London Ambulance Service NHS Trust

Information Security Policy

DOCUMENT PROFILE and CONTROL.

Purpose of the document: An effective Information Security Policy provides a sound basis for defining and regulating the management of information systems and other information assets.
This is necessary to ensure that information is appropriately secured against the adverse effects of failures in confidentiality, integrity, availability and compliance which could otherwise occur.
The specific objectives of this policy and other supporting security policies, procedures and mandates are to:

- Convey to all LAS users, through consistent policy statements, how information assets are to be safeguarded from unauthorised access, modification or deletion;
- Describe the required standards for the acceptable use of information systems and the requirements for accessing and disclosing information assets in accordance with regulations and applicable laws;
- Specify the minimum requirements that allow the LAS to avoid, detect, manage and recover from security incidents with the least disruption to the organisation;
- Ensure delivery partners, including offshore service providers, comply with LAS information security requirements and handle LAS data appropriately;
- Enable LAS to make the best use of its investment in ICT systems and enable the Trust to deliver a first rate service.

.

Sponsor Department: IM&T

Author/Reviewer: To be reviewed by Information Security Team by May 2019.

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
25/05/18	5.1	IG Manager	Document Profile and Control update
15/05/18	4.1	Principal Cyber Security Specialist	GDPR update
05/03/18	3.4	Jacques Du Toit	Peer reviewed
05/02/18	3.3	Giles Thornton	Full review to meet Cyber Essentials requirements and allow for production of supplementary policies
21/12/15	3.2	IS/IG Managers	Addition to S.5.1g to include Cyber Security
10/11/14	3.1	IG Manager	Document Profile and Control update
16/09/14	2.4	IG Manager	Addition of reference following IGG approval and Document Profile and Control update.
15/07/14	2.3	IS Manager	Updated section 4 and introduced new paragraphs in section 5.
25/03/13	2.2	IG Manager	Addition of Implementation Plan

28/05/12	2.1	IG Manager	Doc Profile & Control update
21/12/11	1.5	IS Manager & IG Manager	Further revisions following IGG.
16/12/11	1.4	IS Manager & IG Manager	Further revisions.
26/10/11	1.3	IM&T Security Dept	Revised in line with new policy framework
28/05/11	1.2	IM&T Security Dept	Added review comments
25/02/11	1.1	IM&T Security Dept	Renamed document, formatted document, revised content and removed duplication, Incorporated IGG minor changes
05/02/09	1	IM&T Security Dept	Minor IGG changes
21/12/08	0.3	IM&T Security Dept	Minor IGG changes
19/12/08	0.2	IM&T Security Dept	Incorporated IGG minor changes
11/07/08	0.1	IM&T Security Dept	Initial Draft

***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
ELT	25/05/18	5.0
IGG	13/03/18	4.0
IGG	23/03/16	3.2
SMT	24/09/14	3.0
ADG	27/03/2012	2.0
IM&T SMG Information Governance Group	03/02/2009	1.0

Published on:	Date	By	Dept
The Pulse	25/05/18 (v5.1)	Internal Comms team	Comms
The Pulse	31/10/16 (v3.2)	Governance Administrator	G&A
The Pulse	10/11/14 (v3.1)	Governance Administrator	G&A
The Pulse	25/03/13 (v.2.2)	Governance Co-ordinator	G&C
LAS Website	25/05/18 (v5.1)	Internal Comms team	Comms
LAS Website	10/11/14 (v3.1)	Governance Administrator	G&A
LAS Website	31/10/16 (v3.2)	Governance Administrator	G&A
LAS Website	25/03/13 (v.2.2)	Governance Co-ordinator	G&C
The Pulse	12/03/09 (v.1)	Records Manager	GDU
LAS Website	12/03/09 (v.1)	Records Manager	GDU
Announced on:	**Date**	**By**	**Dept**
The RIB	05/06/18	IG Manager	IG
The RIB	11/11/14	IG Manager	G&A
The RIB	29/05/12	IG Manager	G&C

Equality Analysis completed on	By
20/12/2011	RL, MT, BT, GF
Staffside reviewed on	**By**

Links to Related documents or references providing additional information
See Appendix 1

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 Information Security Policy outlines the approach, methodology and responsibilities for preserving the confidentiality, integrity and availability of LAS information. It is the overarching policy for information security and supported by specific technical security, operational security and security management mandates. It supports the 7 Caldicott principles and 10 data security standards.

