the organisation and its staff as and when they are produced.

3.3 This policy should be read with reference to the Risk Management Policy (TP/005), the Health and Safety Organisation Policy Statement (HS-001), the Uniform Work Wear Policy (OP/001), The Procedure on Station Duties (OP/018) and all other policies, procedures and guidance produced in relation to security, fraud and emergency planning within the LAS, together with relevant guidance from NHSP, where appropriate, such as (but not limited to): SA20 Counter Terrorism Guidance and Olympic and Paralympic Games Counter Terrorism Security Guidance (Ambulance Sector).

3.4 This document applies to all full and part-time members of staff who are either directly employed or contractor members of staff and sets out the general principles and structure of security within the LAS. It will form an

"overarching policy" under which other policies relating to security will rest, such as (but not limited to) policies / arrangements dealing with: violence and aggression (*please note that patient on patient and staff on staff violence fall outside this policy), security of assets, lockdown, access control, staff identification and uniform and fraud.

3.5 Policy objectives are:

3.5.1 To seek to address issues relating to violence against staff.

3.5.2 To protect NHS property and assets and in particular ensure the security of: premises, vehicles, equipment and uniforms belonging to the LAS and to ensure that disposal of any of these is done securely and follows the appropriate procedure.

3.5.3 To seek to ensure the security of drugs and hazardous materials.

3.5.4 To seek to ensure the security of vulnerable and sensitive areas and information within the LAS.

3.5.5 To seek to protect the Trust against those who would bogusly present themselves as LAS staff.

4. Responsibilities

4.1 Trust Board

Corporate responsibility for the Trust's system of internal control and for robust risk management. The Trust Board is responsible for setting the strategic direction and corporate objectives for the Trust. It discharges its functions through a delegated structure designed to ensure effective risk management (see TP/005 Risk Management Policy and Strategy).

4.2 Chief Executive

As Accountable Officer, the Chief Executive is ultimately accountable for the effective security of the LAS and implementation of this policy and has delegated this responsibility to the Director of Human Resources and Organisation Development as the Trust's Security Management Director.

4.3 Security Management Director (SMD)

(Currently the SMD is the Director of Corporate Affairs) The SMD is responsible for ensuring that adequate security management provision is made within the LAS, promoting security at board level, and for monitoring and ensuring compliance with the requirements and directions issued by the Secretary of State, the Department of Health and NHSP relating to security.

4.4 Non Executive Security Director

Responsible for ensuring that the business of the Trust does not compromise the requirements and directions issued by the Secretary of State, the Department of Health and NHSP relating to security.

4.5 Director of IM&T

The Director of IM&T is the Senior Information Risk Owner (SIRO) and is accountable to the Trust Board for electronic information governance and security and responsible for ensuring that electronic information is managed effectively and securely throughout the Trust and that the Trust has appropriate data encryption capabilities in order to protect data that is processed on removable media and reporting information security risks to the Risk, Compliance and Assurance Group.

4.6 Directors

Responsible for ensuring that the principles and guidelines issued to assist in preventing and detecting incidents of violence and abuse, or those for enhancing the security of Trust are implemented within their directorates.

4.7 Corporate Health and Safety Group

The Corporate Health and Safety Group will receive and monitor the results of the quarterly premises inspections and reports relating to security incidents and report to the Risk Compliance and Assurance Group and the Senior Management Group (SMG) as appropriate.

4.8 Information Security Manager

Responsible for maintaining and reviewing information processing systems against key controls to ensure Information Security is maintained, identifying and implementing any configuration requirements required to comply with NHS Information Governance security policy and standards. This includes data encryption capabilities and assuring that the data encryption functionality and procedures used with removable media have been implemented correctly, are of appropriate strength and fit for purpose.

4.9 Local Security Management Specialist (LSMS)

Responsible for assisting the Trust to realise the requirements and directions issued by the Secretary of State, Department of Health and NHSP relating to security.

- Responsible for ensuring that the SMD is fully aware of security issues which may affect the Trust, its staff, patients or the levels of service which it offers.

- Responsible for informing the Internal Security review Group of security issues which may affect the Trust and presenting security surveys to the group from which risk assessments and action plans will be developed.

- To advise on crime reduction measures for Trust properties and activities where employees, patients, the public or Trust assets may be at risk.

- To provide specialist information, guidance and training to assist directors, managers and staff in the performance of tasks and duties relating to security.

- Investigate security incidents in accordance with established practice and legislation and liaise with the Police, NHSP and other relevant parties to secure suitable sanction where necessary.

- To advise the Corporate Health and Safety Group on security issues, events and statistics within the LAS and where appropriate recommend actions to be taken.

