University Hospitals Bristol NHS
NHS Foundation Trust

Information Security – Principles, Guidelines & Procedures

Extended to 30/09/2017

University Hospitals Bristol NHS
NHS Foundation Trust

Version Control / Amendment History

Issue Status	Version	Date	Author	Input/Amendment Description
Draft	0.1	21-02-14	[redacted]	Document Adaption
Approved	1.0	13-03-14	[redacted]	Document Approved
Update	1.1.	15-08-14	[redacted]	Merge existing policy to form Appendix A
Update	1.2	17-11-14	[redacted]	Added links to evidence folder

Reviewers:

Name	Title	Date of Issue	Version
[redacted]	Regulatory Compliance Manager	6 – 3- 14	0.1

Approval Route:

This document requires the following approvals.

Name of Group	Date of Approval	Version
Information Risk Management	13th March 2014	1.0

University Hospitals Bristol NHS
NHS Foundation Trust

Contents

University Hospitals Bristol NHS
NHS Foundation Trust

1. Securing Information – Principles

The Trust's Information Governance Policy states that all information held by the Trust will be:

- Accurate, complete, justifiable, available and timely.
- Used in an appropriate manner.
- Maintained confidentially.
- Securely kept and transmitted to others safely.
- Properly administered.
- Disclosed to others appropriately according to prevailing legislation and regulation.

Based on these policy statements, the principles on which sound network security are based within the Trust are as follows:

- System-based controls to allow appropriate access to information.
- Data loss including inappropriate disclosure on media and permanent loss to the organisation.
- Unavailability of data from malicious software, user actions and other external events.

The sections in this document describe various aspects of information security, taking into account these principles.

2. Physical & Technical Security

2.1 Secure Working Areas – including Perimeters & Entry Controls

Open Public area – Areas where the public are allowed to move freely, such as corridors, waiting areas, some ward environments etc. Security based on general security arrangements, such as staff vigilance, security patrols and CCTV. IM&T equipment will only be placed in these areas if absolutely necessary. Ad Hoc surveys will be conducted to ascertain risks associated with the physical security of IM&T equipment with recommendations to mitigate any potential risk. Security equipment (Kensington Locks, cables, cages etc.) should be used where equipment may be left unattended. Data will not be stored directly on devices in these areas unless networked storage is unavailable. The deployment of PC's in these areas will be reviewed and where possible be replaced with diskless 'Zero Client' devices that cannot store data on them. All PC's will be encrypted.

Controlled Public area – Areas, which the public can be present in, but only following authorised access by staff. Once within these areas, control over the public is again via staff vigilance and CCTV. IM&T equipment will only be placed in these areas if absolutely necessary. Ad Hoc surveys will be conducted to ascertain risks associated with the physical security of IM&T equipment with recommendations to mitigate any potential risk. Security equipment (Kensington Locks, cables, cages etc.) will be used if equipment is to be left unattended at all. Data will not be stored directly on devices in these areas unless networked storage is unavailable. All PC's will be encrypted.

Staff only areas – No member of the general public is allowed access, except on special controlled occasions, when they are accompanied at all times by a member of staff. Staff only areas may also be subject to restriction to only certain staff members and others when accompanied via entry controls. No additional physical security will generally be needed for IM&T equipment in these areas. Data will not be stored directly on devices in these areas unless networked storage is unavailable. All PC's will be encrypted..

Access restricted areas (access to specific staff only) – Where core computing equipment (fileservers, central network equipment) is housed, access will be restricted by physical entry controls (such as digital door locks, swipe cards or similar). Access will only be granted to appropriate staff and will be authorised and managed by the IM&T department. Access by other staff will be accompanied at all times. When required, access can be granted to contractors or other temporary staff, provided the access is removed at the end of the period, which will require changes of codes where used to control access. Visitors to these areas will be required to sign a log detailing entry and exit times and the reason for entry.

