National Cyber Security Centre
a part of GCHQ

NCSC Service Catalogue for Vaccines & Therapeutics

Advice, Support, & Guidance

Authoritative Technical Guidance

The NCSC provides authoritative technical guidance on key cyber security topics relevant to government, academia and industry.

The NCSC provides sector-specific assessments that set out the cyber security landscape for individual sectors of the economy.

Information for board members

The NCSC can support boards in making progress with cyber security plans.

The NCSC has created a **board toolkit** to guide boards on the cyber security questions they should be asking.

Groups and Events

Cyber Security Information Sharing Partnership (CiSP)

A trusted members-only forum for sharing information and experiences across all industry sectors.

Pharmaceuticals-specific **Trust Groups**

The Pharmaceutical Industry Information Exchange (PIIE) provides a closed space for members to discuss challenges in all areas of protective security (physical, persec and cyber security).

Services

Incident Management

Support to enable organisations to respond to incidents affecting them.

Cyber Essentials

A government backed scheme to help organisations better protect themselves .

Support to **Exercising and Testing**

Support to exercises and tests of cyber security and resilience, including attending the exercise itself.

Exercise in a Box is available to help organisations run their own internal cyber security exercises to identify areas for improvement.

Threat Intelligence

Cyber Security Tools

Logging Made Easy – a way for organisations to create a simple end to end network logging capability.

Early Warning – provides notifications of threat events against an organisation's networks including abuse events and vulnerabilities.

Web check/Mail check – prevents users visiting known bad domains and websites, and provides email security compliance.

Threat Intelligence and Actionable Threat Advisories

Updates on the threat landscape faced by the overall sector and specific technologies at multiple levels of classification.

Timely advice on how organisations can manage/ mitigate specific threats to themselves and their supply chain, including Indicators of Compromise.

National Cyber Security Centre
a part of GCHQ

Useful links (valid as at 18/6/21)

Tools

Early Warning - https://www.earlywarning.service.ncsc.gov.uk/?referrer=engagements

Logging Made Easy – https://www.ncsc.gov.uk/information/logging-made-easy

Exercise in a Box – https://www.ncsc.gov.uk/information/exercise-in-a-box

Mail check - https://www.ncsc.gov.uk/information/mailcheck

Web check - https://www.ncsc.gov.uk/information/web-check

Guidance

Top Tips for Staff for staying safe online - https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available

Ransomware guidance - https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

DoS guidance - https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection

Information sharing and accreditation

All NCSC guidance can be found here: https://www.ncsc.gov.uk/section/advice-guidance/all-topics.

CiSP - https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

PIIE – Contact Simon H for more details (simon.h@ncsc.gov.uk)