Security Classifications Policy

1. Introduction

1.1 The new Government Security Classifications Policy was introduced on 02 April 2014 and outlines how the Scottish and UK Government classify information assets to ensure they are appropriately protected. It applies to all information that the government collects, stores, processes, generates or shares to deliver services and conduct business. The same system has been adopted by non-departmental public bodies, local authorities and other government stakeholders to help improve the way key partners share information.

1.2 This policy replaces the current CHS ISMS Guidance: Classification of Information (based on the Government Protective Marking Scheme). It describes how CHS will classify information assets to:

- ensure they are appropriately protected
- support children's hearings business and the effective use of information
- meet the requirements of relevant legislation (including the Children's Hearings (Scotland) Act 2011, Data Protection Act 1998 and Public Records (Scotland) Act 2011) and
- strengthen information sharing protocols with partners

1.3 This policy applies to all information that CHS collects, stores, processes, generates or shares, including information received from or exchanged with external partners.

1.4 All CHS staff, Board members, AST and panel members, and Clerks to the AST have a duty to respect the confidentiality and integrity of information and data that they access, and are personally accountable for keeping information safe in line with this policy and CHS information security policies and procedures.[1]

1.5 The Government Security Classifications Policy classifies information assets into three types: OFFICIAL, SECRET and TOP SECRET. CHS does not have a requirement for the full range of classifications used in Government and is responsible for information assets with an OFFICIAL classification only. Staff, Board members, AST and panel members as well as Clerks must follow the guidance below when classifying OFFICIAL information. Routine

[1] For a list of all Information Security policies and procedures relevant to each role, please see the *Guide to Policies, Procedures and Guidance: Information Governance* and the Information Management resource pages on CHIRP.

Date Approved: 26 August 2014
Date for Review: August 2016

classification of legacy documents will not be carried out, unless it is deemed necessary to do so.

2. Security classification – OFFICIAL

2.1 CHS' information assets should be treated as OFFICIAL. This includes information relating to the day to day business of CHS, the management of public finances, commercial interests, including information provided in confidence. It also includes personal information that is required to be protected under the Data Protection Act 1998 or other legislation (e.g. panel member records).

2.2 There is no requirement to explicitly mark routine OFFICIAL information, however, a limited subset of OFFICIAL information could have more damaging consequences for individuals or CHS if it were lost, stolen or published in the media. This information will require a marking of OFFICIAL–SENSITIVE. A couple examples of OFFICIAL-SENSITIVE information could include: successful/unsuccessful tender documents, information relating to children's hearings; details of complaints investigations.

2.3 Information classified as OFFICIAL-SENSITIVE may also require an additional 'descriptor', to distinguish particular types of information and indicate the need for additional common sense precautions to limit access. Descriptors should be applied to classifications in the format: OFFICIAL-SENSITIVE - Descriptor.

2.4 The following core descriptors are to be adopted by CHS:

Commercial	Commercial or market-sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to CHS or to a commercial partner if improperly accessed. For example, successful / unsuccessful tender documents.
Personal	Particularly sensitive information relating to an identifiable individual, where inappropriate access could have damaging consequences. For example, where relating to children's hearings, complaints, etc.

3. Key principles

3.1 Staff, Board members, AST and panel members, and Clerks must observe the following key principles when managing and providing access to information:

- we must handle all information with care, to prevent loss or inappropriate access
- we all have a duty of confidentiality and a responsibility to safeguard information that we access, manage and share
- we must provide access to sensitive information on a genuine 'need to know' basis only

4. Applying a security classification

4.1 Only the creator or Information Asset Owner (IAO) can classify an asset. Any change to the classification requires the creator or IAO's permission. If they cannot be traced, a classification may be changed, but only once approval has been obtained from CHS' Senior Information Risk Owner (SIRO).

4.2 A file, or group of classified documents or assets, must carry the classification of the highest marked document or asset contained within it (e.g. a file containing OFFICIAL-SENSITIVE and OFFICIAL material must be marked OFFICIAL-SENSITIVE [Descriptor]) unless the OFFICIAL-SENSITIVE documentation can be separated into appendices so that the main body can be distributed widely with fewer restrictions.

4.3 There is no requirement to mark OFFICIAL information. There is also no requirement to retrospectively mark legacy information unless it is in regular use and business need requires it.

