Information Security Guidance
Physical and Environmental Security

Authors:	**Information Security Manager** **Head of Digital Operations** **Head of Technical Services, Property and Support Services Division**
Responsible Lead Executive Director:	**Director of Information and Digital Technology**
Endorsing Body:	**Healthcare Governance Committee**
Governance or Assurance Committee	**Information Governance and Cyber Assurance Committee**
Implementation Date:	**January 2025**
Version Number:	**2.6.7**
Review Date:	**Dec 2026**

CONTENTS

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• Information Security Manager • Head of Digital Operations • Head of Technical Services, Property and Support Services Division
Consultation Process / Stakeholders:	• Director of Information and Digital Technology & Senior Information Risk Owner (SIRO) • Information Governance and Cyber Assurance Committee
Distribution:	• All staff

CHANGE RECORD			
Date	**Author**	**Change**	**Version No.**
March 2017	A Ashforth S Graham J Paterson	First Draft : New guidance identified as a gap after review using SG DL (2015) 17 Information Governance and Security Improvement Measures 2015-2017 (NHSS Information Security Guidance Framework)	2.5
April 2017	A Ashforth	Draft - Minor change – Aim, Purpose and Outcomes regarding eHealth Information Security Management System (ISMS), information security standards and legislation.	2.5.1
May 2017	A Ashforth	Minor change - Aim, Purpose and Outcomes	2.5.2
April 2018	A Ashforth	Reviewed in line with General Data Protection Regulation (GDPR)	2.6
June 2018	A Ashforth	Updated to show new director of Information and digital technology	2.6.1
Aug 2018	A Ashforth	Updated reference to Data Protection Act 2018	2.6.2
Sept 2018	A Ashforth	Data protection statement added into Section 3 - Stakeholders	2.6.3
Oct 2018	A Ashforth	Adapt IS policy for use in General Practice	2.6.4
June 2021	A Ashforth	Scheduled review including updated UK GDPR legislation and Scottish Government CAF,ISPF, CRF guidance to support NIS & the PSAP in References section	2.6.5

Dec 2023	A Ashforth	Scheduled review and rebranding from 'eHealth' to 'Digital' throughout. References Appendix 1 – updated.	2.6.6
Jan 2025	A Ashforth	Updated references appendix for broken link (from 'NHSL Risk Management Framework' with 'NHSL Risk Management Policy') and provided the updated link for the Scottish Government's Records Management Code of Practice. Change all references of 'IG Committee' to 'Information Governance & Cyber Assurance Committee (IG & CAC)' Change all references of 'Healthcare Quality Assurance and Improvement Committee' with 'Healthcare Governance Committee'	2.6.7

1. Introduction

This guidance relates to physical and environmental security and forms part of the overall Information Security guidance for NHS Lanarkshire.

2. Aim, Purpose and Outcomes

The aim of this guidance is to provide a consistent and robust physical and environmental security to ensure the availability of information and telecommunication services within NHS Lanarkshire.

To ensure that INFORMATION SECURITY is maintained

- Ensure that confidentiality and integrity of personal and sensitive information is maintained
- Ensure that information is available to ***authorised*** users
- Ensure that information is not disclosed to ***unauthorised*** people
- To prevent ***destruction*** of information

The purpose of this guidance is to define the standards, and procedures to ensure the legal use of software and information products.

This guidance forms part of the Information Security Management System (ISMS) and should be read in conjunction with all the IS policies.

This guidance has been written in line with the best practice for information security standards ISO 27001 and ISO 27002 and the guidance will be reviewed to meet future changes to this standard.

This guidance has been written to comply with current legislation and the guidance will be updated appropriately to suit new and/or modified legislation. The references appendix will be updated to reflect this legislation.

Staff should consider all physical safeguards where reasonably practicable and without excessive cost.

3. Scope

3.1 Who is the Guidance intended to Affect?

This guidance is for site managers who are responsible for NHSL premises and for Digital staff managing computer facilities such as computer rooms, and communications rooms.
In the interests of clarity all references to ‘site managers’ includes site managers within NHS Lanarkshire and individuals within a GP practice (contracted to NHS Lanarkshire) who have responsibility for site management for their practice.