2. Scope

The documents in the Information Security Policy set apply to all information assets, which are owned and used by LAS for business purposes, or which are connected to any networks managed by LAS.
The documents in the Information Security Policy set apply to all information, which LAS processes, irrespective of ownership or form.
The documents in the Information Security Policy set apply to all members of the LAS and any others who may process information on behalf of LAS.

3. Objectives

This policy documents:

1. Information Security Principles.
2. Governance – outlining the roles and responsibilities.
3. Supporting specific information security mandates – Technical Security, Operational Security and Security Management.
4. Compliance Requirements.

4. Responsibilities

4.1 All Staff

Information Security and the appropriate protection of information assets is the responsibility of all users and individuals are expected at all times to act in a professional and responsible manner whilst conducting LAS business. All staff are responsible for information security and remain accountable for their actions in relation to LAS and other UK Government information and information systems. Staff **shall** ensure that they understand their role and responsibilities, and that failure to comply with this policy may result in disciplinary action. This will be reinforced by yearly mandatory training.

4.2 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is accountable for information risk within LAS and advises the Board on the effectiveness of information risk management across the organisation. Operational responsibility for Information Security **shall** be delegated by the SIRO to the LAS Information Security Officer.
All Information Security risks **shall** be managed in accordance with the LAS Risk Management Policy.

4.3 Information Governance Group

Chaired by the SIRO this Group will monitor the implementation of this policy.

4.4 Information Security Manager

The Information Security Manager is responsible for the day to day operational effectiveness of the Information Security Policy and its associated policies and processes. The Information Security Manager **shall**:

- Lead on the provision of expert advice to the organisation on all matters concerning information security, compliance with policies, setting standards and ensuring best practice.
- Provide a central point of contact for information security.
- Ensure the operational effectiveness of security controls and processes.
- Monitor and co-ordinate the operation of the Information Security Management System.
- Be accountable to the SIRO and other bodies for Information Security across LAS.
- Monitor potential and actual security breaches with appropriate expert security resource.

4.5 Caldicott Guardian

The Caldicott Guardian is responsible for ensuring implementation of the Caldicott Principles and Data Security Standards with respect to Patient Confidential Data.

4.6 Data Protection Officer

The Data Protection Officer is responsible for ensuring that LAS and its constituent business areas remain compliant at all times with the Data Protection legislation, Privacy & Electronic Communications Regulations, Freedom of Information Act and the Environmental Information Regulations. The Data Protection Officer **shall**:

- Lead on the provision of expert advice to the organisation on all matters concerning Data Protection legislation, compliance, best practice and setting and maintaining standards.
- Provide a central point of contact for the legislation both internally and with external stakeholders (including the Office of the Information Commissioner).
- Communicate and promote awareness of the legislation across the LAS.
- Lead on matters concerning individuals' right to access information held by LAS and the transparency agenda.
- To contribute to the development and maintenance of all LAS data protection policies, procedures and processes in relation to the protection of personal data.

- To be the point of contact for the supervisory authority on issues relating to processing of personal data, and to consult with the supervisory authority, where necessary, on any other personal data matters.

4.7 Information Asset Owners

The Information Asset Owners (IAOs) are senior/responsible individuals involved in running the business area and **shall** be responsible for:

- Understanding what information is held.
- Knowing what is added and what is removed.
- Understanding how information is moved.
- Knowing who has access and why.
- How long it is retained for.
- Origins of the data.
- Who it is shared with.

4.8 Senior Responsible Owners

All Senior Managers, Heads of Department, Information Risk Owners and Directors, defined as Senior Responsible Owners (SROs), are individually responsible for ensuring that this policy and information security principles **shall** be implemented, managed and maintained in their business area. This includes:

- Appointment of Information Asset Owners (IAO) to be responsible for Information Assets in their area(s) of responsibility.
- Awareness of information security risks, threats and possible vulnerabilities within the business area and complying with relevant policies and procedures to monitor and manage such risks.
- Supporting personal accountability of users within the business area(s) for Information Security.
- Ensuring that all staff under their management have access to the information required to perform their job function within the boundaries of this policy and associated policies and procedures.

5. Definitions

Term	***Meaning/Application***
SHALL	*This term is used to state a **Mandatory** requirement of this policy*
SHOULD	*This term is used to state a **Recommended** requirement of this policy*
MAY	*This term is used to state an **Optional** requirement*

6. Structure

6.1 The Information Security Policy document set is structured and based on the control guidelines set out in the industry standard ISO27001. This top level document details a set of other policies, procedures and mandate documents, which together constitute the Information Security Policy of LAS (see Appendix 1). All of these documents are of equal standing. Although this document set should be internally consistent, for the removal of any doubt, if any inconsistency is found between this overarching policy and any of the policies, procedures or work instructions, this overarching policy will take precedence. Each of the policies and procedures only contain hig do not, and are not intended to include detailed descriptions of implementation.

