Scottish Social Services Council

Cyber resilience

NCSC board toolkit exercise

National Cyber Security Centre (NCSC)

Established in 2016, NCSC supports the most critical organisations in the UK, the wider public sector, industry, small and medium enterprises as well as the general public.

Publishes practical guidance at **www.ncsc.gov.uk**

NCSC Board Toolkit

Originally produced by NCSC to encourage discussions at a senior level.

Leadership happens at all levels and SSSC would like to see every worker asking these questions within their teams and services.

SSSC is working on an accessible version of this toolkit.

NCSC Board Toolkit

1. How do we defend our organisation against phishing attacks?
2. How does our organisation control the use of privileged IT accounts?
3. How do we ensure that our software and devices are up to date?
4. How do we make sure our partners and suppliers protect the information we share with them?
5. What authentication methods are used to control access to systems and data?

SSSC

Q1. How do we defend our organisation against phishing attacks?

- We filter or block incoming phishing emails.
- We ensure external email is marked as external.
- We stop attackers ‘spoofing’ emails.
- We help our staff.
- We limit the impact of phishing attacks that get through.

Q2. How does our organisation control the use of privileged IT accounts?

- We use 'least privilege' when setting up staff accounts.
- We reduce the impact of attacks by controlling privileged accounts.
- We have strong links between our HR processes and the IT account function.

Q3. How do we ensure that our software and devices are up to date?

- We have defined processes to identify, triage, and fix any vulnerabilities within our technical estate.
- We've created an 'End of life plan' for devices and software that are no longer supported.
- Our network architecture minimizes the harm that an attack can cause.
- Make appropriate use of 3rd party or cloud services and focus where you can have most impact.

SSSC

Q4. How do we make sure our partners and suppliers protect the information we share with them?

- We look to gain confidence that our partners are not vulnerable to cyber attack.
- We implement technical controls to protect our systems even if a partner gets compromised.

Q5. What authentication methods are used to control access to systems and data?

- We take measures to encourage the use of sensible passwords.
- We ensure passwords don’t put a disproportionate burden on staff.
- We implement two factor authentication (2FA) where possible.

Scottish Social Services Council

THANK YOU