London Ambulance Service NHS Trust

Information Security Policy

London Ambulance Service NHS Trust

DOCUMENT PROFILE and CONTROL.

Purpose of the document: This document establishes the Information Security Key Controls that are to be adhered to in line with the Information Security Policy.

Sponsor Department: IM&T Information Security

Author/Reviewer: Information Security Manager. To be reviewed by May 2014

Document Status: Final

Amendment History			
Date	*Version	Author/Contributor	Amendment Details
11/07/08	0.1	Dinshaw Nazir	Initial Draft
19/12/08	0.2	Dinshaw Nazir	Incorporated IGG minor changes
21/12/08	0.3	Dinshaw Nazir	Minor IGG changes
05/02/09	1	Dinshaw Nazir	Minor IGG changes
25/02/11	1.1	Information Security Manager	Renamed document, formatted document, revised content and removed duplication, Incorporated IGG minor changes
28/03/11	2.1	Information Sec Mgr	Added review comments

For Approval By:	**Date Approved**	**Version**
IM&T SMG Information Governance Group	03/02/2009	1.0
Information Governance Group	27/05/11	2.0

Published on:	**Date**	**By**	**Dept**
The Pulse			GCT
LAS Website			GCT
Announced on:	**Date**	**By**	**Dept**
The RIB			GCT

EqIA completed on	**By**
28/03/11	C D-B; SM; BO.
Staffside reviewed on	**By**

Documents or references providing additional information		
Ref. No.	**Title**	**Version**
	Principles of Information Security - NHS Connecting for Health (http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/security)	
	Information Security Technology Techniques – Information Security Management System Requirements 27001: 2005 – British Standards Organisation	

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.

Table of Contents

1. Introduction

This document establishes effective controls to ensure the security of information within the Trust.

These Controls have been approved by the Trust Board for use by all LAS staff and contracted third parties.

2. Objectives

The objective of the key Controls is to ensure that information held by the Trust is maintained to the greatest degree of:

- Availability – information will be available when required.
- Integrity – information will be complete and accurate.
- Confidentiality – information will not be disclosed to unauthorised parties.

3. Scope

Key Controls apply to all users, information, information systems, networks and applications of the Trust or supplied under contract to it.

4. Responsibilities

Director of IM&T

The Director of IM&T is the Senior Risk Owner (SIRO) and is accountable to the Trust Board for Information Security and responsible for reporting Information Security risks to the Risk, Compliance and Assurance Group.

Caldicott Guardian

Responsible for protecting the confidentiality of patient and service-user information and this policy supports the Caldicott function.

Information Security Manager

Responsible for maintaining and reviewing information processing systems against these key Controls.

Information Governance Manager

Responsible for records and information management and liaising with the Information Security Manager in the delivery of effective Information Security.

Information Governance Group (IGG)

Chaired by the Director of IM&T this Group will monitor the implementation of this policy.

Line Managers
Responsible for ensuring staff work in line with the Information Security Policy and these key Controls.

All staff and third parties
Responsible for ensuring information security is appropriately considered and that the Information Security Policy and these key controls are adhered to.

5. Policy Exceptions

Any exceptions to these key controls must be formally requested to the Information Security Manager for consideration.

6. Key Controls Structure

The Trust has identified ten key Control areas for implementation through the Information Management System. Each Key Control section is made up of an Information Security Policy Statement, Control Objective and Control Requirements stating what must be implemented within The Trust. These terms are explained in the Definitions section.

Control Requirements must be followed by all staff to meet Key Control objectives which ensure the Information Security Policy is adhered to.

7. Security Policy and Organisation

Information Security Policy Statement

The Trust will implement and maintain an Information Security Policy for all paper based and electronic information, supporting processes and systems. The information security Policy will be regularly reviewed by the Information Governance Group. An information security organisation framework will be implemented made up of specialist security roles in order to initiate and control the implementation of information security within the organisation.

7.1 Information Security Policy Document

7.1.1 An Information Security Policy document should be approved by management, and published and communicated to all employees and relevant external parties.

7.1.2 The Information Security Policy will be managed and maintained by the Trust's Information Security Manager.

7.1.3 The Information Security Policy must clearly communicate the security posture of the organisation and explain how security is to be implemented.

7.1.4 The Information Security Policy must be authorised and supported by The Trust Board through the Information Governance Group.

7.1.5 The Information Security Policy must include statements of compliance to applicable statutory, regulatory and contractual laws.

7.1.6 The Information Security Policy must be mandated to all Trust staff and published to an accessible location for viewing.

7.1.7 The Information Security Policy must include a Policy Exception statement.

7.2 Review of the Information Security Policy

7.2.1 The Information Security Policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness

7.2.2 The Information Security Policy must be reviewed annually by the Information Governance Group. Any required Policy updates will be made by the Information Security Department.

7.2.3 The Key Controls will be reviewed and updated at the discretion of the Information Security Department however a minimum of two Key Controls must be reviewed annually. Any required updates will be presented to the Information Governance Group for consideration.

7.2.4 The Information Security Management System will be reviewed and updated at the discretion of the Information Security Department.

7.2.5 The IM&T Risk Management Framework will be reviewed and updated at the discretion of the Senior Information Risk Owner.

7.3 Management Commitment to Information Security

7.3.1 Management should actively support security within the organisation through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

7.3.2 The Trust Board, through the Information Governance Group will support and endorse the Information Security Policy.

7.3.3 The Director of IM&T will ensure appropriate management support and resourcing is provided for implementation and ongoing management of the Information Security Policy.

7.3.4 The Information Security Manager will ensure skilled information security professionals are recruited in order to enforce the Information Security Policy.

7.3.5 The Information Security Manager will ensure specialist security advice from external parties will be sought if the appropriate skills do not exist within The Trust.

7.4 Information Security Co-ordination

7.4.1 Information security activities should be co-ordinated by representatives from different parts of the organisation with relevant roles and job functions.

7.4.2 The Information Security Manager will ensure co-ordination of information security initiatives across The Trust.

7.4.3 The Information Security Manager will ensure appropriately skilled departments; management and staff are consulted on issues where specialist internal advice is required.

7.4.4 The Information Security Manager will participate in the Information Governance Group.

7.4.5 The Senior Information Risk Owner will chair the IM&T Risk Management Working Group.

7.5 Allocation of Information Security Resources

7.5.1 All information security responsibilities should be clearly defined

7.5.2 All Trust staff are responsible for ensuring they adhere at all times to the Information Security Policy controls.

7.5.3 Within The Trust will exist a dedicated Information Security Department to implement and manage the Information Security Policy.

7.5.4 The Information Security Manager will identify the appropriate resources required to implement and manage the Information Security Policy.

7.5.5 Implementation of specific Controls may be delegated by the Information Security Manager to other Departments. In these situations the internal asset owner or Department manager assumes responsibility for implementing the identified Controls.

7.6 Authorisation Process for Information Processing Facilities

7.6.1 A management authorization process for new information processing facilities should be defined and implemented.

7.6.2 The use of personal information technology devices on The Trust's computing network is forbidden. If special circumstances arise and a business need can be identified a request must be made to the Information Security Department for consideration prior to the device being used.

7.6.3 IM&T management approval must be sought by any members of staff wishing to implement new information technologies and services.

7.6.4 Any new information technologies and services implemented within The Trust must be tracked through the IM&T Change Approval Board.

7.7 Confidentiality Agreements

7.7.1 Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information should be identified and regularly reviewed.

