London Ambulance Service NHS Trust

IT Forensic Readiness Policy

DOCUMENT PROFILE and CONTROL.

Purpose of the document: This document establishes the IT forensic readiness controls that are to be adhered to in line with the Information Security Policy TP048.

Sponsor Department: IM&T Information Security

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

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
25/05/18	3.1	IG Manager	Document Profile and Control update and minor change
15/05/18	2.2	Principal Cyber Security Specialist	GDPR update
15/09/15	2.1	IG Manager	Document Profile and Control update
08/05/15	1.2	IS Manager	Minor Changes
25/05/12	1.1	IG Manager	Doc Profile & Control update
28/03/12	0.4	ADG/ IS Manager	ADG comments implemented
21/02/12	0.3	IS Manager	Equality Analysis added.
18/01/12	0.2	IG Manager	Reformatting
14/11/11	0.1	IS Manager	Document creation

***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	3.0
SMT	13/05/15	2.0
ADG	27/03/12	1.0
Ratified by		
SMG	16/05/12	1.0

Published on:	Date	By	Dept
The Pulse (v3.1)	25/05/18	Internal Comms team	Comms
The Pulse (v2.1)	15/09/15	Governance Administrator	G&A
The Pulse	28/05/12	Governance Co-ordinator	G&C
LAS Website (v3.1)	25/05/18	Internal Comms team	Comms
LAS Website (v2.1)	15/09/15	Governance Administrator	G&A
LAS Website	28/05/12	Governance Co-ordinator	G&C
Announced on:	Date	By	Dept
The RIB	05/06/18	IG Manager	IG
The RIB	29/05/12	IG Manager	G&C

Equality Analysis completed on	By
17/02/2012	IM&T Equality Assessment Team
Staffside reviewed on	By

Links to Related documents or references providing additional information		
Ref. No.	Title	Version
TP/006	Serious Incident Policy and Procedure	5.1

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 IT Forensic Readiness Policy is a part if the London Ambulance Services (LAS) framework of Information Security Policies. It is designed to help protect the information assets of the London Ambulance Service (LAS) through the application of best practice in IT Forensics and to minimise the costs of an investigation.

IT Forensics is the ability to detect and react to types of security incidents that require the collection, storage, analysis and preparation of digital evidence that may be required in legal or disciplinary proceedings. The IT Forensic Readiness Policy describes the current LAS capability to conduct an examination in a consistent, legal fashion and to ensure the admissibility of evidence relating to an incident. It covers both the proactive forensic monitoring of targeted systems and the reactive investigation of an unforeseen incident.

2 Scope

This Policy supports the objectives of the LAS Information Security Policy (TP048), and applies to all authorised users of LAS information including permanent and temporary staff employed within the LAS, all contractors, locally engaged staff and third parties who have legitimate access to LAS information, LAS information assets and/or the LAS IM&T infrastructure.

The Policy applies to all LAS Information, Communication and Technology (ICT) equipment, networks and software assets.

3 Objectives

Health and Social Care Information Centre (HSCIC), part of the Department of Health Informatics Directorate, recognise a forensic readiness capability will maximise a Trust's ability to preserve and analyse data generated by an ICT system that may be required for legal or management purposes. This requirement is also reflected in ISO 27001, the international standard for information security management systems, which requires organisations to "collect, retain and present evidence that conforms to rules of evidence laid down in relevant laws."

IT Forensics is a key component in the management of information risk and the capability to recover from information related incidents. The LAS IT Forensic Readiness Policy assures the following principles:

Detection

Skilled perpetrators will attempt to cover up their unauthorised actions. A skilled investigator, with ICT forensic tools, can proactively detect security issues and take suitable actions to limit the exposure of an incident. Forensic tools can be used in real-time to collect evidence over a network or used after an event to help understand the events and responsibilities behind an incident.

Deterrence

Security awareness training ensures that staff are aware of what is considered to be appropriate usage of IT systems and that the LAS has the legal right and ability, to

monitor how staff use LAS ICT assets. The combination or knowing what is allowed, and the knowledge that staff are being monitored may deter inappropriate/illegal actions.

Consistency

The use of dependable documented methods ensures forensic monitoring and investigations are conducted in a consistent, repeatable fashion. This reduces the operational risk of a major incident being under-, or part-, investigated or too much resource being expended on minor incidents.

Business Continuity

It is essential that business is able to resume or continue operations despite a security incident. This policy describes the method for isolating systems affected by an incident, allowing other systems to remain operational.

Ownership and Responsibility

Digital evidence is particularly fragile and must be handled extremely carefully to remain admissible. It is essential that at all stages of an incident's investigation there is clearly documented custodian of evidence and a clear list of who was responsible for carrying out actions upon it.

Enforcement and Escalation

Forensic investigations are clearly related to the incident management process. Clear, predefined roles and escalation points assist in reducing impact of an incident and allow the business to recover quicker.