3.2 Who are the Stakeholders

All staff.

NHS Lanarkshire take care to ensure your personal information is only accessible to authorised people. Our staff have a legal and contractual duty to keep personal health information secure, and confidential. In order to find out more about current data protection legislation and how we process your information, please visit the Data Protection Notice on our website at www.nhslanarkshire.scot.nhs.uk or ask a member of staff for a copy of our Data Protection Notice.

4. Principal Content

Physical and environmental security

4.1 Secure areas
Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

4.1.1 Physical security perimeter

Control
Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

Implementation guidance
The following guidelines should be considered and implemented where appropriate for physical security perimeters:

a) security perimeters should be defined, and the siting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment;
b) perimeters of a building or site containing information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur); the exterior roof, walls and flooring of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms, (e.g. bars, alarms, locks); doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level;
c) a manned reception area or other means to control physical access to the site or building should be in place; access to sites and buildings should be restricted to authorized personnel only;
d) physical barriers should, where applicable, be built to prevent unauthorized physical access and environmental contamination;
e) all fire doors on a security perimeter should be alarmed, monitored and tested in conjunction with the walls to establish the required level of resistance in accordance with suitable regional, national and international standards; they should operate in accordance with the local fire code in a failsafe manner;
f) suitable intruder detection systems should be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times; cover should also be provided for other areas, e.g. computer room or communications rooms;

g) information processing facilities managed by the organization should be physically separated from those managed by external parties.

Other information

Physical protection can be achieved by creating one or more physical barriers around the organization's premises and information processing facilities. The use of multiple barriers gives additional protection, where the failure of a single barrier does not mean that security is immediately compromised.

A secure area may be a lockable office or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical access may be needed between areas with different security requirements inside the security perimeter. Special attention to physical access security should be given in the case of buildings holding assets for multiple organizations.

The application of physical controls, especially for the secure areas, should be adapted to the technical and economic circumstances of the organization, as set forth in the risk assessment.

4.1.2 Physical entry controls

Control

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

Implementation guidance

The following guidelines should be considered:

a) the date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and on emergency procedures. The identity of visitors should be authenticated by an appropriate means;
b) access to areas where confidential information is processed or stored should be restricted to authorized individuals only by implementing appropriate access controls, e.g. by implementing a two-factor authentication mechanism such as an access card and secret PIN;
c) a physical log book or electronic audit trail of all access should be securely maintained and monitored;
d) all staff, contractors and external parties should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;
e) external party support service personnel should be granted restricted access to secure areas or confidential information processing facilities only when required; this access should be authorized and monitored;
f) access rights to secure areas should be regularly reviewed and updated, and revoked when necessary.

4.1.3 Securing offices, rooms and facilities

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

Implementation guidance
The following guidelines should be considered to secure offices, rooms and facilities:

a) key facilities should be sited to avoid access by the public;
b) where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of information processing activities;
c) facilities should be configured to prevent confidential information or activities from being visible and audible from the outside. Electromagnetic shielding should also be considered as appropriate;
d) directories and internal telephone books identifying locations of confidential information processing facilities should not be readily accessible to anyone unauthorized.

4.1.4 Protecting against external and environmental threats

Control
Physical protection against natural disasters, malicious attack or accidents should be designed and applied.

Implementation guidance
Specialist advice should be obtained on how to avoid damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disaster.

4.1.5 Working in secure areas

Control
Procedures for working in secure areas should be designed and applied.

Implementation guidance
The following guidelines should be considered:

a) personnel should only be aware of the existence of, or activities within, a secure area on a need to-know basis;
b) unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities;
c) vacant secure areas should be physically locked and periodically reviewed;
d) photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized.

The arrangements for working in secure areas include controls for the staff and external parties working in the secure area and they cover all activities taking place in the secure area.

