ONS Secure Research Service: Assured Organisational Connectivity

Version: **v1.0** **Publication Date:** **31/07/2019**

Author: Andrew Engeli

Date: 31st July 2019

Client Version 1.0

Sign Off			
Version	**Name**	**Position**	**Date of Acceptance**
v1.0	P Stokes	Deputy Director of Methods Data and Research	31st July 2019
v1.0	T Chapple	Head of Secure Research Service Operations	31st July 2019

Table of Contents

1. Introduction

Purpose

This document explains how organisations such as yours can apply to the SRS to connect a machine, or machines, to the data analytic services that we provide. Using these connections, **accredited researchers** who are members of your organisation (see Section 6 below) will be able to work from your organisation site(s) on approved projects on which they are named.

The document explains what safe settings are, how you would provide them within your organisation, and the requirements for signing an agreement with the SRS.

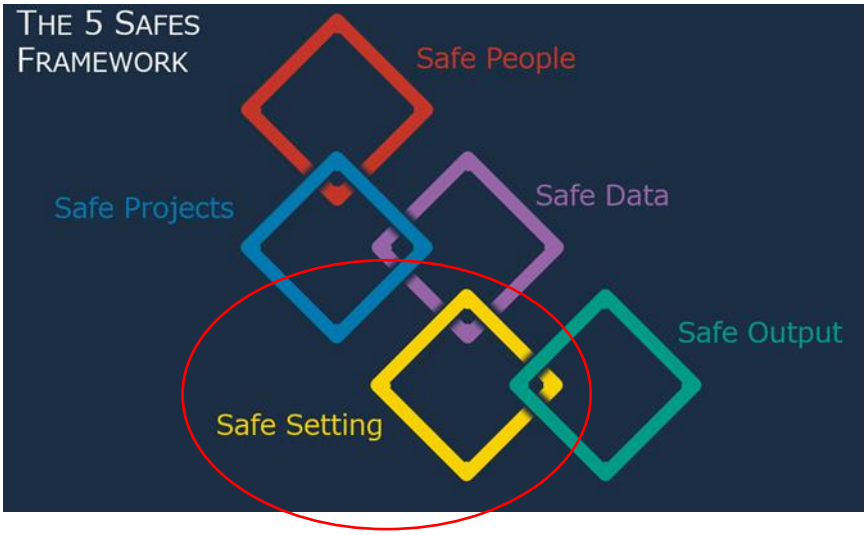
In addition, it explains why we have these requirements and the importance of each for maintaining secure access to our data holdings by the research community.

The document:

- Explains safe settings within the Five Safes framework
- Explains what **Assured Organisational Connectivity** is and how it works
- Explains **Assured Organisational Connectivity** agreements and certification
- Outlines what is needed to sign an **Assured Organisational Connectivity** agreement
- Outlines what is needed to apply for and maintain certification
- Contains additional information that your **accredited researchers** will need to know

2. The Secure Research Service and the Five Safes Framework

The Secure Research Service (SRS) operates within the Five Safes Framework, which is a set of principles that safeguard access to the sensitive data that are available for use by appropriately trained and accredited members of the research community (**Accredited Researchers - AR'S**).

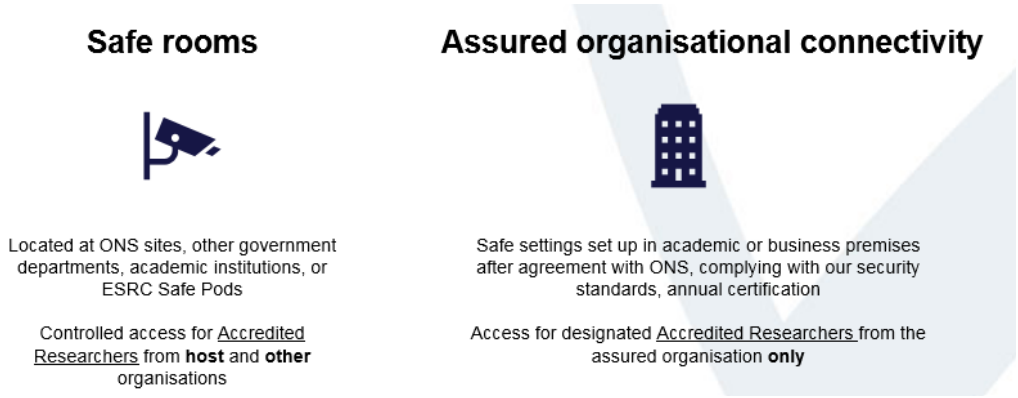


This document explains how the safe settings component of the framework operates and how organisations may apply for be connected to the SRS through the **Assured Organisational Connectivity** scheme.

