The Strategic Framework for a Cyber Resilient Scotland

Action Plans (2023-25)

Vision

"*Scotland thrives by being a digitally secure and resilient nation*"

Digital technology is key to Scotland's future. Scottish Ministers' vision is of a Scotland that thrives by being a digitally secure and resilient nation.

There are four outcomes to achieve this vision:

1. People recognise the cyber risks and are well prepared to manage them

2. Businesses and organisations recognise the cyber risks and are well prepared to manage them

3. Digital public services are secure and cyber resilient

4. National cyber incident response arrangements are effective.

The Scottish Government and its partners will work towards realising these outcomes by implementing four Action Plans: public, private and third sector and a learning and skills Action Plan, delivered by the Scottish Government and its partners between 2023 and 2025.

Scottish Government
Riaghaltas na h-Alba

Learning and Skills Action Plan (2023-25)

1. Increase people’s cyber resilience through awareness raising and engagement

1.1. The CyberScotland Partnership[1] continues to amplify trusted advice and guidance from NCSC across Scotland.

1.2. The Scottish Government and its partners further provide accessible cyber resilience awareness messaging for specific groups, with a particular focus on young people, older people, disabled people and people for whom English is not their first language.

1.3. The CyberScotland Partnership continues to establish itself as the key network for communication and awareness raising for Scotland’s wider cyber ecosystem, and leads the delivery of the annual CyberScotland Week, the CyberScotland.com portal, and the suite of information and advice bulletins.

2. Explicitly embed cyber resilience throughout our education and lifelong learning system

2.1. The Scottish Government and its education and skills partners continue to support the training of educators across the entire education and lifelong learning system to better support the development of learners’ cyber resilience.

[1] The CyberScotland Partnership is a collaboration of national partners working together to improve cyber resilience in Scotland.

2.2. The Scottish Government and its education and skills partners encourage the use and development of effective cyber resilience learning and teaching resources across early years and primary schools, in colleges and universities, in community learning and development, and in vocational training.

2.3. The Scottish Government and its partners put in place guidance for parents and carers on how to build their children’s cyber resilience, including through Parent Club Scotland.

2.4. The Scottish Government and its social care partners continue to support the development of social carers’ ability to assist their service users to be more cyber resilient.

3. Increase people's cyber resilience at work

3.1. The Scottish Government and its partners continue to encourage the take up of cyber resilience training for people working at all levels in organisations, from entry roles to senior management and board level.

3.2. The Scottish Government and its skills partners continue to embed cyber resilience competencies within occupational and professional standards.

4. Develop accessible and inclusive cyber security skills training pathways and effective cyber security careers guidance to help ensure that skills supply meets demand

4.1. The Scottish Government and its partners continue to analyse and monitor data relating to Scotland’s cyber security sector, and to skills demand and supply, in order to better support the Scottish cyber security ecosystem.

4.2. Skills Development Scotland, through its Digital Economy Skills Action Plan 2023-2028, and other members of the CyberScotland Partnership, continue to promote cyber security careers and train careers advisers, with particular emphasis on reaching underrepresented groups, including women, people from ethnic minority backgrounds, disabled and neurodivergent people, and those in disadvantaged, rural and remote areas of Scotland.

4.3. The Scottish Government continues to work with academic and skills partners to increase the number and range of cyber security courses, and at the same time increase the number of students from underrepresented groups. The growth in courses will take account of industry need for professional cyber security skills.

4.4. The Scottish Government works with academic, skills and industry partners to increase the number of employers offering cyber security vocational training opportunities, including apprenticeships.

4.5. The Scottish Government works with academic, education and skills partners to upskill educators so that they can deliver cyber security qualifications and learning opportunities effectively.

4.6. The Scottish Government and skills partners support career progression opportunities for people from underrepresented groups, so that there is more diversity in senior cyber security roles in organisations.

4.7. The Scottish Government and skills partners support and promote new professional standards set for the industry by the UK Cyber Security Council and those in other relevant frameworks, such as the Digital, Data and Technology (DDAT) profession.

4.8. The Scottish Government works with its partners to improve the skills of cyber security professionals in Scotland by providing opportunities to gain professional certification.

4.9. The Scottish Government and its partners support access to more reskilling opportunities for those wanting to move into the cyber security profession.

4.10. Universities and innovation centres continue to undertake cyber security and cyber resilience research and regularly engage with the Scottish Government.

4.11. The CyberScotland Partnership and its skills partners continue to encourage the cyber security industry and cyber security employers to take an active role in community learning, school, college and university education to help nurture future talent.