Legality

The Trust is obliged to conduct all investigations in line with UK laws. The IT Forensic Readiness Policy ensures legal issues, including the rights of employees to reasonable privacy, are considered in advance of investigations.

4 Responsibilities

The Trust **Senior Information Risk Owner (SIRO)** is responsible for coordinating the development and maintenance of forensic policy procedures and standards for the Trust.

The SIRO shall advise the Chief Executive and the Trust Board on forensic readiness planning and provide periodic reports and briefings on progress.

Information Governance Group (IGG)

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

LAS Information Asset Owners (IAOs) must ensure that forensic readiness planning is adequately considered and documented for all information assets where they have been assigned ‘ownership’. Goals for forensic planning include:

- Ability to gather digital evidence without interfering with business processes;
- Prioritising digital evidence gathering to those processes that may significantly impact the Trust, its staff and its patients;

- Allow investigation to proceed at a cost in proportion to the incident or event;
- Minimise business disruptions to the Trust;
- Ensure digital evidence makes a positive impact on the outcome of any investigation, dispute or legal action.

IAOs shall submit plans for forensic readiness to the IM&T Information Security Manager for review along with details of any planning assumptions or external dependencies.

The **IM&T Information Security Manager** is responsible for the management of forensic investigations, maintaining the ability of the Trust to carry out investigations and ensuring appropriate external relationships are in place if an incident requires independent investigation. Additional responsibilities include maintaining software licences and support for Forensic tools.

The Data Protection Officer and the **Information Governance Manager** are able to offer advice on data protection issues within the Trust, particularly on the issue of staff privacy.

The **Serious Incident Group** is a group created to manage the consequences of a serious incident. The Serious Incident Group will make the decision if an IT forensic investigation should take place.

The Trust's **Human Resources Department** will advise and support LAS management on any investigations that involve investigations of members of LAS staff. They will support line managers in considering whether any investigation is required from the IM&T Security function. Where a need is determined, the Trust's normal Disciplinary policy and arrangements will then be implemented.

5 Definitions

For the purposes of this policy the following definitions apply:

IG Forensic readiness	The ability of an organisation to make use of digital evidence when required. Its aim is to maximise the organisation's ability to gather and use digital evidence whilst minimising disruption or cost.
IG Forensic readiness planning	Proactive planning for a digital investigation through the identification of scenarios, sources of admissible evidence related monitoring and collection processes and capabilities, storage requirements and costs.

6 IT Forensic Readiness Policy

6.1 The Need for IT Forensics

Forensic readiness is the ability of the LAS to make optimal use of digital evidence; this has several important benefits including:

- In the event of a serious incident or major IT breach, an investigation can be quickly and efficiently undertaken, minimising disruption to business;
- To provide admissible evidence in criminal activities including fraud, money laundering, blackmail and extortion;
- The ability to demonstrate due diligence and good corporate governance of LAS information assets in the Trust's defence;
- To deal effectively with court orders to release data and show compliance with regulatory or legal requirements;
- The ability to trace the source of information leaks or intellectual property theft;
- Extending the capability of LAS to support Trust disciplinary issues;
- To deter staff from activities that may undermine information security.

6.2 Business Risks that require Digital Evidence Collection

Digital systems and distributed computing offer the LAS great advantages in terms of efficiencies and cost saving. However our increased reliance upon these systems has increased our exposure to risk, something the adoption of good practice and controls can reduce or eliminate. However, it is necessary, as part of incident response, to have the ability to collect and analyse data held on a variety of electronic devices or storage media that may be used as evidence in some future investigation.

6.3 Sources of Business Risks

Business risks that require the use of forensics come from a variety of sources and cover several different types of incident/crime. Within LAS a formal risk assessment is used to identify threats, controls and impact for a particular system. Proactive forensic monitoring is a control available to LAS for reducing threats to any particular system. Closely related to intrusion detection mechanisms, proactive forensic evidence collects, verifies and handles data in a way that is admissible in court. Monitoring and auditing these identified potential targets is likely to detect and deter major incidents. The following tables show potential sources of an incident requiring forensic investigation and the target of an investigation:

Internal Authorised	Authorised users may abuse ICT systems by conducting unauthorised actions. These could include storage of offensive material or stealing information for an outside agent.
Internal Unauthorised	Staff members may attempt to

	circumvent controls to gain access to material they do not have authorisation to view. A cleaner attempting to access a restricted file system would be an example of this.
Internal to External	Users may use LAS ICT facilities to facilitate crimes against external parties. Examples would include mass emailing or launching attacks against an outside web site.
External	Many outside parties, from teenagers acting alone to hostile foreign governments, will attempt to compromise LAS security.