4.1.6 Delivery and loading areas

Control

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

Implementation guidance

The following guidelines should be considered:

a) access to a delivery and loading area from outside of the building should be restricted to identified and authorized personnel;
b) the delivery and loading area should be designed so that supplies can be loaded and unloaded without delivery personnel gaining access to other parts of the building;
c) the external doors of a delivery and loading area should be secured when the internal doors are opened;
d) incoming material should be inspected and examined for explosives, chemicals or other hazardous materials, before it is moved from a delivery and loading area;
e) incoming material should be registered in accordance with asset management procedures on entry to the site;
f) incoming and outgoing shipments should be physically segregated, where possible;
g) incoming material should be inspected for evidence of tampering en route. If such tampering is discovered it should be immediately reported to security personnel.

4.2 Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

4.2.1 Equipment siting and protection

Control

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

Implementation guidance

The following guidelines should be considered to protect equipment:
a) equipment should be sited to minimize unnecessary access into work areas;
b) information processing facilities handling sensitive data should be positioned carefully to reduce the risk of information being viewed by unauthorized persons during their use;
c) storage facilities should be secured to avoid unauthorized access;
d) items requiring special protection should be safeguarded to reduce the general level of protection required;
e) controls should be adopted to minimize the risk of potential physical and environmental threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism;
f) guidelines for eating, drinking and smoking in proximity to information processing facilities should
be established;

g) environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities;
h) lightning protection should be applied to all buildings and lightning protection filters should be fitted to all incoming power and communications lines;
i) the use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments;
j) equipment processing confidential information should be protected to minimize the risk of information leakage due to electromagnetic emanation.

4.2.2 Supporting utilities

Control

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

Implementation guidance

Supporting utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) should:

a) conform to equipment manufacturer's specifications and local legal requirements;
b) be appraised regularly for their capacity to meet business growth and interactions with other supporting utilities;
c) be inspected and tested regularly to ensure their proper functioning;
d) if necessary, be alarmed to detect malfunctions;
e) if necessary, have multiple feeds with diverse physical routing.

Emergency lighting and communications should be provided. Emergency switches and valves to cut off power, water, gas or other utilities should be located near emergency exits or equipment rooms.

Other information

Additional redundancy for network connectivity can be obtained by means of multiple routes from more than one utility provider.

4.2.3 Cabling security

Control

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

Implementation guidance

The following guidelines for cabling security should be considered:

a) power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection;
b) power cables should be segregated from communications cables to prevent interference;
c) for sensitive or critical systems further controls to consider include:

1) installation of armoured conduit and locked rooms or boxes at inspection and termination points;

2) use of electromagnetic shielding to protect the cables;
3) initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables;
4) controlled access to patch panels and cable rooms.

4.2.4 Equipment maintenance

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

Implementation guidance
The following guidelines for equipment maintenance should be considered:

a) equipment should be maintained in accordance with the supplier's recommended service intervals and specifications;
b) only authorized maintenance personnel should carry out repairs and service equipment;
c) records should be kept of all suspected or actual faults, and of all preventive and corrective maintenance;
d) appropriate controls should be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; where necessary, confidential information should be cleared from the equipment or the maintenance personnel should be sufficiently cleared;
e) all maintenance requirements imposed by insurance policies should be complied with;
f) before putting equipment back into operation after its maintenance, it should be inspected to ensure that the equipment has not been tampered with and does not malfunction.

4.2.5 Removal of assets

Control
Equipment, information or software should not be taken off-site without prior authorization.

Implementation guidance
The following guidelines should be considered:

a) staff and external party users who have authority to permit off-site removal of assets should be identified;
b) time limits for asset removal should be set and returns verified for compliance;
c) where necessary and appropriate, assets should be recorded as being removed off-site and recorded when returned;
d) the identity, role and affiliation of anyone who handles or uses assets should be documented and this documentation returned with the equipment, information or software.

Other information
Spot checks, undertaken to detect unauthorized removal of assets, can also be performed to detect unauthorized recording devices, weapons, etc., and to prevent their entry into and exit from, the site. Such spot checks should be carried out in accordance with relevant legislation and regulations.

Individuals should be made aware that spot checks are carried out, and the verifications should only be performed with authorization appropriate for the legal and regulatory requirements.

4.2.6 Security of equipment and assets off-premises

Control
Security should be applied to off-site assets taking into account the different risks of working outside the organization's premises.