All areas - Within any area there should be the facility to protect information assets. Such facilities may be lockable offices or filing cabinets. Use of these facilities within a department should be determined and implemented, including the education of staff. This should be subject to regular review to ensure adequate protection for the information, but appropriate availability to those that need it, when they need it.

Guidance for departmental evaluation:

- External signage for non-clinical buildings, offices and other areas should only give minimum indication of purpose.
- Personal and sensitive information on paper should always be secured in lockable filing cabinets (or similar).
- Doors and windows should be locked when unattended, with external protection considered for windows, particularly at ground level.
- All members of staff should wear ID badges at all times. Visitors should be issued with visitor passes.
- Third party support services should only be allowed in controlled/secure areas, when necessary and such access must be authorised and monitored.
- Data not to be stored locally unless lack of infrastructure requires it. Any personal data stored locally due to lack of central storage will be encrypted.

2.2 Security, Installation & Maintenance of Equipment

The following guidance must be considered when siting equipment and used if possible:

- Computer screens and paper records should be positioned to reduce the risk of overlooking during their use. Screen shields and folders should be routinely used in 'open public' areas.
- Equipment should be sited away from overlooked windows (unless additional window protection is in place).
- Equipment should be sited away from sources of heat, explosion, water, dust and electromagnetic radiation. This includes items such as radiators (heat and water), chemical and gas storage.
- 'Critical' equipment such as servers, network infrastructure should be sited in an appropriately controlled environment, in terms of security, power fluctuation (UPS), fire/smoke detection, fire suppression, temperature, humidity and cleanliness.
- Eating & drinking will not be allowed near 'critical' equipment and will be actively discouraged near other equipment. Staff causing damage to equipment may be responsible for the cost of repair or replacement.
- Equipment should only be installed by IM&T department staff or their approved contractors.
- The IM&T department are responsible for all IM&T equipment maintenance purchased via their department. They are not necessarily responsible for maintenance of equipment purchased by departments on their own.

2.3 Power Supplies

Power supply to equipment should be routinely considered in all new installations. Existing power supply should be regularly reviewed. Both should be undertaken in line with areas detailed below.

Critical systems & infrastructure – Any system that is used for 'Diagnostic support' (e.g. Pathology, Radiology) or 'Direct Provision of Patient Care' (e.g. Pharmacy, Wards, Emergency Departments etc.) must be provided with power supply protection. As a minimum this will be an Uninterruptible Power Supply (UPS). This is required so that in the event of a power failure, the IM&T systems can still be accessed until standby generators can be brought into use, power is restored or continuity activity (fall-back plans) are invoked. UPS equipment must be regularly checked to ensure it has adequate capacity (battery life) and tested in line with the manufacturers' recommendations.

2.4 Cabling Security

Due to the nature of many healthcare premises, full implementation of cabling security is not always possible. The following defines minimum requirements for all installations.

- Power and telecommunication lines should be protected where possible by ducting from source to socket(s).
- Where cables have to be 'clipped' to existing services they must be fastened with metal cable ties to prevent them falling in the event of fire.
- Cables should not be connected to active network equipment when no end device is connected.
- Active network equipment will have port security enabled to prevent unauthorised connections to Trust resources.
- All installations of power and cabling must be protected from environmental threats and comply with legislative and estates department requirements.

2.5 Asset Registers & Secure Disposal of Equipment

The IM&T department maintains an asset register of all IM&T equipment, including detail on all purchases and disposals. The register is accessed through the Trusts service desk and contains details of hardware, software, service history and user details. Equipment that is no longer required or is allocated to another user within the Trust is also tracked on the service desk asset management system. Should the previous owner have any data stored on the PC as opposed to network storage, they are responsible for ensuring that any data they wish to keep is copied to an appropriate storage facility prior to reassignment.

Equipment to be disposed of, will have the hard disc removed and wiped by the use of degaussing equipment that meets CESG recommendations. The serial number of the hard disc is documented against the PC serial number it was extracted from.