6.4 Examples of Incident/Crime Needing Investigation

The following, indicative, list describes the most common examples where an investigation may be required:

Theft of Intellectual Property/Protected Data	The unauthorised copying or removal of programs or sensitive data may involve the use of removable disk or storage, such as an iPod. Breach of Copyright would be an example of such a crime. Forensics can be used to prove a particular piece of equipment was used in such an incident, even if the perpetrator has attempted to cover their tracks.
Damage to or modifications to computer equipment or data	The deliberate damage of a computer system may be to disguise unauthorised activity previously carried out on that device. Examining modifications of equipment may reveal planted devices, such as key loggers or modems, used to bypass normal security mechanisms.
Telecommunications Crime/Hacking	The use of a computer to obtain unauthorised access to computers or network is now common.

	A forensic investigation might gather evidence from multiple devices, including router and firewall logs to establish the source and perpetrator of the attack.
Financial crimes- Identity theft, fraud, forgery, theft of funds, blackmail or extortion	The misuse of a computer to embezzle money, or steal people's identity for financial gain, may leave evidence in ICT systems or on portable media. A forensic study of disks, equipment, logs and email records may provide investigators with evidence to prosecute individuals.
Email SPAM/Denial of Service Attacks	Internal connections may be used to attack other internal or external targets. An investigation may look for evidence of the tools used by hackers.
Creation or planting of viruses, spyware, worms or keystroke recorders	The deliberate introduction of these files poses a major threat to LAS information security.
Disciplinary issue through inappropriate use	This could include the storage of pornographic or hate images or files, email abuse such as SPAM, connecting systems to unofficial networks, or attempted unauthorised access to computer data or programs.
Target Systems	If a LAS system has been compromised through a security incident it may be necessary to collect evidence from the target machine to understand the method and source of the attack.

6.5 Sources and Forms of Digital Evidence

Computers, networks, storage devices and their various peripherals may be used in the commission of various incidents or crimes, or can themselves be the target of an attack. As a result, digital evidence may be collected from a variety of sources, these may include:

PC	This is the main unit which contains the hard disks, motherboard and terminates most connections. Investigations may

	include copying volatile memory
Hard disks (internal and external)	Hard disks may contain evidence in deleted files or partitions not normally visible to users
Routers/Modems/Bridges/ Firewalls	Configurable network devices often contain logs which can be used to attribute a machine to a course of action
Application software	Some applications, such as accounting packages may hold records of fraud or employee records and activities
Wireless cards, or PCMIA cards	Unauthorised devices may be attached legitimate systems to compromise security. The configuration of such a device may provide evidence.
CD-ROM/DVD/Memory sticks/floppy disks	Storage media are often used for stealing or intellectual property. An understanding of encryption, passwords and steganography is required to reveal hidden data
Log Files and Email Records	Many systems produce log files of various activities and emails may be archived. Investigation may involve the detailed study of servers holding this information.
Backup tapes	Actions that transpired over a period of time, or in the past, can be recreated using backup tapes
Digital cameras and video devices inc CCTV	Increasingly camera or video images are used as evidence. A forensic officer must know how to handle this media to preserve evidence
USB/Firewire devices	An array of devices can be connected to PCs through these ports may need investigating
iPods/MP3players/Games consoles	These devices appear to be innocuous entertainment devices, but may be used as mass storage or wireless transmission devices
Mobile Telephones/Smartphones	Increasingly mobile telephony devices can be used for the storage and transfer of information assets. Investigation of this sort of device is becoming increasingly

	common.

7 The Decision to conduct a Forensic Investigation

Forensic investigations may only be instigated via four sources, these are:

1. At the request of the Serious Incident Group investigating a serious incident. Refer to the Serious Incident Policy TP/006;
2. At the request of a senior Human Resources Manager supporting a line Manager investigating possible staff disciplinary cases;
3. In response to an external request made from a recognised HMG agency that has authority to request such information e.g. law enforcement agencies. These enquiries will be handled via the Information Governance Manager.
4. Where an IM&T Security Team audit or risk assessment has revealed a particularly threat warrants proactive monitoring. In the event of suspicious activity being uncovered, the incident will be escalated through the Serious Incident process.

7.1 Cost/Benefit Assessment

Decisions to monitor or investigate a potential incident must be justified by a cost benefit analysis of how much the required evidence will cost to collect and what benefit it provides. The requesting party should request a statement of the resources required to facilitate an investigation from the IM&T Information Security Manager.

7.2 Legality of Investigations

The Trust will ensure that any IT forensic investigations respect the laws that provide employees and individuals with the right to personal privacy.

Consideration is required regarding the privacy of personal data held on LAS ICT systems or the right to seize a staff member's property if they are suspected of using it to conduct a breach of this Policy e.g. mobile phone, iPod, camera, etc.

All potential investigations must be considered from a legal perspective by the Human Resources Department, Legal Department and the Information Governance Manager. The results of such consideration are to be documented.