7.7.2 All Trust staff must ensure confidentially and non-disclosure agreements are in place when dealing with confidential information and third parties.

7.7.3 A definition on confidential information within the Trust must be communicated to staff.

7.7.4 All confidentiality or non-disclosure agreements must comply with applicable laws and regulations.

7.7.5 Commencing staff, permanent or temporary must agree to and sign a confidentiality or non-disclosure agreement as part of an employee contract.

7.7.6 External parties engaged by The Trust to provide contract based services must agree to and sign a confidentiality or non-disclosure agreement.

7.7.7 Trust staff wishing to discuss or disclose information to external parties for business purposes must have the external party agree to and sign a confidentiality or non-disclosure agreement.

7.7.8 All confidentiality and non-disclosure agreements must be drafted, approved and issued by the Trust's internal Legal Department.

7.7.9 Requirements for confidentiality and non-disclosure agreements must be reviewed regularly by The Trust's Legal Department. If changes are required the Trust's Legal Department will amend current confidentiality and non-disclosure agreement templates and communicate these to staff.

7.8 Contact with Special Interest Groups

7.8.1 Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

7.8.2 The Information Security Department will maintain relationships with appropriate special interests groups to ensure staff are up-to-date with the latest information security concepts.

7.8.3 The Information Security Department will maintain relationships with external agencies for threat and vulnerability intelligence and management.

7.8.4 The Information Security Department will maintain an Incident Response process for responding to technical and non-technical security incidents.

7.8.5 The Information Security Department will share intelligence information with other NHS Trust's in the event of a wide-spread security incident.

7.9 Independent Review of Information Security

7.9.1 The organisation's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

7.9.2 The Trust supports a regular independent review of the Information Security Management System.

7.9.3 The Information Security Department will engage a third party to perform a review of the Trust's Information Security Management System on an annual basis.

7.10 Identification of Risks Related to External Parties

7.10.1 The risks to the organisation's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.

7.10.2 External parties requesting physical connections to The Trust's technology networks must have a risk assessment performed by the Information Security Department prior to any connections being made.

7.10.3 External parties requesting logical access connections in order to access Trust information must be authorised by the Information Security Department prior to access being granted.

7.10.4 External parties which have direct physical connections and/or access to manage devices located within The Trust's technology network must have an annual risk assessment performed by the Information Security Department to ascertain if appropriate security controls are in place.

7.10.5 External parties providing software development services to The Trust must have a risk assessment performed by the Information Security Department to ascertain if appropriate security controls are in place.

7.10.6 External parties providing services to The Trust must have legal agreements in place prior to commencing any works.

7.10.7 Internal projects which intend to share information with external parties or make physical connections to The Trust's technology networks must request a risk assessment from the Information Security Department to ascertain if appropriate security controls are in place.

7.10.8 All management staff within The Trust are responsible for ensuring external third parties providing services to The Trust are made aware of their obligations to information security. These obligations must be included in any engagement agreements and must be signed and agreed to by all parties.

7.11 Addressing Security in Third Party Agreements

7.12.1 Agreements with third parties involving accessing, processing, communicating or managing the organisation's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements

7.12.2 Legal agreements with customers and external parties must include statements to ensure The Trust's Information Security Policy and Key Controls will be adhered to.

7.12.2 It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

7.12.3 IM&T is to ensure that any third party service agreements include service definitions, service levels, security arrangements and fallback plans in the event of a major failure or disaster.

7.13 Monitoring and review of third party services

7.13.1 The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.

7.13.2 Service agreements between the Trust and third parties must be monitored and reviewed to ensure service levels are adhered to and information security incidents are managed.

7.13.3 IM&T will review service reports, audit trails and security events generated by third parties.

7.14 Managing changes to third party services

7.14.1 Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

7.14.2 IM&T will account for third party changes through security risk assessments by the Information Security Department and change control procedures. This may include changes to networks, use of new technologies/products and physical locations.

7.14.3 IM&T will account for any change of vendors in change control procedures.

7.14.4 All major changes to critical services must have a security risk assessment performed by the Information Security Department prior to production implementation.

8. Asset Management

Information Security Policy Statement
The Trust will implement and maintain asset registers for paper based and electronic information. This includes asset ownership, classification, people and physical, software and communication and technology devices.

8.1 Inventory and Ownership of Assets

8.1.1 All assets should be clearly identified and an inventory of all important assets drawn up and maintained

8.1.2 All information and assets associated with information processing facilities should be owned by a designated part of the organisation

8.1.3 All Trust assets will be assigned an owner (Information Asset Owner IAO) at Executive Management level. Respective Executive Managers can delegate routine asset management responsibilities to Departmental staff.

8.1.4 All assets will be assigned an Information Asset Administrator responsible for administering systems and applications

8.1.5 All staff assigned Trust assets are responsible for ensuring they are secured at all times.

8.2 Acceptable Use of Assets

8.2.1 Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented

8.2.2 All staff including contracted and external third parties with access and authority to use Trust assets must use them in an acceptable manner.

8.2.3 An Acceptable Use Policy for the use of email, Internet, portable media devices will be created to explain what is deemed acceptable within The Trust. These requirements must be communicated to all staff and contracted external third parties. (See TP/060 Policy for the Acceptable Use of IT and Communications Systems)

9. Human Resources Security

Information Security Policy Statement

The Trust will implement appropriate controls to ensure commencing, current or exiting full-time or temporary staff and third parties are legally bound to preserve confidentiality, understand their security responsibilities and are suitable for the roles they have been asked to perform.

9.1 Roles and Responsibilities

9.1.1 Security roles and responsibilities of employees, contractors and third parties should be defined and documented in accordance with the organisation's Information Security Policy

9.1.2 All commencing permanent or contract staff and authorised external parties must act in accordance with The Trust's Information Security Policy and Acceptable Use Policies.

9.1.3 Roles and responsibilities of commencing permanent or contract staff for information security must be included in employee contracts. These must be signed and agreed to by all new members of staff before commencing and being granted access to information systems.

9.1.4 Roles and responsibilities of authorised external parties for information security must be included in engagement contracts. These must be signed and agreed to before the engagement commences and external parties are granted access to information and systems.

9.1.5 Job descriptions for information security roles within The Trust will be defined by the Information Security Manager.

9.2 Screening

9.2.1 Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks

9.2.2 Background experience checks must be undertaken on permanent and contract staff to ensure appropriate skills and knowledge for the role can be verified prior to commencement.

9.2.3 Background experience checks may be passed to third parties such as employment agencies. Employment agencies will be made aware of information security requirements prior to beginning the selection and screening process.

9.2.4 Third parties engaged by The Trust must include skills and competency statements in legal agreements to ensure appropriate skills will be used to provide services.

9.3 Terms and Conditions of Employment

9.3.1 As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organisation's responsibilities for information security.

9.3.2 All management staff within The Trust are responsible for ensuring commencing permanent and contract staff agree to and sign terms and conditions of employment.

9.3.3 All management staff within The Trust are responsible for ensuring external third parties agree to and sign terms and conditions for the specified engagement.

9.4 Management Responsibilities

9.4.1 Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organisation.

9.4.2 All management staff within The Trust are responsible for ensuring their internal staff are made aware of their obligations to information security. Information Security Policy and procedure locations must be made known to staff.

9.5 Information Security Awareness and Education Training

9.5.1 All employees of the organisation and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function.

9.5.2 All staff are required to complete information security awareness training annually. Training will be provided by the Information Security Department and can be delivered via face-to-face and/or content based web training packages.

