[*Insert Authority Name*] Historic Environment Record Data Management Statement (DMS)

The completion of the DMS should be a joint effort between HER and IT staff.

We recommend engaging wider staff in your authority to raise awareness of the data held and the requirements of the Access Protocol.

Please be aware that this template will be subject to review during the National Security Copy (NSC) Field test project and therefore may be changed following completion of the project.

Author(s):				
Origination Date:				
Reviser(s):				
Date of last revision:				
Review due:	Annually The HER should review the DMS annually for any necessary updates. Tip: Mark a recurring schedule in your calendar and always use the latest template on the HE website.			
Version:				
Status:	Draft The initial version submitted will be treated as Draft Status as it needs to be assessed and approved by HE before being accepted as Final. We may ask for additional information to be added to the document before approval.			
Summary of changes:				
File name/location:				
Authorities covered by the HER:	If the HER covers more than one authority please engage with all stakeholders to inform them of potential and purpose of the NSC.			
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 Add date of last revision where document exists. Enter 'No' if the document does not exist. All other columns will then be not applicable for each document listed.	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 (signed) and Part B, to HIPsTeam@HistoricEngland.org.uk

This Data Management Statement forms part of the Heritage Information Access Strategy (HIAS) ***National Security Copy Code of Practice*** (NSC CoP).

The Code covers 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**, CoP Part1).
2. Exceptional decisions to deposit a security copy with another heritage organisation for safeguarding (covered by the **Access Protocol**, CoP Part 2).

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;

We recommend liaising with wider staff when completing the DMS..

- 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 will 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.

Part A

(*Please complete this section in full*)

The HER system and software

Purpose:

- To know what software/system may be needed to access the data.
- To know who to approach for advice/help in retrieving the data.
- To document where the data is located for non-HER authority staff.
- To ensure documentation for the system if it needs to be replicated/installed elsewhere can be located.
- To ensure systems are adequately documented, particularly database relationships to enable a person to understand how the database functions.

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.

Data

Purpose:

- Which and how many files constitute the HER.
- Volume and number supplied in case of need to temporarily archive with digital data repository.
- Importance of metadata not only for archiving but for understanding the compilation/purposes of each dataset/file.
- Location of supporting paper reference collection in case of need to consult with authority to ensure ongoing management and security.

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/file CD 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

Metadata provides a description of each file making up the HER dataset. In the absence of any staff during the protocol period this information will help a third party understand the nature and purpose of each file/entity within the dataset. Ideally this should be produced at file level and also contain an entity description for each of the fields in a file where relevant e.g. database field name descriptions. This is particularly important for bespoke databases.

Please indicate in the table whether such metadata exists.

The links above take you to metadata templates and examples which can be used to create your own set of metadata.

Digital data backup

Purpose:

- To know the currency of last backup in case of no access to live system/loss of data.
- Latest backup could be held as security copy until full access can be gained/given.
- To document whether multiple copies exist and where they are located/stored.
- To understand whether backups are viable/data has been recovered in the past.
- To understand which procedures are already in place in the event that data may need to be recovered/transferred.

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).

Data Recovery Test: What is this?

This would be a test scenario where for example once a year or every six months, a backup copy would be used to test the backup recovery procedure to demonstrate that this can be done successfully without data loss, corruption, system rejection.

This would not be restored into the live system as that would overwrite the current data. Ideally it would be restored into a system copy/test housing/blank access database. Ideally would also involve system/application restoration as well e.g. on standalone PC.

HER staff should have sight of the restored data in order to check for accuracy or any anomalies. Other staff might not find the subtleties of missing or incorrect data or information that has been restored in the wrong place for example. More minimal checks may involve simply checking that the data is readable.

Please detail these procedures below the table. It is down to YOUR IT and best practice to consider what is suitable for the type of data and system you use.

Backup Monitoring: What is this?

Frequent monitoring for error messages or system alerts established in the event of a backup failure or partial failure.

However, it is important to do test recovery as well, as lack of error messages may not indicate that all is well with the data itself.

Successful Recovery from Backup: What is this?

As opposed to the test recovery above this is where a real life situation has necessitated the recovery of data from backup into the HER database/system.

	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.

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).

Please keep a 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?

Please detail criteria and recovery here or reference an existing document with location identified.

The plan should be detailed enough that someone can work through and follow the instruction step by step to recover data.

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?

Record of training for **HER or other non-IT staff** who have responsibilities in these areas. Demonstrate that you have the appropriate support and training has been provided.

If all these are covered by dedicated IT staff then there is no need to record training. Please state this in the section above.

Responsibilities

Engage with others in the authority. The DMS should be signed by senior management so that they are aware of and understand the NSC protocol and can therefore assist should the need arise.

Aim to cement the HER with wider staff of the authority who could then be called upon in event of a trigger for access to the data.

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:
Who is responsible for testing data recovery? Name: Job title:
Who is responsible for Disaster Recovery and Business Continuity? Name: Job title:
[*Local Authority*] acknowledges the principles and best practice contained in the National Security Code of Practice, including provision for exceptional decisions to deposit a security copy with another heritage organisation for safeguarding, as set out in the Code's Access Protocol.

Signed for and behalf of [*Local Authority*]

By*: ……..

Signature: ……..

Title: ……..
Email:……..
Telephone:……..

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

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

Purpose:

- To understand how secure the data and system are to prevent events that may trigger the protocol.
- Documented security procedures to allow for succession planning and longevity of process.
- Documented so all in authority understand who has access and how data is accessed.

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?

System Security Policy may cover this detail. If so, reference here and supply copy.

Passwords:
We recommend that more than one person has admin access to the HER where appropriate even if not for day to day use. Only one staff member with access to the system and data may prove problematic should that staff member not be available. Avoid generic 'Admin User' profiles and passwords.

However, password distribution and system access must follow authorities' procedures and protocols.

Physical Storage

Purpose

- To provide detail of the scope and location of HER's physical holdings.
- To make those in authority aware as well as outside stakeholders.
- Documented so all in authority understand who has access and how.
- To allow consideration of ongoing management and access in the event of a trigger event.

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

Purpose

- To understand restrictions with the data ahead of potential supply to third party/parties involved in the Access Protocol and data transfer.

Note: During the Access Protocol no data will be supplied to third parties outside of those involved in the Access Protocol and data transfer.

Describe how you manage compliance with UK GDPR and any other legal issues in your data. Other examples include Crown Copyright. Licenced datasets. OS copyright.
Questions to consider: • State whether you have received any advice on UK 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.

Preservation

Purpose

- To know which supporting datasets and information are required for Business Continuity purposes e.g. Enquiry log, licence agreements, data exchange agreements, length of retention. SLAs, contracts.

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 form, Part A (signed) and Part B, to HIPsTeam@HistoricEngland.org.uk

Appendix 1: Data and file recovery log

Purpose

- To understand the stability of the database/system and therefore understand if risk of loss is high or not.
- To demonstrate that regular tests are being carried out to ensure the viability of backups

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

Appendix 2: Training log

Purpose

- For non-IT staff to demonstrate competence in these skill areas.

Staff name	Date	Training undertaken	Follow-up/Action