7.3 Types of Possible Investigation

Investigations may either be:

- Proactive forensic monitoring of a user, or group, as part of an investigation where suspicious behaviour is suspected.
- A reactive investigation where an incident, or suspected incident, has occurred. The LAS Serious Incident Policy (TP006) defines how incidents are categorised, escalated and investigated.

8 LAS Forensic Investigation Methodology

8.1 Aptitude and Preservation of Evidence

Any task in a forensic investigation will be conducted by a person suitably trained and competent to carry out that task. The IM&T Security Manager will determine if an internal or external investigation is appropriate.

Investigations will be documented, including a description of all processes applied to obtain evidence. A chain of evidence will be created and preserved demonstrating where evidence has been stored and under whose care from capture until presentation.

The forensic investigation process shall preserve the integrity of original evidence by ensuring sufficient security measures, legal advice and procedural measures to ensure the evidence requirement are in place. Any processes applied to copies of evidence should be repeatable and achieve the same results.

Investigations will be conducted legally respecting local jurisdictions and the human rights of individuals.

8.2 LAS Forensic Resources

8.2.1 People

The Information Security Manager is trained to carry out various levels of forensic investigation. LAS recognises that on-going staff training is essential to maintain a forensic investigation capability.

8.2.2 Working Space

Working space is available for LAS IT forensic investigations in a secure LAS building. The site has extensive physical security measures and highly restricted access.

8.2.3 Evidence Storage

The area allocated for forensic investigations has a secure, lockable cupboard for the storing of collected evidence. All evidence is labelled according to the LAS forensic investigation procedures and packaged appropriately to protect it from damage and electromagnetic interference.

8.2.4 External resources/arrangements

For serious incidents it is necessary to escalate the forensic investigation process to external bodies, as there is limited expertise in LAS. Where necessary it could be escalated to law enforcement, Health and Social Care Information Centre or other HM Government agencies. The responsibility for escalation lies with the team assigned through the implementation of the Serious Incident Policy.

9 Building Evidence-based Cases - Forensic Investigation Procedures

A forensic investigation needs to go beyond identifying a wrong-doer or discovering how an incident occurred; it is required to provide a body of evidence that can stand

up to detailed scrutiny, often by outside authorities. An investigation may involve many separate facts, both technical and testimonial, that are gathered together and presented as a logical argument.

A forensic case consists of:

a) Initial investigation by the Cyber team, who will deem if further investigation is required.

b) Engagement of a third party to use forensic tools to build a body of evidence that is applicable to its context e.g. presentation to a court of law, disciplinary hearing, etc.

c) The ability to record testimonial evidence, including witness statements, attesting to the facts around an incident.

d) The presentation of available facts in a logical, unbiased argument.

The LAS Cyber team will oversee the third party implementing a forensic investigation; and will plan each examination to ensure evidence is admissible through suitable collection methods, transportation and preservation methods.

10 Staff Education, Training and Awareness

LAS ICT users are made aware of the possible monitoring of their activity through the Policy for the Acceptable Use of IT and Communications Systems (TP/060)

IMPLEMENTATION PLAN	
Intended Audience	All staff
Dissemination	The Pulse and the LAS Website
Communications	Announced in the RIB
Training	The following training requirements are recognised: • HR Staff require an understanding of IT investigations and how to request an investigation; • The Serious Incident Group require training in how to request an IT forensic investigation and the associated cost and legal challenges; • The IM&T Security Team will be required to maintain the capability to run IT forensic investigations.

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**
Compliance will be measured in terms of the number and success rate of investigations.	Annually through reports to IGG	IS Manager report through to Information Governance Group	RCAG	Policy review following feedback from RCAG

Legislation and Guidelines

It is LAS policy to fully comply with all applicable legislation and regulations, in particular, the following :

Official Secrets Act 1989
The Computer Misuse Act 1990
Data Protection Act 2018
Freedom of Information Act 2000
Environmental Information Regulations 2004
The Human Rights Act 1998
The Equality Act 2010
Privacy and Electronic Communications Regulations 2003 and 2004
The Regulation of Investigatory Powers Act 2000
The Interception of Communications Act 1985
Electronic Communications Act 2000
The Design Copyright and Patents Act 1988
Police and Criminal Evidence Act 1984
Crime and Disorder Act 1998
Civil Contingencies Act 2004
The Health and Safety at Work Act 1974
The Lawful Business Practice Regulations 2000
The Public Records Act 1958
Access to Health Records Act 1990 (where not superseded by Data Protection legislation)
The Crime and Disorder Act 1998
The Caldicott 2 and 3 Reviews and subsequent reports
The Information Governance Toolkit
Re-use of Public Sector Information Regulations 2005
DoH Confidentiality – NHS Code of Practice
The NHS Care Record Guarantee