East of England Ambulance Service NHS Trust

Electronic Information Security Policy

Document Reference:	POL076
Document Status:	Approved
Version:	V1.0

DOCUMENT CHANGE HISTORY		
Initiated by	**Date**	**Author (s)**
IGG	15/05/19	Andy Marrs, IT Security & Resilience Manager
Version	**Date**	**Comments (i.e., viewed, or reviewed, amended approved by person or committee)**
Draft V0.1	20/11/19	Presented to and approved by IGG

Version	Date	Comments (i.e., viewed, or reviewed, amended approved by person or committee)
V1.0	12/03/2020	Approved by Compliance and Risk Group
V1.0	21/02/2022	6 month extension approved by Compliance and Risk Group
V1.0	18/07/2022	Extension to October 2022 approved by Compliance and Risk Group

Document Reference	
Recommended at Date	IGG 20/11/2019
Approved at Date	Compliance & Risk Group 18/07/2022 (extended)
Valid Until Date	October 2022
Equality Analysis	30/10/19
Linked procedural documents	All IM&T policies
Dissemination requirements	All staff/ East24
Part of Trust's publication scheme	Yes

The East of England Ambulance Service NHS Trust has made every effort to ensure this policy does not have the effect of unlawful discrimination on the grounds of the protected characteristics of: age, disability, gender reassignment, race, religion/belief, gender, sexual orientation, marriage/civil partnership, pregnancy/maternity. The Trust will not tolerate unfair discrimination on the basis of spent criminal convictions, Trade Union membership or non-membership. In addition, the Trust will have due regard to advancing equality of opportunity between people from different groups and foster good relations between people from different groups. This policy applies to all individuals working at all levels and grades for the Trust, including senior managers, officers, directors, non-executive directors, employees (whether permanent, fixed-term or temporary), consultants, governors, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with the Trust.

All Trust policies can be provided in alternative formats.

Contents

Appendices

1. Introduction

1.1 This Policy Document supports the Information Security Policy Statement approved by the Board of EEAST and is supported by Information Security Staff Guidelines and other specific guidelines.

1.2 This policy has been drawn from the other NHS Information Security Policy documents and covers all the management decisions, intentions and rules relating to information and IT Security, that are applicable throughout the Trust. Its audience is thus those personnel responsible for security in the Trust, plus Contractors and relevant Service Providers (e.g. BT, Microsoft).

1.3 This Electronic Information Security Policy determines the minimum level of security to be achieved, in line with NHS policy in general, for Trust IT Support and Application systems, and establishes the criteria against which results are to be checked for security compliance.

1.4 This Policy document covers security requirements for the following:

- Confidentiality
- Integrity
- Availability
- Accountability
- Non-Repudiation

1.5 The Health and Social Care Network (HSCN) Security Policy and succeeding policies remain extant in appropriate context.

1.6 The policies contained in this document are the policies adopted by the Trust. This document must be used in the context of the Trust delivery of its own services but also in the context of working with other services.

1.7 This policy extends to cover all electronic media and transmission of same by whatever method.

2. Purpose

2.1 The Electronic Information Security Policy provides a framework for Security Guidelines produced by the EEAST

2.2 Each derived set of policies or guideline may provide more detailed information relevant to specific subjects, procedures or service and may be also by Service Providers, as part of their security documentation, to show their approach to applying security.

2.3 Each EEAST Provider shall demonstrate their compliance with the principles of this policy via the following outline

2.3.1 Producing their Information Security Policy

2.3.2 Performing their Security Risk Assessment

2.3.3 Applying their Security Risk Management

2.3.4 Satisfying their Security Acceptance Criteria

2.4 To establish a Trust-wide approach to information security

2.5 To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of Trust data, application, networks and computer systems.

2.6 To define mechanisms that protect the reputation of the Trust and allows the Trust to satisfy its legal and ethical responsibilities.

3. Duties

3.1 Information Security Infrastructure

3.1.1 The EEAST Board has overall accountability for all matters relating to security

3.1.2The Board shall delegate the responsibility for Information Security to the Compliance and Risk Group of the Board. All security and risk matters will be referred to that committee

3.1.3 The Executive responsibility for Information Security and Governance shall be the Chief Information Officer for the Trust, who heads the IM&T directorate. The EEAST shall report to this post on information security, in addition the Trust will report to DoH on issues relating to security in the National Programme.

3.2 Information Security Responsibilities

3.2.1 This policy requires that individuals understand their information security responsibilities

3.2.2 IM&T Technical Managers

The IM&T Technical Managers must ensure they:

- Understand the risk to IM&T systems and the information that is stored on them.
- appropriate security measures to reduce the likelihood and impact of potential risks.
- Ensure that new IM&T systems provide an adequate level of security and do not compromise the existing infrastructure.
- Are an integral part of the NHS Security fora.

3.2.3 Directors & Departmental Managers

EEAST Directors and senior members of staff must:

- Ensure that all new staff are aware of their security responsibilities.
- Ensure that staff have appropriate training for the systems that they are using.
- Ensure that unauthorised staff are unable to access IM&T systems and information stores.

- Determine the level of access to be granted to specific individuals.
- Authorise new information systems that will have an impact on the security of the existing infrastructure
- Ensure that documentation is maintained for all critical job functions.
- Ensure that all staff sign confidentiality agreements as part of their contract of employment.

3.2.4 IM&T Security and Resilience Manager

The IM&T Security and Resilience Manager is responsible for the implementation and enforcement of the Information Security Policy.

Responsibilities include:

- Monitoring and reporting on the status of IM&T security within EEAST.
- Ensuring that the Electronic Information Security Policy is implemented throughout EEAST.
- Ensuring compliance with relevant legislation and regulation.
- Ensuring that personnel are aware of their responsibilities and accountability of information security.
- Monitoring for potential security breaches.
- Reporting security issues to the Head of IM&T.
- Acting as an advisor on information security matters.

3.2.5 Staff

Staff, including contract and temporary workers, are:

- Responsible for conformance to the Electronic Information Security Policy.
- Expected to raise information security concerns with the IM&T Security and Resilience Manager.
- Required to be aware of possible security breaches

3.2.6 The objectives of the Director responsible for IM&T in relation to Information security are to:

- Ensure that all parties are provided with clear terms of reference
- Establish dialogue between all concerned
- Develop and agree consolidated security policies, standards and procedures
- Discuss security-relevant issues to agree strategies and actions to address them
- Minimise security dependencies and assumptions between all the various parties
- Monitor and maintain the effectiveness of various security solutions deployed.

3.3 Allocation of Electronic Information Security Responsibilities

3.3.1 The Chief Information Officer shall be held accountable to the Board for the secure operation of the Trust and its IT and Telephony systems

4. Definitions

4.1 Any expression to which a meaning is given in the Health Service Acts, or in the Financial Directions made under the Acts, shall have the same meaning in this Policy

4.2 In addition in this Policy, unless the context otherwise requires, the following terms have the following meanings:

"Trust" EEAST

"Board" The Board of the Trust

"Chair" The person appointed to lead the Board and to ensure that it successfully discharges its overall responsibility for the Trust as a whole. The expression 'the Chair of the Trust' shall be deemed to include the Vice-Chair of the Trust if the Chair is absent from the meeting or is otherwise unavailable

"CESG" Communications-Electronics Security Group, the Information Security arm of GCHQ, and the National Technical Trust for Information Assurance within the UK

"**Chief Executive"** The chief officer of the Trust "Committee" A committee created by the Trust "Director" A Member of the Trust

"Chief Information Officer The chief officer with responsibility for IM&T

"Executive" The senior management team of the Trust consisting of the Chief Executive, Executive Directors and EEAST Directors; "Executive Director" An Officer Member of the Trust;

"Line Manager" The person to whom an employee is accountable "NHS" National Health Service

"EEAST Director" A senior manager designated as director by the Chief Executive

"Officer" An employee of the Trust. In certain circumstances, Officer may include a person who is employed by another Trust or by Third Party contracted to the Trust who carries out functions on behalf of the Trust

"Vice-Chairman" The Non-officer Member appointed by the Trust to take on the Chairman's duties if the Chairman is absent for any reason.

4.2.1 Where the title Chief Executive, Director of Finance and Commissioning, or other named Officer is used in this Policy, it shall be deemed to include such other Directors or Officers who have been authorised to represent them.

4.2.2 A reference to the singular shall include the plural and vice versa.

4.2.3 A reference to a gender shall include any gender.

4.2.4 References to any statute or statutory provision include reference to that statute or statutory provision from time to time amended, extended or re-enacted.

4.2.5 References to a statutory provision shall include any subordinate legislation made from time to time under that provision.

4.3 Further definitions:

Access Right Permission for a specified User to have access to given data.

