[InsertAuthorityName] Historic Environment Record

Data Management Statement (DMS)

# Overview

|  |  |
| --- | --- |
| **Author(s):** |  |
| **Origination Date:** |  |
| **Reviser(s):** |  |
| **Date of last revision:** |  |
| **Review due:** | Annually1 |
| **Version:** |  |
| **Status:** |  |
| **Summary of changes:** |  |
| **File name/location:** |  |
| **Authorities covered by the HER:** |  |
|  |
| **Related policies:** | Date of last revision | Revision required? | Review Cycle | Location |
| *Systems Security Policy**Recording Policy**Disposals Policy**Disaster Recovery Plan**Business Continuity Plan**Index to Reference Collection**Recording Manual**Prioritised list of backlog* | e.g. 2018 | yes | annually | C:drive/foldername |
| *Does the HER manage any other databases that have not been fully integrated into the main HER e.g. UAD, HLC, legacy database)?* | If yes, please detail here: |
|  **Contact** **HIPsTeam@HistoricEngland.org.uk** **if you have any queries when completing this form.****Please send your completed form,** [**Part A**](#_Part_A) **(signed) and** [**Part B**](#_Part_B)**, to** **HIPsTeam@HistoricEngland.org.uk** |

1 Before reviewing the DMS, please check to see if there is an updated version of the template on the [Historic England website.](https://historicengland.org.uk/research/support-and-collaboration/heritage-information-access-simplified/national-security-copy-nsc/)

This Data Management Statement forms part of the [Heritage Information Access Strategy (HIAS)](https://historicengland.org.uk/research/support-and-collaboration/heritage-information-access-strategy/) ***National Security Copy Code of Practice*** (NSC CoP).

The Code of Practice governs two main types of security copying:

1. Consistent routine backups where security copies are made of a heritage dataset by an organisation (covered by the **Data Management Statement**). This security copy is referred to as the National Security Copy 1.
2. Exceptional decisions to deposit a security copy with another heritage organisation for safeguarding (covered by the **Access Protocol**). This is the National Security Copy 2.

Please refer to the Code of Practice before completing the DMS.

# The DMS:

* Provides information needed to recover data and systems following a disaster, accident or other disruption to the HER service;
* Identifies and defines the roles and responsibilities of those involved in backups and data security;
* Confirms relevant staff are informed about secure data handling and backups;
* Identifies (or signposts existing documentation containing details of) any copyright in the data or access licences;
* Identifies (or signposts existing documentation containing details of) any legal restrictions or statutory regulations which affect deposit of the data (e.g. personal or confidential data);
* Is an overarching document that refers to related standard HER policies where these have been completed by the HER.

When the Access Protocol is invoked, the DMS should be included in the supporting documentation accompanying the data being deposited.

Historic England aims to coordinate each year a number of rehearsals of the process to prepare a security copy and test its effectiveness. You may be invited to participate in a rehearsal as part of the annual monitoring of NSC compliance.

# DMS Part A

## *(Please complete this section in full)*

## The HER system and software

|  |
| --- |
| Give a brief description of the systems and software that you use. Describe who developed the system and how it is maintained. Please supply a link or reference to relevant documentation, including licences.Please edit the standard text below as appropriate and include any additional information that you feel is relevant. *The HER includes textual data in a computerised database using [software, version], which is linked to spatial data in digital form on a Geographic Information System (GIS) using [software, version].**The [ ] software is off-the shelf package/bespoke/open-source developed and supplied [under licence] by [ ].**The database is stored on the [corporate network/exegesis hosted/other] at the following location [ ].**The GIS layer is stored on [ ] at the following location [ ] and is/is not part of a corporate GIS.**Programme components are installed on [] and accessed via [].**[The HBSMR system stores data in a SQL Server database, and uses Access for the user interface.]* *General ICT support is provided by [ ] and can be contacted on [ ].**Specialist support for the software is provided by [ ] and can be contacted on [ ].**A database model (e.g. entity relationship diagram) is stored at [drive/folder/file]**Supporting documentation including details of any codes, abbreviations and terminology utilised in the database and GIS is stored at [drive/folder/file].**Licences required include:* |

## Data

|  |
| --- |
| Please provide a top-level, overview description of the data held. |
| **Data Type** | **Range of formats involved** | **Volume/File size** | **Location** | **Existing metadata\*\*****/catalogue?** |
| Database |  |  | e.g. server and location | Yes/No |
| GIS Layer |  |  | e.g. server and location | Yes/No |
| Linked digital files | e.g. PDF, csv, xls, tiff, jpeg |  | e.g. Drive/folder/file | Yes/No |
| Stand-alone digital files\* | e.g. csv, xls, PDF, tiff, jpeg, Microsoft Word |  | e.g. Drive/folder/fileCD storage location | Yes/No |
| Paper-based information sources | e.g. Site-specific paper files, aerial photographs, historic maps |  |  | Yes/No |
|  |  |  |  |  |
|  |  |  |  |  |
| \*For example, may include NMP, HLC, UAD, EUS data not integrated into the HER system, digital grey literature PDFs etc. These may be located on servers or stored on external media such as CDs, HDDs.\*\* Metadata to accompany each of the digital and non-digital components of the HER should include as a minimum: file name, file type, description of the data and purpose, date of creation, date of last update, origin, restrictions of use, and rights information. Advice on the creation of metadata can be found at <https://archaeologydataservice.ac.uk/advice/guidelinesForDepositors.xhtml>; <https://www.ukdataservice.ac.uk/manage-data/document/metadata.aspx> and <https://www.agi.org.uk/agi-groups/standards-committee/uk-gemini> |