9.5.3 Divisions and Departments may request the Information Security Department to perform tailored information security awareness sessions. The Information Security Manager will oversee the development of these sessions to ensure the content is applicable to the request.

9.6 Disciplinary Process

9.6.1 There should be a formal disciplinary process for employees who have committed a security breach.

9.6.2 The Trust will implement a formal disciplinary process to deal with staffs who have committed breaches of information security. This

process is part of The Trusts larger staff disciplinary process and is not unique to information security breaches (see Disciplinary Policy and Procedure HR/08/01).

9.6.3 The Trusts Information Security Manager will participate in any disciplinary process where a breach of information security has occurred.

9.7 Termination Responsibilities

9.7.1 Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.

9.7.2 All employment contracts must contain legal clauses binding exiting full-time and contracted staff to maintain the confidentially of Trust information and intellectual property.

9.7.3 It is the responsibility of The Trusts Human Resources Division to ensure all staff contracts include confidentiality clauses.

9.7.4 All Trust Managers are responsible for ensuring their full-time and contracted staffs are aware of their obligations when beginning, transferring and exiting the employ of The Trust.

9.8 Return of Assets

9.8.1 All employees, contractors and third party users should return all of the organisation's assets in their possession upon termination of their employment, contract or agreement. All Trust Managers are responsible for retrieving assets from exiting staff. Assets include, but are not limited to any information technology equipment such as Laptops, removable media, Personal Digital Assistants, remote access tokens and anything of a confidential nature.

9.8.2 An exit form must be signed by exiting staff and Trust Management to prove assets have been recovered. These forms are to be sent to the Human Resources department for cross referencing with IM&T registers and archiving.

9.9 Removal of Access Rights

9.9.1 The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

.

10. Physical and Environmental Security

Information Security Policy Statement
The Trust will implement physical and environmental controls to ensure assets and facilities are appropriately protected from unauthorised access, interference, intentional damage or natural disasters.

10.1 Physical security perimeter

Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.

10.1.1 The Trust will perform regular risk assessments on physical site facilities in order to review and determine if appropriate controls are in place commensurate to the value of assets located within the site.

10.1.2 Perimeter walls of Trust facilities must be of solid construction with no gaps which could possibly be compromised by unauthorised persons.

10.1.3 Perimeter doors and windows of Trust facilities must be secured with appropriate locking and control mechanisms to ensure against unauthorised entry or break-in. Locking and controls mechanisms include CCTV, infra-red alarms, hard keys, barrel door locks, electronic door locks, key pads, swipe and proximity cards, window locks and locking bars.

10.1.4 Perimeter doors and windows of Trust facilities must be locked at all times when unattended.

10.1.5 External door and window protection will be installed for ground level facilities which contain sensitive Trust information processing assets and equipment.

10.1.6 External alarms and building intrusion detection systems must comply with applicable safety standards. Alarms must be tested regularly by the appropriate organisations to ensue they are in good working order.

10.1.7 Perimeter fire doors must be alarmed and comply with local fire code and applicable safety standards. These doors will be tested regularly by the appropriate organisations to ensue they are in good working order.

10.1.8 Where possible, manned reception areas will exist for all Trust facilities which contain control rooms and sensitive information processing assets and equipment. These reception areas must be manned with trained security personnel.

10.1.9 Physical barriers such as gates will be implemented to separate and control access between manned reception areas and internal facilities.

10.1.10 Entry doors to critical control rooms and information processing facilities must be closed and locked at all times. Entry doors to these areas must not be propped open or left ajar. Devices should be installed on these doors to ensure they shut automatically after a

member of staff enters or leaves the room.

10.1.11 Entry doors to critical control rooms and information processing facilities must be monitored by CCTV.

10.2 Physical entry controls

10.2.1 Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

10.2.2 Entry doors to critical control rooms and information processing facilities must be controlled by an audit capable access control system. Where this is not possible a manual process must be put in place to sign guests in and out of these areas via a manual log book. The log booked must be retained for audit purposes.

10.2.3 Access controls systems must be able to log who entered/exited and the date and time of those actions. These logs must be retained for audit and investigation purposes.

10.2.4 Access control logs for critical control rooms and information processing facilities must be retained for a period of 12 months. If the system or process is not capable of archiving for this duration these logs must be archived to appropriately secured media and provided to The Trusts Information Security Department.

10.2.5 All Trust employees, contractors, third party users and visitors must wear Trust issued identification badges at all times. Trust staff encountering anyone without a visible ID badge should ask to see relevant identification.

10.2.6 Third parties who provide support or maintenance to critical control rooms and information processing facilities must only be granted the appropriate level of access when required. Standing access for these persons must be approved by the Information Security Department.

10.2.7 The Information Security Department will regularly review access controls to critical control rooms and information processing facilities.

10.3 Securing offices, rooms, and facilities

10.3.1 Physical security for offices, rooms, and facilities should be designed and applied.

10.3.2 The Trust will ensure all offices; rooms and facilities are appropriately secured. The level of security applied will depend on the role of the office or room which will be determined through regular risk assessments by the Information Security Department.

10.3.3 Security of offices, rooms and facilities will conform to local operational health and safety standards.

10.4 Protecting against external and environmental threats

10.4.1 Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.

10.4.2 The Trust will ensure its physical assets are appropriately protected from external and environmental threats through regular risk assessments and management of a Business Continuity Programme.

10.4.3 Combustible materials must not be stored within critical Emergency Operation Centres or information processing facilities.

10.4.4 Fire fighting equipment such as fire extinguishers, fire suppression and sprinkler systems will be installed within rooms, offices and facilities and must be maintained to local fire code standards.

10.4.5 Fire alarm systems must be tested on a regular basis.

10.5 Working in secure areas

10.5.1 Physical protection and guidelines for working in secure areas should be designed and applied.

10.5.2 Emergency Operation Centres and information processing facilities must remain locked at all times. Doors to these areas must not be left ajar or propped open.

10.5.3 Third parties must be escorted within Emergency Operation Centres and information processing facilities at all times. Authorisation for standing access must be approved by The Trusts Information Security Department.

10.5.4 Staff without standing access to Emergency Operation Centres and information processing facilities who require access for business purposes must be escorted at all times.

10.5.5 Eating and drinking within information processing facilities is not permitted.

10.5.6 In the face of operational demands, it may not be possible to adhere to these controls. A decision will be made by the Gold when these controls are not in effect.

10.6 Public access, delivery, and loading areas

10.6.1 Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

10.6.2 All public access delivery and loading areas must be regularly risk assessed to ensure they are appropriately secured.

10.6.3 Public access delivery and loading areas must not directly connect to information processing facilities.

10.6.4 Public access delivery and loading areas must be designed so external parties cannot gain direct access to The Trusts facilities without authorisation.

10.7 Equipment siting and protection

10.7.1 Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

10.7.2 The Trust will implement and maintain appropriate environmental control systems within information processing facilities to protect against excess temperature, humidity, loss of power, electromagnetic fields, lightning strikes and fire. These controls must be regularly tested and maintained by the appropriate third parties.

10.7.3 Systems requiring special controls will be segregated from standard systems and identified appropriately. The Trust's Information Security Department should perform risk assessments to ensure controls are appropriate for the value of the system or device.

10.8 Supporting utilities

10.8.1 Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

10.8.2 The Trust will ensure supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning are installed and maintained.

10.8.3 The Trust will ensure utility services are regularly inspected by the appropriate organisations. Where necessary safety certificates should be requested to prove compliance with applicable safety standards.