7. Information Security Principles

7.1 The core information security principles are to protect the following information/data asset properties:

- Confidentiality (C) – protect information/data from breaches, unauthorised disclosures, loss of or unauthorised viewing.
- Integrity (I) – retain the integrity of the information/data by not allowing it to be modified.
- Availability (A) – maintain the availability of the information/data by protecting it from disruption and denial of service attacks.

In addition to the core principles of C, I and A, information security also relates to the protection of reputation; reputational loss can occur when any of the C, I or A properties are breached. The aggregation effect, by association or volume of data, can also impact upon the Confidentiality property.
For the LAS, the core principles are impacted, and the effect aggregated, when any data breach relates to patient medical data.

8. Supporting Policies, Procedures & Mandates

8.1 The Information Security Policy is developed as a pinnacle document which has further policies, procedures, mandates, standards and guides which enforce and support the policy as described in the 'Structure' section. The supporting documents are grouped into 3 areas: Technical Security Procedures, Operational Security Policies and a Security Management Policy. The Information Security Policy is closely aligned to the LAS Information Governance Strategy and relies upon, and supports, the LAS Physical Security Policy.

- Technical Security Mandates – These are internal procedures documented, owned and followed by the IM&T Directorate.
- Operational Security Policies – These are trust level policies that are documented and owned by members of the IM&T Directorate but apply to the trust as a whole and as such require trust level approval.
- Security Management Policy – This policy is documented and owned by the IM&T Directorate but supplements other directorate's policies with information security specific input where required.

9. Compliance Requirements

9.1 Legislation

LAS is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation **shall** be devolved to employees and agents of LAS, who **may** be held personally accountable for any breaches of information security. LAS **shall** comply with all relevant legislation; this includes but is not limited to:

- Data Protection legislation
- Freedom of Information Act 2000
- Health & Social Care (Safety & Quality) Act 2015
- Computer Misuse Act 1990

9.2 Audit

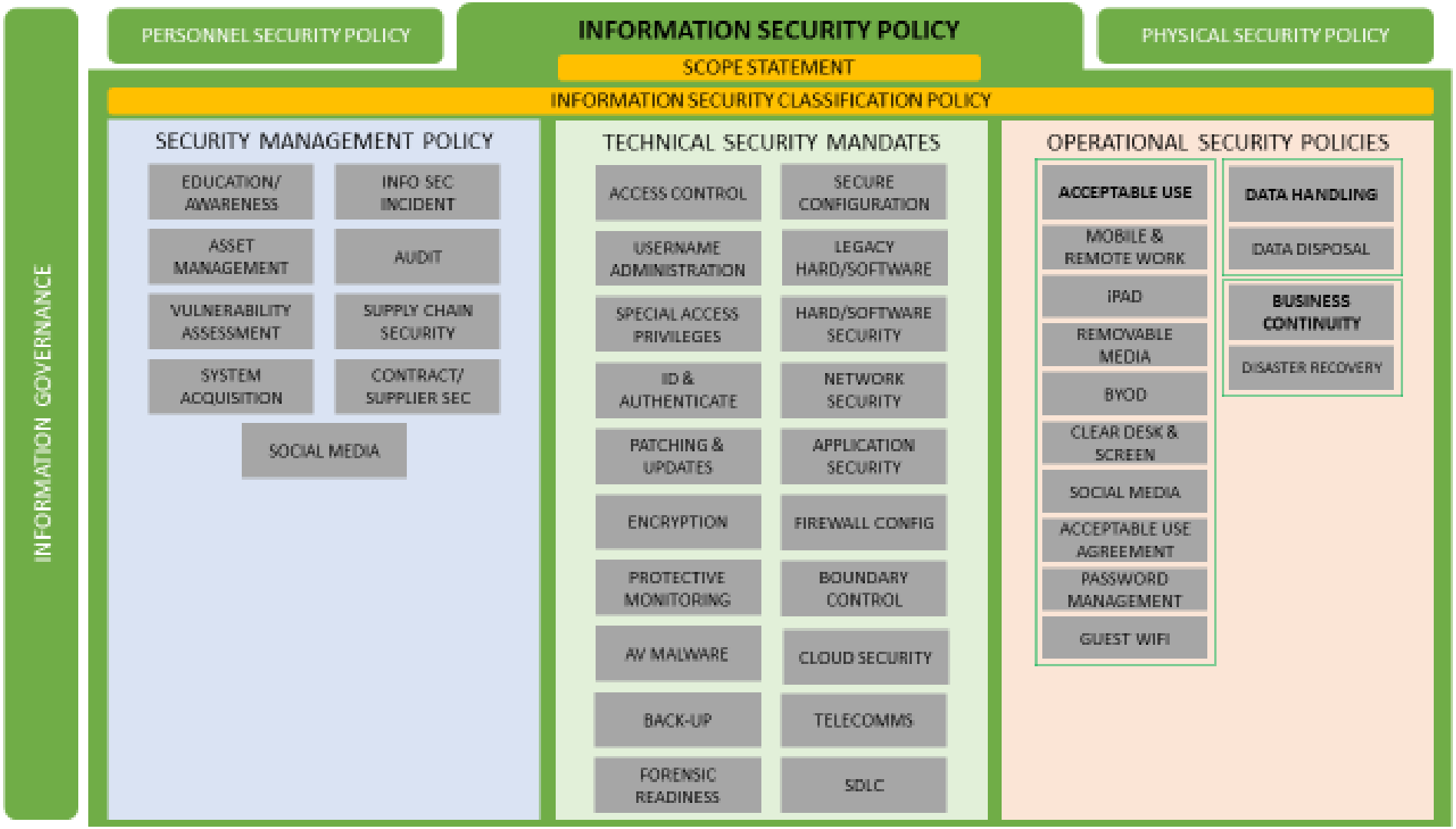
Audit will be performed as part of the ongoing LAS Audit Programme and the Information Security Officer **shall** ensure appropriate evidence and records are provided to support these activities at least on an annual basis.

