BrisDoc Patient care by people who care

NHS

Information Security Policy

Version:	Owner:	Created:
2.0	Deb Lowndes (Head of Business Information and Projects)	5th January 2011
Published:	**Approving Director:**	**Next Review**
20th February 2023	Nigel Gazzard (Managing Director)	5th January 2025

Contents

Introduction

Information is a vital asset and resource within BrisDoc. It plays a key part in the management of the organisation, service planning and performance management as well as supporting all of its business activities and is a vital element in the delivery of patient care.

BrisDoc acquires, maintains, shares and uses information of a personal and/or confidential or otherwise sensitive nature to support the above, including patient information, information about employees and corporate “business” information. With this comes a requirement to provide suitably robust security arrangements to maintain the confidentiality, integrity and availability of information in accordance with legislation, guidance.

This Information Security Policy is an integral part of BrisDoc’s Information Governance Management System and is derived from the Information Governance Policy and supports BrisDoc’s mission to deliver excellent patient care.

Document Purpose

The purpose of this policy is to provide clear direction, support and commitment to maintaining the confidentiality, integrity and availability of information obtained, held, used and shared by BrisDoc.

All information would be classified as 'Confidential' and should be treated as such as defined in DoH Confidentially (NHS Code of Practice Nov 2003), BrisDocs Data Protection, Confidentially and Disclosure Policy and Information Governance Policy.

Information should be handled in a way which is compliant with General Data Protection Regulations (GDPR) as implemented in the Data Protection Act 2018.

The purpose of this Information Security Policy is to ensure that information and records are identified and managed in such a way as to ensure that:-

- The confidentiality of information is preserved, ensuring that only those with the “right to access” can do so;
- The integrity of information is maintained, ensuring that it can be relied upon for decision making;
- The availability of information is maintained, ensuring that it is available when and where it is required,
- Accountability is maintained through the definition of roles and responsibilities and the maintenance of logs etc to provide an audit trail of actions impacting on records and information;

The above will all be achieved within the context of a robust risk management system which will ensure that BrisDoc’s approach to security is based on balancing operational requirements for the sharing and use of information with effective controls to protect these.

Related Documents

1) Information Governance Policy
2) Code of Expectations and Standards of Behaviour
3) Network Security Policy
4) Incident Reporting Policy
5) Business Continuity-Disaster Recovery
6) DoH Confidentially (NHS Code of Practice Nov 2003),
7) Data Protection, Confidentially and Disclosure Policy

Scope of This Policy

This policy applies to information in all its aspects, whatever form the information takes (words and numbers, sound recordings and medical images), whatever means are used to store it (printing or writing on paper or electronic storage) and whatever means are used to transmit it (by hand, via fax, over computer networks or by post), as the information must always be appropriately protected.

It applies to all information whether personally identifiable or not.

All persons employed by or contracted by BrisDoc are subject to this policy. Where individuals are employed by a third party the principles and requirements of this policy will be set out and agreed within the service contract.

Asset Management

Inventory of Assets

BrisDoc will maintain an inventory of all of its information related assets covering;

- information: databases and data files, contracts and agreements, system documentation, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information. The inventory will be maintained by the Service/Functional Manager supported by Head of Business Information and Projects as required;

- software assets: application software, system software, development tools, and utilities. The inventory will be maintained by the Head of Business Information and Projects;

- physical assets: computer equipment, communications equipment, removable media, and other equipment. The inventory will be maintained by the Head of Business Information and Projects;

- services: computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning. The inventory will be maintained by the Service Manager;

- people, and their qualifications, skills, and experience. The inventory will be maintained by the HR Manager;

The inventory will also record the ownership of each asset which maybe spread across the operational management team as appropriate. Appendix A – Asset Template.

Physical and Environmental Security

Secure Buildings

All BrisDoc sites have physical access to the buildings controlled by either a staffed reception desk and/or physical access controls.

All visitors to BrisDoc's premises are required to sign in and out and wear a visitors badge at all times. It is the responsibility of the service manager to ensure this is adhered to.