Availability Ensuring that data is protected from loss and ensuring that it is available to authorised Users whenever and wherever required.

Biometric Authentication User Authentication via personal checks, e.g. fingerprint or eye scan.

Certification Trust An organisation trusted by one or more Users to create and assign Digital Certificates, for which it is responsible for their lifetime.

Confidentiality The safeguarding of information from access by unauthorised personnel or processes.

Data Classification The assignment of a category to information - on the basis of its level of sensitivity or its assignment to modification or destruction.

Digital Certificate A data structure issued by a Certification Trust that is Digitally Signed via its own Private Key, in order to provide a higher level of identity assurance than just a User-Id and Password pair.

Digital Signature Part of a Digital Certificate that is Encrypted via the sender's Private Key that can be used to verify its authenticity by the receiver.

Encryption A mathematically derived process involving data coding to achieve Confidentiality, anonymity, time-stamping, and other security objectives**. Integrity** The completeness and accuracy of information assets. **Non-Repudiation** Legally acceptable assurance that transmitted information has been issued and received by correct and authorised persons.

Private Key That part of an asymmetric Key-pair that is to be known only by its owner.

Privilege The bestowal of an Access Right (especially for System Administrators).

Public Key Infrastructure The set of services, personnel, policies and procedures needed to create, manage, store, distribute and revoke Digital Certificates.

Registration Trust An organisation that is responsible for performing the administrative tasks to establish the use of Digital Certificates. **Two-Factor Authentication** A User Authentication mechanism that relies on something the User has (e.g. Smart Card), and what the User knows (Password).

4.4 Abbreviations

HSCNSP	NHS Network Service Provider
NASP	National Applications Service Provider
NCRS	NHS Care Records Services
PKI	Public Key Infrastructure
DoH	Department of Health

5. Security Organisation

5.1 Document Framework

5.1.1 The documentation framework for Information Security is as follows:

Document Title	Content	Review Period
Information Security Policy Statement - Overview document setting the principles of Electronic Information Security in EEAST	Principles	2 years
Information Security Policies - Detailed electronic information security requirements covering all the management decisions, intentions and rules relating to electronic information and IT Security that apply to the EEAST	Requirements	2 years
Information Security Guidelines - Detailed guidelines based on	Implementation Detail	As required

Document Title	Content	Review Period
elements of Electronic Information and IT Security requirements e.g. Remote Access to EEAST networks		
Information Security Operating Procedures - Guidelines to inform operational use of systems and processes to maintain compliance with legislation and external policies and procedures e.g. Internet use	Process Description	As required

5.2 Information Security Management

5.2.1 Information Security covers all development and operational aspects related to the provision of IT and Telephony Services for the EEAST. These services may be supplied by other contracted parties, including the provision of IT support facilities or IT healthcare applications.

5.2.2 Authorisation Process for Information Processing Facilities

5.2.3 The Head of IM&T, or delegated agents, shall authorise all IT facilities from a security viewpoint, before processing on live data is permitted.

5.3 Specialist Information Security Advice

5.3.1 Security Consultants from the DoH and selected consultancy firms may provide specialist security advice to EEAST if required. The Head of IM&T will manage specialist advice

5.4 Security of Third-Party Access

5.4.1 Identification of Risks from Third Party Access

5.4.1.1 Where there is a business need for Third Party access to systems or information assets, a Security Risk Assessment (with feedback to the Head of IM&T) shall be carried out to identify any requirement for specific security measures. The Security Risk Assessment shall be performed before any contract is agreed, and shall comply with EEAST Risk Management

5.4.2 Network Services Provision to Third Parties

5.4.2.1 Access to any facilities by Third Parties shall not be provided until the appropriate security counter-measures have been implemented, evidence has been provided and a contract has been signed defining the terms of the connection, when it shall be subject to annual review

5.4.3 Security Requirements in Third Party Contracts

5.4.3.1 Arrangements involving Third Party access to systems or information assets shall be based on a formal contract containing (or referring to) all of the necessary security conditions to ensure security compliance

5.4.3.2 Upon approval of connections and related service access approval, but before access is given to Third Parties, the following shall be achieved:

- All Third-Party staff seeking to access data and/or systems shall be screened at an agreed level.
- Where such Third Parties require access to data and/or systems, written approval shall be obtained from the data/system owner.

5.4.4 Authorisation of Third-Party Connections

5.4.4.1 Default access by Third Parties to IT assets shall be set to no

access. Access rights shall be authorised by the Head of IM&T. Access by a Third Party to IT assets shall be for the minimum necessary period of time. The granting of Access Rights shall follow the principle of Least Privilege and be based upon a valid need-to-know.

5.4.4.2 Third Party access to IT assets shall be authorised only in cases where there is a clearly defined business need. The access facility provided shall always limit the Third Party to the agreed method of access, the agreed Access Rights, and the agreed level of functionality.

5.4.4.3 Third Party access to IT assets requires the prior approval of the asset owner, the information process owner, and IT operations, as appropriate, plus the Head of IM&T, who shall review any changes to the conditions upon which the Third-Party access was previously granted.

5.4.4.4 The procedures and processes associated with the granting of Third-Party access shall be defined by the relevant Service Provider, and shall be subject to approval by the Head of IM&T.

5.4.4.5 Once access has been given; the following shall be achieved:

- All physical access to systems shall comply with Section 8.
- Each approved Third-Party connection shall be reviewed by IM&T Security and Resilience Manager for compliance with IT Security Policies and Standards at a period of normally 12 months, unless required more frequently due to high risks or previous non-conformance.
- Any Third-Party security deficiencies from contracts (including Risk Registers for Service Level Agreements) discovered by the Trust shall be reported to the Head of IM&T, and then if necessary, to the Compliance and Risk Group and Director of Finance and Commissioning for escalation.

5.4.5 Outsourcing Risk Assessments and Contracts

5.4.5.1 A Security Risk Assessment shall be applied prior to any Outsourcing contract, and all deployed staff shall be screened at an agreed level.

5.4.5.2 The security requirements of Outsourcing for the management and control of any system, network or desktop environments shall be defined in a contract agreed with the Outsourcer.

5.4.5.3 Each System Owner shall maintain a register of approved Contractors and their Subcontractors for annual service access checks.

5.4.6 Additional Conditions for Outsourcing Software Development

5.4.6.1 For Outsourcing of software development, the following additional security points shall also be covered for compliance:

- Contractual requirements for quality of code
- Testing before installation to detect malicious code, e.g.Trojan code
- Secure control of test data and related facilities
- Avoidance of malicious software within developed code
- Secure patching and upgrades to operational software

5.4.7 Monitoring Security of Outsourcing Contracts

5.4.7.1 Once an Outsourcing contract has been established, it shall be reviewed by the Head of IM&T for compliance with IT Security Policies and Standards, at a period of normally 12 months.

6. Asset Classification and Control

6.1 Accountability for Assets

6.1.1 Inventory of Assets

6.1.1.1 The EEAST Managed Service Providers shall identify physical assets and the relative value and importance of these assets in the form of inventories to ensure that effective asset protection takes place, providing Security Risk Management for

Head of IM&T approval.

6.1.1.2 An inventory shall be drawn up and maintained of the important assets associated with each information system. Each asset shall be clearly identified, and its ownership and security classification agreed and documented, together with its current location.

6.1.2 Information System Assets

6.1.2.1 Assets shall be associated with information systems, including information, software, physical and service assets.

6.2 Information Classification

6.2.1 Classification Guidelines

6.2.1.1 Data Classifications may include project-sensitive data and patient-sensitive data.

6.2.1.2 Classified project data is as covered as follows:

- INTERNAL data – whose disclosure would cause some damage,
- PRIVATE data – whose disclosure would cause adverse damage,
- CONFIDENTIAL data – whose disclosure would cause material damage – but excludes higher levels that are not be processed on the NHS Network.

6.2.1.3 Classified patient data is as defined by the current data protection legislation, as follows (with NHS levels):

- PERSONAL data (NHS PRIVATE) – relating to an individual, who can be identified from the data, and including any expression of opinion about the individual, or intentions of others.
- SENSITIVE PERSONAL data (NHS CONFIDENTIAL) – PERSONAL data including information on racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, commission of offences or court proceedings.

6.2.2 Information Labelling and Handling

6.2.2.1 IT data owners (usually originators) shall classify information for proper protective measures to be effective. Data ownership policies govern the life cycle of data starting with creation, classification, storage, dissemination, and replication, ending with archiving and destruction.

6.2.2.2 Discretionary protective markings (as summarised in Annex A) of INTERNAL, PRIVATE or CONFIDENTIAL shall be used for classified data, i.e. with a prefix of NHS and an optional suffix descriptor of PATIENT IDENTIFIABLE INFORMATION, COMMERCIAL, FINANCE, STAFF or ADMINISTRATION.

6.2.2.3 It shall be noted that the NHS CONFIDENTIAL classification applies only to data whose compromise would adversely affect the NHS reputation or would cause substantial distress to individuals, so shall be protected by Encryption on Laptops and on E-mail, but any higher classifications (e.g. that would cause material damage or worse) shall be confined to stand-alone NHS computer systems.

7 Personnel Security

7.1 Security in Job Definitions and Resourcing

7.1.1 Security in Job Responsibilities

7.1.1.1 Identified security roles need to be supported by job definitions (or clear terms of reference) with reporting lines to EEAST Board.

7.1.2 Personnel Screening and Policy

7.1.2.1 Verification checks on all staff that handle information shall be carried out at the time of job applications. This shall include character references, curriculum vitae, academic or professional qualifications, and identity checks e.g. DBS as appropriate.

7.1.3 Confidentiality Agreements

7.1.3.1 Employees and Contractors shall sign a Confidentiality

Agreement as part of their initial terms and conditions of employment, which shall include their responsibility for security.

7.1.4 Terms and Conditions of Employment

7.1.4.1 All employees' terms and conditions shall state their responsibility for Information Security. Actions to be taken if the employee disregards security requirements shall be included.

7.2 Security Training

7.2.1 Information Security Education

7.2.1.1 All information system Users and specific Groups shall be regularly provided with sufficient education, training and supporting reference materials to allow them to comply with relevant Information Security regulations and to properly protect IT assets.

7.3 Security Incidents and Malfunctions

7.3.1 Incident Reporting

7.3.1.1 An Information Security incident is defined as an action taken that may reduce, compromise or threaten the Confidentiality, Integrity or Availability of the data or systems of EEAST. Reporting shall be done via the Trust Incident Reporting system. The aim is to ensure the efficient management, investigation and resolution of security incidents.

7.3.2 Incident Processing

7.3.2.1 Where it is suspected that there has been a security breach, the subsequent actions shall depend on the nature, severity and circumstances surrounding it. A common process shall be used for the processing of all security incidents that occur within the scope of this EEAST Information Security Policy. A security breach is any action or event that is in breach of this Information Security Policy - regardless of whether the incident has, or could have, resulted in assets being lost, damaged, misused or information being disclosed.

7.3.3 Incident Resolution

7.3.3.1 For each information security breach, an appropriate

manager shall maintain a record throughout the conduct of the investigation and the resolution of the breach. Each information security breach shall be categorised at a severity level that determines the seniority of management required to handle its investigation.

7.3.4 Incident Learning

7.3.4.1 It is important to learn from incidents, so that they can be avoided in future. This shall be achieved by the use of effective post-incident analysis, with lessons learnt and remedies.

7.3.5 Disciplinary Process

7.3.5.1 Non-compliance with the EEAST Information Security Policies, Standards or Procedures shall be considered as grounds for disciplinary action.

8 Physical and Environmental Security

8.1 Secure Areas

8.1.1 Physical Security Perimeter

8.1.1.1 Physical security protection shall be achieved through a series of barriers at different points throughout the service organisation. The requirements and location of each barrier depends upon the value of the assets and services to be protected, as well as the associated security risks and existing protective measures. Each level of physical protection for Service Providers shall have a defined security perimeter, around which a consistent level of security is maintained, according to its associated classification, as defined in the Section 6.2.

8.1.1.2 For an IT server (or other computer facility) the security perimeter could be defined as a high security area (such as a sealed-off area of the building for classified data), a server room, a locked office, or be based on some other form of physical boundary. EEAST Service Providers shall have the security of their server rooms approved by the Head of IM&T or delegated Trust before use.

8.1.2 Physical Entry Controls

8.1.2.1 Appropriate entry controls shall be provided around each area reserved for highly classified data, to ensure that only authorised personnel are allowed access. Visitors to NHS IT sites containing classified data shall be both escorted and supervised at all times, except for special concessions (e.g. maintenance arrangements).

8.1.2.2 Where it is necessary to permit access to any EEAST system by a visitor, such as access to a telephone switch, voice recording or ancillary equipment by a telephone or other engineer, the NHS person who invited the visitor on site shall undertake the task of supervision. The initiator of the visit is generally best qualified to comprehend the visitor's legitimate remit and distinguish between that and other illegitimate activity.

8.1.3 Securing Server Rooms and Offices

8.1.3.1 Locations housing facilities for information processing that support classified or critical business activities, e.g. EEAST Data Centres shall require a high level of physical security protection. The selection and design of the site shall take account of the possibility of damage from fire, flooding, explosion, civil unrest, and other forms of natural or man-made disaster. Consideration shall be given also to any security threats that are presented by neighbouring accommodation.

8.1.4 Working in Secure Areas

8.1.4.1 Additional controls and procedures shall be used to enhance the security of secure areas, including controls for personnel or visitors working in the area, considering the following:

- Unsupervised working shall be prohibited, both for safety reasons, and to prevent opportunities for malicious activities.
- Rooms shall be locked and barred for unescorted access by anyone, with staff identification taking place on entry, and records being kept of staff entry and exit.

8.1.5 Delivery and Loading Areas

8.1.5.1 Server rooms and data centres shall be protected from unauthorised access. An isolated delivery and loading area (for supplies and equipment deliveries) shall be provided to reduce the opportunities for unauthorised access to each server room.

8.2 Equipment Security

8.2.1 Equipment Siting and Protection

8.2.1.1 Information processing equipment shall be sited or protected to reduce the risks from environmental hazards and opportunities for unauthorised access.

8.2.2 Power Supplies

8.2.2.1 Equipment shall be protected from power failures or other electrical anomalies, as far as reasonable. EEAST and its Service Providers, according to the requirements of their contract schedules, shall use a suitable electrical supply. Back-up generators and Uninterruptible Power Supply (UPS) facilities are recommended if processing is required to continue during prolonged power failures. Adequate supplies of safely stored fuel shall be available to ensure that the generator can perform for a prolonged period.

8.2.3 Cabling Security

8.2.3.1 Power and telecommunications cabling carrying data or supporting information services shall require protection from interception or damage, diverse routing may be deployed in appropriate locations.

8.2.4 Equipment Maintenance

8.2.4.1 Equipment shall be correctly maintained to ensure its continual

Availability and Integrity. In particular, the following shall apply:

- Equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications.
- Only authorised maintenance personnel shall carry out repairs and servicing of equipment.

- Records of all faults or suspected faults shall be kept together with all preventative corrective maintenance.

8.2.5 Security of Equipment Off-Premises

8.2.5.1 Regardless of ownership, equipment used outside NHS premises for information processing to support business activities shall be authorised by management. The security provided shall be equivalent to that for on-site equipment used for the same purpose, taking into account the risks of working outside of NHS premises. Information processing equipment includes all forms of personal computers, organisers, mobile phones, paper or other forms, which are held for home working or being transported away from the normal work location.

8.2.6 Secure Disposal and Reuse of Equipment

8.2.6.1 Storage devices or media containing NHS data shall be physically destroyed or securely overwritten using CESG approved methods to prevent subsequent compromise of information. All data storage devices shall be checked to ensure that any NHS data and licensed software have been removed or overwritten prior to disposal.

8.3 General Controls

8.3.1 Removal of Trust Property

8.3.1.1 Employees or contractors, without formal management authorisation shall, not take Trust equipment, information or software, off-site. Where necessary and appropriate, equipment shall be logged out and logged back in when returned. Spot checks shall be undertaken to detect unauthorised removal of property. Individuals shall be made aware that such checks will be conducted.

8.3.1.2 If hardware is lost or stolen, it shall be reported via the Trust's incident reporting system. If any CONFIDENTIAL data is lost, it shall be reported to the Director responsible for IM&T who shall report to the Compliance and Risk Group.

9 Communications and Operations Management

9.1 Guidance and policy regarding IT and Information security can be found on the NHS Digital web site http://digital.nhs.uk

9.2 Operational Procedures and Responsibilities

9.2.1 Documented Operating Procedures

9.2.1.1 Clear operating procedures shall be prepared for all operational computer systems, to ensure a correct and secure operation. This applies to systems provided by Third Parties or via Outsourcing. Documented procedures are required for system development, maintenance and testing. Operating procedures shall be treated as formal documents and any changes shall be authorised by the appropriate manager.

9.2.2 Operational Change Controls

9.2.2.1 Formal management responsibilities and procedures shall be used to ensure satisfactory control of all changes to equipment, software or procedures. The aspects covered shall include Version Control and Configuration Control with Audit Records in case recovery is needed. Operational programs shall be subject to Change Control, even for emergency fixes.

9.2.3 Reporting of Incidents, Weaknesses And Malfunctions

9.2.3.1 EEAST and Service Provider management shall ensure that compliant procedures are in place and known by staff and contractors, for the reporting of any suspected security weaknesses (or threats to) systems or services. Users shall report these matters to their Line Managers as quickly as possible. Users shall be informed that they shall not, in any circumstances, attempt to prove a suspected weakness. This is for their own protection, because their action in testing the weakness might worsen the situation.

9.2.4 Segregation of Duties

9.2.4.1 Segregation of duties is a method that shall be used for reducing the risk of accidental or deliberate system misuse. Therefore, the management or execution of certain duties or areas of responsibility shall be separated, in order to reduce

opportunities for unauthorised modification or misuse of information or services. In small sites with limited resource, this method of control may be difficult to achieve, but the principle shall be applied as far is possible and practicable.

9.2.5 Separation of Development, Test and Operational Environments

9.2.5.1 The development of new application or system software shall be kept separate from the production environment. The development staff shall not normally have access to production systems. For occasional and essential support purposes, the development staff may be granted special access for a limited period. Test data shall be desensitised unless everyone present has need-to-know access. Production systems shall be protected from the effects of outages in other environments, such as test, development and office automation.

9.2.6 External Facilities Management

9.2.6.1 The use of Third-Party Facilities Management contractors involving access to EEAST facilities, shall comply with Section 5.4.

9.3 System Planning and Acceptance

9.3.1 Project Initiation

9.3.1.1 IT Security activities shall be performed at the project initiation and definition stage, with Security Risk Assessments (including impact and vulnerabilities), and IM&T Security and Resilience Manager involvement.

9.3.2 Capacity Planning

9.3.2.1 Projection of future computer capacity requirements shall be made to ensure that adequate processing power and storage remain available. The projections shall take account of new business and systems requirements as well as current and projected trends in computer and network use. This shall ensure there is adequate resilience to overload situations.

9.3.3 System Acceptance Criteria

9.3.3.1 In order for computer managers to ensure that the requirements and criteria for acceptance of new computer systems are clearly defined, agreed, documented and tested, the following system criteria shall be considered:

- All performance, resilience and computer capacity requirements have been met.
- Agreed security controls are implemented, as required by Security Risk Assessment.
- Demonstrated compliance with Section 11.1.3 on Security Development has been met.

9.3.4 Business Continuity Planning

9.3.4.1 Emergency fallback facilities shall provide a temporary means of continuation by Service Providers after damage or failure of equipment.

9.4 Protection Against Malicious Software

9.4.1 Terminology Definition

9.4.1.1 Malicious software covers all software, which has been deliberately designed to harm or abuse the resources of computing systems. Malicious software types include (but are not limited to) computer viruses, Trojan horses, worms, logic bombs, file infectors, malicious macros, malicious scripts (e.g. Java, ActiveX), mobile code, malicious cookies and hidden software for launching denial-of-service attacks (sometimes generically called Viruses).

9.4.2 Virus Controls

9.4.2.1 It is NHS policy to formally establish its virus checking process, supported by the relevant Service Desk, to manage virus protection. The early detection of virus infections on data media and networks shall be assured by Service Providers, implementing NHS-approved and up-to-date virus checking software, on all NHS systems and for all portable devices.

9.4.3 Virus Management

9.4.3.1 Detection and prevention controls to protect against malicious software awareness for System Administrators shall be implemented. Protection against malicious software shall be based on security awareness, appropriate system access and change management controls.

9.4.4 Awareness

9.4.4.1 The mandatory level of User awareness is as follows:

- Virus protection awareness shall be provided by the EEAST
- IM&T personnel and shall include protection procedures and incident handling.
- Remote Users who do not normally Log-On for extended periods shall periodically update their virus definition files manually via their Service Desk services or as appropriate.

9.4.5 User Responsibilities

9.4.5.1 Users of systems shall comply with the following:

- Individuals receiving data media (from any source e.g. E-mail systems or public networks) have the responsibility for ensuring it is checked for viruses prior to its use.
- Individuals intending to pass on data media within EEAST or to external Third Parties shall ensure that it is first checked for viruses.
- Individuals not covered by automatic virus checker updates shall check at least weekly for updates.
- Individuals are responsible for reporting breaches in Virus controls.

9.5 Housekeeping

9.5.1 *Information Back-Up*

9.5.1.1 Most Disaster Recovery solutions are based on manually backing-up data for subsequent manual recovery. In these cases, adequate back-up facilities shall be provided to ensure that all essential business information and software can be recovered

following a computer disaster or media failure. This is particularly important in the case of laptop and PDA devices.

9.5.2 Operator Logs

9.5.2.1 Computer operators for systems (including Outsourcers) shall maintain logs of work events. Operator logs shall be subject to regular, independent checks against operating procedures.

9.5.3 Fault Logging

9.5.3.1 Faults shall be reported and corrective action taken. Faults reported by Users regarding problems with information processing or communication systems shall be logged. There shall be clear procedures for handling of reported faults including:

- Reviewing fault logs to ensure that faults have been satisfactorily resolved.
- Reviewing corrective measures to ensure that security controls have not been compromised
- Ensure that the action taken is fully authorised and appropriate.

9.5.4 Environment Monitoring

9.5.4.1 The environment of information processing facilities shall be monitored where necessary, to ensure compliance with Section 8.2. Temperature, humidity and power supply quality shall be monitored where necessary to identify conditions, which might adversely affect the correct operation of information processing equipment in EEAST, this is particularly important when storing media for Voice Recordings.

9.5.5 System Administration

9.5.5.1 When a system first becomes operational, its System Administrator shall initially check that all development facilities (e.g. compilers and test tools) have been removed, and that User and configuration files are correctly initiated to meet the system owner's requirements.

9.6 Network Management

9.6.1 Network Controls

9.6.1.1 The HSCN SP shall define EEAST network infrastructure security measures, for Head of IM&T or delegated Trust, including the following:

- Physical controls.
- Network mapping.
- Routers and firewalls.

9.7 Media Handling and Security

9.7.1 Management of Removable Media

9.7.1.1 EEAST Service Providers shall establish clearly documented procedures for the management of removable computer media (tapes, fixed or removable disks, cassettes, printed reports, etc.), according to the sensitivity of the data therein.

9.7.2 Disposal of Computer Media

9.7.2.1 Computer media shall be disposed of securely when no longer required. Classified information shall not be leaked to outside persons through inappropriate disposal of computer media, so techniques such as Recycle Bin emptying of CONFIDENTIAL files shall be used. Clear procedures shall be established by Service Providers for the secure disposal of media to minimise the risk, in accordance with their contract schedules.

9.7.3 Information Handling Procedures

9.7.3.1 Procedures for handling and storing information shall be established by Service Providers to protect such information from unauthorised disclosure or misuse. Procedures shall be developed for handling information, consistent with its classification level in electronic documents, computing systems, networks, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, and any other CONFIDENTIAL items.

9.7.4 Security of System Documentation

9.7.4.1 Service Providers shall define security measures for

handling their system documentation, as it can contain a range of CONFIDENTIAL information (e.g. descriptions of application processes, procedures, data structures, authorisation processes, and special access to classified data).

9.8 Exchange of Information and Software

9.8.1 Information Exchange\Sharing Agreements

9.8.1.1 Formal agreements shall be established for exchanges of information and software (whether electronic or manual) between EEAST and any external Third Party e.g. Out of Hours Service Providers. The security content of the agreement shall reflect the classification of the information involved.

9.8.2 Security of Media in Transit

9.8.2.1 Computer media can be vulnerable to unauthorised access, misuse or corruption during physical transportation, e.g. when sending media via the postal service or via a courier. The controls specified in Section 7.3 on Information Handling Procedures shall be applied to safeguard computer media being transported between sites.

9.8.3 Electronic Commerce Security

9.8.3.1 E-commerce security requirements shall be specified within relevant EEAST applications, including the means of Authentication, Encryption and Non-Repudiation.

9.8.4 Security of Electronic Mail

9.8.4.1 E-mail has a number of different characteristics from traditional forms of business communications, such as its speed, message structure, degree of informality and vulnerability to unauthorised actions. Controls shall therefore be applied to reduce any business or security risks that may be presented by the use of E-mail. Any CONFIDENTIAL data sent via E-mail shall use DoH-approved Encryption mechanisms. In normal circumstances it is inappropriate to send patient data over email services

9.8.5 Security of Electronic Office Systems

9.8.5.1 The Compliance and Risk Group shall approve

Electronic Commerce and Electronic Office systems (e.g. Office Automation and Organisers) used within the EEAST provided services.