10.8.4 The Trust will implement uninterruptable power supplies within its Emergency Operations Centres and information processing facilities. These will form part of The Trust's power contingency plans which should also include back-up generators for critical operational and information processing services.

10.8.5 Emergency Operation Centres and information processing facilities must be fitted with emergency lighting in the case of power failure.

10.8.6 Critical systems in support of Emergency Operations Centres and information processing facilities should have power provided from separate utility providers circuits as a fail-safe measure.

10.9 Cabling security

10.9.1 Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

10.9.2 Network cabling will be appropriately secured against damage and interference and not accessible or visible to the public or non-authorised persons.

10.9.3 Network cabling must be separated from power cabling to prevent interference.

10.9.4 Network cables must be clearly labelled so as to identify there purpose or association to a particular device. These should be documented for reference and change management purposes.

10.9.5 All network cables must be shielded to protect against electromagnetic interference.

10.9.6 Access to network patch panels and cable rooms must be controlled and only accessible by authorised support staff. Common areas should not be used to house this type of equipment.

10.10 Equipment maintenance

10.10.1 Equipment should be correctly maintained to ensure its continued availability and integrity.

10.10.2 Trust management is responsible for ensuring equipment is appropriately maintained in accordance with manufacturer recommendations.

10.10.3 Only authorised, trained persons should perform maintenance on equipment. This work must be scheduled and managed through the IM&T Change Management Process.

10.10.4 Equipment maintenance log records must be kept for audit purposes.

10.11 Security of equipment off-premises

10.11.1 Security should be applied to off-site equipment taking into account the different risks of working outside the organisation's premises.

10.11.2 Equipment and media assets taken off Trust premises must not be left unattended in public places and must be secured at all times.

10.11.3 Laptop computers must be carried as hand luggage and kept within a purpose designed bag to protect the device from damage.

10.11.4 LAS supplied connections and equipment used for home working purposes must be authorised by the appropriate Trust management staff and a risk assessment of the premises

10.12 Secure disposal or re-use of equipment

10.12.1 All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

10.12.2 Equipment and media which is to be disposed of must be sanitised appropriately. This must be commensurate to the sensitivity of the data contained within the item.

10.12.3 Equipment and media known to contain Patient Information must be sanitised prior to recycling or destruction. Certificates confirming sanitization should be kept for audit and compliance purposes.

10.12.4 Processes within The Trust which require the creation, storage, transmission or destruction of Patient Information should be regularly risk assessed by the appropriate internal division.

11. Communications and Operations Management

Information Security Policy Statement
The Trust will implement appropriate controls to ensure secure and controlled operational running of information management and technology assets and processing facilities.

11.1 Documented operating procedure

11.1.1 Operating procedures should be documented, maintained, and made available to all users who need them.

11.1.2 IM&T managers will maintain operating procedures for system activities associated with information processing and communication facilities. These are to include details of processing/handling of information, backup procedures, error handling instructions, support contacts and special instructions.

11.2 Change management

11.2.1 IM&T will follow strict change control procedures. These are to include:

- identification and recording of Request For Change (RFC) documents.
- planning and testing of changes.
- assessment of the potential impacts, including security impacts, of such changes.
- documentation of fallback procedures and responsibilities.
- communication of change details to all relevant persons.
- formal review of proposed RFC's by the Change Advisory Board (CAB).

11.3 Separation of development, test, and operational facilities

11.3.1 Development, test, and operational facilities should be separated to reduce the risks of unauthorised access or changes to the operational system.

11.3.2 IM&T will ensure development and operational software runs in different environments.

11.3.3 IM&T will ensure test environments emulate operational environments as closely as possible.

11.3.4 IM&T will ensure sensitive data never enters test environments.

11.4 Controls against malicious and mobile code

11.4.1 Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.

11.4.2 A formal policy will be established prohibiting unauthorised software. Critical systems will be regularly reviewed for exceptions to this policy and the presence of any unauthorised files will be investigated.

11.4.3 IM&T will install and maintain malicious code detection and repair software. This software will check data being read from email, removable media and networks. Checks will take place at different locations (eg. file servers as well as desktop computers).

11.4.4 IM&T will put into place business continuity plans to recover from malicious code outbreaks.

11.4.5 Where the use of mobile code is authorized, the configuration should ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.

11.4.6 IM&T will block the use of non-critical mobile code.

11.4.7 Where mobile code is critical, resources available to the mobile code will be controlled to that of least permissions required.

11.4.8 Where mobile code is critical, cryptographic controls will be used to authenticate mobile code.

11.5 Information back-up

11.5.1 Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

11.5.2 IM&T will back-up all information on network servers and will keep accurate and complete records of these.

11.5.3 IM&T will store backups in a secure remote location.

11.5.4 IM&T will test backup media regularly.

11.5.5 IM&T will produce documentation on restoration procedures. These will be regularly reviewed.

11.6 Network Security controls

11.6.1 Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

11.6.2 NHS Connecting for Health approved Encryption methods and

strengths must e used when data is passing over public networks or wireless networks.

11.6.3 IM&T will log and monitor relevant network events.

11.6.4 IM&T will establish responsibilities involved in the management of remote connections and equipment.

11.6.5 Trust networks must be configured and managed in accord with Information Security Department Technical Security Requirements.

11.6.6 Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

11.6.7 Security for network services (e.g. private network services, firewalls) is to be agreed upon, including security features, service levels and management requirements.

11.6.8 A Technical Security Requirements document must exist to ensure network services are appropriately secured.

11.6.9 Users should only be provided with access to the services that they have been specifically authorized to use.

11.6.10 Network services within The Trust will be managed and maintained by the IM&T Directorate.

11.6.11 The IM&T Directorate will ensure appropriate network operating procedures are in place and documented.

11.6.12 The IM&T Directorate will ensure appropriate network operating procedures exist to control access to The Trust's networks. Access can only be granted under authority from the IM&T Directorate and must be based on the principal of least privilege.

11.6.13 The IM&T Directorate will control the management of network changes through the IM&T Change Control process.

11.6.14 The IM&T Directorate will develop Technical Security Requirements to ensure network and device designs and configurations are appropriately secured prior to production implementation.

11.6.15 The IM&T Directorate will ensure NHS Connecting for Health security recommendations for connections to external agencies, non-trusted networks and remote access connections are implemented.

11.6.16 Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

11.6.17 The IM&T Department will implement Technical Security Requirements and configurations for routing device controls in accordance with networking and security industry good practice.

11.7 Management of removable media

11.7.1 Removable media leaving the Trust must be authorised and records kept. If the contents of the media are no longer required, data should be first made unrecoverable.

11.7.2 Removable media must be stored in a safe, secure environment.

11.7.3 The use of personally owned removable media on Trust computing devices is not permitted.

11.8 Physical media in transit

11.8.1 Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organisation's physical boundaries

11.8.2 Only Secure couriers are to be used in the exchange of sensitive information.

11.8.3 Appropriate packaging to protect the media from physical damage must be used during transport.

11.8.4 Devices storing sensitive information must either be securely transported by a Trust staff member, must be encrypted or sealed in a registered tamper proof via secure transport.

11.9 Disposal of media

11.9.1 Media should be disposed of securely and safely when no longer required, using formal procedures.

11.9.2 Media containing sensitive data that requires disposal must be sanitised to US Department of Defence levels to ensure that information is not recoverable.

11.9.3 If a third party service is to be used in disposal, their controls and experience will be verified. Validation certificates must be provided to The Trust as proof of sanitizing or destruction.

11.9.4 Disposal of media will be logged to provide an audit trail.

11.10 Information exchange policies and procedures

11.10.1 Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.

11.10.2 All sensitive data leaving the Trust in the form of electronic communications will be encrypted to a level in accordance with Connecting for Health recommendations.

11.10.3 IM&T will disseminate information highlighting the dangers of non-electronic forms of communication. This includes paper, telephone calls, answering machines and facsimile machines.

11.10.4 Paper containing sensitive information is not to be left unsecured.

11.10.5 Employees will be aware of those in the vicinity when revealing sensitive information over the telephone.

11.10.6 Employees will not leave sensitive information on answering or fax machines, as these may be replayed in the presence of non-authorised persons

11.10.7 Agreements should be established for the exchange of information and software between the organisation and external parties.

11.10.8 IM&T will create formal agreements between the Trust and external parties should information need to be exchanged. These must be reviewed and approved by The Trusts Legal Department.

11.10.9 Electronic transmission will be encrypted at a minimum encryption standard in accord with NHS Connecting for Health requirements.

11.10.10 Both parties will be made aware of the successful execution of each stage of an exchange: transmission/dispatch and receipt.

11.10.11 Only Secure couriers are to be used in the physical exchange of sensitive information.

11.10.12 Information involved in electronic messaging should be appropriately protected.

11.10.13 Electronic messages containing sensitive information must only be sent via NHS Mail or Outlook with encryption levels in accord with NHS Connecting for Heath recommendations. See 'TP/063 Acceptable usage of IT and Communications Equipment Policy'.

11.11 Publicly available information

11.11.1 The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification.

11.11.2 Trust information created for the express purpose of Internet publishing to non-Trust staff and partnering organisations must be classified as Public information. This type of information should be approved by the Information Security Department in accordance with Data Protection requirements.

11.11.3 Sensitive information made available to Trust staff and partnering organisations via the Internet must be protected with 128 bit SSL encryption and two factor authentication. Web servers storing this

information must be built in accord with Information Security Department Technical Security Requirements for Web Servers.

11.11.4 The integrity of information stored on publicly available systems will be protected with approved NHS Connecting for Health encryption algorithms.

11.11.5 Web servers must exist within a zoned network architecture. Web traffic must be controlled in order to prevent unauthorised parties on the Internet from compromising web facing systems and gaining access to internal Trust networks.

11.12 Logging and Monitoring

11.13.1 Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

11.13.2 IM&T will audit certain user activities and archive these for future troubleshooting and investigations.

11.13.3 Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.

11.13.4 System monitoring results will be reviewed regularly according to the sensitivity/criticality of the system in question.

11.14 Protection of log information

11.14.1 Logging facilities and log information should be protected against tampering and unauthorized access.

11.14.2 Log information for systems storing sensitive information will be kept in a secure area, accessible only by Domain Administrators and Information Security staff.

11.14.3 The capacity of this area will be monitored regularly, to ensure that there is sufficient storage space to store new log information. Logs will be archived, stored and deleted in accord with Data Protection requirements.

11.14.4 Administrator and system operator activities will be logged on server systems and archived in accord with Data Protection and Information Security Department requirements.

12. Access Control

Information Security Policy Statement

The Trust will implement appropriate controls to ensure physical and logical access to paper based and electronic information, physical assets, information processing facilities, business processes and core operating functions is authorised to the least amount of access required by staff to perform their roles.

12.1 Access control policy

An access control policy should be established, documented, and reviewed based on business and security requirements for access.

The Trust will implement Access Control standards for physical and logical assets.

12.2 User registration

There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

- Trust management staff are responsible for ensuring commencing staff, transferring staff, staff on extended leaves of absence and exiting staff are identified and made known to The Trust's Human Resources and IM&T Directorates.

- The following controls for user registration and de-registration of standard user accounts must be followed:

  Account Creation

  i. Only authorised IM&T staff can create new User Accounts for access to Information Technology (IT) resources.

  ii. All new User Account requests must be processed through The Trusts Human Resources Directorate.

  iii. Newly created User Accounts must be authorised by the Human Resources Directorate and relevant Directorate management.

  iv. Directorate Managers are responsible for advising the Human Resources Directorate when new staff commence with The Trust.

  v. Authorisation for new User Accounts must be captured by IM&T and archived for audit purposes.

  vi. New User Account requests must capture the required

level of access to Trust IT resources (e.g. email, folders, Internet).

vii. Principle of Least Privilege must be enforced on all User Accounts

viii. User Accounts must be unique to the account holder.

ix. Trust Staff may only be issued one User Account unless under authority of the Director of IM&T (e.g. special access administration/access accounts).

x. User Accounts must adhere to IM&T naming standards.

Account Change

i. Only IM&T authorised IM&T staff may change User Accounts for access to IT resources.

ii. Authorisation for changes to User Accounts must be authorised by the relevant Directorate Manager.

iii. Directorate Managers are responsible for advising the Human Resources Directorate when staff move Departments or Directorates.

iv. A formal request for User Account change must be raised through the IM&T Service Desk including manager authorisation and details of the change.

Account Termination

i. Only authorised IM&T staff may terminate User Accounts for access to IT resources.

ii. Directorate Managers are responsible for advising the Human Resources Directorate when staff leave the LAS or move department.

iii. User Accounts must only be terminated under authority from the Human Resources Directorate.

iv. A formal request for User Account termination must be raised through the IM&T Service Desk including manager and Human Resources Directorate authorisation.

Account Suspension

i. User Accounts may be suspended if a member of staff is found to be in breach of LAS policy.

ii. User Accounts may only be suspended under authority of the relevant Directorate Manager and approved by the IM&T Director and/or Information Security Manager.

iii. A user whose access has been suspended may request reconsideration of the decision by the relevant Directorate Manager.

iv. Account suspension incidents must be tracked for potential investigative purposes.

Account Maintenance

i. IM&T will implement standards for User Account management in accord with NHS Connecting for Health recommendations.

ii. User Account maintenance must be performed periodically by the IM&T Directorate.

iii. User Accounts which have not logged into Trust IT resources for a period of 90 days will be disabled.

iv. User Accounts which have not logged into Trust IT resources for a period of 120 days will be deleted.

12.3 Privilege management

The allocation and use of privileges should be restricted and controlled.

12.3.1 The following controls for user registration and de-registration of privileged user accounts (those which have additional rights over standard user accounts) must be followed:

Account Creation

i. Only authorised IM&T staff may create new User Accounts for access to production systems.

ii. All new Privileged User Account requests must be made to the Information Security Department for approval.

iii. Newly created Privileged User Accounts must be authorised by the Information Security Manager and relevant Directorate management.

iv. Authorisation for new Privileged User Accounts must be archived by Information Security Department for audit purposes.

v. The Information Security Department must keep a register of all Privileged User Accounts.

vi. Principle of Least Privilege must be enforced on all User Accounts.

vii. Privileged User Accounts must be separate from Standard User Accounts.

viii. Privileged User Accounts must adhere to IM&T naming standards.

Account Change

i. Changes to Privileged User Accounts must first be approved by the Information Security Department.

ii. Authorisation for changes to Privileged User Accounts must be authorised by the relevant Directorate Manager.

Account Termination

i. The Information Security Department must be notified immediately of any exiting staff who use Privileged User Accounts.

ii. Privileged User Accounts must be disabled immediately after the member of staff has left the LAS.

iii. IM&T must implement a process for monitoring Privileged User Account use.

Account Suspension

i. Privileged User Accounts may be suspended at any time under authority from the IM&T Director, IM&T Senior Management Team or Information Security Manager.

Account Maintenance

i. IM&T must implement standards for Privileged User Account management in accord with NHS guidelines.

ii. Privileged User Account maintenance must be performed monthly by the Information Security Team.

iii. Privileged User Accounts which have not logged into LAS IT resources for a period of two weeks will be disabled.

iv. Privileged User Accounts which have not logged into Trust IT resources for a period of 14 days will be disabled.

v. Privileged User Accounts which have not logged into Trust IT resources for a period of 30 days will be deleted.

12.4 User password management

The allocation of passwords must be controlled through a formal management process.

12.4.1 Password management for The Trust's standard and privileged user accounts is the responsibility of the IM&T Directorate

12.4.2 New user accounts will be issued a temporary password. The password management system will enforce an immediate change once the user has logged on.

12.4.3 Temporary passwords must be unique and conform to standard user account password standards.

12.4.4 Staff requesting a new or replacement password must first be positively identified by IM&T staff. Passwords must not be issued to staff until the identity of the requestor can be verified.

12.4.5 Passwords must never be communicated via third parties, in clear text or via unprotected communication channels (eg. unencrypted email).

12.4.6 Passwords must never be stored in unencrypted form on computing devices or media.

12.4.7 Default vendor passwords must be immediately changed to conform to The Trusts standards.

12.5 Review of user access rights

12.5.1 Management should review users' access rights at regular intervals using a formal process.

12.5.2 Privileged access rights to Patient Information must be reviewed by the Information Governance Group every 6 months.

12.5.3 Management should review all other user access rights at regular intervals.

12.5.4 Changes to privileged accounts must be logged for compliance and audit purposes.

12.6 Password use

12.6.1 All standard user account passwords must be a minimum of 7 alphanumeric characters in length. Passwords cannot be easily guessable words.

12.6.2 The system for managing passwords must be set to recycle passwords every 60 days.

12.6.3 The system for managing passwords must be set to remember the last 12 passwords.

12.6.4 Staff are responsible for keeping passwords secret at all times.

12.6.5 Staff must not write passwords down.

12.6.6 Staff must not share passwords.

12.6.7 Exceptions to this will be considered by the Director of IM&T or by Gold if operational requirements dictate.

12.7 Unattended user equipment

12.7.1 Users should ensure that unattended equipment has appropriate

protection

12.7.2 All desktop computing systems will enforce a password protected screensaver which will enable after 10 minutes of user inactivity.

12.7.3 All Staff must log out of computing systems at the end of each day or if the system is to be unattended for a long period of time. Computing systems should not be left logged in and locked overnight.

12.7.4 Portable computing devices such as Laptops and Personal Digital Assistants must be stored in a secure cabinet or room when not in use for extended periods.

12.8 Clear desk and clear screen policy

12.8.1 A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

12.8.1 Staff must ensure their workspace is cleared of sensitive information at the end of every day.

12.8.2 Staff must lock Patient Information and all other types of identified sensitive information in secure storage at the end of every day.

12.8.3 Staff must ensure sensitive information which is printed is collected immediately from the printer and stored appropriately.

12.8.4 Incoming and outgoing mail points which may send or receive Patient Information must be secured appropriately. A risk assessment should be performed on a case by case basis.

12.9 Remote diagnostic and configuration port protection

12.9.1 Physical and logical access to diagnostic and configuration ports should be controlled.

12.9.2 Logical access to network diagnostic and configuration ports will be controlled by the IM&T Directorate.

12.9.3 IM&T will ensure physical network diagnostic and configuration equipment is located within secure facilities, rooms and cabinets at all times. Cabinets containing this type of equipment must be locked at all times. Access should be logged for compliance and audit purposes.

12.9.4 IM&T will ensure unused network device ports, services or facilities are disabled.

12.10 Segregation in networks

12.10.1 Groups of information services, users, and information systems should be segregated on networks.

12.10.2 Emergency Operation Centre network segments should be physically and logically separated from back office support systems.

12.10.3 Emergency Operation Centre network segments should be monitored by Intrusion Prevention Systems.

12.10.4 Systems containing Patient Information should exist in a highly secure network segment which enforces internal policy enforcement points such as routers and enterprise class Firewalls.

12.10.5 Segregation must exist between internally managed networks and any untrusted networks. These must be separated by policy enforcement points such as routers or enterprise class firewalls.

12.10.6 Web services should be designed in a multi-tiered network architecture to ensure web, application and database platforms are not at risk of compromise from the Internet.

12.10.7 Network segments attached to the Internet must implement Intrusion Prevention systems to monitor inbound traffic for malicious activity.

12.10.8 Wireless network segments must be monitored by Intrusion Prevention Systems specifically designed for monitoring radio wave networks.

12.11 Secure log-on procedures

12.11.1 Access to operating systems should be controlled by a secure log-on procedure.

12.11.2 All Operating Systems must display a legal logon notice prior to logon. The notice must be approved by The Trust's Legal Department.

12.11.3 The number of unsuccessful logon attempts to Operating Systems before the account is disabled must be set to 5.

12.11.4 All Operating Systems and applications must hide or mask password characters so they cannot be viewed by unauthorised parties.

12.11.5 All Operating Systems and applications must not transmit passwords in clear text.

12.12 User identification and authentication

12.12.1 All users should have a unique identifier (UserID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.

12.12.2 All staff authorised to access The Trust's IT systems must be issued a unique UserID and password.

12.12.3 IM&T service desk staff must implement procedures for accurately identifying staff when calling to have a UserID password reset.

12.12.4 Generic UserID's may be used for temporary staff, however account passwords must be reset by the IM&T Directorate once the account is handed to a new temporary staff member.

12.13 Password management system

12.13.1 Systems for managing passwords should be interactive and should ensure quality passwords.

12.13.2 The password management system must be able to enforce the use of individual user IDs and passwords to maintain accountability.

12.13.3 The password management system must allow users to select and change their own passwords and include a confirmation procedure to allow for input errors.

12.13.4 The password management system must enforce a choice of quality passwords.

12.13.5 The password management system must enforce password changes.

12.13.6 The password management system must force users to change temporary passwords at the first log-on.

12.13.7 The password management system must maintain a record of previous user passwords and prevent re-use.

12.13.8 The password management system must not display passwords on the screen when being entered.

12.13.9 The password management system must store password files separately from application system data.

12.13.10 The password management system must store and transmit passwords in protected (e.g. encrypted or hashed) form.

12.14 Information access restriction

12.14.1 Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.

12.14.2 The principle of least privilege must be used when provisioning access to Trust information and systems.

12.14.3 Restrictions to access for sensitive network applications and systems should undergo a regular risk assessment to determine the appropriateness of existing access controls and permissions.

12.14 Mobile computing and communications

12.14.1 A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.(See Laptop Security Policy TP/043)

12.14.2 Mobile computing devices such as Laptops, Personal Digital Assistants, Smartcards, Mobile Phones, Digital Recorders and USB Drives must only be configured and issued to staff by the IM&T Directorate.

12.14.3 Laptop computers, Personal Digital Assistants and USB Drives must be configured with encryption software prior to being issued.

12.14.4 Laptop computers with wireless interfaces enabled must not be able to connect to wired and wireless networks simultaneously.

12.14.5 Laptop computers should be issued to staff with a physical locking device or cable lock.

12.14.6 Information from mobile computing devices must be backed-up to network drives regularly.

12.14.7 All mobile computing devices should be configured with protection against malicious software programmes.

12.14.8 All staff authorised to use mobile computing devices must be trained in the use of such devices prior to receiving them.