The Trust will ensure it is compliant with The Waste Electrical and Electronic Equipment (WEEE) Directive when disposing of equipment. Copies of the Duty of Care: Controlled Waste Transfer Notes can be found here.

The IM&T department follow and implement the guidelines detailed within the Trusts policy for the Disposal of Computer Equipment available from http://nww.avon.nhs.uk/dms/Default.aspx?sid=0&s2id=1313

2.6 Protection against Malicious Software

The Trust sets the following controls as policy to address the risk of reduced integrity and availability of its information assets:

- All software installed on Trust assets will be appropriately licensed.
- The IM&T service desk must authorise any installation of software.
- The IM&T department is responsible for the installation and regular update of anti-virus software on all appropriate machines (servers and clients).
- Users wishing to use removable media must be registered with the Trusts USB inventory. All removable media will be virus checked when used.
- Any suspicion of virus infection must immediately be reported to the IM&T service desk.
- Procedures for reporting and handling virus attacks, and recovering from them are to be implemented.
- Equipment is deployed to report, limit and mitigate against malicious 'hoax' attacks.
- Staff will be trained to have an awareness of the above controls and their responsibilities.

2.7 Network Management & Security

Responsibility for the Trusts network is segregated from the responsibility for computer operations. Responsibility of control over the Trusts network is allocated to the appropriate people within the IM&T department, namely the Trust Network Manager.

The Trust Network Manager is responsible for the implementation of appropriate controls listed below. Network service security in the organisation will be fully documented, reviewed and updated within the Network Security Policy.

(a) Enforced access pathways

Users will only be provided with direct access to the services they have been specifically authorised to use. Access to services will, by default, be covered by the user registration control for access to systems. Management controls and procedures to protect the network are defined in the following sections.

- Enforcing the use of specified security gateways for external network users (remote access servers & facilities) necessitates the completion of an intranet based form by the staff member's line manager.
- The use of wireless networks will be secured by implementation of current industry standard encryption technologies, such as AES, WPA2 and 802.1x.

(b) Node authentication

Where groups of remote users are connected to a secure, shared computer facility further connection can be made via node authentication as an accepted method.

(c) Remote diagnostic port protection

IM&T and other departments managing hardware infrastructure will ensure that any remote diagnostic port on hardware they manage is protected and there are robust procedures for allowing authenticated access by others such as system suppliers.

(d) Network segregation

Segregation of networks in to separate logical segments will be promoted by the IM&T department in the development of organisational (and wider) infrastructure.

3. Access Control

3.1 User Access Control & Management

Controlling access to information is one of the key elements of organisational compliance with legislation such as the Data Protection Act. A summary document can be accessed here.

(a) System access control principles

The following statements are the rules that will be applied to controlling access to any information system within the Trust, by employed staff and third parties. 'Information Asset Owners' must ensure that due consideration is given to application of controls detailed below by appropriate staff.

- Access to systems and information are granted on a need to use and need to know basis.

- Setup and regular maintenance of access controls in systems will take account of all relevant legislation and regulations. Advice must be sought from the Information Governance lead, who may seek expert legal/technical advice.
- Access controls will be based on user roles. For CfH applications, national Role Based Access Control (RBAC) policy will be followed, which may be supplemented by additional local policy as required.
- Access controls and authorised users will be reviewed regularly.
- As a general rule, administration staff should see minimal clinical data, accepting there are some administration roles that need clinical information and that some clinical information can be inferred by administration data (clinic purpose etc.).
- Allocation and use of privileges (feature that allows a user to override normal controls) will be restricted and controlled. They will be allocated on a 'need to use' basis and on an 'event-by-event basis.' Record of allocation will be kept by system managers.

(b) Granting & maintaining user access

All multi-user systems will have a formal process for requesting and removing access. Initially a new user will be required to complete an Email and Network Connection form which can be found here. Formal records of all users, past and present, will be kept. The process for a system can be combined with that of others or kept separate. It is envisaged that core systems managed within the organisation would be subject to one process and management, whereas other systems may require separate processes.

Processes will include:

- Allocation of a unique User ID. The use of generic User IDs is only permitted in limited circumstances and must be agreed by the Information Governance lead who will control the circumstances under which these are used.
- Authorisation of the access request will be granted from from a line manager or 'Information Asset Owner', who is responsible for confirming the provisional user has a 'need to use' and 'need to know' the information contained within the system that is accessible via their user role.
- Notification to the user of their responsibilities under this and associated policy, and their acceptance of those via the employee's signature or formal response.
- Confirmation to the staff who create the access that the requirements of the process are complete before the access is created and issued.
- Access change request procedure, authorised by line management or Information Asset Owner, usually on the basis of changed role or enhanced responsibilities.
- Access revocation procedure, authorised by line management or Information Asset Owner, initiated by user leaving or other request for revocation such as a role change.

- Access to CfH applications will be managed under national policy, upheld by specific local Registration Authority Policy and processes, which is generally in line with the principles detailed above.
- All procedures to grant and manage user access will be integrated with Human Resources processes for new starters/leavers, role changes and temporary absence.
- System Managers will conduct a review of unused accounts on a regular basis and will as a default notify the IM&T helpdesk who will disable access to any account that has not been used for 3 or more months consecutively.
- System Managers will conduct reviews of active accounts in relation to lists of leavers to identify any account still in use after a staff member has left. Any accounts found not to be in use should be notified to the IM&T helpdesk who will disable access.

3.2 System Access Control Requirements

System management & Information Asset owners will identify the requirement for the use of automatic terminal identification, where there is potential and need for limiting access to a system or system function to particular locations. For example there may be a need to limit access to certain functions on a Theatre system to terminals within operating theatre locations. If access restrictions to a location can be applied, in operational terms and the system can support them, they will be applied.

Log on procedures within systems will disclose the minimum information about the system to prevent unauthorised users being provided with log on details. The following are minimum standards for systems to meet. Not all systems will currently meet these, and these discrepancies should be identified in a system specific security statement. Systems that do not meet these criteria will be developed to do so. If development is too costly, then these criteria will be set as a minimum for eventual replacement systems:

- A general warning notice that access should only be by authorised users will be shown at the commencement of log on procedures.
- When an error occurs with a log on attempt, systems will not detail what is incorrect (i.e. will not display a message such as 'incorrect password', they will simply report a phrase such as 'log-on details incorrect').
- Systems will only allow five incorrect log on attempts and will record all details connected with these log on attempts.
- Following five unsuccessful log on attempts systems will freeze accounts for a minimum of thirty minutes or if possible until specific authorisation to unfreeze the account is given by system management.
- Following successful log-on, systems will display date and time of last successful log on and details of any unsuccessful log on attempts, to prompt authorised users to notice failed log-on attempts, which may be unauthorised.

- Log on procedures will have a maximum time length for completion of the procedure, recommended as no more than 2 minutes. If log on details are not completed successfully in that time the log on should terminate.
- All information systems will feature password control. As with log on procedures, the following policy elements will be applied to all systems, unless evaluation finds that cost or system architecture does not support it. In such circumstances the statements will be applied to replacement systems.

3.3 User password management

Password allocation will be managed via formal processes as part of user registration and account maintenance. The processes will:

- Require users to agree to a statement to not share or record passwords.
- Ensure users are aware of the need to change passwords.
- Issue initial passwords by means of face to face contact, where ID can be verified, either via the IT dept. or system training.
- All users will be required to change initial passwords immediately.
- Users can reset forgotten passwords from the logon Gina by answering three questions from a selection presented upon registration with the Trusts Single Sign On system (SSO).
- Re-issue forgotten passwords following positive identification of the user, if necessary via a face to face meeting, where ID is checked. The new password will expire when first used, requiring the user to set a new one of their own.
- For Smartcard & PIN management see separate national policy.