It is important to know that the SRS is an accredited **data processor** under the Digital Economy Act 2017 (the Act). What this means is that the SRS does not own the data that is made available through the service and **data owners** are separately identified in the Act. Whenever the SRS acquires data that is to be made available to the research community, an agreement is signed with the **data owners** that specifies the conditions under which data can be accessed and any restrictions that may be placed on individual datasets. As part of this process, **data owners** typically wish to know information about how Five Safes will apply to their dataset. This will include detailed information about the safe settings in which data may be accessed.

3. Safe settings

Currently, the SRS supports access to data in two kinds of safe settings: safe rooms and through **Assured Organisational Connectivity**.



Safe Rooms are settings that may have a number of fixed terminals that are dedicated for secure research and which are access controlled through a booking or reservation system. Safe rooms will typically be equipped with video cameras or other monitoring systems. Safe rooms are generally open to all **accredited researchers** irrespective of whether or not they are full time employees of the organisation operating the safe room. There is a growing Safe Room Network available at research sites across the UK and details of locations may be obtained from us. ONS is interested in promoting the regional and geographical reach of its services and in ensuring access to all segments of the researcher community and will work with organisations who are interested in hosting safe rooms. The connectivity arrangements for safe rooms are described in a separate document and if you are interested in hosting one or require more information, please contact: research.support@ons.gov.uk.

Most organisations, whether Government Departments or other public bodies, academic institutions, or third sector/commercial organisations operating within the research community, will wish to develop safe settings under the **Assured Organisational Connectivity** (AOC) scheme. The **AOC** operates as a mark of assurance to the SRS, **data owners**, and other stakeholders. It is intended to demonstrate that organisations hosting safe settings understand their obligations, can meet the technical requirements for connectivity, have appropriate controls in place, and agree to maintain current and accurate records of connections and activity.

4. How Assured Organisational Connectivity Works

The SRS approach to **Assured Organisational Connectivity** recognises that every research institution or organisation wishing to connect to our services is different. For example, some institutions (typically but not always) academic institutions may have large, multi-site campuses that are largely open to members of the public. Other institutions (for example, many government departments) have strict access controls to all areas of their site and do not permit unaccompanied visitors.

Why this matters is that **data owners** are generally interested in understanding exactly who may have access to data and outputs in safe settings. It is important to understand that access to data and outputs may include glancing at the screen of a computer on which sensitive data are displayed or looking at statistical results that have not yet been cleared for publication. If **data owners** have a legitimate concern that people who are not **accredited researchers** and not named on a specific project have access to data and outputs they are unlikely to agree to release their data to the research community. And unless SRS is assured that these things will not happen, we will withhold **AOC certification** and work with the organisation concerned to meet the required standards.

Generally, no matter what kind of organisation that is requesting certification, there are two factors that will need to be considered for all machines that may be wished to connect to the SRS under AOC certification; who has credentials on machines to be connected and where machines are located.

		Number of accredited researchers who are credentialled on machine	
		one	many
Number of people who can access where machine is located	one	Typically a single office	Single office with access to other members of a team
	many	Open plan office or lab where others may be non-ARs	Often found in Government departments

In order to apply for access under the AOC certification, requesting organisations will need to carefully consider these two factors for each machine to be connected and will need to provide appropriate safeguards (and documentation) in each case.

5. Assured Organisational Connectivity agreements and certification

Assured Organisational Connectivity works within a two-part framework; the **AOC agreement** between the organisation applying for connectivity and the SRS (which is a set of legally binding documents that need to be signed by both parties) and the **AOC certification** (which is a guarantee that all connectivity arrangements are up to date and operating according to the agreement).