All buildings will either have intruder alarms which are set when the buildings are unoccupied or 24-hour security staffing. It is the responsibility of the Service/Base Manager to complete the Buildings Security Assessment and Action Plan as in Appendix B, this should be reviewed annually and actions arising should be dealt with in a timely manner.

Secure offices and storage

All offices containing Personnel or Patient information will be fitted with secure cupboards and/or cabinets which are sufficient to store the information held. Keys to such cupboards and cabinets are managed locally, thought should be given to holding copies of keys in an alternative location for backup, each site may vary in its approach dependent of the service opening times.

No confidential or restricted information is to be left unattended either during, or outside of, work hours. Such information must be secured in the storage provided. There is a strict "clear desk" policy in respect of such information when unattended at all locations where appropriate.

It is the responsibility of each Service/Base Manager to monitor and manage as appropriate.

PC Locations and Shoulder Surfing

Where possible PCs & Monitors should be located facing away from patients and staff so as to restrict the view of on-screen data, to restrict shoulder surfing. The term shoulder surfing refers to any act of observation, usually by looking over the shoulder, to gain private information. The classic example of shoulder surfing is someone looking over your shoulder while you type in your code at an ATM or cash register. It is really any situation where private and sensitive information can be observed by untrusted third parties.

To prevent shoulder surfing there are some easy ways to protect yourself. Situational awareness is always the best defence. Knowing who is around you and what they are doing will usually trigger the right response to help you protect yourself.

Security of IT Equipment

All BrisDoc IT equipment must be sited in such areas that do not present an immediate risk of theft or unauthorized access. In particular: -

Servers, routers, switches etc must be secured in dedicated server rooms requiring dual factor authentication or comms cabinets which are kept locked.

Where possible PCs should be sited away from windows and doors but where this is not possible the use of locking cables should be considered.

All network cabling should be protected in trunking as far as the desktop i.e., it should, as far as possible be channelled through the fabric of the building or in trunking as far as the floor/wall port, cables from server to floor box are run below floors, from floor box, cabling will be routed via an umbilical which is simply a method of containing and managing the cables.

All electronic equipment which stores, or is capable of storing, sensitive information which is to be removed from BrisDoc premises must be signed for by the recipient. For example, removing backup devices should be recorded in the backup log for the site.

This should be monitored and managed by the Head of Business Information and Projects and issues reported to the Service/Base Manager.

Back-up and restore

BrisDoc ensures that all servers are backed up on a nightly, weekly and monthly basis.

Back up tapes are to be stored in a fire-proof safe. Consideration should be given to the possibility of storing these of site if practical.

Back-ups will be subject to a programme of test restoration in order to confirm that they have been successful and can be recovered, this is the responsibility of the Head of Business Information and Projects and appropriate 3rd Party supplier. Reliance cannot be placed on occasional file recovery for assurance of this process.

Users should not store important information on the hard drives of their PC/laptop or on removable media as this will not be backed up and thus its restoration cannot be guaranteed. Data should be stored on either the users local drive or the shared drive for the site.

Disposal

All media, whether electronic, including hard drives, mobiles drive, fax machines, photocopiers, USB devices, CDs, DVD's and PC Hard Drives etc must be disposed in the appropriate manner.

The Head of Business Information and Projects in conjunction with the Service/Base Manager (as required) is responsible for deciding when IT equipment, and any related ancillaries, are obsolete or due for replacement.

The decision is based on a combination of whether the item in question is still functional and fit for purpose, and whether it falls under the planned refresh policy/budget.

When IT equipment is deemed obsolete (i.e., redundant for its original purpose), the following considerations should be taken into account before condemning it:

- Can the item in question be redeployed within the organisation
- Is there an outstanding lease, hire or contract agreement in place

- Can it be used as a source of parts for other equipment
- Can it be sold, part exchanged or donated.

The procedure for the Disposal of IT Equipment and Associated Hardware can be found in Appendix C.

Access Control

User registration, review and deregistration

Access to BrisDoc information systems is only to be granted upon receipt of an authorised request, from a line manager. Regular reviews are undertaken to ensure access rights remain appropriate and processes are in place to immediately remove access rights upon termination of employment.