Standards for quality passwords:

- User selection of passwords will include a confirmation procedure to check for user error when inputting the new password.
- Complex passwords that contain a combination of upper and lower case characters and numbers, with a minimum length of eight characters are mandatory.
- Password change will be enforced every sixty days as a minimum.
- Each password change cannot be repeated for a minimum of five changes.
- Passwords will not be displayed in readable format on screen at log on or change.
- Initial or reset passwords performed by the IM&T helpdesk will be set to require an immediate change at first/next log on.
- Passwords will be stored in an encrypted form using a one-way algorithm.

3.4 Remote access and other external connections

Any access to systems via computers not directly connected to the organisation's network will be considered remote access or an 'external' connection. The security features for this will be in line with Connecting for Health requirements.

Whilst technical detail is not included here, the core principles will be that any access method will follow industry standard security controls and include 'strong authentication' on the principle of 'two factors'. This may be via a token authentication method or a onetime pin number transmitted via SMS to a mobile telephone registered in the Trusts Active Directory database, in addition to a username and password. The principle is the control is based on something you know (password) and something you have (token).

Users who wish to access the Trust remotely are required to be authorised by their line manager, who will complete an on-line form authorising the request.

Any remote access solution implemented will not allow the transfer of data from the server to the local PC, nor will they allow printing unless via a secure link that ensures data is not left on the local machine.

3.5 Application access control principles

Multi-user information systems within the Trust will have an inactivity time-out. The time-out period will vary to take into account dependent operational and clinical requirements following authorisation of the system owners, Caldicott Guardian and Information Governance lead.

The system element of the access control policy requires that the following controls should be considered for all information systems within the Trust, and applied via system specific security policy:

- Security groups based on user role and team/department will be set up that have access to data via a matrix of access rules developed by the system owners.
- Access to system functions will be restricted for each user role.
- Add, Amend, Create, Delete and view access permissions will also be a facet of user role tables.

3.6 Monitoring system access & use

Systems will be capable of logging events that have a relevance to potential breaches of security. These logs will be kept for a minimum period as defined by the Trusts Information Governance lead. The logs will cover the following events as a minimum standard:

- Log on attempts – recording User Ids, dates and times of failure of attempt.

- Creation, amendment and deletion of data – recording User Ids, dates and times.
- Where possible views of data.

Each system management role will develop procedures for monitoring the use of each system. Regular standard processes to examine failed access attempts, data manipulation spot-checks and any other logged system event will be a part of management of each system.

Users will be informed of monitoring activity and their responsibilities to ensure appropriate access and use of data. The organisation reserves the right to suspend, limit or remove access from any user suspected or convicted of misuse.

All monitoring of systems will be within Lawful Business Practice Regulations (2000) and the Regulation of Investigatory Powers Act (2000). The above monitoring only relates to systems where no personal use is permitted. Limited personal use is only permitted for email and internet usage with the permission of the users' line manager.

3.7 Third party access requirements & outsourcing

Any requirement to access information by someone who is not a member of staff will be considered 'third party' access. The requirement and associated risks will be documented and assessed for control.

Where risks from third party access have been identified, contractual arrangements will be put in place to manage the risks. The manager of the contract will ensure this is undertaken with advice from the Information Governance lead.

A standard 'Confidentiality/Non-disclosure' agreement is available for use or adoption into contracts.

Off-site access to systems – 'Network' access for suppliers or partner organisations will be via an approved NHSnet connection (adhering to NHSnet connection codes/policy) or secure internet gateways.

In addition to the above, the elements that will be included in any support arrangement are:

- Identification, awareness and understanding of responsibilities (inc. legal compliance requirements).
- Service level agreements on availability of service (accessibility of information), integrity (quality checks) and confidentiality.
- The right of audit.

4. Systems Development and Data Collection

A process for assessing new information processing functions will be used.

