The Schedule Part 8

SECURITY REQUIREMENTS

8. SCOPE

This schedule sets out the security requirements and constraints which The Contractor shall meet and comply with all aspects of Service Provision to The Trust. For the purposes of this schedule, IT related terminology will retain its commonly accepted meaning. Unless otherwise specified, the responsibility of The Contractor under this Schedule Part 8 is limited to those parts of the assets and premises of The Trust or of The Contractor which are controlled or influenced by The Contractor in the course of delivery of services to The Trust. The Contractor shall not be responsible for breaches of, or failures in, security in those assets or premises over which it only has an influence which can be overridden or manipulated by The Trust or other third parties.

8.1. GENERAL

8.1.1. The Contractor, and any person engaged or employed by The Contractor or by his agent in connection with this Contract, shall comply with the requirements of the NHSiS IT Security Policy, Manual and Guidelines, including Codes of Confidentiality for contract and patient information. In addition, the contract shall fulfil the obligations set out in Caldicott Guidelines ("Security Policies"). The Trust shall produce all above mentioned documentation within 30 days of contract signature.

8.1.2. The Contractor shall undertake to deliver all services to The Trust from designated sites or locations which have been agreed in advance with The Trust, and shall not change the site or location of any service provision without obtaining the prior agreement of the Trust unless it can demonstrate that security shall not be compromised as a result of such change in site or location. The Trust reserves the right to deny such approval or require specific security measures at The Contractor's expense to counter any additional risks. Such approval will not be unreasonably withheld, but in the event it is withheld then the Contractor reserves the right through the Change Control procedure to vary the Service and Charges if it can reasonably demonstrate that in

not being allowed to change the site or location of service provision it is not able to maintain the level of service or pricing.

8.1.3. Where sharing of resources or assets is permissible, The Contractor shall be responsible for determining the relevant new security profile using applicable NHSiS minimum standards, where applicable and provided to the Contractor in advance, and an approved formal method of risk analysis, and for the submission of all revised security profiles and/or policies to The Trust for approval prior to implementation. (not applicable – dedicated system, not shared – no control over Trust assets either?). Subsequent changes to the Security Policiesand their respective procedures will be controlled under the provisions of Change Management.

8.1.4. The Contractor shall be responsible for the operation and management of Security Policies, their measures and procedures with respect to those assets, sites and IT systems over which The Contractor has direct control. The Contractor shall be responsible for ensuring that Security Policies, their measures and procedures are approved by The Trust . In the event that Security Policies do not exist or are not being complied with, the procedures at Para 8.4.3. will apply. Implementation of any additional security measures or procedures shall be subject to the provisions of Change Management.

8.1.5. Changes to the Security Policies, their measures or procedures, as a result of new risk arising exclusively from changes to the environment, locations or services under the direct control of The Contractor, and the remedying of deficiencies in respect of the above as notified by The Trust, shall be the responsibility of The Contractor. All new risks should be notified to The Trust as soon as The Contractor is aware of the risk.

8.1.6. Changes to the Security Policies' measures or procedures which arise as a direct result of changes to IT Security rules or requirements, or which impact upon or alter IT Security Policies or procedures of IT systems over which The Contractor has control, or sites belonging to The Trust and for which The Contractor has control, shall be implemented within the provisions of Change Management. The Trust shall be responsible for costs incurred by The Contractor as a direct result of such changes, where those costs are attributable to delivery of services to The Trust,

but excluding any change arising from obligations on The Contractor under law or as a result of other direct obligations on The Contractor arising from, for example, other agreements.

8.1.7. Where The Contractor stores and processes personal data for The Trust, The Contractor shall co-operate with and support The Trust such that subject access requests, and any compliance orders or judgements against The Trust, can be met within prescribed timescales, provided always that the Contractor is given sufficient notice to permit compliance. Access to archive or historic data held by The Contractor shall be provided as a mandatory service in accordance with the Data Archiving and Retention policy stated in Schedule Part 7. Any changes to procedures requested by The Trust as a result of such requests, order or judgements will be subject to the provisions of Change Management, excepting that The Trust shall not be responsible for any remedial action necessary for The Contractor to comply with obligations under law that apply directly to The Contractor. The Trust must register all appropriate information and systems with the Data Protection Registrar and The Contractor must register as a service provider.