## Digital data backup

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Back up procedures:** Please fill in the table below regarding backups for the HER database, GIS, digital reference collection and system files (where relevant). If an option doesn’t suit your arrangements you can add your own text.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Backups made? | Type of Backup | Backup frequency | No. of copies | Backups retained for |
| HER Data | Choose an item. | Choose an item. | Choose an item. |  | Choose an item. |
| GIS Data | Choose an item. | Choose an item. | Choose an item. |  | Choose an item. |
| Digital Ref. Collection | Choose an item. | Choose an item. | Choose an item. |  | Choose an item. |
| System Files | Choose an item. | Choose an item. | Choose an item. |  | Choose an item. |

Additionally, please explain who is responsible for making the backups (HER officer/in-house IT service/external IT Service/automatic backup to cloud/other) and where they are stored (on site/off-site/external hard-drive or disc tape/remote server/commercial data repository/other).Please detail for both the data and the system files (where relevant e.g. if bespoke software).**Testing back up procedures:**Please fill in the table below regarding backup testing and recovery for the HER database, GIS, digital reference collection and system files (where relevant).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Regular data recovery tests? | Backup copies monitored/ examined? | Successful recovery from backup? | Loss or corruption of data/files past two years? |
| HER Data | Choose an item. | Choose an item. | Choose an item. | Choose an item. |
| GIS Data | Choose an item. | Choose an item. | Choose an item. | Choose an item. |
| Digital Ref. Collection | Choose an item. | Choose an item. | Choose an item. | Choose an item. |
| System Files | Choose an item. | Choose an item. | Choose an item. | Choose an item. |

Please keep a cumulative log of any recovery tests, incidents of lost or corrupted data/files in Appendix 1 as part of the DMS.Please give details of the criteria you use in the testing process. Are procedures for data recovery adequately documented? |

## Training

|  |
| --- |
| Record training undertaken by staff responsible for digital security, storage and backup procedures, Disaster Recovery and Business Continuity in Appendix 2. Keep this log updated as part of the DMS. Is the training adequate for the present needs of the service? What further training is required? |

## Responsibilities

|  |
| --- |
| Who is responsible for keeping this Data Management Statement up to date?Name:Job title:Email:Telephone: |
| Who is responsible for data backups?Name:Job title:Email: Telephone:  |
| Who is responsible for testing data recovery?Name:Job title:Email:Telephone: |
| Who is responsible for Disaster Recovery and Business Continuity?Name:Job title:Email Telephone: |

# Part B

## *(Please either complete this section in full, or provide references and links to where information is held within existing policy documentation)*

## Data Security

|  |
| --- |
| Please describe how anti-virus and firewall protection is managed, and how access and passwords are controlled. Who is responsible for data security? Are these procedures adequately documented? |

## Physical Storage

|  |
| --- |
| Give a brief description of where paper-based sources are held, explaining if these are held in the office, in basement storage, off-site storage or commercial storage. Is the storage secure? Who has access?Give details whether these have been digitised, including any backup and storage arrangements for the digitised copies. |
| Questions to consider:Have you deposited paper-based sources (record cards, maps, reports, photographs) in a local record office or museum?Has each component been assessed to decide on the length of retention? |

## Legal Compliance

|  |
| --- |
| Describe how you manage compliance with GDPR and any other legal issues in your data.  |
| Questions to consider:* State whether you have received any advice on GDPR in the data that you collect, whether there are any restrictions on the reuse of third-party data
* Consider whether any permissions need to be obtained to enable reuse of the datasets for the national security copy, or to enable sharing with relevant organisations.
* State whether the HER system is covered by a Data Protection Impact Assessment (DPIA), even if this is a null return i.e. no personal information covered by GDPR is held in the HER.
 |

## Preservation

|  |
| --- |
| Identify and briefly describe data that must be retained to provide HER services and for legal or regulatory reasons, e.g. under an SLA with a neighbouring authority.  |
| Questions to consider:* How will you decide which data and information sources should be retained and preserved?
* Consider which information sources and other documents are important to support business processes and should be retained. If paper-based sources have been successfully digitised, consider whether the physical material could be deposited in a local record office. What time or effort would be involved in preparing the data?
 |

Please send your completed DMS form, Part A and Part B, alongside the signed Code of Practice to HIPsTeam@HistoricEngland.org.uk

If the HER has submitted a signed Code of Practice in the last 5 years and since then there has been no major staffing changes in HER management, the Code does not need to re-submitted.

# Appendix 1: Data and file recovery log

This backup testing and recovery log should be cumulative, in subsequent versions please add to the previous log rather than starting over.

|  |  |  |  |
| --- | --- | --- | --- |
| Event e.g. recovery test or incident | Date | Description | Result/Action |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Appendix 2: Training log

This training log should be cumulative, in subsequent versions please add to the previous log rather than starting over.

|  |  |  |  |
| --- | --- | --- | --- |
| Staff name | Date | Training undertaken | Follow-up/Action |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |