

Secure Remote Access Service (SRAS) Application Form Advice Notes

1. If you are unsure if you have an Encryption System installed, please select "No".
2. Staff should use this section to advise Digital Services why they require the service.
Examples are as follows:
 - Access via web browser to Active Directory fileshares and secure access to University online systems and services when in a remote location;
 - Access via a University owned encrypted laptop to full use of University systems, regardless of your physical location.

The applicant should also briefly indicate the business justification for the request such as the benefit to the Faculty or Department.

3. The applicant must ensure that all devices used to connect using SRAS have fully updated University Standard Anti-Virus/Malware, Firewall and other security patches installed. For example, all critical Microsoft patches should be installed via Microsoft Update.
4. SRAS logs will contain date and times of user access in order to meet IT security audit requirements.
5. Users must report the inability to receive text messages on their registered mobile device so that the issue can be investigated.

3rd Party System Owner Responsibilities

6. Once a 3rd party application is received by the IT Service Desk, there is likely to be a need for direct contact between the IT Service Desk and System Owner to understand the full requirements for access on a case-by-case basis. This will include:
 - Agreement to the copying of System Owners on all email communication related to SRAS.
 - Agreeing the duration of access required for support purposes.
 - Provisioning of user accounts with appropriate access controls on systems to be supported by the 3rd Party on behalf of the System Owner.
7. All 3rd Parties who have access to University data need to sign the University's Third Party Processing Agreement. If this has not already been signed prior to applying for SRAS, then this must happen before the SRAS service will be provided. A copy of the signed form will need to be attached to the SRAS request form by the System Owner when sending to the Digital Services IT Service Desk, if not supplied in a previous SRAS application related to the same 3rd Party Organisation. In addition, the Corporate Planning & Governance department have recommended that 3rd parties are supplied with a copy of the University's Data Protection Policy.

Please note: in the case of a 3rd Party organisation making multiple SRAS applications for individual employees, only one copy of the Third Party Processing Agreement is required to be provided by the System Owner along with the application forms.

8. Those 3rd Party supported systems will require **Individual Associate Staff Accounts** to be created for each 3rd Party employee engaged in support, for auditing purposes. This is controlled by the System Owner.

Each individual 3rd party employee will be required to complete a separate SRAS 3rd Party Application Form.

PLEASE NOTE: It is the responsibility of the System Owner to liaise with the IT Service Desk and other Digital Services technical staff as required to ensure that the appropriate Individual Associate Staff Accounts and access controls are provisioned to support the SRAS Application.

Where feasible, the remote system which the 3rd Party user requires access to should be authenticated against Active Directory (AD).

Where non-AD local authentication accounts are to be provided for access to 3rd Party supported systems, this is the sole responsibility of the System Owner to supply.

For further advice, please contact the Digital Services IT Service Desk on 028 9536 7776 or email servicedesk@ulster.ac.uk