4.4 It is important to note that applying too high a protective marking can inhibit access, lead to unnecessary and expensive protective controls, and reduce business efficiency. Conversely, applying too low a protective marking may lead to damage or distress and/or inappropriate disclosure.

4.5 The sensitivity of an asset may change over time so it may be necessary to reclassify assets. IAO's are responsible for regularly reviewing their information assets and the relevancy of the classifications applied to them.

4.6 When applying a security classification to a document, it must be in CAPITALS at the top and bottom of each page, in the centre of the header and footer. When working with emails, the classification should be included in the subject line.

4.7 When letters or other communications are sent to external recipients who are members of the public or an organisation which does not require a classification to be shown, then only CHS' copy, whether electronic or paper should be classified.

5. Handling information

5.1 Information must be handled with care to avoid loss, damage or inappropriate access. For example, when handling panel papers, panel members should ensure they do so in line with the *Keeping Information Safe* key tips.

5.2 Information must be shared responsibly, for business purposes. CHS has established information sharing protocols with key partners, including Scottish Government, SCRA and local authorities. Please refer to these protocols for guidance on what information can be shared with partners and how this sharing should take place.

5.3 Information assets and equipment must be stored securely when not in use. CHS operates a clear desk policy and screens must be locked when left unattended. For further information about handling information appropriately, please see the *Information Security Policy, Keeping Information Safe* guidance and *Acceptable Use Policy*.

5.4 Where it is necessary for staff or Board members to take information assets out of the office environment they should be protected in transit, not left unattended and stored securely. Please note, that OFFICIAL-SENSITIVE documentation must not be removed from the office environment in paper or on unsecured mobile devices. Please refer to the *Acceptable Use Policy* for further information.

5.5 When discussing business in public or by telephone, appropriate discretion should be exercised. Details of sensitive information should be kept to a minimum.

5.6 Particular care should be taken when sharing information with external partners or the public; for example, emails, faxes and letters should only be sent to named recipients at known addresses. When sending OFFICIAL-SENSITIVE information by post, please refer to the *Secure Transfer of Information* guidelines.

5.7 It is helpful to include special handling instructions when sending OFFICIAL-SENSITIVE information. For example, when sending emails, you can include a sentence advising the recipient of the content of the email and how it should be handled:

'**Handling Instructions:** *the contents of this email are confidential - please retain securely and destroy when no longer required for admin purposes*.'

5.8 Access to OFFICIAL-SENSITIVE information must be granted on a 'need to know' basis only. However, in some cases, it may be necessary to share sensitive material with individuals/organisations without the necessary access controls, for example when immediate action is required to protect life or to stop a serious crime. In these cases, CHS must be informed as soon as possible after disclosure.

6. Roles and responsibilities

6.1 Accidental or deliberate compromise, loss or misuse of CHS information may lead to substantial damage and distress and may even constitute a criminal offence. Individuals are personally responsible for protecting any CHS information or other assets in their care.

6.2 CHS has a *Managing Information Security Incidents Procedure* in place to aid the detection and reporting of information security incidents. This procedure can be found on CHS' website and on CHIRP, alongside a summary guidance document - *Reporting information security incidents*.

6.3 IAO's are responsible for identifying any OFFICIAL-SENSITIVE information and for putting in place appropriate business processes to ensure that it is securely handled.

7. Monitoring and Review

7.1 Classified information should be kept under review and reclassified when the need for the classification no longer applies. CHS' SIRO is responsible for ensuring compliance with this policy and for reviewing its ongoing effectiveness.

Document Control

Title	Security Classifications Policy
Author	Ava Wieclawska, August 2014
Approved by	Senior Management Team
Date of approval	26 August 2014
Version number	1.0
Review frequency	Every two years
Next review date	August 2016

Status Control

Version	Date	Status	Author	Amendments to policy	Approved by
0.1	20/02/2014	Draft	Ava Wieclawska	New policy to reflect changes in the Government Security Classifications Policy to be introduced on 02 April 2014	SMT
0.2	05/06/2014	Draft	Ava Wieclawska	Review period extended from 6 months to 2 years.	
1.0	26/08/2014	Final	Ava Wieclawska	Final policy approved by SMT.	SMT