9.8.6 Publicly Available System

9.8.6.1 EEAST Line Managers shall be responsible for the following Internet matters:

- Authorising which Users may have access to the public Internet and NHS Intranets.
- Preventing use of Internet facilities by unauthorised staff or persons supporting business usage.
- Taking action with any Users whose use of their Internet access Privileges is deemed inconsistent with this Information Security Policy.

9.8.6.2 Internet Service Providers shall be responsible for the following:

- Providing Internet connectivity from the EEAST network via an agreed controlled exit mechanism, e.g. a firewall, proxy server architecture, as defined by the HSCN SP.
- Providing Users with only approved standard software for access to the Internet, Users shall demonstrate a business need and be approved by their Line Managers.
- Checking for unacceptable use of Internet access and blocking of prohibited sites that have been identified.

10 Access Control

10.1 Business Requirements for Access Control

10.1.1 Access Control Policy

10.1.1.1 Business requirements for access control shall be defined and documented, and access shall be limited to what is defined by these requirements. Access control rules and rights for each User or Group shall be clearly stated in an access policy statement. Service Providers and Users shall be given a clear statement of their access control business requirements, including

the use of Role-Based Access Controls for NHS CAS and NCRS applications.

10.2 User Access Management

10.2.1 User Registration

10.2.1.1 EEAST line managers are responsible for ensuring that only those people appropriately trained, qualified and experienced have access to the parts of the NHS CAS and other applications that they are legitimately required to use to fulfil the role defined for them as follows:

- Approval from relevant system owners and Line Managers shall be required to confirm that the level of access given is appropriate for the business purpose, and does not compromise any requirements for segregation of duties.
- New Users of systems shall formally indicate their agreement to be bound by their rights and responsibilities.
- A formal record of all persons Registered to use the IT service shall be maintained.
- Periodic checking for, and removal of, redundant User Accounts shall be performed.
- A formal process shall be required for Line Managers to review and notify changes in access requirements when Users move to new parts of applications not previously authorised.
- Removal of Access Rights shall apply for Users who have changed positions, where access levels are no longer appropriate, or where Users have left EEAST.
- The principal of Least Privilege shall be used to limit permanent access to a minimum number of Users, and to use minimum default access permissions.

10.2.1.2 A formal User Registration Trust process shall be established and maintained (for NCRS, complying with appropriate security requirements to ensure that only Users with the proper Trust can gain access to systems and the information on the

systems, and to limit the functions they are able to perform. This access process shall define which Users or Groups (including Service Desk support) shall have, which levels of access to each application, and who shall authorise such access. The process shall also include the following:

- Approval from relevant system owners and Line Managers shall be required to confirm that the level of access given is appropriate for the business purpose, and does not compromise any requirements for segregation of duties.
- New Users of systems shall formally indicate their agreement to be bound by their rights and responsibilities.
- A formal record of all persons Registered to use the IT service shall be maintained.
- Periodic checking for, and removal of, redundant User

Accounts shall be performed.

- A formal process shall be required for Line Managers to review and notify changes in access requirements when Users move to new parts of the EEAST and the NHS.
- Removal of Access Rights shall apply for Users who have changed positions, where access levels are no longer appropriate, or where Users have left EEAST.
- The principal of Least Privilege shall be used to limit permanent access to a minimum number of Users, and to use minimum default access permissions.
- For NCRS applications, issuing of Smart Cards with Encryption Keys, using NASP facilities.

10.2.2 Privilege Management

10.2.2.1 The allocation and use of Privileged Access Rights (e.g. for Administrators) shall be restricted and controlled by a formal authorisation process including the following:

- The Privileges associated with each system shall be defined, together with staff that can be allocated any such Privileges, based on the minimum requirement for their role.
- It shall provide and maintain a record of all Privileges allocated.
- A separate User-Id from those used for normal business use shall be assigned for Privileged access.
- A formal process shall be included for the review and checking of Privileged Access Rights, at least at annually.
- Only the System Administrator shall provide and maintain Users with their minimum access Privilege to perform their duties.
- Access shall be authorised only in response to an authorised change request or a documented problem report, and shall be removed following completion of work.
- All Access Rights and Privileges shall be subject to occasional IM&T Security and Resilience Manager Security Audits.
- There shall be a formal User Registration and Deregistration procedure for granting access to all information systems and services.

10.2.2.2 Access to information services shall be controlled through a formal User Registration process, which shall include:

- Checking that the User has authorisation from the system owner for the use of the information system or service.
- Ensuring Service Providers do not provide access until authorisation procedures have been completed.
- Maintaining a formal record of all persons Registered to use the service.
- Removing Access Rights of Users who have changed positions or have left EEAST.
- Periodically checking for and removing redundant User Accounts.

10.2.3 User Password Management

10.2.3.1 System Administrators shall communicate new Passphrases to Users in a secure manner with an appropriate proof-of-identity check of the intended Users. Service Providers shall provide these mechanisms, including the use of initial Passphrases for this purpose. The Password management system will achieve the following:

- Enforce the use of individual passphrases, to maintain accountability.
- Enforce a minimum length for passphrases of 15 characters.
- Prevent access to a user account exceeding 10 consecutive failures.
- Where users select passphrases force them to change preset Passphrases on first use.
- Record previous user passphrases preventing the reuse of the last 5 passphrases

10.2.3.2 Trust staff may have access to certain nationally hosted systems that do not allow password changes. In these cases, it is beyond the control of the Trust to enforce password changes therefore section 10.2.3.1 of the policy does not apply.

10.2.4 Review of User Access Rights

10.2.4.1 A formal review process shall be conducted at regular intervals to review User Access Rights. These reviews shall be every 6 months and include revalidation of User Access Rights and Privileges granted to Users.

10.3 User Responsibilities

10.3.1 Password Use

10.3.1.1 System Administrators, service desk personnel and any other individuals capable of resetting passphrases shall not reveal passphrases unless the information owners or authorised users have first provided definitive evidence substantiating their identity.

10.3.1.2 Additionally, resetting procedures shall ensure that Users comply with the following:

- Change Passphrases following any possible compromise or suspected security breach.
- Change Passphrases regularly to be within their life span before reaching their expiry.
- Change Passphrases temporarily assigned by the Service Desk immediately on first use

10.3.1.3 For DoH NCRS, the NASP shall define the procedures for the management and support of Level 3 Registration and Authentication, together with the means of changing Passphrases on User Smart Cards, and these facilities shall be supported by EEAST.

10.3.2 Unattended User Equipment

10.3.2.1 To prevent unauthorised use of a terminal already connected, the system shall require that the Identification and Authentication process is repeated, via a screen saver, after a specified period of inactivity, before work can be continued.

10.4 Network Access Control

10.4.1 Policy on Use of Network Services

10.4.1.1 The HSCN SP shall define a range of controls required to achieve and maintain security in the NHS Network, which is to become part of the Critical National Infrastructure. All Service Providers shall implement controls to ensure the security of data in this network, and the protection of connected services from unauthorised access.

10.4.1.2 A register shall be maintained which covers all categories of connectivity into or from the networks, including interactive dial-in, internal modems, internal inter-network connections, connections with public networks, and Information Service Provider links.

10.4.1.3 As a condition of gaining access to the IT network, every Third Party shall secure its own connected systems in a manner consistent with NHS requirements. The DoH reserves the right to Audit the security measures in effect on these connected systems without prior warning. The NHS also reserves the right to immediately terminate network connections with all Third Party systems not meeting such requirements. EEAST computers or networks shall only be connected to Third Party computers or networks after the Head of IM&T or delegated Trust has determined that the combined system shall be in compliance with security requirements.

10.4.2 Enforced Path

10.4.2.1 The HSCN SP shall determine any NCRS enforced paths. Prior to moving software to production status, all special access paths shall be removed, so that access may only be obtained via normal secured channels.

10.4.3 User Authentication for External Connections

10.4.3.1 Remote Access (i.e. dial-in) shall be subject to Authentication. Authentication must be two factor, of which one factor must be a user account, and the other a unique dialler account. Two-Factor Authentication shall be used for remote access to NCRS.

10.4.4 Node Authentication

10.4.4.1 NCRS connections to remote computer systems shall be Authenticated, e.g. via Digital Certificates. Both the destination computer and the source communicator node shall authenticate the user who initiates a transfer. Service Providers shall do this before the transfer is executed.

10.4.5 Remote Diagnostic Port Protection

10.4.5.1 Access to diagnostic ports shall be securely controlled, and Service Providers shall prevent unauthorised remote diagnostics. Diagnostics shall not be performed unless authorised by the Head of IM&T or delegated Trust. Network control devices, diagnostic equipment, security firewall systems and Encryption Key

Management systems shall be stored in physically secure locations which automatically notify accesses made to those locations.

