National Cyber Security Centre
a part of GCHQ

Assured Cyber Incident Response Scheme Enhanced Level

Working Practices

v1.1

January 2025

A review will take place October – December of each year for publication the following February.

Document Owner

National Cyber Security Centre (NCSC). All material is UK Crown Copyright ©.

Document History

Date	Version	Change
December 2024	1.0	First issue
January 2025	1.1	Update to Security section concerning clearances.

Abbreviations/Definitions

Agreement	Means the "assurance ecosystem agreement" entered into between the NCSC and the Company, including all Schedules, as amended from time to time.
Company (and "Companies" shall be interpreted accordingly)	Means the company which is, or is applying to become, a member of the Scheme.
Customer	Means the organisation which contracts with the Company for the provision of CIR Services.
CIR Head Consultant	Means the person in the Company responsible for the technical delivery of CIR Services.
CIR Service Owner	Means the person in the Company with overall responsibility for the provision of CIR Services.
CIR Service(s)	Means cyber incident response service(s) which provide direct support to organisations when they become victims of a cyber incident.
CIR Team	Means the team of individuals at the Company carrying out the CIR Services.
NCSC	Means the National Cyber Security Centre.
Scheme	Means the Cyber Incident Response Scheme – Enhanced Level.
Scheme Standard	Means the standards which must be met to be part of the Scheme as set out in the 'Assured Cyber Incident Response Scheme – Enhanced Level Scheme Standard' document.
We/Us/Our	Means the NCSC.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

You/Your	Means the Company.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

About the Assured Cyber Incident Response Scheme – Enhanced Level

Scheme Membership Obligations

1. This document sets out certain obligations on all Scheme members and outlines how the NCSC and Scheme members will work together. You must read it in conjunction with the Scheme Standard and the Agreement.

Communications

2. The NCSC's CIR Scheme Management Team prefers to receive email to the inbox ncscindustryassurance@ncsc.gov.uk. The inbox is normally monitored during standard office hours.

Personnel

3. The personnel requirements are laid out in Section A of the Scheme Standard and are the minimum requirements for remaining in the Scheme. Should any of the named personnel change, you must request an edit to your Company information by emailing the NCSC's CIR Scheme Management Team within five working days.

4. You must maintain an accurate organogram of the staff who are regularly involved in your incident response functions and make it available to the NCSC on request.

Subcontractors

5. If you sub-contract you must ensure that all sub-contractors meet any relevant qualification and security clearance requirements set by the Customer, and the requirements set out in the Agreement.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

Buyers' Guide

6. The NCSC has produced a Buyer's Guide which you must supply to all prospective Customers. It explains the differences in assurance between the wo levels, 'Enhanced' and 'Standard' of the CIR scheme and seeks to provide guidance on when each might be appropriate.

7. The Buyers' Guide also explains which aspects of your service the NCSC assures, and which aspects are the Customer's responsibility to check.

Ongoing Membership Obligations and Re-validation

8. In accordance with the Scheme Standard and the Agreement, we will provide you with a template for returning your annual management information report.

9. In addition, we will review every Company's membership of the Scheme every two years, as a minimum, in accordance with the Agreement. We will publish a review schedule and template and will ask you to submit updated case-study-based evidence to show that you routinely work with Customers through all stages of the NCSC's defined incident response lifecycle (available at https://www.ncsc.gov.uk/collection/incident-management/incident-response), and that you continue to meet all aspects of the Scheme Standard. We expect the process to be largely paper based but also reserve the right to interview the CIR Head Consultant.

10. Should a review fail to meet the Scheme Standard, the NCSC will state what remediation outcomes are required and agree a timeframe for achieving an improvement in accordance with the Agreement. Depending on the nature of the improvements, the CIR Head Consultant and CIR Service Owner are accountable for implementing the necessary actions.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

11. The NCSC will proactively seek feedback from Customers on the quality of the CIR Service received and the Customer's satisfaction. In the event of poor feedback or complaints, the NCSC will engage with the Company to seek improvements and resolution, in accordance with the terms in the Agreement.

12. The NCSC expects all Companies to give the best advice to Customers about what activities they believe should be undertaken. However, we recognise that sometimes the Customer either decides not to take the advice or does not wish the Company to undertake particular activities. In such cases, the NCSC will not penalise the Company if it does not meet elements of the Scheme Standard as a result, providing the Company accurately documents the recommendations made, and the Customer's decisions and, wherever possible, reasons for rejecting the recommendations.

Presentation of Information

13. While not mandatory at the point of application, once your Company is a member of the Scheme, you must routinely present information in specific, common formats for interchange with other organisations. This includes:

    a. presenting overall structured Threat Intelligence using the latest version of STiX™ (available https://oasis-open.github.io/cti-documentation/stix/intro.html).
    b. mapping the Tactics, Techniques and Procedures (TTPs) of an attacker to the MITRE ATT&CK® framework (available https://attack.mitre.org/) where the framework contains the TTPs in question.
    c. generating and using SIGMA rules (available https://sigmahq.io/docs/basics/rules.html) for host detection.
    d. generating and using SNORT® rules (available https://www.snort.org/) for network detection.
    e. generating and using YARA Signatures (available https://yara.readthedocs.io/en/stable/) for file and memory artefact identification.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

f. using the Traffic Light Protocol (TLP) as published by FIRST (available https://www.first.org/tlp/).

Security

14. At least one senior person within the CIR Team must hold a Developed Vetting (DV) clearance. If no-one in the CIR Team holds a current DV clearance, the NCSC may be able to sponsor a clearance.

15. We will accept applications from companies with a CIR Team without a DV clearance. If successful they will join the Scheme but will have limited operational access to the NCSC until a DV clearance is completed. An application for DV must be submitted within 2 months of you being accepted into the scheme.

16. The CIR Service Owner is responsible for ensuring all staff and contractor clearances remain valid. Where a clearance is not sponsored by the NCSC, the CIR Service Owner must seek authorisation from the relevant sponsor to use the clearance for Scheme purposes.

17. If a member of staff holding an NCSC-sponsored clearance leaves the Company, their clearance will remain valid for a maximum of three months to allow transfer to an alternative employer or sponsor.

18. In accordance with paragraph 11 of the Scheme Standard, you must maintain an in-date Cyber Essentials Plus certificate for all the systems on which information relating to Customers' engagements is stored and processed. This requirement applies to all Companies joining the Scheme from 1st December 2024. Companies which were Scheme members prior to this date have until 31st March 2025 to upgrade their Cyber Essentials certificate and provide a certificate number to the NCSC's CIR Scheme Management Team.

Social Values and Scheme 'Give Back'

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©

19. All members of the Scheme must apply for the NCSC Cyber League and, if successful, remain active members of the community for the duration of their membership of the Scheme. More information on the NCSC Cyber League is available https://www.ncsc.gov.uk/information/cyber-league.

20. At the request of the NCSC's CIR Scheme Management Team, and as part of the Company's commitment to social value giveback under the Agreement, the Company will put forward one technical speaker to deliver an agreed technical presentation at one event in a given 2-year period.

21. The Company must ensure that they have appropriate representation at events hosted by the NCSC and will ensure they actively participate in matters relating to the Scheme.

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to ncscinfoleg@ncsc.gov.uk. All material is UK Crown Copyright ©