- The **AOC agreement** is typically signed for a period of five years (although a variation can be requested at the time that the agreement is negotiated). Unless the agreement is abrogated within that period it will continue to govern connectivity arrangements between the organisation and the SRS. No matter what the size or configuration of the organisation requesting access, each organisation will typically only ever have to sign one agreement at a time. After five years, organisations may apply to renew their agreements.
- **AOC certification** takes place on an annual basis (every 12 months) and is typically a 'light touch' process to guarantee that all aspects of the organisational agreement remain current and enforced. The presumption for recertification, if an organisation chooses to request it, is that it will typically be granted as long as all requirements are met. Before any **accredited researchers** can apply for remote access at their place of employment (other than through safe rooms), an organisation will need to have current AOC certification.

6. How to sign an Assured Organisational Connectivity agreement

If you wish to pursue an **Assured Organisational Connectivity** agreement with the ONS, you will need to, at a minimum, be able to do the following;

Provide the name and position of the Designated Authority within your organisation who will be the signatory for the AOC agreement and who will assume ownership of the legal and financial penalties specified in the agreement and in the Act. Typically this may be a Pro Vice Chancellor for External Relationships in an academic institution, a Trustee in a charity, a Director or member of the SCS in a Government Department, or a Director (Executive) in a commercial organisation). *Normally this person will not be an **accredited researcher** or user of the SRS* (a waiver for this provision may be granted upon request).

Provide the name and position of the Designated Point of Contact for all operational matters regarding SRS connectivity and who have ownership of the AOC certification process. Typically this might be a Pro Vice Chancellor or Director for Research in an academic institution, a Director in a charity, a Director or member of the SCS in a Government Department, or a Director (non-executive or Associate) in a commercial organisation. *Normally this person will not be an **accredited researcher** or user of the SRS* (a waiver for this provision may be granted where it can be demonstrated that all senior executives of an organisation are also **accredited researchers**, which may be the case for a very small number of organisations operating in the charitable or commercial sectors).

When the agreement is signed, your organisation will be committing to:

- Providing and maintaining an up to date register of machines that will be connected to the SRS. You will typically need to supply the *MAC addresses* of each machine to be connected, the client name, and the source IP address (a waiver for this provision may be granted upon request). All machines need to be *wholly owned by your organisation* and connectivity should not be requested for any personal machines or devices.
- Providing an maintaining an up to date register of the location of each machine to be connected including the IP address (see below). This register should include an accurate description the physical and technical access controls to each machine. Where machines are located in spaces that may be accessed by persons other than the **accredited researchers** named on a project, there will need to be an explanation of how the machine (and data and outputs) will be secured. For example, we may ask for a physical description of the space and of how entry and exit is monitored, and we may require the use of privacy screens, desk dividers, etc. where other physical controls do not restrict access to connected machines.
- Providing and maintaining an up to date register of accounts for **accredited researchers** that will be requesting access to the SRS and an indication of which machines (see above) that they will be authorised to use by your organisation. All **accredited researchers** requesting access through an AOC agreement will need to be either:
    - full-time or full-time equivalent contractual employees of your organisation (*Short-term or non-contractual research staff should normally seek access to the SRS through the safe room network*)

      or

- full-time or full-time equivalent contractual employees of another organisation that also has a current AOC certification and who are named **accredited researchers on** the project(s) being conducted under your agreement. *Your organisation will be responsible for ensuring that **accredited researchers** from external organisations who are accessing the SRS through your connectivity agreement are included in your register (see Section 7) and have accounts appropriately designated on specified machines.*

The AOC agreement will be tailored to reflect the specific details of your organisational connectivity needs and the combination of technical, physical, and human factors described above. However, the AOC agreement will specifically preclude:

- The use of any personal machines or devices to connect to the SRS.
- The use of wireless networks to connect to the SRS (a waiver for this provision may be granted upon request, where it can be satisfactorily demonstrated that the network achieves or exceeds the security standards of the GovWiFi network and/or the Government Minimum Cyber Security Standard[1] and that there is no satisfactory hard-wired alternative. Laptop computers will need to be connected via ethernet unless the other conditions of this waiver policy can be adequately demonstrated and all location and access requirements in this policy have been satisfactorily met).
- The use of VPN to connect to the SRS (a waiver for this provision may be granted where an organisation-wide VPN is mandated as part of that organisation's security controls. Typically this provision will apply only to Government Departments and specialised Research Institutions, and will need to be verified by the SRS Security team as meeting ONS-compliant VPN security standards).
- Access to the SRS for any machine located in a public space (i.e. one where there are no physical controls or monitoring of access). Laptops may not be used for connectivity in any location other than the one for which they are approved and designated in the register maintained by your organisation as part of certification (see Section 7).