New information collection – Where personal information is to be collected via an existing tool, that is not a new bespoke system, or new functionality for an existing system, then an assessment must be made that the collection and methods meet with legal requirements. For example, the use of Excel or Access to record personal information. The Information Governance Manager will implement an assessment process and periodically audit the use of such tools to ensure all data collections are recorded via revising information flow maps and asset registers.

New systems – Any requirement for a new system, regardless of size & cost will be put through the process for assessment.

Significant new function (of existing system) – It is important to draw distinction between new function and change to existing system function. Both will have impact on information, however changes to existing functions are covered by the policy controls and processes associated with change control.

4.1 Separating Operational and Development Facilities

Development of supplied systems – Where the contracted supplier controls the development environment, overall compliance with ISO27001 will be sought in contractual arrangements. This will include controls over staff access to development and live environments and development tools.

In-house developed systems – In line with supplied systems, the following elements must be considered and applied if possible:

- Development environments should run on different processors, or in different virtual environments.
- Compilers, editors and system utilities should not be accessible from operational systems when not required.
- Rules for transfer of software/code from development to operational status should be defined, including reversal procedures & linkage to change control.
- *On-site 'Test' environments of supplied & in-house developed systems* – Each system will evaluate the feasibility of a 'test' environment. This will be used for training, system update testing and functionality development testing. Access request and control policy/procedures for each system where there is an 'onsite test' environment will incorporate requirements for user access to that as well. On-site test environments will:
    - Contain 'dummy' data. This may be an anonymised copy of 'live' data, but in such a way that individuals cannot be identified.
    - Clearly identify at the 'log-in' and during usage that the user is in the 'test' environment as opposed to the 'live', to prevent data being entered to the wrong system.

4.2 Requirements Analysis and Specification

Information Governance leads will be involved in the development of new information system functionality (including new systems and development to existing systems) and processes to ensure that all governance requirements are included, this will if necessary be to the level of a full 'Privacy Impact Assessment':

Security – Security controls required will reflect the business value of the information assets based on risk assessment of failure of a system or absence of the information to the organisation.

Confidentiality – The Information Governance lead will ensure that compliance with the Data Protection Act (1998) and Common Law duty of confidentiality are paramount concerns during system and process developments.

Integrity/Quality – In line with compliance with the fourth data protection principle, data quality will be a specific element of system/process analysis and specification.

4.3 Capacity Planning

The IM&T department (and any other responsible for system capacity) will monitor system capacity. This will include network bandwidth, storage capacity and system response times.

The system manager will provide details of their requirements of the systems, in terms of total number of users, expected volumes of concurrent usage, peak usage timings, disk space requirements and system development requirements.

The IM&T department will advise and guide on the required resources, lead times and costs of the co-ordinated development plan.

A system for agreeing priorities to capacity developments will be agreed across the Trust and implemented by the IM&T steering group (or equivalent).

4.4 Acceptance of developments

New systems, existing system upgrades/new versions will only be installed following the definition of formal acceptance criteria. System Owners are responsible for co-ordinating the acceptance criteria and involving the required areas of the organisation. The following are controls that should be considered:

- Performance and capacity requirements (in terms of response times & other capacity elements.
- Preparation and testing of routine operating procedures (such as standard reports etc.).
- Testing of security controls (passwords, usernames, information access controls).
- Business continuity arrangements & tests.
- Backup of system and application data schedules.

- Disaster Recovery arrangements and tests that take into account the services requirement for Recovery Point Objectives and Recovery Time Objectives.
- Training provision to all appropriate staff, including education/communication of upgrades.

System owners should document the acceptance criteria, both prior to and post installation.

4.5 Change Control and Outsourced Development

All changes to existing systems will be subject to change control procedures that will evaluate the potential impact of change on system security, data quality and availability elements. Two forms of changes are covered:

- In built system functions, such as switches for mandatory fields or user definable code lists.
- Vendor controlled changes, where alteration to software code is required, for the addition of new data collection, processing or functionality.

