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

Third Sector Action Plan (2023-25)

1. Third sector organisations embed cyber resilience into their governance, policies and processes

1.1. Third sector organisations include cyber resilience within their governance structures, by managing cyber risk as part of business risk and by designating a board member/senior manager responsible for cyber resilience within the organisation.

2. Third sector organisations improve their understanding of cyber risks

2.1. Third sector organisations improve their access to and use of threat intelligence, situational awareness reports and alerts to inform their understanding of risk and mitigation.

2.2. Third sector organisations become active members of the Scottish Cyber Information Network within NCSC's

2.3. Cyber Security Information Sharing Partnership (CISP) (where eligible).

2.4. Third sector advisory and regulatory bodies to embed cyber threat and risk information within their advice and guidance.

3. Third sector organisations advance their cyber assurance by embedding cyber security standards, regulations and compliance

3.1. Third sector organisations adopt appropriate cyber security standards and assurance mechanisms.

3.2. Third sector organisations, with consideration of their risk and threat environment, use the NCSC Small Charities Guide, Cyber Essentials and Cyber Essentials Plus (where applicable) to protect against the most common cyber attacks.

3.3. Third sector organisations use the NCSC Supply Chain Security Guidance to increase their understanding of supply chain risks and establish baseline good practices.

4. Third sector organisations improve their staff's cyber resilient behaviour

4.1. The CyberScotland Partnership[1] supports third sector organisations to access appropriate and relevant cyber resilience training and awareness raising for staff at all levels of the organisation.

5. Third sector organisations increase opportunities for professional development of IT and cyber security staff

5.1. Third sector organisations promote and encourage development opportunities for their cyber security workforce, including:

- ensuring that development opportunities are inclusive
- ensuring that cyber security upskilling and reskilling opportunities are available whenever possible, including the uptake of cyber security apprenticeships
- promoting the adoption of best practice and cyber security professional standards.

6. Third sector organisations prepare for, respond to and recover from cyber incidents

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

6.1. Third sector organisations have effective cyber incident response plans in place and test them at least annually.

6.2. Third sector organisations regularly exercise against the most common cyber attack scenarios at a technical, operational and strategic level through use of NCSC Exercise in a Box.

6.3. Third sector organisations subject to cyber attacks report these to Police Scotland and, for charities, notify the Scottish Charity Regulator (OSCR).

6.4. The CyberScotland Partnership encourage the use of the Incident Response helpline, managed by the Cyber and Fraud Centre Scotland, for advice and support.