Administrative Data Research Network

An ESRC Data Investment

Secure Environment Policy

PUBLIC

01 JULY 2015

Version: 01.00

T +44 (0)1206 873435
E help@adrn.ac.uk
www.adrn.uk

Scope

In order to support ADRN's commitment to protect the privacy and confidentiality of data subjects a suite of Information Assurance policy documents have been developed that provide a framework for ADRN operations and to guide practice across all ADRCs and the ADS. This document outlines the ADRN policy in relation to Secure Environment Policy. All ADRCs will in addition have local procedures that outline how these policies are operationalised.

Other associated documents include:

ADRN030 Information Security Principles

ADRN031 Trusted Third Party Policy

ADRN033 Data Movement Policy

ADRN034 Data Retention and Destruction Policy

This document does not cover information security policy for Trusted Third Parties, which can be found in ADRN031

Contents

For defintions of terms please see For defintions of terms please see the ADRN glossary at http://www.adrn.ac.uk/using-the-network/documentation

1. Secure Environments Policy

An ADRN Secure Environment comprises:

- Data centres or their equivalent e.g. the location where the de-identified research data are held and processed
- Secure data access facilities e.g. the places in which researchers access de-identified research datasets (for example, safe rooms or safe settings)

It is acknowledged that in some ADRCs these two functions are contained within the same physical location.

This policy sets out the standards that each ADRC must adhere to and the requirements for other parties that may contribute to a Secure Environment.

ADRN1: ADRN will always operate to protect the privacy and confidentiality of data subjects.

1. All facilities must have current CLAS[1] [CESG Listed Advisor Scheme] accreditation. This will ensure that all ADRCs operate to equivalent standards (Official Sensitive) in such areas as physical security, firewall provision and controls over staff with access to sensitive data.
2. The ADRCs are responsible for ensuring that clear written agreements are in place with external service providers in order that all parties understand their roles and responsibilities in ensuring ADRN Information Assurance.
3. The ADRCs will ensure that all researchers who access research datasets have Accredited Researcher status.

[1] CESG is the Information Security arm of GCHQ. CESG protects the vital interests of the UK by providing advice and guidance to the UK government on the security of communications and electronic data, in partnership with industry and academia. http://www.cesg.gov.uk/Pages/homepage.aspx

4. The ADRCs will ensure that the secure environment contains a separate (virtual or physical) secure area (a 'staging area') where the data can be processed (e.g. success of linkages checked and derived variables created) prior to allowing researchers access to de-identified data.

ADRN4: ADRN will ensure data are accessed safely and securely.

1. All ADRC staff are required to have security clearance at an level appropriate to their role. The ADRC will determine the level of security clearance required by staff in different roles after taking advice from a CLAS consultant.

2. Requests for modification of software or release of accredited researcher specific syntax into an ADRC secure environment will be considered by each ADRC on an individual case by case basis, taking into consideration the impact on information security.