It is the responsibility of the user to make sure that all user names and passwords are kept safe and secure. All passwords should be remembered and not written down. Under no circumstances should a password be given to anyone else.

User accounts

All users of BrisDoc's information systems must have individual user accounts. Generic accounts should be avoided, as these invalidate audit trails. This applies equally to administrator accounts.

Administrator accounts, should have a strong password. This should not be shared with staff and should only be used by appropriate personnel or 3rd parties as appropriate. Under no circumstances should the administrator account be used for administrative activities; this should always be done using the user account of an individual with administrative privileges.

BrisDoc's Network Policy details this process further.

IT Service Continuity and Recovery

Business Continuity Arrangements

Given the nature of BrisDoc's business activities there is a large dependency on information and information systems to support day to day operations and these dependencies must be acknowledged as part of the Business Continuity planning systems.

All functions, departments and users who have a dependency on information and information systems must map these, identifying the potential impacts of loss of service, and must define the maximum tolerable loss of service that can be sustained. This data is used to develop an appropriate resilient infrastructure and to ensure systems and services can be recovered within the required timeframes. Appendix D – IT System Business Impact Analysis Template.

Building Resilience

BrisDoc must ensure that its information and IT infrastructure is sufficiently resilient to meet the business needs of the organisation, whether these are provided by in-house or contracted out

services. Out-sourced contractors will, as part of their contracts and service level agreements, be required to provide assurance that the resilience requirements set out by BrisDoc have been, and are continuing to be, met.

Business continuity

It is the responsibility of information and system users to ensure that they and their departments have adequate arrangements in place to maintain services, to an agreed level, during the recovery of systems i.e. where necessary alternative "manual" processes must be developed which can be operated during system down time. Staff must be made aware and/or trained, so that they are able to cope with a business continuity situation and should have access to contacts etc. Ideally where possible business continuity scenarios should be tested, this is the responsibility of each Service/Site Manager in conjunction with the Head of Business Information and Projects.

Recovery Arrangements

BrisDoc, either internally or in conjunction with out-sourced contractors, will clearly define the recovery time requirements for all critical information systems. These recovery times, and the methods of recovery, will be built into service level agreements and contracts. Service providers will, as part of their contracts, be expected to undertake appropriate recovery testing, the results of which should be reported to the BrisDoc along with details of any remedial actions required. This is the responsibility of each Service/Site Manager, the Head of Business Information and Projects and the 3rd Party Supplier to define and manage.

Information Security Incident Management

The purpose of this section is to detail the Incident Management approach and process for reporting, investigating and managing information security Incidents / events.
An incident can generally be described as an event which has or could lead to a breach of policy, security, confidentiality or legislation or regulation. It also embraces the day-to-day problems encountered by users such as faults etc. In summary these can be defined as:

- Operational - Day to day operational issues.
- Policy - Represents any failure to comply with BrisDoc's Governance Policy and its supporting standards
- Security: these fall into one of three areas
    - **Confidentiality** – that is, incidents related to accidental or intentional leakage of confidential data, passwords and the like to unauthorized persons and organizations.
    - **Integrity** – that is, accidental or intentional damage to or inaccuracies in data.
    - **Availability** – that is, accidental or deliberate, disruption or absence of information and information services i.e. systems being "down", pc's not functioning correctly etc

Incident Reporting

Individuals may become aware of actual or potential “incidents” through a variety of means, e.g. a system malfunction, a system being down or general observations regarding working practices. In all instances, it is the individual’s responsibility to ensure such incidents are reported through the appropriate channels and that such reports are directed to the most appropriate managers for investigation and resolution.

In order that the incident may be properly recorded and responded to it is essential that they are, in the first instance reported to their line manager and/or IT lead. In the event of a “breach” the SIRO MUST be alerted immediately.

When raising an incident it is useful to provide the following information.

- End User
- Asset No
- Asset location
- Site
- Problem Summary
- Problem Description
- Priority

Where incidents are classified as being of an operational nature, i.e. user queries and minor faults, these will be dealt with by line managers and/or IT staff.