8.1.8. The Trust shall ensure that IT Security provisions and procedures, including storage of back-up and archive media, do not prevent effective audit of the back-up process.

8.1.9. The Contractor, his employees and agents shall, in their execution of tasks on behalf of The Trust, comply with all existing and future relevant, related legislation, in so far as it relates to the Contractor, his employees and agents including:

a) Data Protection Act 1998
b) Police and Criminal Evidence Act 1984
c) Copyright, Designs and Patents Act 1988
d) Computer Misuse Act 1990
e) Public Records Act 1958
f) Open Government : Code of Practice on Access

Where compliance with future legislation requires change to the service, such change shall be subject to Change Management except where such obligations under law are placed directly upon The Contractor.

8.2. PERSONNEL

8.2.1. The Contractor shall operate recruitment and sub-contracting policies and procedures such that the identity, bona fides and suitability of persons employed or engaged in service delivery under this Contract can be effectively verified and to reject persons where such verification fails

8.2.2. The Contractor shall undertake to identify in conjunction with The Trust, any formal security clearance requirements for persons employed or engaged on delivering services under this Contract, or other applicable persons employed or engaged by The Contractor, having regard to their necessary or potential access to Confidential Information by virtue of function or use of premises or facilities. The Contractor shall ensure in conjunction with The Trust that such clearances are undertaken, obtained and maintained, and that no person is given access to Confidential Information unless any necessary clearances have been obtained in advance.

8.2.3. The Contractor shall limit access to The Trust's information on a need to know basis and ensure that access to computer systems and facilities used to provide services to The Trust is limited to those with a bona fide requirement to have such access. The Contractor shall identify those individuals employed or engaged by The Contractor whose access to facilities and systems, or control of services, could give them unconstrained access to The Trust's information or the ability to deny The Trust use of their systems and information. The Contractor shall employ one or more of separation of duties, procedures and audit, as agreed with The Trust, to constrain and monitor the actions of such individuals to legitimate actions within The Trust. The Contractor reserves the right to vary the service and charges if such constraints imposed upon it by Trust after contract signature require additional resources to be employed by the Contractor.

8.2.4. The Contractor shall ensure that all persons engaged or employed by it who may have access to The Trust's data or facilities, or whose actions may impact on operational services to The Trust, are made aware through instructions, training and other methods, of their security responsibilities , and that they understand all applicable security instructions, controls and measures with which they must comply or which they must operate.

8.2.5. The Contractor shall immediately revoke permissions, trust and access relevant to The Trust's data, facilities and services for persons whose services in connections with this Contract, or more generally, are terminated, or whose requirement for such access otherwise ceases. Where, in the opinion of either The Contractor or The Trust the circumstances of any termination are such as to warrant it, The Contractor shall revoke such permissions, access and Trust on issuing notice of termination. The Trust shall be responsible for notifying The Contractor of persons whose services have been terminated, where The Contractor is required to revoke permissions, Trust and access relevant to The Trust's data.

8.3. SECURITY POLICY

8.3.1. The Contractor shall produce, agree with The Trust and maintain a statement of security policy which clearly states the security framework and regime to be applied in the delivery of the services and to protect The Trust's information, allocates responsibilities within The Contractor's organisation and identifies how the requirements of the policy will be promulgated and enforced. The policy will be consistent with and support the NHSiS IT Security Policy. The policy will identify how the security requirements and rules of The Trust as expressed and referenced in this Schedule Part 8 will be applied and operated in conjunction with those of The Contractor. Following agreement, The Contractor shall implement and operate the policy, monitor its effectiveness, and amend and maintain the policy as considered necessary, or as required by The Trust. In the latter case, such changes will be subject to Change Control procedures. The Contractor's Policy must detail security breach investigation and reporting responsibilities.