10.5 Operating System Access Control

10.5.1 Terminal Log-On Procedures

10.5.1.1 Log-On screens shall request the User to Log-On, providing prompts shall be provided until the User has a successful Log-On. Systems shall ensure that Users can change Passphrases on-line. The utilities that provide this facility shall enforce the following:

- Confirmation of the old Password is required.
- New Password shall be entered twice by the User.
- Passphrases shall not be displayed in clear text to the screen.

10.5.2 User Identification and Authentication

10.5.2.1 For systems that do not include PERSONAL SENSITIVE data, e.g. the IT Support System, User Identification and Authentication shall be via a Password per User-ID.

10.5.3 Password Management System

10.5.3.1 Service Providers shall specify Password management systems for effective, interactive facilities that ensure quality Passphrases, e.g. minimum length, composition and lifetime.

10.5.4 Use of System Utilities

10.5.4.1 Use of system utility programs shall be limited and tightly controlled, e.g. via Access Rights. Storage media facilities used on production computer systems shall not contain compilers, assemblers or other general-purpose utilities which may be used to perform development functions or compromise the security of the system unless absolutely necessary.

10.5.5 Duress Alarm to Safeguard Users

10.5.5.1 There are currently no requirements in the EEAST for duress alarms.

10.5.6 Terminal Time-Out

10.5.6.1 When User sessions remain unused for an extended

period of time, the system shall invoke a screen saver or session suspension mechanism. Re-establishment of the session may then occur only after Users have been re-authenticated by re-entering their correct Password.

10.5.7 Limitation of Connection Time

10.5.7.1 Service Providers shall specify ways of limiting the daily period during which terminal connections are allowed to their computer services if handling classified data, to reduce the window of opportunity for unauthorised access.

10.6 Application Access Control

10.6.1 Role-Based Access Control

10.6.1.1 The NHS CAS application shall be subject to Role-Based Access Control from the Service Provider.

10.6.1.2 NCRS applications shall be subject to Role-Based Access Control from Service Providers, including Security Standards for Sealed Envelopes, Patient Consent, Legitimate Relationships and Anonymisation/ Pseudonymisation.

10.6.2 Information Access Restriction

10.6.2.1 Users of IT systems shall be provided with access to application information and functions, only in accordance with their Access Rights. In the case of database access, this may require an associated Log-On by the User to determine Privileges.

10.7 Monitoring System Access and Use

10.7.1 Event Logging

10.7.1.1 Service Providers shall specify their event logging and Audit tools for Head of IM&T or delegated Trust approval.

10.7.1.2 Access to Audit Logs shall be strictly controlled by Service Providers, shall be protected from deletion, disablement, modification or fabrication, and shall be retained for at least 12 months. Wherever possible, there shall be a separation of duties between overall system security and Audit Logs security. Audit Logs shall be analysed and administered only by appropriately

trained staff. Audit Logs shall be written to media with storage space assured, in order to avoid over-writing or deletion of information.

10.7.2 Monitoring System Use

10.7.2.1 Security alerts, suspicious activity or unusual occurrences shall be investigated and reported to the Head of IM&T for EEAST. Service providers will also be responsible for investigating and notifying alerts to the Head of IM&T. EEAST will deal with any subsequent action. The provision of a real-time alert facility to a specific terminal shall be considered. Suitable system utilities or Audit tools shall be required to interrogate Audit Logs.

10.7.2.2 The results of all monitoring activities shall be reviewed regularly, the frequency of reviews depending on the assessment of the risks involved.

10.7.3 Clock Synchronisation

10.7.3.1 The NHS CAS Service Provider shall provide clock synchronisation.

10.7.3.2 NCRS clock synchronisation shall be specified by the NASP.

10.8 Mobile Computing and Tele-Working

10.8.1 Mobile Computing

10.8.1.1 The HSCN SP and the Head of IM&T or delegated Trust for EEAST shall specify central facilities for NCRS and EEAST mobile computing and tele-working to be used by EEAST.

10.8.1.2 When using mobile computing facilities, e.g. notebooks, palmtops, laptops and mobile phones, special care shall be taken to ensure that business information is not compromised. Care shall be taken when using mobile computing facilities in public places (e.g. cars, aeroplanes, trains, etc.), meeting rooms and other unprotected areas.

10.8.1.3 Sufficient protection shall be in place to prevent theft and unauthorised access to or disclosure of any information stored or processed by these facilities. For example, laptops shall be powered off whilst in transit, so as to be protected by their start-

up controls, and stored and carried separately from their removable media where possible. It is important that when such facilities are used in public places, care is taken to avoid the risk of overlooking by unauthorised persons.

10.8.1.4 Mobile computing facilities shall not be left unattended and shall always be carried as hand baggage when using public transport, if so permitted by the transport provider. Wherever possible, equipment shall be physically locked away when not in use and shall be provided with an appropriate form of access control to prevent any unauthorised access to EEAST applications and NCRS or other information.

10.8.2 Tele-Working Procedures

10.8.2.1 Tele-working uses communications technology to enable staff to work remotely from locations external to normal company sites (home, public or customer sites). Remote locations shall be protected to prevent the theft of equipment or information and to prevent unauthorised remote access to EEAST internal systems, locally held data, applications and services, or any misuse of facilities. Tele-working shall be authorised by management.

10.8.2.2 Line Managers shall ensure that a written instruction, governing procedures and standards to control tele-working activities, is in place and to all relevant members of staff. Tele-working shall only be authorised after management is satisfied that appropriate security controls are in place, that comply with this Information Security Policy

11 Systems Development and Maintenance

11.1 Security Requirements of Systems

11.1.1 Security Requirements Analysis and Specification

11.1.1.1 Statements of business requirements for new systems or enhancements to existing systems, shall define, according to analysed risks, the requirements for security controls, e.g. for

Confidentiality, Integrity, Availability, Authentication, Access Control, Accounting, Audit and Encryption. Specifications shall normally focus on the automated controls to be incorporated in the system, but the need for supporting manual controls shall be considered.

11.1.2 Security Analysis

11.1.2.1 Security controls incorporated in computer systems could be compromised if the information system support team and the Users are not aware of them. Security controls shall therefore be explicitly defined by Service Providers, as a result of their Security Risk Assessment.

11.1.3 Security Development

11.1.3.1 The Head of IM&T or delegated authority shall monitor each stage of the development of security by Service Providers. The development life cycle phases to be evaluated, with relevant items, shall include analysis, design and implementation. System Security Acceptance shall be performed in accordance with Section 9.3.3 on System Acceptance Criteria.

11.1.3.2 The Head of IM&T or delegated Trust shall include the following monitoring techniques on Service Providers:

- Document inspection during specification.
- Design reviews during development stages.
- Facility checks for development and testing.
- Functional testing of IT Security measures.
- Penetration testing during implementation.
- Witnessing System Acceptance Testing.
- Sampling of security awareness training.
- Checking the security aspects of pilot trials.

11.1.3.3 The Head of IM&T or delegated authority shall not accept the system for operational use unless sufficiently satisfied with the Service Provider's results from all these monitoring

activities and shall be empowered to instigate Security Audits whenever required.

11.2 Security in Application Systems

11.2.1 Input Data Validation

11.2.1.1 Appropriate controls and Audit Logs, in accordance with Section 10.7, shall be designed into application systems, including User written applications and end-user computer systems. These shall include Service Provider facilities for validation of input data.

11.2.2 *Internal Processing Validation*

11.2.2.1 Data correctly entered into an application system can be corrupted by processing errors or through deliberate acts. Validation checks shall be incorporated by Service Providers into systems to detect such corruption. The design of applications shall ensure that restrictions are implemented to minimise the risk of processing failures leading to a loss of Integrity.

11.2.3 Message Authentication

11.2.3.1 The Service Provider shall define Message Authentication facilities for NHS CAS and other systems that meet the requirements of EEAST and Department of Health in relation to the messaging with Out of Hours and Other services.

11.2.3.2 The NASP shall define NCRS Message Authentication facilities.

11.2.4 Output Data Validation

11.2.4.1 Data output from an application system shall be validated by Service Providers to ensure that the processing of stored information is correct and appropriate to the circumstances. Systems shall be constructed to ensure that, having undertaken appropriate validation, verification and testing, the output shall always be correct.

11.3 Cryptographic Controls

11.3.1 *Policy on Cryptographic Controls*

11.3.1.1 The regulations and any national restrictions that might apply to the use of cryptographic techniques and to the issues of international flow of Encrypted information shall be covered wherever needed within the DoH Encryption standards.

11.3.1.2 Facilities that generate, distribute and account for cryptographic material shall be subject to an appropriate level of physical protection and access control. Any cryptographic technique, system or algorithm used to protect the Confidentiality, Integrity or Availability of DoH information shall be approved by DoH.

