Document Security Classification Policy

Author:	**Head of Response, Resilience & Preparedness**
Responsible Lead Executive Director:	**Director of Public Health**
Endorsing Body:	**Corporate Management Team**
Governance or Assurance Committee	**Information Governance**
Implementation Date:	**September 2019**
Version Number:	**1.3**
Review Date:	**September 2025**
Responsible Person	**Head of Response, Resilience & Preparedness**

Table of Contents

CONSULTATION AND DISTRIBUTION RECORD	
Contributing Author / Authors	• Martin Gordon • John Duncan
Consultation Process / Stakeholders:	• Carol McGhee • Gordon Smith • Audrey Bevan • William McCutheon • Lesley Cordiner • Frances Brownlie • Chris Sanderson • Angela McMahon • Ina Tanish • Yvonne Tennant • Joyce Galloway • Paul Cannon • Corporate Management Team • Information Governance Committee
Distribution:	• All staff. • NHS Lanarkshire intranet

CHANGE RECORD			
Date	**Author**	**Change**	**Version No.**
10/05/2023	M. Gordon	review dates and footer details.	1.3

1 Introduction

This policy applies to all employees of NHS Lanarkshire (NHSL) who receive, handle or generate information. This can be in any form including verbal or written. Central to this policy is the recognition that all information generated, received and recorded by NHSL in the course of its business activity has a value and requires an appropriate level of protection and management.

The policy has been developed to reflect good practice as established by the Cabinet Office document; Government Security Classifications May 2018 version 1.1, the Public Records (Scotland) Act 2011 and associated Records Management Standards (ISO 15489). This policy outlines the minimum requirements for NHSL staff however the good practice documents can be referenced for further guidance.

2 Aim, Purpose and Outcomes

This policy outlines how documents may be classified for security, protection and management of information in line with relevant legislation and records management standards.

The purpose of the policy is to ensure adequate security and management is applied to all information generated or received in the course of NHSL activities and that an appropriate approach is taken to the naming of electronic documents. The policy also has the explicit purpose of identifying individual employee's responsibility for the appropriate management of information recognising the need for confidentiality and integrity.

3 Scope

This policy is applicable to all NHSL employees and the responsibilities with regards appropriate management of information and confidentiality is included within the organisations code of conduct.

The policy is applicable to all information received, generated and held by NHSL either in hard or electronic format.

The policy is developed to complement and comply with relevant data protection and freedom of information legislation. Where any doubt exists the classification of the document should be done in consultation with NHSL Board Secretary.

The protection of medical records is not within the scope of this policy.

This policy should be read in conjunction with;

- NHSL Administrative Records Policy.
- The Cabinet Office document; Government Security Classifications May 2018 version 1.1. This is available from www.gov.uk. at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715778/May-2018_Government-Security-Classifications-2.pdf

4 Principal Content

The principles of this NHSL policy follow those outlined in the Cabinet Office document; Government Security Classifications May 2018 version 1.1, the Public Records (Scotland) Act 2011 and associated Records Management Standards. This document describes Her Majesties Government's administrative system for the secure, timely and efficient sharing of information. It is not a statutory scheme but operates within the framework of domestic law, including the requirements of the Official Secrets Acts (1911 and 1989), the Freedom of Information Act 2000 and Data Protection legislation. This policy refers to the Freedom of Information (Scotland) Act 2002 (FOISA) as the applicable legislation in Scotland.

These document sets out six policy principles for document security and management. These are;

1. All information NHSL needs to collect, store, process, generate or share to deliver services and conduct Board business has intrinsic value and requires an appropriate degree of protection and management.

2. All NHSL employees have a duty of confidentiality and a responsibility to safeguard any NHSL information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training.

3. Access to sensitive information must only be granted and shared on the basis of a genuine 'need to know' and an appropriate level of personnel security control.

4. Information received from or exchanged with external partners must be protected in accordance with any security marking, relevant legislative/regulatory requirements, including any international agreements and obligations.

5. All documents created by NHSL or required by NHSL must be stored on the NHSL Corporate File Store (NHSL R:drive).

6. All documents must adopt an appropriate file naming convention.

The security classification applied must be appropriate to the sensitivity of the information. The classification needs to be proportionate and defendable. The management of information must also be in line with the expectations of the originator of any information received including from external agencies and partners.