If the “incident” is deemed to be a breach of policy, security or legislation this will be reported immediately to the Head of Business Information and Projects and will be dealt with in accordance with the following procedure.

When an information security incident occurs there are a number of things that need to be done in a formal manner so that the incident is properly documented and channelled into the process of incident management. This process should be undertaken using the BrisDoc’s Standard Incident Reporting process.

Verify the incident

When an incident occurs there are a number of things that need to be done to put the initial investigation on a good footing.

Formally record that an incident has happened within the Audit South West DAC Tool in the category Information Security Incident.

- Record what the incident is believed to be
- Record the potential impact from the incident
- Make a case for an initial investigation
- Report to senior management
- Allocate or apply for resources/funds to complete the initial investigation
- Raise the requirement for further resources/funding if the initial investigation is positive.

Involve all interested parties

It is essential to ensure that all parties that will be required to take action are involved as early as possible. Discussion of the event or knowledge of the occurrence of the incident should be kept strictly to only those that have a clear need to know. The more people who are aware of the incident, the more opportunity there is for people to interfere, hamper or compromise the investigation. This helps to ensure the suspect (if there is one) does not become aware of the investigation and does not get any access through which they might be able to delete evidence or cover tracks.

Identify an incident manager

An incident manager should be identified, to manage the investigation. This may be either a manager from a non-related service or area. If required expert resources maybe sought to manage the incident.

The incident manager should be aware of, or have direct access to other who are aware of; the prevailing laws such as the Data Protection Act, Regulation Investigation Powers (RIP) Act and the Human Rights Act so that he is able to ensure that an individual's privacy and human rights are maintained. This is especially important because the investigation may prove the suspect's innocence.

Prepare investigation documentation

An incident management log should be established to record all actions taken in the investigation, the results and the evidence secured as a result.

It is critically important that all actions taken within an investigation can be accounted for within a chronological sequence in case the incident results in legal action. This is especially important in relation to the access and recovery of IT based evidence. The Incident Manager is responsible for ensuring that the incident log is current and accurate.

Decide on the course of the initial investigation

The first task of the investigation team is to consider what could be done to investigate the incident in a passive manner without alerting the instigator(s). The objective should be to collect enough evidence to make a decision about further active investigation. It is important that the team documents what will be undertaken as a part of the initial investigation in as much detail as possible to avoid criticisms of bias or 'fishing'.

Identify specialist skills required

It is important to identify early on whether specialist skills will be required, such as computer imaging, computer forensics or network monitoring, and where those skills will come from.

Additionally, it is essential to provide training, for the people who are likely to be involved in an incident if required.

Estimate & Agree budget requirements

Estimate potential costs and agreement that these can be funded in order that the investigation can be progressed.

Information Risk Assessment and Management

The purpose of this section is to detail BrisDoc's approach to information risk assessment and it's management programme.

Responsibilities

Assessment

- SIRO – Nigel Gazzard
- IAO – Deb Lowndes
- IAA – all relevant managers
- ISM – Deb Lowndes

Management /Reporting

- IG Board and Caldicott Guardian – Dr Kathy Ryan

Process

The purpose of this section is to detail the steps involved in carrying out the assessment within BrisDoc.

The steps involved in carrying out the assessment are

Step 1: Catalogue the system(s).
Step 2: Define the foci of interest.
Step 3: Define the threat sources.
Step 4: Define the threat actors.
Step 5: Identify the risks and estimate Risk Levels.
Step 6: Prioritise and present the risks.

Catalogue the system(s)

Data assets will be identified by staff who can speak authoritatively about the way in which the data is used, considering such incidents as unavailability, destruction, disclosure and modification. The Information Asset Register will be used to document the findings.

Assets are described in terms of

- Information Asset Description,
- Supports the following activity (note types of data):
- Asset Owner,
- Supplier
- Unavailable up to 3 hours, 1, 3 days or one week
- Local preventative measures
- Storage/Backup method/issues
- Risk Assessment

Define the foci of interest

BrisDoc will be particularly careful to protect all data whose release or loss could cause:

- harm or distress to patients or staff;
- restriction on BrisDoc's ability to deliver service;
- damage of BrisDoc's reputation;
- financial loss or exposure to BrisDoc;
- major breakdown in information systems, information security or information integrity;
- significant incidents of regulatory non-compliance.