Change requests will be made via an authorisation process controlled by system management and system owners. Following receipt of request, system management will undertake analysis of the impact of changes. Significant change proposals that have not originated from the user base will be tested with users prior to commitment to change. System management and the user base will create a set of formal acceptance criteria for each change.

Where a system has a test environment all changes will be carried out their first and evaluated against the acceptance criteria prior to being installed in live systems.

Changes will be scheduled with the user base to ensure minimum disruption to operational business.

System management will ensure any changes to system documentation resulting from change will be put in place.

4.6 Operating System Changes

When it is necessary to change or update an underlying operating system, applications will be reviewed and tested to ensure that integrity has not been compromised. The IM&T department (and suppliers) will lead changes to operating systems ensuring that sufficient time is allowed for testing.

4.7 Restrictions to Changing Software

Both in-house and vendor supplied software will be controlled by restricting responsibility to authorise changes to system management and system owners. Changes to vendor-supplied software will be governed by contractual agreement with the supplier.

4.8 Covert Channels and Trojan Code

The organisation will protect itself from covert channels and Trojan code that allow unauthorised access to information by applying the following controls:

In-house developed software – Application developers will be bound by contract terms of employment and job description responsibilities from inserting covert channels and Trojan code.

Vendor supplied software – Contractual arrangements will ensure that the vendor does not insert covert access channels or Trojan code. Should these be found to be present in any vendor supplied software, contracts will contain appropriate penalty or termination clauses agreed by legal departments.

5. Maintenance and Operations

5.1 Operational Change Control

Poor change control is one of the major factors relating to system failure. By default the system management for each system is responsible for the application of change control procedures for their system.

The following elements must be considered when developing change control procedures:

- Identification and recording of significant changes.
- Assessment of the potential impact of such changes.
- Formal approval procedure for proposed changes.
- Communication of changes to all relevant personnel.
- Formal acceptance or revocation procedures for changes.

Change control procedures must be applied in the following circumstances:

- Changes to datasets collected.
- Changes to standard report provision.
- Changes to user procedure (& documentation).
- Changes to operational system provision procedures (backups etc.).

5.2 Housekeeping, Backup & Logs

All systems will have a solution that protects the data. This will typically be a configuration that utilises technologies such as a pair of Storage Area Network (SAN), that will be configured for data redundancy and performance benefitting from the use of a Redundant Array of Independent Disks (RAID) that are mirrored to a backup datacentre. The data will then be backed up to an appropriate backup device or archive.

Each system manager will determine the appropriate backup procedure using the following guides, with advice from the IM&T and Information Governance lead:

- Regularity of backup – typically once every twenty-four hours, seven days a week. The frequency of backups can be changed depending upon user requirements.
- Storage and protection of backup media – Storage of removable backup media will be in a location remote from the main system, but subject to at least the same environmental and physical protection as the main system.
- As part of backup procedures regular testing and full restoration of backups to a separate system should be implemented.
- The retention period for backup information is typically twenty days before tapes are recycled, whilst every month the monthly backups are kept for a year before being recycled.
- Backup media will be degaussed, wiped and appropriately disposed of following decommissioning.
- Backup media will be regularly replaced to avoid wear and tear.
- IM&T operational staff will maintain a backup activity log for each system being managed.

Security of System Files & Documentation

Operating documentation for systems, both paper and electronic will, as a default, be considered 'organisational sensitive' information, as they contain information that could be used to cause damage to systems. It will therefore be stored securely and only available to those with a justified need to access it. System documentation includes data structures, network structures, authorisation processes.

5.3 Technical System Audit

Any required/planned audit will take account of risk to business operations and be planned around required timing. Factors to be included are: the removal of key staff to meet with auditors, the scope of checks and the requirement for production of audit reports from the system. Access to any software tools or reports that form part of audit of a system will be restricted to specific individuals.