12.14.9 All mobile computing devices must adhere to Information Security Department Technical Security Standards.

12.14.10 All new mobile computing devices must undergo a risk assessment by the Information Security Department.

13. Systems Acquisition, Development and Maintenance

Information Security Policy Statement

The Trust will implement appropriate controls to ensure newly acquired or developed system and application designs identify security requirements prior to production release and are implemented in a controlled and secure manner.

13.1 Security requirements analysis and specification

13.1.1 Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.

13.1.2 Security requirements for new information systems must be identified at the planning phase of the development or acquisition project.

13.1.3 A risk assessment should be conducted as part of any business case to acquire or develop new information technology systems.

13.1.4 Contracts with suppliers engaged to develop or support newly acquired or developed systems and applications must include information security, confidentiality and non-disclosure agreements. These contracts should also include a Key Controls compliance statement.

13.1.5 Formal testing and sign-off must occur prior to newly acquired or developed systems and applications being released into production environments.

13.2 Input data validation

13.2.1 Data input to applications should be validated to ensure that this data is correct and appropriate.

13.2.2 Validation checks must be implemented when processing sensitive information to ensure against out-of-range values, invalid characters in data fields, missing or incomplete data, exceeding upper and lower data volume limits, unauthorized or inconsistent control data

13.2.3 Period reviews of sensitive data fields must be conducted to ensure their validity and integrity.

13.2.4 Procedures must exist for responding to validation errors and for testing the plausibility of sensitive input data.

13.2.5 Procedures must exist defining the responsibilities of all personal involved with sensitive data input processes.

13.2.6 An activity log of sensitive data input processes should be kept for audit purposes.

13.3 Policy on the use of cryptographic controls

13.3.1 A policy on the use of cryptographic controls for protection of information should be developed and implemented.

13.3.2 Cryptographic controls must be implemented in accord with NHS Connecting for Health recommendations.

13.3.3 A risk assessment must be conducted to determine which algorithms and encryption systems are most appropriate commensurate to the sensitivity of the information and/or the value of the asset in question.

13.3.4 All mobile devices which have the ability to store sensitive information locally must be encrypted.

13.3.5 Sensitive information which traverses untrusted networks must be encrypted.

13.3.6 Requirements for encryption key managed must be determined by the Information Security Department.

13.3.7 Encrypted traffic entering the Trusts networks from untrusted networks must be decrypted before reaching filtering and scanning gateways.

13.3.8 Key management should be in place to support the organisation's use of cryptographic techniques.

13.3.9 All key management strategies and architectures must be reviewed and approved by The Trusts Information Security Department prior to production implementation.

- The following procedures must exist for key management systems:

    i. key generation techniques including public key certificates

    ii. key distribution to intended users including key activation

    iii. key storage and authorisation to access stored keys

    iv. Key updating

    v. Key compromise

    vi. Key revocation lists

    vii. Business Continuity

    viii. Key archiving & back-up

    ix. Key destruction

    x. Audit logging of key management processes

13.4 Control of operational software

13.4.1 There should be procedures in place to control the installation of software on operational systems.

13.4.2 The installation of software on information technology systems must be authorised and performed by the IM&T Directorate.

13.4.3 Applications and operating systems must be tested and approved prior to production release.

13.4.4 A configuration control system must be used to manage software library and operating system updates.

13.4.5 Previous versions of application software must be retained as a contingency measure.

13.5 Protection of system test data

13.9.1 Test data should be selected carefully,and protected and controlled.

13.9.2 Patient Information must not be used in test environments.

13.5.3 Other types of sensitive information must first be scrubbed or masked before being used in a test environment.

13.5.4 Other types of sensitive information to be used in test environments must first be authorised by management.

13.5.5 Test environments requiring the use of production data must have equal security and access controls.

13.5.6 Test environments that are no longer required which contained sensitive information must have operational configurations and hard disk drives wiped before being re-used.

13.5.7 System acceptance testing must be performed prior to production release.

13.6 Change control procedures

13.6.1 The implementation of changes should be controlled by the use of formal change control procedures.

13.6.2 Changes to information technology systems must follow the IM&T Divisions Change Control process. This includes applications, development source code, operating systems, physical devices, network and telecommunications equipment.

13.7 Restrictions on changes to software packages

13.7.1 Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.

13.7.2 Vendor supplied software packages should not be modified from their original versions. If this is required the Vendor should be contacted for specific instructions or support on how to carry out the changes without compromising functionality or security.

13.7.3 Only The Trusts IM&T Directorate is authorised to consider changes to vendor supplied software packages.

13.7.4 Any changes must be fully documented and carried out under the IM&T Directorates Change Control process.

13.8 Information leakage

13.8.2 Opportunities for information leakage should be prevented.

13.8.2 Administrative controls such as policy communication and education and awareness training must be implemented to ensure staff are aware of their responsibilities towards the confidentiality of information while under the employ of The Trust.

13.8.3 Where practical content monitoring systems should be implemented to log and block sensitive outgoing information by members of staff.

13.9 Outsourced software development

13.9.1 Outsourced software development should be supervised and monitored by the organisation.

13.9.2 Where software development is outsourced, the following points should be considered:

i. Licensing arrangements, code ownership, and intellectual property rights.

ii. certification of the quality and accuracy of the work carried out.

iii. escrow arrangements in the event of failure of the third party.

iv. rights of access for audit of the quality and accuracy of work done.

v. contractual requirements for quality and security functionality of code.

vi. testing before installation to detect malicious and Trojan code.

13.10 Control of technical vulnerabilities

13.10.1 Timely information about technical vulnerabilities of information systems being used should be obtained, the organisation's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

13.10.2 The Trusts Information Security Department is responsible for managing technical vulnerability alerting and advising internal departments of relevant updates to be applied.

13.10.3 IM&T management staff are responsible for ensuring staff participate in vulnerability management processes and support the patching recommendations made by the Information Security Department.

13.10.4 All web facing systems and internal systems storing sensitive information must be regularly reviewed by the Information Security Department to ensure appropriate controls are in place to mitigate against technical vulnerabilities.

13.10.5 Any security patching or system updating related to technical vulnerabilities must be performed under a Request For Change.

13.10.6 Security patches must be tested and signed off by the relevant management staff before being deployed to production systems.

13.10.7 An automated scan of information technology systems must be conducted annually to identify current security patch levels and potential configuration vulnerabilities which may require remediation.

14. Incident Management

Information Security Policy Statement

The Trust will implement appropriate controls to ensure information security incidents are detected, reported, responded to and resolved within an acceptable timeframe and that incident types and reporting and escalation Procedures are communicated to staff.

14.1 Reporting information security events

14.1.2 Information security events should be reported through appropriate management channels as quickly as possible.

14.1.3 The Trusts Information Security Department will create and make aware a formal information security incident reporting procedure document. This will include:

- The process of reporting incidents.
- Key contacts and escalation points.
- A form/template to assist in reporting incidents.

14.2 Reporting security weaknesses

14.2.1 All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.

14.2.2 The Trusts Information Security Department will create and make aware a formal information security weakness reporting procedure document. This will include:

- The process of reporting weaknesses.
- Key contacts.
- A form/template to assist in reporting weaknesses.

14.3 Responsibilities and procedures

14.3.1 Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.

14.3.2 The Trusts Information Security Department will create incident response procedures to cover different information security incidents. These will cover:

- Identification of the cause of the incident
- Containment of affected systems if necessary
- Communication with those involved/affected by the incident.
- Planning and implementation of corrective action
- Collection of evidence as necessary
- Documentation of emergency actions and reporting of these to management.