9.3 Review

This policy **shall** be reviewed annually by the IGG. The Information Security Officer **shall** be responsible for ensuring the review is conducted in good order and follows due process for approval.

The Information Security Officer is accountable for providing the results of ongoing reviews of information security implementation across LAS. This includes support to the annual Information Governance Toolkit return.

IMPLEMENTATION PLAN				
Intended Audience	All staff			
Dissemination	The Pulse			
Communications	RIB			
Training	As part of staff annual mandatory training			
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**
Staff training	Weekly on HEAT	Information Security Team reporting to Head of SSA, IM&T	IM&T SMT, IGIST, IGG	Findings and actions will be recorded in the minutes of the relevant group meetings and passed to the Information Security Team for action.
Security breaches and serious incidents	An annual IGG meeting will be used to discuss compliance and appropriate actions for performance improvement e.g. change training content in light of experience.	Information Security Manager will monitor and report to IGG	Risk Compliance and Assurance Group will monitor outcomes and recommendations	Update training and awareness to reflect findings Make policy changes to reflect new/ unforeseen circumstances


INFORMATION GOVERNANCE
PERSONNEL SECURITY POLICY
INFORMATION SECURITY POLICY
SCOPE STATEMENT
PHYSICAL SECURITY POLICY
INFORMATION SECURITY CLASSIFICATION POLICY
SECURITY MANAGEMENT POLICY
EDUCATION/ AWARENESS
INFO SEC INCIDENT
ASSET MANAGEMENT
AUDIT
VULNERABILITY ASSESSMENT
SUPPLY CHAIN SECURITY
SYSTEM ACQUISITION
CONTRACT/ SUPPLIER SEC
SOCIAL MEDIA
TECHNICAL SECURITY MANDATES
ACCESS CONTROL
SECURE CONFIGURATION
USERNAME ADMINISTRATION
LEGACY HARD/SOFTWARE
SPECIAL ACCESS PRIVILEGES
HARD/SOFTWARE SECURITY
ID & AUTHENTICATE
NETWORK SECURITY
PATCHING & UPDATES
APPLICATION SECURITY
ENCRYPTION
FIREWALL CONFIG
PROTECTIVE MONITORING
BOUNDARY CONTROL
AV MALWARE
CLOUD SECURITY
BACK-UP
TELECOMMS
FORENSIC READINESS
SDLC
OPERATIONAL SECURITY POLICIES
ACCEPTABLE USE
MOBILE & REMOTE WORK
IPAD
REMOVABLE MEDIA
BYOD
CLEAR DESK & SCREEN
SOCIAL MEDIA
ACCEPTABLE USE AGREEMENT
PASSWORD MANAGEMENT
GUEST WIFI
DATA HANDLING
DATA DISPOSAL
BUSINESS CONTINUITY
DISASTER RECOVERY