National Security Copy

Code of Practice

Overview

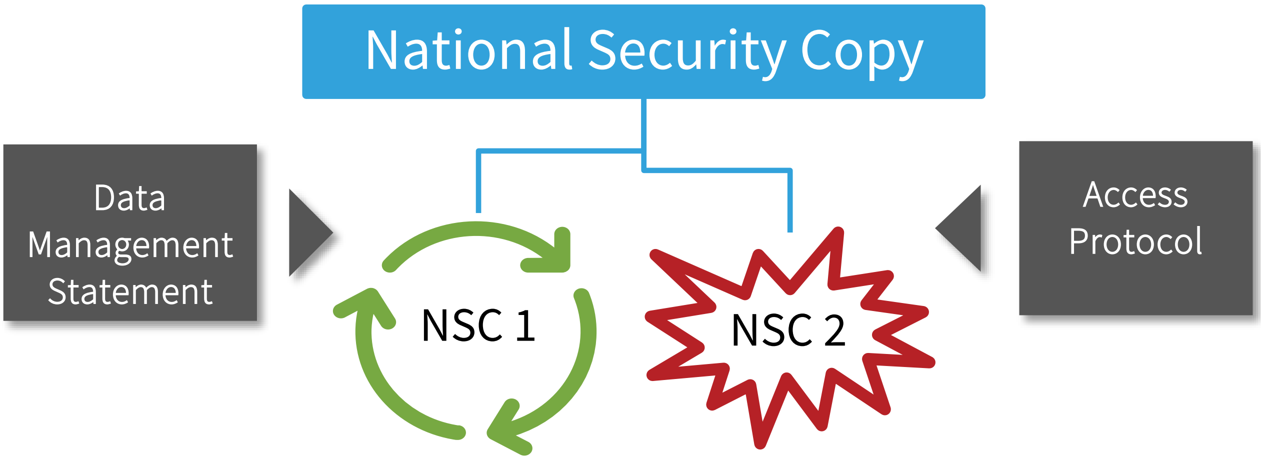
The Heritage Information Access Strategy (HIAS) is a programme of interlinked projects designed to simplify and improve public access to heritage data held or generated by Historic England (HE), by Local Authority Historic Environment Records (HERs) and by other bodies. The need to ensure the safety of this data is stated in these HIAS principles: “Historic England should, on behalf of the nation, ensure that a security copy of all such data exists” and “such data or knowledge should not be at risk of loss, fragmentation, inundation (in data), or system obsolescence”.

The National Security Copy Code of Practice (NSC CoP) establishes trust in the long-term preservation and access of historic environment records created and held by HIAS partners. The code provides managers of historic environment resources with details of principles and practices they must commit to for the National Security Copy. Compliance with the code provides authorities with a high level of confidence that heritage data will be safeguarded.

The Code of Practice covers two types of security copying to safeguard data maintained as the National Security Copy (NSC):

- NSC 1: Consistent routine backups where security copies are made of a heritage dataset by an organisation — covered by the NSC Data Management Statement (DMS); and
- NSC 2: Exceptional decisions to deposit a security copy with another heritage organisation for safeguard — covered by the Access Protocol (AP).

The responsibilities of the HER’s host authority are as follows: to follow the principles outlined in this Code of Practice; to create and continually update a DMS; and in unforeseen circumstances to safeguard heritage data by enacting the AP. The responsibilities of Historic England are to provide guidance for the creation of the DMS; engage the sector in the process of protecting heritage data; and to oversee the capture of the NSC 2.



The principles

2.1 People managing heritage data and information have the appropriate skills, training, and support for their roles.

Each organisation should have staff trained in managing data and information, and in using heritage datasets. Staff should understand the requirements for data security and backups and be supported in these tasks. In practice:

- The roles and responsibilities of those involved in backups and data security should be clearly defined and named in the DMS.
- All relevant staff should be informed about secure data handling and backups.

2.2 Organisations should look after heritage data securely and in ways that are consistent with best practices and the public good.

Each organisation should follow best practice in the management of heritage data including backups, storage and access. In practice:

- A DMS should be prepared and kept up to date. This statement should provide the information needed to recover data and systems following a disaster, accident, or other disruption to the service.
- Database Rights and any third-party copyright in the data or access licences should be clearly identified.
- Any legal restrictions or statutory regulations, which affect the deposit of the data should be identified (for example, personal or confidential data in a DPIA).

2.3 Organisations should have effective regular backup processes.

Each organisation is responsible for ensuring that consistent and regular backups are completed of their heritage data and applications. In practice, staff should discuss the backup routines with their IT service providers and ensure that:

- Databases, GIS applications and other data are backed up at regular intervals and in line with best practice recommendations.
- Backups are retained for a minimum of 30 days with additional monthly and annual backups retained in line with best practice recommendations.
- It is possible to restore data and systems back to date before a technical failure or accidental loss occurred.

2.4 Each organisation will put in place internal measures to monitor and test the effectiveness of the backup process.

Each organisation is responsible for monitoring and testing the effectiveness of their backup procedures. In practice staff should ensure that:

- The process of restoring data from backups is tested at least annually to make sure that the data is accurate and as expected.
- Backups are tested following changes in systems, software, or the organisation to make sure that relevant data is being captured, and the process of restoring data works as expected.
- The DMS is updated to reflect any changes that may have occurred in systems, software, the organisation of data, or in backup procedures.

2.5 Each organisation will report how they are protecting their data.

Each organisation commits to creating and updating a DMS and reporting any changes that may impact on the sustainability of their service. In practice:

- Organisations will take part in the audit process where they will submit a DMS using the most recent template to Historic England.
- Organisations commit to completing the HE / ALGAO Annual Survey, which monitors changes in service provision and the presence of an updated DMS.
- Organisations will review their DMS at least once a year and send updated versions to Historic England's Heritage Information Partnerships Team (HIPs).

2.6 Each organisation with concerns over the security of its heritage data agrees to proactively notify Historic England and relevant stakeholders.

In advance of potential service disruptions, heritage organisations should contact Historic England and consult relevant stakeholders, including ALGAO (England), neighbouring historic environment officers, and other bodies (e.g. local archives) to discuss whether the Access Protocol needs to be enacted. In practice staff should:

- Proactively consult senior management and contact relevant stakeholders to assess and monitor identified risks to the heritage database.
- Ensure heritage data protection is covered by organisational Disaster Plans.
- Keep the DMS up to date so that the information needed to enact the AP is available.

2.7 Each organisation will support the Access Protocol in the exceptional circumstance that the NSC 2 needs to be taken to safeguard data.

In the exceptional circumstance that a National Security Copy is taken, organisations agree to facilitate the Access Protocol. In practice:

- Ensure staff are familiar with the Access Protocol and what it would entail for their specific organisation.
- A copy of the heritage datasets can be made and stored with a third-party host for safekeeping.

[*The HER's host authority]* acknowledges the principles and best practice contained in the National Security Copy Code of Practice, including the steps set out in the NSC Data Management Statement which monitors the routine backing up of data and the NSC Access Protocol which supports the exceptional decision to deposit a security copy with a third-party host for safekeeping.

Signed for and behalf of [*the HER's host authority]*

By*: …………………………………

Job title: …………………………...

Signature: ………………………..

Email: ……………………………...

Telephone: ………………………...

*We recommend the signatory is part of the HER senior management team.