Define the threat sources

A Threat Source is a person or organisation that desires to breach security and ultimately will benefit from the breach in some way. Threat sources are likely to include, but are not limited to:

• Disaffected employees;
• Investigative Journalists;
• Criminals – organised criminal groups, fraudsters etc.
• Hackers;
• Service competitors.

The threat categories are grouped into the following areas:

- Logical threats;
- Communications threats;
- Failures of equipment;
- Errors;
- Physical threats.

The level of the threat acknowledges not only the actions of BrisDoc staff but also the actions of legitimate third parties and outsiders.

Define the threat actors

A **Threat Actor** is a person who actually performs the attack or, in the case of accidents, will exploit the accident. Examples:

- If a Foreign Intelligence Service (FIS) subverts an employee, then the FIS is the Threat Source and the employee is the Threat Actor;

- If a system develops a fault and sends information to people it should not, the recipients become Threat Actors, the Threat Source is the person to whom they send the information and who benefits from the information.

Identify the risks and estimate Risk Levels

For each source and actor perform a risk assessment based on

Assess the Likelihood

Use the descriptors below to assess the LIKELIHOOD of a risk to the confidentiality and security of personal information during transfer and on receipt				
Probable	Possible	Unlikely	Rare	Negligible

Good chance of occurring	Reasonable chance of occurring	Unlikely to occur	Will only occur in rare circumstances	Will only occur in exceptional circumstances

Assess the Impact

Use the descriptors below to assess the IMPACT of a loss of personal information on the individual and the organisation					
0	**1**	**2**	**3**	**4**	**5**
Minor breach of confidentiality affecting one individual	Potentially serious breach. Less than 5 individuals affected or risk assessed as low, e.g. files were encrypted	Serious potential breach and risk assessed high, e.g. unencrypted records of up to 20 individuals	Serious breach of confidentiality, e.g. up to 100 individuals affected	Serious breach with either particular sensitivity, e.g. sexual health details, or up to 1000 individuals affected	Serious breach with the potential for ID theft or over 1000 individuals affected
Minimal discernible effect on the organisation - media interest unlikely	Damage to staff member's reputation. Possible media interest, e.g. celebrity involved	Damage to the organisation's reputation, some local media interest that may not go public	Damage to the organisation's reputation, low-key local media coverage	Damage to the organisation's reputation, local media coverage	Damage to the NHS' reputation, national media coverage

Calculate Risk Ratings

Use the likelihood and impact assessments to rate the identified risks.

RECORD the likelihood and impact of a loss when transferring personal data as High, Medium or Low					
	LIKELIHOOD OF OCCURRENCE				
IMPACT	Probable	Possible	Unlikely	Rare	Negligible
5	HIGH	HIGH	HIGH	MEDIUM	LOW
4	HIGH	HIGH	HIGH	MEDIUM	LOW
3	HIGH	HIGH	MEDIUM	MEDIUM	LOW
2	HIGH	MEDIUM	MEDIUM	LOW	LOW
1	MEDIUM	MEDIUM	MEDIUM	LOW	LOW
0	LOW	LOW	LOW	LOW	LOW

Risk Treatment

Risk treatment steps include risk reduction, risk retention, risk avoidance and risk transfer.

These steps require consideration of:

- risk assessment results for accuracy and completeness;

- risk treatment options and their implications. Options may include:

reduction;

retention;

avoidance;

transference.

The risk treatment will be recorded in the information asset register, for subsequent presentation and review to the IG Board.

Maintenance of the Risk Assessment

All organisations are subject to change brought about by modifications to the operational and technical environments. These in turn change the risks presented to the organisations, resulting in a requirement to review any previously conducted Risk Assessments. Consequently, this Risk Assessment will be conducted at least annually, and also following major changes to BrisDoc's infrastructure or the purposes for which it is used.

Incident Reporting

Information incident reporting will be in line with BrisDoc's risk management incident reporting processes and will be reported as soon as possible.