The **Assured Organisational Connectivity** will also require your organisation to have a clear set of policies regarding breaches that includes how and what sanctions may be applied. Breaches that should be addressed in the policy must include how your organisation will address:

- Cases of *individual* **accredited researcher** misconduct or breach of policy.
- Instances of *systematic* **accredited researcher** misconduct or breach of policy.
- Cases of technical or infrastructure breaches (i.e. unauthorised access to a connected machine, hacking of accounts).

[1]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/719067/25062018_Minimum_Cyber_Security_Standard_gov.uk__3_.pdf

7. How to achieve and maintain Assured Organisational Connectivity certification

In order to achieve and maintain AOC certification, your organisation will need to:

- Provide the name and position of the single point of contact for all matters relating to technical and infrastructure connectivity. This person will also be responsible for maintaining the register of machines, locations, and accounts, and ensuring that it is current and accurate. *Normally this person will not be an accredited researcher or user of the SRS.*
- Provide the name and position of the single point of contact with responsibility for IT security and assurance. In the event of any breach of the AOC agreements or any major cyber event that may compromise the security of the connectivity agreements this person will be responsible for communications with the SRS Security Team. *Normally this person will not be an accredited researcher or user of the SRS.*

To achieve initial certification (which will take place at the same time the **Assured Organisational Connectivity agreement** is signed) it may be necessary for a team from the SRS to conduct a site visit. In order to maintain certification your organisation will need to:

- Ensure all registers are current and up to date.
- Notify SRS of any changes to the current certification (e.g. adding machines or locations).
- Provide access to those registers to the SRS, if requested, within 48 hours (2 working days).
- Permit a site inspection from an SRS team, if requested, within five working days of the request.
- Demonstrate continued compliance with all aspects of the **Assured Organisational Connectivity agreement**.

To apply for annual (12 month) recertification you will need to (in addition to the above) provide a usage report that explains the volume and usage of the SRS connection(s) from your organisation. *The SRS team will assist you in the preparation of this report to reflect your particular organisational connectivity arrangements.* Typically the recertification process will be light touch with an affirmative presumption of renewal. In some cases we may request a site visit to verify major changes and updates.

8. For your accredited researchers requesting access through Assured Organisational Connectivity

All of the **accredited researchers** seeking access to the SRS through your **Assured Organisational Connectivity** agreement will be asked to sign a separate document (the **Accredited Researcher Access Registration**). This declaration tells us (and you) that individual **accredited researchers** understand their responsibilities under your specific AOC agreement and that they are aware of your organisations policies and sanctions in the case of breaches of that agreement.

In order to be eligible to sign the Accredited Researchers AOC Registration researchers will need to be either:

- full-time or full-time equivalent contractual employees of your organisation (*Short-term or non-contractual research staff should normally seek access to the SRS through the safe room network*)

  or

- full-time or full-time equivalent contractual employees of another organisation that also has a current AOC certification and who are named **accredited researchers on** the project(s) being conducted under your agreement. *Your organisation will be responsible for ensuring that **accredited researchers** from external organisations who are accessing the SRS through your connectivity agreement are included in your register (see Section 7) and have accounts appropriately designated on specified machines.*

Doctoral students and part-time research associates would not typically be considered full-time or full-time equivalent employees under this policy and will probably need to access the SRS through the **Safe Room Network** (see Section 3).

Copies of blank Accredited Researchers AOC Registration forms will be provided when AOC agreements are signed and may also be obtained from us on request).

Accredited Researchers Assurance Declarations will need to be countersigned by the person who is the owner of the register of machines, locations, and accounts that are required for certification. If an accredited researcher is a member of another organisation that has a current **AOC certification** in place but is being granted access through your connectivity agreement, their Accredited Researchers AOC Registration will also need to be countersigned by the single point of contact within their own organisation responsible for maintaining the required registries (see Section 7).

Once the declaration has been countersigned, a copy will need to be forwarded to the SRS and placed on file. Once the declaration has been received and verified by the SRS team, we will notify **accredited researchers** (and the organisational signatory authority) that the researcher has now been approved for access under the AOC agreement.

9. Other things you need to know

Organisations will only need to sign one **Assured Organisational Connectivity** agreement. In cases where your organisation may need to add additional machines, locations, or **accredited researcher** accounts, this can be done through the certification process. For example, if a university wishes to add a new Institute of research Laboratory to an existing agreement, this can be done by updating the current certification. In this event, the SRS will need to be notified and will need to approve all additional provision (machines, locations, **accredited researchers**) before it can be activated.

These **Assured Organisational Connectivity** policies are routinely shared by the SRS with **data owners**, who may choose to give blanket approval for use of their data under agreements governed by them. However, **data owners** may request review of individual **Assured Organisational Connectivity** agreements and retain the right to withhold access to their data under those individual agreements. In such cases, the SRS will work closely and transparently with your organisation to explore whether modifications can be made to the agreement to facilitate access approval.

If your organisation is a victim of a major security threat (such as a cyber attack with penetration) not directly related to the SRS connection, but in which the SRS still maintains a legitimate interest, the AOC agreement will specify the appropriate actions that will be needed to be taken. Recognising that such events are sensitive and may have reputational consequences, we will work with your organisation to create a process for notifying us of such events that is secure and confidential. Typically such matters will be handled only by our Security Team (who will work with yours to resolve any issues arising from such incidents). Our standard policy will include suspension of the connectivity arrangements for your organisation for a limited period of time (typically 2 hours) while we conduct verification and diagnostic procedures at our end. We will notify your organisation immediately of any suspension and also of the progress and outcome of our own investigations.

Your organisation is responsible for all the commitments that are made by it under the **Assured Organisational Connectivity** agreements, including the behaviour of your employees who use the SRS as **accredited researchers**. The agreements exist as a cooperative and mutually binding set of arrangements that enable your organisation and the SRS to work together in upholding and enforcing the provisions of the Act. Working together, we can ensure that we maintain the highest standards of security and ethics while promoting appropriate access to sensitive data for accredited members of the research community.

10. If you have an existing agreement with us (as of July 1st 2019)

It is possible that your organisation already has an existing agreement with SRS for connectivity to our services or has applied for such an agreement and that application is pending. A small number of agreements were signed prior to our adoption of the AOC certification process within the framework of the Act. *If you are unsure if your organisation, or any unit within your organisation, has an existing connectivity agreement, you may contact us and we will see whether any application has been made and if an agreement has been signed.*

If your organisation already has an agreement with us, we will continue to use that agreement and to provide the specified access to our services until migration to AOC certification has taken place.

*For the time being, no action is required on your part. However, we will be unable to provide access to any datasets not already included and approved by **data owners** in your current agreement and we will not be able to approve any new access requests by **accredited researchers**.*

However, we will be beginning the transition to certification for existing agreements. We will contact you and make arrangements for your organisation to implement the necessary registers and procedures to achieve certification in an orderly fashion. If you need help with that process, our team will assist you to make the transition as smooth as possible. Generally, that transition will not affect any access by **accredited researchers** nor restrict their ability to work on their approved projects. We will have all transitions completed by June 30th 2020 at the latest.

If your organisation has already applied for connectivity under existing policies, but no agreement has yet been signed, we will work with you to make the application under the **AOC framework**. In some cases, where agreements have been negotiated but not formally signed, we may allow connectivity for a limited time (up to three months) while we work with you to transition the negotiated agreement to meet the AOC framework standards. Again, that transition should not affect any access by **accredited researchers** nor restrict their ability to work on their approved projects.

If you have any questions or concerns about existing agreements or applications, please do not hesitate to contact research.support@ons.gov.uk and we will make sure that we discuss them with you as soon as possible.