Implementation guidance
The use of any information storing and processing equipment outside the organization's premises should be authorized by management. This applies to equipment owned by the organization and that equipment owned privately and used on behalf of the organization.

The following guidelines should be considered for the protection of off-site equipment:

a) equipment and media taken off premises should not be left unattended in public places;
b) manufacturers' instructions for protecting equipment should be observed at all times, e.g. protection against exposure to strong electromagnetic fields;
c) controls for off-premises locations, such as home-working, teleworking and temporary sites should be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office;
d) when off-premises equipment is transferred among different individuals or external parties, a log should be maintained that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment.

Risks, e.g. of damage, theft or eavesdropping, may vary considerably between locations and should be taken into account in determining the most appropriate controls.

Other information
Information storing and processing equipment includes all forms of personal computers, organizers, mobile phones, smart cards, paper or other form, which is held for home working or being transported away from the normal work location.

It may be appropriate to avoid the risk by discouraging certain staff from working off-site or by restricting their use of portable IT equipment;

4.2.7 Secure disposal or re-use of equipment

Control
All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Implementation guidance
Equipment should be verified to ensure whether or not storage media is contained prior to disposal or re-use.

Storage media containing confidential or copyrighted information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

Other information
Damaged equipment containing storage media may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded. Information can be compromised through careless disposal or re-use of equipment.

In addition to secure disk erasure, whole-disk encryption reduces the risk of disclosure of confidential information when equipment is disposed of or redeployed, provided that:

a) the encryption process is sufficiently strong and covers the entire disk (including slack space, swap files, etc.);
b) the encryption keys are long enough to resist brute force attacks;
c) the encryption keys are themselves kept confidential (e.g. never stored on the same disk).

Techniques for securely overwriting storage media differ according to the storage media technology.

Overwriting tools should be reviewed to make sure that they are applicable to the technology of the storage media.

4.2.8 Unattended user equipment

Control
Staff should ensure that unattended equipment has appropriate protection.

Implementation guidance
All staff should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Staff should be advised to:

a) terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;
b) log-off from applications or network services when no longer needed;
c) secure computers or mobile devices from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

5. Roles and Responsibilities

Authors/Contributors:	Information Security Manager Head of Digital Operations Head of Technical Services, Property and Support Services Division
Executive Director:	Director of Information and Digital Technology & Senior Information Risk Owner (SIRO)
Endorsing Body:	Information Governance and Cyber Assurance Committee

It is the responsibility of site managers to review security on their sites at regular intervals in respect of information security, both manual and electronic, to verify that the site adheres, wherever possible to the appropriate controls provided in this guidance that are relevant to their site circumstances.

6. Resource Implications

No resource implications

7. Communication Plan

This guidance will be managed through the Corporate Policies intranet site and will be announced through the staff briefing.

8. Quality Improvement – Monitoring and Review

To be reviewed at regular intervals by Information Security Manager.

9. Equality and Diversity Impact Assessment

This guidance meets NHS Lanarkshire's EDIA [X] (tick box)

10. Summary of Frequently Asked Questions (FAQs)

N/A

11. References Appendix 1

The principal Acts of Parliament, Scottish Government circulars, and internal guidance documents relevant to this guidance are:

- UK General Data Protection Regulation (GDPR)
- Network and Information Systems Regulations 2018 (NIS Regulations)
- National Cyber Security Centre Cyber Assurance Framework
- Scottish Government Public Sector Cyber Resilience Framework
- CEL 25 (2012) NHS Scotland Mobile Data Protection Standard
- Civil Contingencies Act 2004
- Computer Misuse Act 1990

- Copyright, Design and Patents Act 1988
- Data Protection Act 2018
- Freedom of Information (Scotland) Act 2002
- MEL 2000 (17) Data Protection Act 1998
- NHSL Risk Management Policy
- Public Records (Scotland) Act 2011
- Regulation of Investigatory Powers (Scotland) Act 2000
- Scottish Government Records Management Code of Practice for Health and Social Care
- SG DL (2015) 17 Information Governance and Security Improvement Measures 2015-2017 (NHSS Information Security Policy Framework)
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000