Audit of key technical controls will be scheduled based on risk priorities and the overall development programme for IM&T systems.

6. Potential Information Security Breaches

6.1 Forensic readiness

Forensic readiness is defined as 'the capability of an organisation to use digital evidence in a forensic investigation'. For digital evidence to be used in an

investigation it must be recovered and analysed in a systematic, standardised and legal manner in order to ensure its admissibility in legal or disciplinary terms.

The scenarios that may require digital evidence include:

- Alleged illegal activity such as storage of illegal images.
- Alleged breaches of the use of personal data and confidentiality.
- Unauthorised access to, or use of IT systems.
- Fraud, deception.
- Disciplinary issues such as accidents, negligence, malpractice, abuse of privileges.

The sources of evidence include:

- Electronic patient & staff records (featuring strong audit trails)
- Smartcard access control (featuring strong audit controls)
- Email archive
- Internet monitoring tools.
- Firewall logs.

6.2 *Identification of need for investigation:*

Potential incidents will be reported either to the IM&T helpdesk, the Risk Management function or the Information Governance team.

Regardless of initial reporting these areas will consider and engage others as required. This is most likely in the case of information governance and risk management.

Initial investigation will include consideration as to whether digital evidence is required and if so how quickly and securely it needs to be gathered. This decision will be based on the likelihood of degradation of the evidence or potential tampering.

6.3 *Responsibility for investigation:*

The Information Governance team will lead any investigation under the authority of and reporting to the SIRO of the Organisation.

6.4 *Preservation of evidence:*

It is possible that evidence will need to be gathered swiftly to ensure its robustness and at the time of investigation specific expert advice will be taken. It may be advisable to temporarily remove the use of the system that is the source of evidence from users in order to preserve the evidence until it is extracted. However it is

noted that this in some cases may have impact on operational business. The SIRO will determine if access to a system should be withdrawn temporarily to allow evidence to be extracted, basing the decision on the business impact of removing all access against the seriousness of the matter under investigation.

6.5 Allegations of illegal activity:

Where an allegation of illegal activity that potentially includes use of the organisation's computer systems is made then it is vital that response to such an incident is swift. The following must be considered:

- Protection of staff investigating the incident from associated allegation. For example if illegal images are alleged to be kept, then staff investigating must not access these images as that act is also illegal.
- Removal of equipment in a safe manner to preserve evidence. If a PC is suspected of having illegal material and is powered off, then it must not be powered on. If it is on, power must be removed, the PC must not be shut down normally. For a laptop the battery must be removed.

University Hospitals Bristol NHS
NHS Foundation Trust

Appendix A:

Generic Accounts:

It is Trust policy that all users have individual usernames and passwords if they are required to access information systems as part of their job role.
The Trust recognises that in some circumstances a generic user account may be required for access to legacy systems that may not support individual accounts, or to provide access to shared folders and some email groups.
A generic account will be subject to the following constraints;

- A generic account should have a contact person (with telephone details) within the department using the account so permissions, denials and issues can be verified. They would NOT be an IT manager of this account.

- The account will be used to access clinical and non-clinical information in such a way as to facilitate working with that information. The account could have access to specified shares and clinical systems, in which case a user would use their own individual username and password e.g. a ward account would be for access to Clinical Systems and Intranet only and would have no access to the Internet or Trust Email.

- Any subsidiary application will request an individual username and password i.e. logging into Medway from a generic account would require the correct user credentials to successfully login. Single Sign On (SSO) will be disabled to prevent accidental sharing of usernames and passwords.

- Generic email accounts cannot be used to logon to a PC.

- Generic email access is controlled by permissions within Outlook.

- Access to a generic email account is gained by adding the generic account to an individual's existing email profile within Outlook.

- A generic email user can only "Send on Behalf of" from the account.

- An "Out of Office" message has to be created /edited/deleted by the IM&T helpdesk.