4.1 NHSL Document Control Hierarchy.

Each classification provides for a baseline set of personnel, physical and information security controls that offer an appropriate level of protection against a typical threat profile. As a minimum, all NHSL information must be handled in compliance with legal and regulatory obligations and reduce the risk of loss or inappropriate access. A framework of controls is provided as an annex to the Government Security Classifications document.

The majority of information and/or documents generated or received by NHSL will most likely be categorised as 'OFFICIAL'. This does not however preclude the possibility of documents of higher categories being received therefore all NHSL employees must have an understanding of the classifications.

Document Security Classification

Documents may need controls above the baseline applied in specific circumstances. These need controlled on a risk managed basis. To achieve this all documents marked above OFFICIAL must be referred to the Corporate Management Team (CMT) for endorsement of the additional controls.

Prior to submission to CMT the advice and guidance of the Board Secretary must be sought. The nature of the enhanced classification, additional controls and the rationale must be recorded on the document control notification (Appendix 1). The complete document and control notification must be submitted together to CMT for endorsement.

Please note that the above control process is applicable to all document types. Notwithstanding this any communications generated, including e-mails, may be classified by the individual in line with this policy as they deem appropriate. However, it must be understood that this classification may be overturned if later challenged.

NHSL shall control information using the following classifications:

1. 'OFFICIAL' – Information is managed by the individual generating or handling the information. This information may be hosted, if deemed necessary, on public and/or internal network and web pages. Information may be shared with partner agencies. Information may be recorded on the Information Asset Register.

2. 'OFFICIAL SENSITIVE' – Information shall be managed in line with the additional controls specified by the originator. This information may be hosted on internal network if deemed appropriate. It may be shared with partners (subject to the same additional controls) if a specific need exists. This information shall not be hosted on public web pages. Information shall be recorded on the Information Asset Register.

3. 'SECRET/TOP SECRET' – NHSL is unlikely to generate or receive information of this nature. This information, if received, shall not be held on internal network or any public web pages. Advice on specific security arrangements should be sought from the originators. As a minimum hard copy must be held in a locked file within a locked room with restricted and controlled access. Electronic copy must be held in a secure and encrypted file. Information shall not be recorded on the Information Asset Register.

Note: Classification markings can assist in assessing whether exemptions to the FOISA may apply. However, each freedom of information request must be considered on its own merits and the classification in itself is not a justifiable reason for exemption. It is therefore important that staff (including contractors) who handle, or are likely to handle sensitive assets, understand fully the impact of such legislation and how it relates to their role.

In addition, NHSL will manage documents by:

1. Storing on NHSL Corporate Server (R: drive).
   The Corporate servers must reflect the function of NHSL and have a folder structure that reflects the sub-functions of every Corporate Department which are controlled by the function's Senior Management Team.

2. Appropriate file naming.
   All files must be named following a file naming convention which clearly identifies the author, document subject, descriptive file name and version control.

3. Security Sharing Classification.
   This describes how the information can be shared using Red Amber Green rating. A red status considerably restricts the method by which information can be shared. The Good Practice Guide and NHS ISMS provides further information.

5 Definitions

The following provides an abridged description of the classifications.

5.1 Official

All routine NHSL business, operations and services should be treated as OFFICIAL - many departments will operate exclusively at this level. This includes a wide range of information, of differing value and sensitivity, which needs to be appropriately protected as per government guidance e.g. against hackers, criminals etc. The management of this information must comply with legal, regulatory and international obligations.
This includes:

- The day to day business of NHSL service delivery and finances.
- Exchange of information with partners.
- Public safety, criminal justice and enforcement activities.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under Data Protection legislation or other legislation (e.g. health records).

➢ **Security Requirements:**

- All NHSL information must be handled with care to prevent loss or inappropriate access, and deter deliberate compromise or opportunist attack.
- Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them in line with local business processes.
- Baseline security controls reflect commercial good practice.

➢ **Marking:**

There is no requirement to explicitly mark routine 'OFFICIAL' information. However, baseline security measures must be enforced through good practice whether the documents are marked or not.