- Liaise with the Police, NHSP, the Centre for the National Protection of Infrastructure (CPNI), Counter Terrorism Security Advisors CTSAs) and other stakeholders and act on their behalf as required in the best interests of the LAS, to safeguard the Trust, and it's activities.

- The LSMS will liaise with the Trust's Local Counter Fraud Specialist (LCFS) where security issues are raised by theft cases. The LCFS will be the first point of contact in such cases and will liaise with the Police as necessary.

- The LSMS will communicate with the police together with the CPS and/or any other appropriate body / stakeholder to pursue an appropriate outcome and who will also ensure that the member of staff has been / is being sufficiently and appropriately supported.

- The LSMS will produce a written work plan outlining their security management work priorities for the coming year and an annual report of progress in meeting the work priorities at the end of the year.

- The LSMS will ensure that all reported incidents of breaches of security are reported to NHS Protect via the Security Incident Reporting System (SIRS).

4.10 Senior Managers

Senior Managers (as defined by the Senior Managers' Conference list and likely to be a head of department or senior lead for an operational complex or number of stations) are responsible for the management of risk locally and for day to day implementation of policies and strategy within their own area, the security of staff, vehicles, buildings and assets within their areas of operational responsibility and of ensuring that security principles and

guidelines are implemented and that staff are supported in implementing these and comply with such procedures issued to assist in preventing, reducing and detecting incidents of security breaches (eg violence, aggression, intrusion and theft) together with those for safe disposal of assets and for maintaining the security of the LAS, in line with Line Managers' responsibility to enforce and enact the Trust's policies, procedures and initiatives

Examples of Responsibilities:

- Initiate appropriate action according to Trust policies procedures and initiatives where necessary.
- Develop and maintain channels for effective three-way communication within the operational structure i.e. staff/employees, external environment and the corporate whole of the LAS. Ensure that all staff are aware of and understand the policies and procedures of the Trust.
- Ensure that all incidents are properly reported (using LA52/277), thoroughly investigated, and graded, ensuring that lessons are learnt from such incidents and that the outcomes are reported appropriately.
- Actively support members of staff who have been the victim of either physical or verbal abuse, or any other form of harassment at work.
- Undertake and follow up quarterly premises inspections, signing them off and resolving, where possible, matters locally or informing other appropriate departments (HS/001).

4.11 Managers (DSOs and Team Leaders)

Part of the operational, station and complex management team, Managers ensure that staff are fully supported and that station premises, vehicles and equipment are well maintained and remain available at all times, taking remedial action as appropriate, enforcing and enacting the Trust's policies, procedures and initiatives.

- Manage staff according to LAS policy.
- Act as managerial support and deal effectively with staff welfare issues.
- Ensure that staff operate in a safe working environment and resolve and related problems as quickly as possible.
- Provide managerial support to deal with problems at scenes of incidents and on station.
- Carry out investigations and provide reports as necessary liaise with and support the work of investigating officers and report on updates of progress and outcomes of incident investigations to the LSMS.

4.12 Local Counter Fraud Specialist (contracted out)

Undertakes a range of activities to counter fraud within the Trust on a local level.

4.13 Emergency Preparedness Unit (EPU)

Provide specialist expertise in Major Incident response and event management. Custodian of the Major Incident Plan and provider of major incident training. Authors of contingency plans to meet external requirements/risks/threats. Available to attend scenes or provide advice by phone. Able to support Gold Command and support Silver Command at scene as required.

4.14 Health, Safety & Risk

Provides advice throughout the organisation on matters relating to Health and Safety. Co-ordinates and advises as required on all Corporate Health and Safety Risk assessments in order to minimise those risks to an acceptable level to help ensure the provision of a safe working environment and equipment that is suitable and fit for the intended purpose.

4.15 Estates

Responsible for the provision/issuing of ID passes, following line manager's authorisation, in line with security guidance and to appropriately prioritise security related Estates issues that have been reported so that the LAS, its staff or assets are not left vulnerable to any breaches of security. To liaise with the LSMS over such issues and raise any concerns over the security of LAS premises.

4.16 Logistics

The ADO for logistics is responsible for the safe disposal of vehicles in accordance with SA20C 'Security considerations for ambulance decommissioning and disposal' (NHS Protect).

4.17 All employees

Responsible for following policies, procedures and initiatives of the LAS and reporting all security incidents in which they are the victim (i.e. they have been abused, assaulted or had property stolen) or they witness or of which they become aware (e.g. unauthorised access, theft of or damage to property etc).

- Responsible for co-operating with the principles and guidelines issued to assist in preventing and detecting incidents of violence and abuse, or those for enhancing the security of the LAS, and in line with Procedure on Station Duties (OP/018).

- Must make dynamic risk assessments for all incidents to which they respond, to assess the potential for danger or injury to themselves and balance their obligations of providing emergency healthcare with the safety of themselves, patients or other members of the public .