- all incidents must be reported immediately by the member of staff involved
- incidents resulting in major or catastrophic must be escalated immediately to the SIRO
- the Managing Director Team will ensure that external bodies are notified as appropriate.
- all incidents will be investigated to an extent commensurate with their potential severity;
- as a minimum, the line manager should consider whether appropriate action has been taken, whether any lessons can be learned from identification of root or contributory causes, and whether any further action is necessary
- for more serious incidents, a formal investigation and Root Cause Analysis must be carried out;
- lessons learned will be shared with stakeholders as appropriate.

Incidents will be categorised into information governance related categories in accordance with Department of Health guidance, namely: -

Category	Examples Include
Loss from or on NHS premises	1. Loss of health record from department 2. Loss of computer from stores

Theft from or on NHS premises	1. Theft of laptop from ward 2. Theft of personnel files from department
Loss from outside NHS premises	1. Loss of memory stick at home 2. Loss of health records by courier
Theft from outside NHS premises	1. Theft of laptop from car 2. Theft of Blackberry from home
Insecure disposal	1. Sale of computer with un-wiped hard drive 2. Disposal of confidential papers in domestic waste bin
Unauthorised disclosure	1. Sharing of login names and passwords 2. Inappropriate access to health record 3. Computer hacking
Other	1. Non-compliance with Subject Access Request 2. Contractual income/financial loss

Appendix A - Asset Template (example)

Asset #	OLD Asset Pre Apr-14	Description	Location	Purchase Date	Windows	Office Gold Disc Checked on 17.12.13
000110		OptiPlex 790	Downstairs Desk - Traci	39814		
		Windows 7 Professional			Windows 7	
		Microsoft Office Single Image 2010				Yes
003123		Dell Professional P2210 56cm(22") monitor VGA,DVI-D,DP (1680x1050) Black UK		O ct-11		
003043		Avaya Telephone				
003124		Lexmark Printer		Unknown		

Appendix B - Buildings Security Assessment Form & Action Plan

(This form is based on the General Practice Risk Assessment provided by Adam Tuckett Avon IM&T Consortium – With thanks to IG toolkit resource pack).

Buildings Security Assessment Form and Action Plan

Building Assessed: _____ Assessed By: _____

Date of risk assessment: _____

Date of previous risk assessment: _____

1. Is access to the outside of the building controlled i.e. covered by CCTV?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
2. Does the outside of the building have security lighting, floodlighting or street lighting?		
Yes / No	Risk Level:	Action Plan:

	High/Low/Medium	
3. Are there warnings on windows, visible alarms etc that warn potential intruders that there are physical security measures in place?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
4. Are accessible windows suitably protected with locks?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
5. Do the downstairs windows have security bars?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
6. Are the windows closed and checked every evening?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
7. Are blinds closed and checked every evening?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
8. Are skylights suitably protected by bars and locks?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
9. Are external doors suitably protected e.g. by 5 lever locks?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
10. Is there a burglar alarm with intruder monitors covering all areas especially those containing IT equipment or records?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
11. Is the alarm system connected to a police station or call response centre?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:

12. Are you able to ensure all keys stored on site are not obvious and any instructions regarding key instructions or keypad codes are stored securely?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
13. Are keypad codes changed regularly?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
14. Are alarm codes changed regularly?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
15. Are staff aware of the procedure for challenging unidentified visitors in controlled areas?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
16. Do staff ensure that the Drug Cupboard or the access to the Drug Cupboard is logged and managed appropriately?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
17. Do staff ensure that paperwork is not left unattended in the Consultation Area or other sensitive areas?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
18. Are screensavers in use on computers that are used to display information about patients?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
19. Are identity passes/cards worn by all staff at all times?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
20. Are identity passes/cards worn by all visitors at all times?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:

