# Policy on Cyber Security Assessments and Certifications

| | Version 1 |
|---|---|
| | A University wide policy for the management of Cyber Security Assessments and Certifications<br><br>**the place of useful learning**<br><br>The University of Strathclyde is a charitable body, registered in Scotland, number SC015263 |

| Version control and history | | | |
|---|---|---|---|
| Title | Description | Author | Approval Date |
| Policy on Cyber Security Assessments and Certifications V 0.4 | Draft for Approval by the Information Strategy Committee | Catherine McMillan | Draft for the ISC to approve. Produced 22/1/2024 |
| Policy on Cyber Security Assessments and Certifications V 0.4 | Including additional comment from the CDIO. For re-consultation with the Cyber Security Operational Group and the Information Security Strategic Risk Group | Catherine McMillan | Draft Produced 3/2/2024 |
| Policy on Cyber Security Assessments and Certifications V 0.5 | Including additional comment from the CDIO.<br><br>Adding in delegate for CDIO | Catherine McMillan | Draft Produced 6/2/2024 |
| Policy on Cyber Security Assessments and Certifications V 0.6 | Including additional comment from the CDIO.<br><br>With “the” removed from the University’s formal name in the text but not in the template. | Catherine McMillan | Draft Produced 6/2/2024 |
| Policy on Cyber Security Assessments and Certifications V1.0 | Approved Version | Catherine McMillan | 21/2/2024 |

# Contents

# Policy on Cyber Security Assessments and Certifications

## 1 Background

Different parts of the University will, from time to time, seek to:

- Gain certification for their cyber security stance
- Complete a document or questionnaire for an external partner to allow their cyber security arrangements to be assessed
- Alter their security arrangements to comply with a particular cyber security standard or framework
- Provide a statement to an external partner that the University has or meets a particular standard, framework, or certification
- To take out insurance or similar that requires an assessment of cyber security arrangements

The types of certifications might include Cyber Essentials Plus, ISO 27001, Scottish Government's Cyber Resilience Framework or similar from other governments. Documents and questionnaires might be unique to a particular external funder, research partner, teaching partner or insurer.

Assessing our Cyber Security arrangements can be very complex. Certifications can often cover only a subset of the Institution. This means, for example, if a funder is told that the University has Cyber Essentials Certification, then it is important to ensure that the relevant part of the University is covered. Individual security arrangements can differ in different parts of the organisations. It is vital that the information provided during certification processes, or to external partners is correct, even when that information is highly technical and presents a complex situation.

Some of the information that must be included in such certifications or assessments can only be centrally provided by Information Services, other information must be provided locally. The Chief Digital and Information Officer (CDIO) must have oversight of all certifications and assessments.

This policy aims to avoid any misunderstandings or unintentional inaccuracies in the information provided to certification bodies, external partners and insurers while ensuring that high-level oversight.

## 2 Policy

- All cyber security certifications must be signed off by the CDIO (or their delegate)
- All questionnaires and information relating to Cyber Security for external partners must be approved by the CDIO (or their delegate)
- Certification bodies and assessors must be agreed in advance with the ISD Cyber Security Team
- The proposed scope of the certification must be approved by the ISD Cyber Security Team before engaging with an assessor

- Some information to be assessed can only be provided by ISD. The area of the University seeking certification must meet with the ISD Cyber Security team and agree what information should be locally provided.
- No certification should be undertaken, and no questionnaire/document provided relating to Cyber Security arrangements without involving the ISD Cyber Security team.
- Any certificate must include “University of Strathclyde” as the name of the legal body
- No one should provide information to an external partner regarding the University having a particular certification unless ISD has confirmed that the relevant part of the Institution is covered by the scope of that certification.

For any Cyber security assessments or certification, the ISD Cyber Security Team will advise and ensure that appropriate approval processes are followed to ensure the best chance of success. The early involvement of the Cyber Security Team is therefore encouraged.