14.4 Learning from information security incidents

14.4.1 There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

14.4.2 The Trusts Information Security Department will record and review information security incidents. This may indicate incident trends which may then be utilised to reduce future occurrences.

14.5 Collection of evidence

Where a follow-up action against a person or organisation after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

14.5.1 Control Requirements

Information Security will develop and maintain strict procedures detailing the collection of evidence. This will include:

- Use of forensic tools/techniques to maintain evidently integrity.
- Secure storage of electronic or non-electronic evidence.
- Legal considerations to be taken into account.

15. Business Continuity Management

Information Security Policy Statement
The Trust will implement management processes to ensure the timely resumption of services to the public in the event of unforeseen service outages.

15.1 Including information security in the business continuity management process

15.1.1 A managed process should be developed and maintained for business continuity throughout the organisation that addresses the information security requirements needed for the organisation's business continuity.

15.1.2 The Trust will develop and maintain processes for business continuity.

This will encompass Identification of critical business processes,

- Understanding risks to the Trust and their potential impact.
- Identification and consideration of preventative/mitigating controls.
- Ensuring that business continuity is incorporated into the Trust's structure.
- Responsibility will be assigned to an appropriate level in the Trust.
- Purchasing insurance where deemed necessary.
- Testing and updating of plans and processes.

15.1.3 Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security.

15.1.4 The Trust will identify events that may cause interruptions to operations. This will be followed by a risk assessment to determine the probability and impact of such interruptions.

15.1.5 Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

15.1.6 Development of business continuity plans will consider the following:

- Agreement of responsibilities.
- Identification of acceptable loss of information or services.
- Procedures to recover and restore operations as well as post-recovery and restoration procedures.

- Education of staff in the agreed procedures and processes.
- Testing, reviewing and updating of plans.
- Documentation of all agreed procedures and processes.

15.2 Testing, maintaining and re-assessing business continuity plans

15.2.1 Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective.

15.2.2 Business continuity plans will be tested regularly in line with the test schedule. The results of test will be recorded and reviewed. Testing will cover the following:

- Technical recovery testing
- Testing recovery at an alternate site
- Testing third party services
- Complete rehearsals
- Any weaknesses found, or changes in business arrangements will require an update to business continuity plans.

16. Compliance

Information Security Policy Statement

The Trust will implement appropriate controls to ensure breaches of any statutory, regulatory or contractual law does not occur and expert legal counsel will be contacted to advise on legal compliance matters.

16.1 Identification of applicable legislation

16.1.1 All relevant statutory, regulatory, and contractual requirements and the organisation's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organisation.

16.1.2 IM&T will identify and subsequently document all statutory, regulatory and contractual requirements applicable to the Trust in relation to information security. These will be defined and documented.

16.2 Intellectual property rights (IPR)

16.2.1 Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

16.2.2 IM&T will create policies to define the legal use of software products and intellectual property rights. Staff will be made aware of this policy and ramifications for breeching it.

16.2.3 IM&T will only acquire software through reputable sources. Licenses proving ownership of software are to be kept securely.

16.2.4 IM&T will monitor for unauthorised/unlicensed software using appropriate audit tools.

16.2.5 The Trust will not duplicate media content (film, audio, books, articles, etc) from sources other than those allowed by copyright law.

16.3 Protection of organisational records

16.3.1 Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

16.3.2 The Trust will categorise records by record types. These will be clearly labelled including the required retention period.

16.3.3 IM&T will store electronic media in line with manufacturer's recommendations.

16.3.4 IM&T will utilise electronic media that will ensure acceptable recovery times for records.

16.3.5 A retention schedule will be created, detailing records and their associated retention period as per statutory, regulatory or contractual requirements.

16.3.6 Where necessary, records will be stored securely to meet statutory, regulatory or contractual requirements.

16.4 Data protection and privacy of personal information

16.4.1 Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

16.4.2 An organisational data protection and privacy policy will be created and maintained. Staff will be made aware of the existence of this policy. The policy will take into account all appropriate legislation.

16.5 Prevention of misuse of information processing facilities

16.5.1 Users should be deterred from using information processing facilities for unauthorized purposes.

16.5.2 Employees will be asked to sign an agreement stating that they understand and accept the scope of authorised use of information processing facilities as well as any monitoring that may take place.

16.5.3 Prior to system log-on, a message will be displayed outlining the Trusts ownership of the system and that unauthorised access is not permitted.

16.6 Regulation of cryptographic controls

16.6.1 Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations.

16.6.2 IM&T will seek legal advice in relation to restrictions on the usage of encryption.

16.6.3 The use of encryption in cross-border information transactions must be reviewed by The Trusts Legal and Information Security Departments prior to the transaction taking place.

16.7 Compliance with security policies and standards

16.7.1 Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

16.7.2 Managers within the Trust will regularly review compliance of security policies and requirements within their area of responsibility. Records of reviews and results shall be maintained

16.7.3 If non-compliance is found, the cause will be determined, followed by corrective actions and a subsequent review which may require The Trusts official disciplinary process to be invoked.

16.8 Technical compliance checking

16.8.1 Information systems should be regularly checked for compliance with security implementation standards.

16.8.2 IM&T will check the technical compliance of information systems either manually or with the assistance of tools. Results will always be reviewed by an experienced systems engineer.

16.8.3 Internet facing systems and devices should be checked annually by an independent third party to ensure security requirements compliance.

16.8.4 Internal systems and devices should be scanned regularly to ensure security requirements compliance.

16.9 Information systems audit controls

16.9.1 Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes.

16.9.2 Prior to auditing live systems, planning will occur. Items that will be considered include:

- Requirements and scope of the audit.
- Where possible auditing will be restricted to read-only access to the systems in question.
- All procedures, requirements, scope and responsibilities will be documented.
- Auditing should be carried out by personnel independent of the activities audited.
- Any special circumstances.

16.10 Information systems audit controls

16.10.1 Access to information systems audit tools should be protected to prevent any possible misuse or compromise.

16.10.2 IM&T will store auditing tools separately to operational or development tools. Appropriate access controls will be used to secure these tools.

16.10.3 IM&T will store system documentation securely with permissions in line with a need-to-know basis.

IMPLEMENTATION PLAN	
Intended Audience	All LAS Staff
Dissemination	Available to all staff on the Pulse and to the public on the LAS website.
Communications	Revised Policy to be announced in the RIB and a link provided to the document.
Training	Information Security training is provided to new staff at Corporate Induction and to existing staff through a three year core training refresher course for support staff and via online IG training. Information Security training will be preformed via awareness sessions, presentation and as when required
Monitoring	This will be monitored via gap analysis exercises, audits, spot checks, Incident statistics etc This will be made available to the Information Governance Group and Senior Managers Group to ensure corporate and departmental compliance with obligations.

17. Definitions

Asset;
Anything that has value to the organisation

Availability;
The property of being accessible and usable upon demand by an authorized entity

Confidentiality;
the property that information is not made available or disclosed to unauthorized individuals, entities, or processes

Information Security;
Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

Information Security Incident;
a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

Information Security Management System (ISMS);
part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

NOTE: The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

Integrity;
the property of safeguarding the accuracy and completeness of assets

Need-to-know;
Describes the restriction of data which is considered very sensitive and aims to discourage "browsing" of sensitive material by limiting access to the smallest possible number of people.

Principle of Least Privilege;
Access to information and resources which is restricted based on user necessity and legitimate purpose within their job role or function.