- To take personal responsibility to ensure that they have a pass / ID on them at all times while on Trust property / duty (see Uniform Work Wear Policy OP/001).

5. Definitions

5.1 Stakeholders:

- **NHS Protect (NHSP) –** Part of the NHS Business Service Authority. NHSP has overall responsibility for all policy and operational matters related to the management of security within the NHS.

- **CPNI –** Centre for the Protection of National Infrastructure is a government organisation that provides security advice to businesses across the national infrastructure.

- **CTSA (**Counter Terrorism Security Advisor) **-** Police Counter Terrorism Security Advisor providing protective and counter terrorism security advice to support businesses taking into account both conventional and non-conventional terrorist techniques with the aim of reducing any vulnerability to terrorist threats.

5.2 General Definitions:

- **Espionage –** The act of inappropriately obtaining protected information without authorisation.

- **Terrorism –** The systematic use of violence and intimidation through fear and threats to achieve a goal.

- **Lockdown -** Lockdown is the process of controlling the movement and access – both entry and exit – of people (NHS staff, patients and visitors) around a trust site or other specific trust building/area in response to an identified risk, threat or hazard that might impact upon the security of patients, staff and assets or, indeed, the capacity of that facility to continue to operate. A lockdown is achieved through a combination of physical security measures and the deployment of security personnel.

- **SIRS –** Security Incident Reporting System. This is an electronic portal that requires NHS organisations to report all incidents of security breaches directly to NHS Protect and it will enable each organisation to use the data collected for management reporting purposes. The numbers of reported incidents are audited annually and the audited results are then published.

- **Security Incident –**
  - Verbal abuse or physical assault
  - Property (including physical and intellectual assets, including information) is stolen, damaged or compromised

- Unauthorised access
- Bombing / bomb hoax
- Shooting
- White powder / white powder hoax (designed to cause fear by use of a contaminant eg chemical, biological, radiological).

5.3 Criminality:

- **Physical Assault -** The intentional application of force to the person of another, without lawful justification, resulting in physical injury or personal discomfort.

- **Non Physical Assault –** The use of inappropriate words or behaviour causing distress and / or constituting harassment.

- **Criminal Damage -** When any individual, without lawful excuse, destroys or damages property belonging to another, intending to destroy or damage such property or being reckless as to whether such property is destroyed or damaged.

- **Theft -** The dishonest appropriation of property belonging to another with the intention of permanently depriving the other of it.

- **Robbery –** The threat or use of violence at the time, or immediately prior to stealing, putting any person in fear of being then and there subjected to force

- **Burglary –** Entering any building, or part of a building, with the intent of stealing anything or inflicting anyone with grievous bodily harm or actually stealing or inflicting grievous bodily harm on anyone or of doing unlawful damage to the building or anything within it.

- **Taking a Motor Vehicle (or Other Conveyance) without Authority –** Taking any conveyance for own or another's use, without having the consent of the owner or other lawful authority or, knowing that any conveyance has been taken without such authority, driving it or allowing oneself to be carried in it.

- **Handling Stolen Goods -** Dishonestly receiving goods known or believed to be stolen, or dishonestly undertaking or assisting in their retention, removal, disposal or realisation by or for the benefit of another person, or arranging to do so. (Stolen goods includes not only goods physically stolen but also those obtained by blackmail or fraud).

- **Blackmail -** Making an unwarranted demand with menaces with a view to gain for self or another or with intent to cause loss to another unless done so with reasonable grounds for making the demands or that the use of menaces is a proper means of reinforcing the demand.

- **Fraud -** Fraud is a type of crime which can be difficult to identify. A non-violent and sometimes entirely paper-based activity, fraud tends towards being invisible and there may not be any immediately apparent victim. The Fraud Act 2006 created new offences which include: Fraud by false representation, fraud by failing to disclose information, fraud by abuse of position, possession etc of articles for use in frauds, making or supplying articles for use in frauds, obtaining services dishonestly. Fraud within the LAS is targeted by the Local Counter Fraud Specialist (LCFS), and while a secure environment will have robust defences against acts of fraud and these will form part of the security measures within the LAS, it is not the intention within this document to detail fraud types and counter fraud measures. Further information can be obtained from the Trust's LCFS.

6. Incidents

6.1 All incidents of security breaches, no matter how small, are to be reported via an incident report form (LA277 for violence and aggression, LA52 for all other incidents) and directly to the local management team / line manager who will liaise with the LSMS. By reporting all such incidents, necessary action can be taken, lessons learnt and future risks minimised.