5.2 Official Sensitive

This an extension of the 'Official' classification where information requires greater control. NHSL have, for the purposes of this policy, designated this as a separate classification.

Some 'OFFICIAL' information could have more damaging consequences if it were lost, stolen or publicly available. This information should still be managed within the 'OFFICIAL' classification tier, but may attract additional measures to reinforce the 'need to know'. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', documents should be conspicuously marked: '**OFFICIAL–SENSITIVE'** at the top and bottom of each page of the document.

5.3 Secret

Very sensitive information that requires protection against a higher level of threat than would be typical for the 'OFFICIAL' level. This includes sophisticated, well-resourced and determined threat actors, such as some highly capable serious organised crime groups and some state actors.

Reasonable steps will be taken to protect information and services from compromise by these actors, including from targeted and bespoke attacks. It is highly unlikely that any information either generated or received by NHSL would fall within this category.

The effect of accidental or deliberate compromise would be likely to result in any of the following:

- Directly threaten an individual's life, liberty or safety (from highly capable threat actors).
- Cause serious damage to the operational effectiveness of highly valuable security or intelligence operations.
- Cause serious damage to the security and resilience of Critical National Infrastructure (CNI) assets.
- Cause major impairment to the ability to investigate or prosecute serious organised crime.

➢ **Security Requirements:**

- Make accidental compromise or damage highly unlikely during storage, handling, use, processing, transmission, transport or disposal.
- Offer an appropriate level of resistance to deliberate compromise by forced and surreptitious attack.
- Where possible, detect actual or attempted compromise and help to identify those responsible.

➢ **Marking:**

All information in this category should be clearly and conspicuously marked **'SECRET'**. Information that requires more restrictive handling due to the nature or source of its content may merit a special handling instruction.

5.4 Top Secret

Exceptionally sensitive information that directly support (or threaten) the national security of the UK or allies and requires extremely high assurance of protection from all threats. It is highly unlikely that any information either generated or received by NHSL would fall within this category.

➢ **Security Requirements:**

- Prevent accidental or deliberate compromise or damage during storage, handling, use, processing, transmission, transport or disposal.
- Offer robust resistance against compromise by a sustained and sophisticated or violent attack.
- Detect actual or attempted compromise and make it likely that those responsible will be identified.

➢ **Marking:**

All such information should be clearly and conspicuously marked **'TOP SECRET'.**

6 Special Handling Instructions

Security classifications are the principle means of indicating the sensitivity of information and the requirements for its protection. Special handling instructions are additional markings which can be used in conjunction with a classification marking to indicate the nature or source of its content, limit access to designated groups, and / or to signify the need for enhanced handling measures. Special handling instructions should be used sparingly and only where the sensitivity justifies strict restrictions on information sharing.

Organisations may apply a DESCRIPTOR to identify certain categories of **sensitive** information and indicate the need for common sense precautions to limit access. Where descriptors are permitted they must be supported by local policies and business processes. Descriptors should be used in conjunction with a security classification and applied in the format: '**OFFICIAL-SENSITIVE [DESCRIPTOR]'** for example 'OFFICAL SENSITIVE [FOR YOUR EYES ONLY]'.

7 Legal Framework

The UK classification system operates within the framework of domestic law. This includes:

- Official Secrets Act 1989
- Data Protection Legislation
- Freedom of Information Act 2000 (Policy covers Freedom of Information (Scotland) Act 2002)
- Public Records Act 1967
- Public Records (Scotland) Act 2011

8 Good Practice

Refer to the good practice guide for further information on how to comply with this policy.

9 Quality Improvement – Monitoring and Review

This policy shall be subject to routine review based on a maximum period of three years or where new information and/or lessons are identified that materially impacts the provisions made within the policy.

10 Equality and Diversity Impact Assessment

This policy meets NHS Lanarkshire's EDIA √

11 References

- **Government Security Classifications Version 1.1 / May 2018 -** (© Crown copyright 2013 You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence.)

12 Appendix 1 – Control Notification.

Document Title				
Document Type				
Recorded on Information Asset Register	YES		NO	
Author				
Classification				
Identified Risk				
Rationale				
Board Secretary Comments				
Corporate Management Team Decision				
Date				
Review Date				