8.3.2. The Contractor shall determine, implement and operate security measures, procedures and controls arising from The Contractor's

agreed Security Policy, monitor their effectiveness, and make such changes as necessary from time to time or as required by The Trust. The Contractor shall advise, notify and agree with The Trust the nature and details of such measures, procedures and controls, where required by and at the discretion of The Trust. Subsequent changes will be governed by Change Control procedures.

8.3.3. The Contractor, and any person engaged or employed by The Contractor or by his agent in connection with this Contract, shall ensure that services delivered comply with the Trust's Security Policies, as provided by The Trust pursuant to Schedule Part 7, for the applications and computer systems concerned. The Contractor shall identify to The Trust any computer system or application under its direct control which comes to his notice and for which a security policy or statement approved by The Trust is not available, and agree with The Trust any remedial action or specific arrangements in such cases, which will be governed by Change Control procedures.

8.4. ORGANISATION, MANAGEMENT AND RESPONSIBILITIES

8.4.1. The Contractor shall be responsible for all aspects of security of Contractor managed, controlled or provided:

a) operational site/s and computer systems
b) development site/s and computer systems

8.4.2. The Contractor shall maintain the Security Policy (Schedule Part 8, section 8.3.2) to meet The Trust's Security and Data Protection requirements as advised to the Contractor pursuant to Schedule Part 7.

8.4.3. The Contractor shall provide The Trust with contact details for staff within The Contractor's organisation with responsibility for security as The Contractor deems appropriate or as required by this Contract. The Contractor shall maintain and update such contact information in line with changes in organisation, services and security requirements.

8.5. SECURITY INCIDENT MANAGEMENT AND REPORTING

8.5.1. The Contractor shall report with appropriate detail and without unreasonable delay any loss of documents or other media containing The Trust's data over which he exercises control and which contains Confidential Information, and any other loss or damage to any other assets of The Trust over which he has control. The reporting shall be in accord with the NHSiS Security Manual, to be provided pursuant to Schedule Part 7.

8.5.2. For IT systems, networks and sites under the control of The Contractor, The Contractor shall report with appropriate detail any actual or suspected security incident (including loss of integrity or availability) involving The Trust's information, assets or facilities, and any weakness in computer systems or procedures identified, which might give rise to a breach, without delay within Working Hours. Information on such incidents and weaknesses shall be protected on a need-to-know basis, and documentation of these matters will be suitable protected against unauthorised disclosure.

8.5.3. The Contractor shall, in the case of an actual or suspected security incident, take any reasonable steps to contain the situation or reduce the impact as considered necessary by The Contractor or as reasonably required by The Trust. The Contractor shall take reasonable steps to avoid the destruction of any evidence which may be necessary to the investigating officers.

8.5.4. The Trust shall reserve the right to investigate any or all suspected or actual security incidents which occur during the processing or storage of information belonging to The Trust, or involve the loss or compromise of The Trust's assets. The Contractor shall, in such circumstances, allow the representatives of The Trust all reasonable access to premises and records, and shall co-operate with The Trust's representatives during their investigations. Costs arising from the investigation of security incidents upon equipment or software owned by, or exclusively managed by, The Contractor will be the responsibility of The Contractor, excepting that if a security incident is caused, directly or indirectly, by the actions of The Trust reasonable costs shall be paid by The Trust.

8.5.5. The Trust shall be responsible for the routine scheduled monitoring of all access logs, audit trails and other diagnostic aids relating to the computer systems, facilities and equipment provided and operated by The Contractor and used to deliver services to The Trust, in order to identify actual or attempted breaches of security. The Trust shall, without unreasonable delay, notify The Trust of any irregularity.

8.6. SITE SECURITY

8.6.1. The Trust shall ensure that an appropriately secure physical environment (e.g. access controls, safety standards, emergency procedures, and fire controls and procedures) is provided and maintained in respect of any premises or sites used by The Contractor for the provision of services to The Trust or for the storage of information on behalf of The Trust.