11.3.1.3 Business Managers, System Managers and the DoH shall determine the level of cryptographic protection that shall be employed based on the risks. The types of Encryption, cryptographic Keys and algorithms used will depend on the level of protection required and Data Classifications.

11.3.2 Encryption

11.3.2.1 The NHS cryptographic standards currently approved by the DoH are as shown on the NHS internal web page: http://systems.digital.nhs.uk/infogov/security/infrasec/iststatements/dataenc_html

11.3.2.2 Cryptographic techniques for Confidentiality of CONFIDENTIAL data shall apply to the following:

- Encrypting links to enhance privacy in the network infrastructure.
- Encrypting E-mail to protect messages sent over public networks.
- Encrypting storage media units/files that require special protection.
- Encrypting Passphrases for hacker protection on servers and networks.

11.3.2.3 Digital Signatures and Certificates as defined by the NASP shall be used to protect Integrity, e.g. for electronic documents, electronic payments, funds transfer, contracts and agreements, via Private Keys for Digital Signatures and

Authentication held in the User's Smart Card. For maximum security, these Private Keys shall never be held in the User terminal.

11.3.3 Digital Signatures

11.3.3.1 The NASP shall define NCRS Digital Signature services for LSP and EEAST use and DoH approval.

11.3.4 Non-Repudiation Services

11.3.4.1 The NASP shall define NCRS Non-Repudiation services for LSP and EEAST use and DoH approval.

11.3.5 Cryptographic Key Management

11.3.5.1 The NASP shall define NCRS Cryptographic Key services for LSP and EEAST use and DoH approval.

11.3.5.2 Key management shall provide the methods for the secure generation, exchange, use, storage and discontinuation of the cryptographic Keys used by the cryptographic mechanisms. The protection shall be adequate to prevent the Keys from being used in any compromising situations and to ensure that Keys issued by DoH remain the property of DoH.

11.3.5.3 Keys shall be capable of being revoked prior to the end of their validity period if compromised or misused and also upon the User's request. Key management processes shall address dealing with compromised Keys and revoking Keys.

11.3.5.4 Before a Key expires, the User shall be automatically notified of such pending expiration. Keys shall be valid for a period to be agreed between the NASP and DoH.

11.3.5.5 The distribution of Private Keys shall be in accordance with procedures approved by the DoH, and Key Certificates shall be used.

11.3.5.6 The NASP shall issue clear and explicit instructions to react to potential breaches caused by NCRS cryptographic services. These instructions shall also include those for a disloyal employee seeking to sell the proper decryption Key for Encrypted vital information.

11.3.5.7 The NASP may employ a Trusted Third Party for delivery

of NCRS PKI solutions. The maintenance of Keys used for Encryption, Authentication and Digital Signatures is essential, as these may need to be reproduced several years after the transactions for which they were used.

11.4 Security of System Files

11.4.1 Control of Operational Software

11.4.1.1 Service Providers shall implement the following controls to minimise the risk of corruption of live IT systems:

- The updating of the operational program libraries shall only be performed upon authorisation from the information system support manager for the application.
- If possible, only executable code shall be held on operational systems.
- Executable code shall not be implemented on an operational system until evidence of comprehensive successful testing and User acceptance is obtained.

11.4.2 Protection of System Test Data

11.4.2.1 System and acceptance testing by Service Providers usually requires substantial amounts of test data that is as close as possible to the live data. The use of live databases containing personal data shall be avoided. If such data is used, it shall be de-personalised before use to ensure that it fully complies with current data protection legislation.

11.4.2.2 Access Control to Program Source Library Service Providers shall define the control mechanisms for their source code.

11.5 Security in Development and Support Processes

11.5.1 Change Control Procedures

11.5.1.1 Application owners shall ensure that all proposed system changes are processed via the Change Control process, in accordance with the Section 9.3, and are reviewed to ensure that they do not compromise the security of either the system or the operating environment.

11.5.2 Technical Review of Operating System Changes

11.5.2.1 Periodically, it is necessary to change the operating system (e.g. the installation of a new release). When changes occur, the application systems shall be reviewed by Service Providers to ensure that there is no adverse impact on security.

11.5.3 Restrictions on Changes to Software Packages

11.5.3.1 As far as possible (and practicable), vendor-supplied software packages shall be used without modification. In circumstances it may be deemed essential to modify software packages.

If changes are deemed essential, then the original software shall be retained and the changes applied to a clearly identified copy and fully documented, so that they can be re-applied if necessary, to future software upgrades.

11.5.4 Outsourced Software Development

11.5.4.1 The contractual aspects of security for outsourced software developments shall conform to Outsourcing in Section 5.4.

12 Business Continuity Management

12.1 Aspects of Business Continuity Management

12.1.1 Business Continuity and Disaster Recovery Overview

12.1.1.1 There shall be a managed process in place to develop and maintain Business Continuity Plans throughout EEAST. This process shall involve EEAST and Service Providers identifying and reducing the risks from deliberate or accidental threats to vital services, for approval by the Compliance and Risk Group.

12.1.1.2 Plans shall be developed to enable business operations to be following failure or damage of vital services or facilities. Owners of business resources and processes shall be involved in the development and production of these plans which shall include

Disaster Recovery steps.

12.1.1.3 Project staff from the system owner's department shall be responsible for initiating Disaster Recovery with Service Providers, and for involvement with Business Continuity Planning. The IM&T Security and Resilience Manager or delegated Trust may be represented to ensure the compliance of each project with this EEAST Electronic Information Security Policy.

12.1.1.4 Each Disaster Recovery Plan shall describe who is responsible for executing which component of the plan, and indicate nominated alternatives, as required. It shall establish the members of its Disaster Recovery Planning team from technical and operational representatives and ensure that those responsible for executing the plan are involved with its production and testing.

12.1.2 *Business Continuity and Impact Analysis*

12.1.2.1 Each project's Disaster Recovery Plan shall begin by identifying events that can cause interruptions to business processes, e.g. equipment failure, flood and fire. Depending on the results of these assessments, a strategy plan shall be developed to determine the overall approach to the project Disaster Recovery Plan, which shall be endorsed by EEAST management and by the Compliance and Risk Group.

12.1.3 Writing and Implementing Continuity Plans

12.1.3.1 Plans shall be developed to maintain or restore business operations in the required timescales following interruption of critical business processes. The planning process shall focus on the required business objectives, e.g. restoring of specific services to customers in an acceptable amount of time. The services and resources that shall enable this to occur shall be considered, including staff and resources, as well as fallback arrangements for IT processing facilities.

12.1.4 Business Continuity Planning Framework

12.1.4.1 There shall be a managed process in place for developing and maintaining Business Continuity Plans, throughout

the organisation. A strategy plan, based on appropriate Risk Assessment, shall be developed for the overall approach to Business Continuity Planning.

12.1.4.2 Disaster Recovery Plans quickly become out of date because of changes in business or organisation. In order to prevent the effectiveness of the plan being degraded, regular updating is essential to protect the investment in developing the initial plan.

12.1.4.3 Responsibility shall be assigned for identifying and applying changes to the plan. Individual changes shall be applied at least quarterly. This process shall be reinforced by a brief annual review of the complete plan.

12.1.5 Testing, Maintenance and Re-Assessing Business Continuity Plans

12.1.5.1 Disaster Recovery Plans may fail on being invoked, often because of incorrect assumptions, oversights or changes in equipment or personnel. They shall therefore be tested regularly to ensure that they are up to date and effective. Such tests shall also ensure that all members of the recovery team and other relevant staff are aware of the plans.

12.1.5.2 The testing schedule for Disaster Recovery Plans shall indicate how and when each element of the plan shall be tested. It is recommended to test the individual components of the plans frequently. Various techniques shall be used in order to provide assurance that the plans operate in real life.

13 Compliance

13.1 *Compliance with Legal Requirements*

13.1.1 Identification of Applicable Legislation

13.1.1.1 Information systems shall comply with all relevant UK Legislation, Policies, Standards and guidance, consistent with the business needs of EEAST.

13.2 Intellectual Property Rights

13.2.1 Legislative, regulatory and contractual requirements

shall place restrictions on the copying of proprietary material covered by intellectual property rights, as in Copyright, Design and Patents Act. In particular, they shall require that only material that is developed by EEAST, or licensed or provided by the developer to EEAST, can be used.

13.2.2 Proprietary software products are usually supplied under a licence agreement that limits the use of the products to specific machines and shall limit copying to the creation of back-up copies only. Software copyright shall be adhered to.

13.3 Safeguarding of Organisational Records

13.3.1 Important EEAST records shall be safeguarded from loss, destruction and falsification.

13.3.2 Where electronic storage media is chosen, procedures to ensure the ability to access data (both media and format readability) throughout the retention period shall be included, to safeguard against loss due to future technology change.

