# St George’s, University of London

# Assured Remote Access

# to the Office for National Statistics’ Policy

## 1 Introduction

1.1. St George’s, University of London (SGUL) provides a Virtual Private Network (VPN) enabling access to the Office for National Statistics’ (ONS) Secure Research Service (SRS). Research staff at SGUL will sometimes require access to data held by the ONS on the SRS. A register of Accredited Researchers who are permitted to access ONS data will be managed and maintained by the Joint Research and Enterprise Services (JRES). The Deputy Principal for Research is responsible for the assured access contract between ONS and SGUL. This policy sets out the rules by which staff should adhere to when requesting access.

## 2. Purpose

2.1 The purpose of this policy is to detail the requirements for staff and technology for accessing the ONS SRS and to ensure the security and integrity of access to the ONS SRS.

## 3. Eligibility:

3.1 Granting technical access to the SRS VPN will be given when the following conditions are satisfied:

a. Permission for the applying Accredited Researcher (AR) has been granted by the ONS
b. The AR has completed the Accredited Researcher Assurance Registration form.
c. Director of JRES will inform IT Services regarding the ARs’ authorisation to access the SRS
d. The AR has sourced the appropriate IT kit from IT Services.

## 4. IT Kit:

4.1 The following conditions must be satisfied to gain access to the SRS VPN:

- Access to the SRS will only be applied to SGUL issued corporate and managed devices (laptop or PC).
- The laptop will be encrypted.
- The device must not be End of Life (EOL).
- A privacy screen must be used.
- The device meets the ONS’ minimum specification.

## 5. Conditions of Use

- No unauthorised user(s) should be provided with access to the laptop.
- We will only provide SRS VPN access to the usernames of the named individual(s) authorised by the JRES.
- Access to the SRS environment should only occur in places for which permission has been obtained, for example from the ARs' designated office within the named Institute in SGUL or at their residence (if permission for home working has been obtained).
- Access to the SRS environment should not occur within common areas such as a staff restaurant or coffee lounge.
- We will not provide access to personally owned user devices as part of a Bring Your Own Device Policy (BYOD).
- Should we be informed by the ONS or the JRES about removing access we will do so immediately.
- Providing access to others utilising your credentials will result in a withdrawal of the service.
- When access is no longer required the accredited researcher must inform IT directly so that access is removed.

## 6. Supporting Policies and Documentation

This policy should be read in line with associated standards, policies and arrangements including:
Password Policy
Records Management Policy
Information Retention Policy
Information Management Policy
Information Security Policy
Data Protection Policy
Core Regulations - Use of IT

## 7. Policy Review and Maintenance

This policy will be reviewed and updated, annually, or as needed, to ensure that the policy remains aligned with changes to relevant laws, contractually obligations and best practice.

## 8. Help and Advice

Please contact ITAV@sgul.ac.uk for any help or advice.