8.6.2. The Trust shall operate and maintain procedures and controls such that unescorted access to specific areas and facilities utilised for the delivery of services to The Trust, or to store The Trust's data, is limited to those engaged or employed by The Trust or The Contractor and who have a bona fide requirement for such access. Where, in the opinion of The Trust, such access to facilities or The Trust's data requires specific security vetting or clearance, The Contractor shall ensure that access is permitted only to staff who have been granted the necessary clearance. The Contractor shall not be liable for any degradation in the service due to delays on the part of The Trust in granting such clearances.

8.6.3. The Trust shall operate and maintain suitable arrangements to control and monitor visitors to all premises under the control of The Trust and from where The Trust's data is stored, accessed, printed or despatched such as to minimise the risk of any security breaches and security incidents which may impact upon The Trust arising from actions by such visitors.

8.6.4. The Contractor shall maintain controls to prevent unauthorised access to, or use of, terminals or devices used in the delivery of services which allows the Contractor to remotely access The Trust's data or computer systems, but The Contractor shall not be similarly responsible for terminals and devices used by The Trust to access its computer systems and data.

8.6.5. The Contractor and persons engaged or employed by The Contractor shall comply with the security, emergency, building works and health and safety procedures and arrangements applicable at that site, as notified to the Contractor by The Trust. The Contractor shall within a reasonable period advise The Trust where the requirements in these respects of any site conflicts or appears to conflict with other security obligations of The Contractor under this Contract and agree appropriate action. Such action will be subject to Change Control as appropriate.

8.7. ADMINISTRATION OF ACCESS CONTROLS

8.7.1. The Contractor shall take the appropriate steps which have been proposed by The Contractor and agreed with The Trust to ensure that access to and use of computer systems upon which The Trust's information is being stored or processed is limited to authorised personnel.

8.7.2. The Contractor shall ensure that where specific security clearances are required by The Trust in order that The Contractor's staff may undertake particular tasks, only staff possessing such clearances will be able to gain access to information connected with that task.

8.7.3. Where the Contractor requires to set up remote diagnostic and maintenance facilities for The Trust, it shall first obtain the consent of The Trust . The Trust reserves the right to deny such approval or require specific security measures to counter the additional risks. A log of any remote support activity must be retained for audit purposes. The Contractor shall not be responsible for any and all degradation in the service where this restriction results in the Contractor taking longer to fix faults.

8.7.4. Except where explicitly agreed between The Trust and The Contractor, it shall be the responsibility of The Trust to manage the procedures for authorisation of new users and the responsibility of The Trust to administer the password access systems relating to normal user access to The Trust's applications and facilities.

8.7.5. The Contractor shall not introduce or permit the introduction of applications which provide access to The Trust's operational data other than to authorised Trust users, including those with Trust clearances in the employ of the Contractor.

8.7.6. Where there is an identified need for terminals or IT computer systems belonging to The Contractor or his agents to be connected to IT computer systems or networks (including voice networks) belonging to The Trust, the terminals and links shall be configured to provide the minimum access to Contractor personnel compatible with carrying out authorised tasks on behalf of The Trust and maintaining the service levels stated in Schedule Part 12. The Contractor shall identify to The Trust the nature of the connected systems and links and their use and duration, and propose, agree and implement security measures to counter the risks to The Trust's information and systems. The implementation and operation of such links and measures shall be at The Contractor's expense. No connections to, or use by, The Trust's systems shall occur until The Trust's prior approval has been obtained. The Contractor shall not be responsible for service degradation due to delay by The Trust in granting such approval. Subsequent changes will be controlled and authorised under Change Control procedures.

8.8. TECHNICAL CONTROLS

8.8.1. The Contractor shall ensure, for computer systems over which The Contractor has control (including software) and which store, process or transmit The Trust's data, that all controls (e.g. hardware, software, communications security) relating to those computer systems or components are correctly implemented and operated. The Contractor shall ensure that all controls installed or operated by The Contractor meet the requirements of the Trust's IT Security Policy, and are compliant with any mandatory standards of the Trust, that are communicated pursuant to Schedule Part 7. Where The Contractor identifies deficiencies these shall be notified to The Trust for consideration within the provisions of Change Control.

8.8.2. The Trust shall have the right to test, inspect, analyse and audit the security functionality and capabilities of all computer systems owned, managed, controlled or operated by The Contractor which store or process The Trust's operational data, or any other sensitive data of The Trust at times agreed with the Contractor. Where deficiencies are found which are due to a failure on The Contractor's part, The Contractor shall be required to remedy any deficiencies at his own expense.

8.8.3. The Contractor shall take all reasonable precautions to ensure that all computer systems and equipment operated and controlled by The Contractor and used for delivering services to The Trust use appropriate (or agreed) security measures and are sited, installed and operated such that they are protected from accidental disruption.

8.8.4. The Trust shall make available to The Contractor details of mandatory IT security standards that apply to particular systems or information of The Trust. The Contractor shall take these into account in providing maintenance, enhancement and development services. The Contractor shall be responsible for the costs of security measures required to comply with these standards where the need for compliance or change arises from requirements of The Contractor.

8.9. COMMUNICATION AND TRANSMISSION SECURITY

8.9.1. The Contractor shall undertake to comply with all future instructions issued by The Trust in respect of the transmission of Trust information by electronic or other means. Where additional work is necessary to comply with these instructions, this will be subject to Change Control procedures.

8.10. MEDIA SECURITY AND DISPOSALS

8.10.1. A destruction certificate signed by two of The Contractor's staff must be provided to The Trust in respect of all protected information which is destroyed by The Contractor. By agreement The Contractor may instead return all such material to The Trust for destruction. An audit log must be maintained of all destroyed media.

8.10.2. All waste material of any kind, which contains information belonging to The Trust, shall be disposed of by The Contractor using a method, which ensures that information contained therein, is not compromised. All waste shall be stored in a manner commensurate with the sensitivity of the information whilst disposal is awaited.

8.10.3. All paper-based waste material that is used or produced by the Contractor, which contains Confidential Information, shall be disposed of by The Contractor in accordance with current security regulations as are advised to the Contractor pursuant to Schedule Part 7, and in accordance with the regulations referenced in Para 8.2.1.

8.10.4. The Contractor shall ensure that all information (other than protected information) held on magnetic media shall be destroyed by either destroying the media or by overwriting the data in an approved manner when it is no longer required. Magnetic media may be released to a third party (including repair and maintenance suppliers) only after any sensitive data has been over-written in accordance with procedures agreed by The Trust. Media removed from site by The Contractor should be logged 'out' and 'in' for audit purposes.

8.10.5. Where recycling of paper or other waste containing information belonging to The Trust is proposed, The Contractor shall ensure that

the recycling is carried out in a manner which does not compromise the information contained therein. The Contractor shall consult and agree with The Trust on the appropriateness of any proposed scheme.

8.11. MONITORING AUDIT TRAILS AND RECORD KEEPING

8.11.1. The Contractor shall, in the course of providing development or enhancement services to the Trust, ensure that audit requirements as detailed by the Trust for each computer system and application correspond to the needs of The Trust, that the requirements are implemented in a secure manner and that all relevant records are archived for the appropriate retention periods as advised to the Contractor under the Trust's Data Archiving and Retention policies pursuant to Schedule Part 7.

8.11.2. The Contractor shall ensure that no change is made to any computer system under its control such that previous audit trails are no longer accessible.

8.11.3. The Contractor shall, for all computer systems under its control subject to Change Control, maintain a record of all changes (other than changes as a result of routine hardware maintenance/minor repair) made against each computer system, with all dates, actions, personnel involved, reasons for change and Trust reference. The Contractor shall retain such records for a minimum period of six months, and make such records available to The Trust on request.

8.11.4. The Contractor shall operate and utilise the journal and audit facilities available on the computer systems operated and managed by The Contractor which store, transmit and process Trust's data for the purposes of effective security management and control. The Contractor shall make such journals and audit trail data available to The Trust on request. The Contractor shall ensure that relevant records are archived for appropriate retention periods under the Trust's Data Archiving and Retention policies.

8.12. SECURITY OF DEVELOPMENT & ENHANCEMENT SERVICES

8.12.1. The Contractor shall define, agree with The Trust and operate procedures to be followed by its staff providing development, maintenance, enhancement to ensure that such work:

a) Follows the NHSiS and, other standards identified by The Trust to the Contractor for IT security (including the documentation of security policies and the use of risk analysis).
b) Is compliant with and allows for applicable NHSiS and Government mandatory standards, and applicable legal requirements as identified by The Trust to the Contractor.

8.12.2. The Contractor's procedures shall ensure that security is adequately addressed at the following stages when performing maintenance, development or enhancement work:

- analysis;
- design;
- implementation;
- testing;
- acceptance; and
- delivery

8.12.3. Where enhancement or redevelopment work is likely to result in changes to the security of a system, The Contractor shall assist The Trust in impact analysis to assess the security impact of such changes. To this end, The Contractor shall employ a recognised and formalised method of risk analysis and management, which is agreed by The Trust to be suitable for the type of information and computer system involved, such method to be agreed prior to the commencement of any enhancement or redevelopment work.

8.12.4. The Contractor shall ensure that all security requirements defined in the initial system specification, or which will become otherwise known to be necessary, are addressed when undertaking development and enhancement work on behalf of The Trust.

8.12.5. The Contractor shall ensure that as part of maintenance and support services any need for change or revision of applicable computer system security policies or measure arising from such service actively is identified to The Trust. In such cases security documents which are configuration items maintained by The Contractor shall be updated by The Contractor and submitted for approval by The Trust in accordance with the relevant procedures.

8.12.6. The Contractor shall ensure, for enhancements and developments for which it is responsible, that where such work includes the production of security documentation it is submitted to The Trust for both informal and formal review in accordance with The Trust's current procedures. In cases where The Contractor's responsibilities do not extend to the production of the security design and documentation, The Contractor shall identify to The Trust any issues or design aspects arising from such enhancement and development work which need to be taken into account by those responsible for the security elements of the design. The Contractor, in undertaking support for any enhancement or development, shall identify to The Trust any case where the new element to be supported does not appear to be covered by an approved policy. In such cases Para 8.4.3 shall apply.

8.13. AUTHORISATION OF CHANGES

8.13.1. The Contractor shall have trust to carry out repair or replacement tasks which have the effect of reverting the hardware or software used for delivery of service to The Trust to a pre-existing authorised state where this is essential to maintain the availability of a computer system. Such actions must be logged by The Contractor with their reasons.

8.13.2. The Contractor shall not implement changes to the hardware or software belonging to, or used for delivery of service to, The Trust where such change may modify access restrictions, or may impact security controls (including aspects of the system relevant to resilience, availability or integrity) without having given notification in advance and obtaining any necessary authorisation from The Trust. The Contractor shall not be held liable for any delay by The Trust in providing the appropriate authorisations to The Contractor.

8.13.3. The Contractor shall not, through its use or access to The Trust's premises, instigate or make changes to the fabric of buildings, building power supply arrangements and circuitry, or other building wiring including data and voice circuits, where such buildings are owned or leased by The Trust without the prior authorisation of The Trust.

8.13.4. Change Control procedures will be implemented by The Contractor such that all changes made to hardware or software used to deliver services to The Trust will be recoverable in case of Contractor or other error.

8.13.5. The Contractor shall ensure that facilities are available to achieve adequate separation of development and production environments, such that changes or modifications to the computer system or application can be comprehensively tested without risk of damage or disruption to the production service during the testing process.