6.2 It is important, especially for any violence or abuse related incidents, that all relevant information is obtained:

- the assailants/patients full details (name, address etc.)
- full description details of the incident
- exact location details of the incident
- full details of injuries sustained, which may include photos
- full details of any Police Officers attending the scene including contact telephone numbers, collar numbers and station deployed from
- full details of any witnesses to the event
- information regarding any immediate action taken by the manager.
- Details of the follow-up investigation, detailing reasons why the incident may have happened, what learning has come out from the incident and any measures being put in place to help reduce the likelihood or prevent future similar events.

7. Risk Assessments

7.1 The LSMS produces a work plan towards the end of each financial year, which will include a programme of security risk assessments / surveys to be undertaken during the following financial year and may include risk assessments relating to;

- Physical security - of buildings and objects
- Premises – the physical buildings in which Ambulance staff and other professionals work, where patients are treated and from where the business of the Ambulance Service is delivered

- Assets – irrespective of their value, this includes materials and equipment used to deliver healthcare. In respect of staff, professionals and patients this also relates to personal possessions they retain whilst working in or providing services to the Trust
- Prevention and management of violence and aggression

7.2 Where appropriate, a local safety or security risk assessment to identify areas where aggression or violence, theft, loss or security problems are likely, will be undertaken by managers and /or their delegated representative with support from the LSMS as appropriate. This may lead to changes in workplace layout, identification of training needs, etc, as specified in the developed action plans resulting from the risk assessment.

7.3 The completed risk assessment will be retained on the premises it relates to for future reference of staff and others as necessary. A copy will also be sent to the LSMS.

7.4 The line manager is responsible for discussing the procedures and issues arising from the risk assessment with their manager and the LSMS before implementation.

7.5 Discussions between the LSMS and local manager will include a decision of where the identified risks should be placed;
- Local risk register
- Escalated via The Corporate Health & Safety Group

7.6 Risk will be reported, recorded and reviewed in accordance with the detail described within TP/035 Risk Reporting and Assessment Procedure.

8. Lockdown Risk Profile

8.1 There will be a risk assessment of each LAS site to determine its potential vulnerability to threat (criminal or terrorist) and its capability, if any, of either partial or full lockdown, with reference being made to the ambulance service specific guidance on lockdown produced by NHS Protect.

9. Consultation

Organisations cannot implement effective security measures operating independently. To be effective they need to work in conjunction with and in consultation with partner agencies.

9.1 There are benefits in working with other agencies, particularly in ensuring best practise on safety and security issues.

9.2 Sharing information and having consistent policies and procedures will assist in avoiding problems arising, or in reducing risks when unavoidable.

9.3 Representation by the LSMS of the LAS on appropriate Internal and National Ambulance Service Security sub-groups is therefore essential for the Trust to maintain effective security for all staff, premises and assets, in line with partner organisations.

9.4 Partners in this sense include patients, staff, other NHS Trusts, NHS Protect and the Centre for Protection of National Infrastructure (CPNI) Local Police Authorities, Local Authorities, Consultants and Contractors.

9.5 The Trust Board is committed to the implementation of a two-way communication process utilising various routes in order to ensure that information is timely and effective. This requires managers to adopt good communication leading to an understanding of the correct information being relayed on which decisions may need to be taken.

10. Effectiveness

10.1 A key part of the monitoring and auditing process is the role of information obtained from the Trust's Incident Reporting procedure in addition to the security surveys and subsequently developed risk assessments and action plans.

10.2 The Trust will examine all incidents including “near misses” that are recorded on the Incident Reporting system. This should highlight concerns and emerging trends, which will enable procedures and practices to be introduced or changed where necessary to improve the security environment of the Trust.

IMPLEMENTATION PLAN TEMPLATE	
Intended Audience	All LAS Staff
Dissemination	Available to all staff on the Pulse and to the public on the LAS website
Communications	Policy to be announced in the RIB and a link provided to the document
Training	The LAS may make provision for all staff to receive instruction and training to allow them to carry out their duties without risk of injury. Specifically, Conflict Resolution Training (CRT) and CRT refresher training will be provided to operational staff. Local Security Leads will be able to access training from the LSMS specifically on what is expected from their role and how they can access further guidance from the LSMS.

Monitoring:

Aspect to be monitored	Frequency of monitoring AND Tool used	Individual/ team responsible for carrying out monitoring AND Committee/ group where results are reported	Committee/ group responsible for monitoring outcomes/ recommendations	How learning will take place
Duties (paragraph 4)	Quarterly Premises Inspections	Senior Health, Safety and Risk Advisor reports to the Corporate Health and Safety Group	Senior Management Team (SMT).	Dissemination of changes to practice, training and lessons via the Area Quality Committees
How the organisation risk assesses the physical security of premises and assets (paragraph 7)	Quarterly update of risk assessments carried out	LSMS reports to The Corporate Health and Safety Group		
How action plans are developed as a result of risk assessments (paragraph 7)	Quarterly update of action plans resulting from risk assessments			