21. Are visitors escorted at all times in secure areas?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
22. Is a log of visitors maintained?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
23. Is IT equipment situated where it cannot be viewed by visitors or the public from outside the premises?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
24. Are deliveries to and collections from the site, supervised?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
25. If a back door or loading bay is used to receive deliveries – is this secured when not in use?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
26. Is new equipment stored securely prior to installation?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
27. Is the movement of IT equipment out of the site subject to authorisation and control? i.e. use of laptops and portable equipment off site.		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
28. Are lock down devices used to secure IT equipment?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
29. Are laptops and other portable equipment stored securely overnight?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
30. Are back-up Tapes stored securely, for example in the site safe?		
Yes / No	Risk Level:	Action Plan:

	High/Low/Medium	
31. Is IT equipment asset marked?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
32. Do assets have visible ID markings?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
33. Is electronic equipment stored away from the risk of burst water pipes?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:
34. Is electronic equipment stored away from the risk of splashing from taps or sinks and the risk of water running from windows or condensation?		
Yes / No	Risk Level: High/Low/Medium	Action Plan:

Any there any other observations from the review?

Date of Next Review: _____

Review Carried Out By: _____

Action Plan Follow-up Date _____

Appendix C- Disposal of IT Equipment and Associated Hardware Procedure

Responsibility

Clearance, for the disposal of obsolete and/or redundant IT equipment, is agreed by the Head of Business Information and Projects and the Service/Base Manger This dual sign-off endorses the initial decision, whilst referring to the refresh policy/budget and the asset register for confirmation that specific items are due for disposal.

Disposal Procedure

The following steps form part of the physical disposal process:

- Removal of data from equipment. Initially it is the users and or Service/Base Manager to responsibility to remove the data. The following items should be checked/removed, all personal/desktop data, recycle bin, bookmarks and favourites.
- The equipment should then be moved to Osprey Court for checking and disposal.

- This will be checked by the Head of Business Information and Projects to ensure data has been removed, the installed software will also be reviewed, the Head of Business Information and Projects will manage any related software asset or licence issues.
- Collection by third party for secure, and environmentally friendly, destruction and disposal. Where the computer is to be scrapped, the hard disk will be sent to a secure 3rd party for disposal.
- Completion of relevant paperwork, e.g., asset register(s) to be updated, filing of paperwork from the disposal company.

Appendix D – IT Systems Business Impact Analysis Template

Information Asset Register (Major/Key Assets only)									
Site Name									
Date of assessment:				Unavailability impact & continuity actions					
				Highlight when impact is reported as incident and further when disruption is unacceptable					
Information Asset Description - (note format and system name where appropriate)	Supports the following activity (note types of data):	Asset Owner / Manager	Supplier (if appropriate - list all relevant)	Unavailable up to 3 hours	Unavailable 1 day	Unavailable 3 days	Unavailable 1 week	Local preventative measures	Action plan
EMIS PCS (clinical system)(Hosted by EMIS in Leeds.)	Patient care and operational practice business	Practice manager / IT Manager	EMIS	Report to EMIS support. Revert to paper base system.	Escalate to practice IT Manager and EMIS account Manager. Continue on paper.	Report to Avon IM&T lead for practice. Continue to manage and chase EMIS.	Practice at risk	Appointment book backed up daily. Llyod George notes on premises.	
Docman	Supporting system for patient care.	Practice manager / IT Manager	PCTi	Report problem to PCTi	Escalate and chase. Inform IT Manager	Continue to Manage situation.	Report to Avon IM&T lead for practice	Original paperwork stored for 3 months.	

1. Change Register

Date	Reviewed and amended by	Revision details	Issue number
JAN 2011	DL	DRAFT	DRAFT
MAY 2011	DL	Initial review by DD	1.1
MAY 2011	DL	Add appendices	1.2
SEPT 2011	DL	Clarified responsibilities, completed disposal policy , add ref to code of expectations and relation of policy to patient care	1.3
Oct 2011	DL	Typos and addition of implementation check list	1.4
Oct-2012	DL	Addition of sections Information Security Incident Management and Information Risk Assessment and Management	Vn 1.5
June-2014	DL	Amendments to reflect correct job titles	Vn 1.6
June-2016	DL	Annual review	Vn 1.7
Oct-2018	SP	Review in line with GDPR with review of changes by DL	Vn 1.8
Oct-2020	DL	Version reviewed – No amendments	Vn 1.9