13.3.3 Data storage systems shall be chosen such that required data can be retrieved in a manner acceptable to a court of law, e.g. all records required can be retrieved in an acceptable timeframe and in an acceptable format.

13.4 Data Protection and Privacy of Personnel Information

13.4.1 All EEAST processes shall be subject to appropriate legislation and in particular to current data protection legislation, and the Caldicott Guardian report on patient identifiable data.

13.5 Prevention of Misuse of Information Processing Facilities

13.5.1 All Service Providers and Users shall comply with Computer Misuse Act 1990.

13.6 Collection of Evidence

13.6.1 It is necessary to have adequate evidence to support action against a person or organisation, as stated in Electronic Communications Act 2000 (Chapter C7) and Regulation of Investigatory Powers Act 2000 Chapter 23. Whenever this action is an internal disciplinary matter, the EEAST disciplinary guidelines

shall be followed, but for matters concerning the UK police force, their own procedures shall apply.

13.7 Reviews of Security Policy and Technical Compliance

13.7.1 Compliance with Security Policy

13.7.1.1 Information systems shall be reviewed against this Information Security Policy, and the technical platforms and information processing facilities checked for compliance with security implementation standards. Managers shall ensure that all security procedures within their area of responsibility are carried out correctly. Systems shall be regularly reviewed to ensure compliance with security policies and standards.

13.7.1.2 System owners for information systems shall sponsor regular reviews of the compliance of their systems with this Information Security Policy, with security standards and with any other relevant security requirements.

13.8 Technical Compliance Checking

13.8.1 Information systems shall be periodically checked for compliance with security implementation standards. Technical compliance checking involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance checking requires specialist technical assistance. It is performed manually (supported by appropriate software tools, if necessary) by an experienced Information Governance professional. An automated software package can be employed, which generates a technical report for subsequent interpretation, by a technical specialist.

13.8.2 Compliance checking also covers, for example, penetration testing, which may be carried out by independent experts, specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for checking how effective the controls are in preventing unauthorised access due to these vulnerabilities. Caution shall be exercised in case success of a penetration test could lead to a compromise of the security of the system and inadvertently exploit other vulnerabilities.

13.9 System Audit Considerations

13.9.1 System Audit Controls

13.9.1.1 The Head of IM&T or delegated Trust or external Security Consultants shall perform security reviews of systems according to their stage of development, as in Section 11.1.

13.9.1.2 Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimise the risk of disruptions to business processes, using the following guidelines:

- Audit requirements shall be planned and agreed with the owners of the application.
- The scope of the checks shall be agreed and controlled.
- The checks shall normally be limited to read-only access to software and data.
- Other types of access (other than read-only) shall be allowed only for isolated copies of system files, which shall be erased when the Audit is completed.
- Information system resources for performing the checks shall be explicitly identified and made available.
- Requirements for special or additional processing shall be identified and agreed with Service Providers.
- All access shall be monitored and logged to produce an Audit

Log.

- All procedures, requirements and responsibilities shall be documented.

13.9.2 Protection of System Audit Tools

13.9.2.1 Audit tools (software or data files) shall be safeguarded to prevent any possible misuse or compromise by unauthorised staff. They shall be separated from development and operational systems and not held in tape libraries or User areas – unless given an appropriate level of additional security protection.

13.10 Consultation Standard

13.10.1 EEAST will endeavour to ensure that National Policy documents are based on best practice, satisfy clinical governance requirements and are operationally robust. In order to meet this aim, the views of key parties are actively sought at various stages throughout the policy development process, before being signed off by appropriate National Leads. This includes: Relevant site/unit leads, Staff-Side, Access Lead, National Clinical Team, Executive Team, Board and where appropriate, national agencies (e.g. NSPCC, NPSA) and professional bodies (e.g. NMC).

Appendix A – NHS Data Classifications and Measures

In general, EEAST will adopt the DoH Data Classifications for project and patient data and shall be as follows:

(a) ABOVE CONFIDENTIAL – kept only on stand-alone computers – not on HSCN/NCRS.

(b) CONFIDENTIAL, e.g. Medical Records, Customer reports, Commercial information.

(b) PRIVATE or INTERNAL, e.g. Demographic data, Internal reports, Development files.

(c) PUBLIC or UNCLASSIFIED, e.g. publicity data from Internet, external Web pages.

Classified document labelling shall be applied in document headers and footers with the above classification levels preceded by NHS and optionally followed by one of the descriptors PATIENT IDENTIFIABLE INFORMATION, COMMERCIAL, FINANCE, STAFF or ADMINISTRATION.

The following minimum DoH security measures for classified data apply

CLASSIFICATION SECURITY MEASURE	***CONFIDENTIAL (but not ABOVE)***	***PRIVATE or INTERNAL***	***PUBLIC or UNCLASSIFIED***
Maximum Damage	*Adverse*	*Some*	*None*
Example Document	*Commercial Data*	*Internal Report*	*External Webpage*
Document Labelling	*Mandatory*	*Preferresd*	*Unnecessary*
Local Authentication	*Password*	*Password*	*Optional*
Dial-in Authentication	*Strong[1]*	*Strong[1]*	*Optional*

CLASSIFICATION SECURITY MEASURE	***CONFIDENTIAL (but not ABOVE)***	***PRIVATE or INTERNAL***	***PUBLIC or UNCLASSIFIED***
Storage Encryption	BitLocker[2] or PGP[2]	Optional	None
E-mail Encryption	*PGP[2] or Outlook[3]*	*Optional*	*None*
Media Disposal	*Empty Recycle[4]*	*File Deletion*	*Unnecessary*
Fax Transmission	*In Attendance*	*Private Label*	*Free*
Postal Methods	*Double Wrap*	*Private Label*	*Free*

NOTE 1: Strong Authentication (Biometric or Two-Factor Authentication) is preferred for INTERNAL or PRIVATE data and is strongly preferred for CONFIDENTIAL data.

NOTE 2: BitLocker or PGP can be used for Encryption of Files or E-mails, the latter being applicable across different E-mail systems (e.g. Trust and Contractor) provided both systems have common System Administration (coordinated by the Trust IT Support Team).

NOTE 3: Outlook/Exchange E-mail Encryption is invoked where possible in Microsoft Outlook via 'Options-Security-Encrypt', but this applies to internal E-mail only, i.e. with address suffix of @eastamb.nhs.uk, because it is not portable across different blends of E-mail server, e.g. between the EEAST Service and its Service Providers.

NOTE 4: Care is needed with CONFIDENTIAL data to ensure that file deletion is permanent on fixed disks, by removing deleted files from the Recycle Bin.

Appendix B – References

Information Security Management – Code of Practice, ISO/IEC17799:2000.

Information Security Management – Specification Guidance, BS7799-2:2002.

Data Protection Act 2018

Human Rights Act 1998 (Designated Derogation), Statutory Instrument 2001, #3644.

Health and Safety at Work Act 1974, Elizabeth II, Chapter 37, ISBN 0 11 085625 2.

Computer Misuse Act 1990, Chapter 18, ISBN 0105418900.

Electronics Communications Act 2000, Chapter C7, ISBN 0 10 540700 3.

Regulation of Investigatory Powers Act 2000, Chapter 23, ISBN 0 10 542300 9.

Copyright, Design and Patents Act 1988, Chapter 48, ISBN 0105448885.

CCTA Risk Analysis and Management Method, Insight Consulting Limited.

Electronic Government Strategic Framework – Registration and Authentication.

Electronic Government Interoperability Framework – Identity, Office e-Envoy.

Caldicott Report on the Review of Patient-Identifiable Information, Dept of Health.

NHS Incident Management Policy, Alistair Donaldson, Dept of Health.

Appendix C – Equality Impact Assessment: Executive Summary

Document Reference:	Document Title: Information Security Policy
Assessment Date: 31/10/19	Document Type: Policy
Responsible Director: Medical Director	Lead Manager: Andy Marrs
Conclusion of Equality Impact Assessment:	
Recommendations for Action Plan:	
Risks Identified:	
Approved By a Member of the executive team	
Yes	**No**
Name: Clare Chambers	Position: Head of IM&T
Signature – by email	Date: 31/10/19
This whole document should be stored with the master document	

Appendix D – Monitoring Table

What	Who	How	Frequency	Evidence	Reporting Arrangements	Acting on Recommendations	Change in practice and lessons to be shared
Access to Systems & Information is appropriate to the role of the individual	IT Security & Resilience Manager	Random audit & Service Desk records	Annual	Group Membership, system access level	Report to go to IGG and DPST	IM&T	Discussed at IGG and disseminated to the appropriate staff