|  |  |  |  |
| --- | --- | --- | --- |
|  | | | |
| NIS Annual Report | | | |
| **Publication date:** | 17 May 2023 | **Contact:** | Cyber Security Team |
| **Team:** | Infrastructure and Security of Supply |
| **Email:** | cybersecurityteam@ofgem.gov.uk |

© Crown copyright 2021

The text of this document may be reproduced (excluding logos) under and in accordance with the terms of the [**Open Government Licence**](http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/).

Without prejudice to the generality of the terms of the Open Government Licence the material that is reproduced must be acknowledged as Crown copyright and the document title of this document must be specified in that acknowledgement.

Any enquiries related to the text of this publication should be sent to Ofgem at:

10 South Colonnade, Canary Wharf, London, E14 4PU. Alternatively, please call Ofgem on 0207 901 7000.

This publication is available at [**www.ofgem.gov.uk**](http://www.ofgem.gov.uk). Any enquiries regarding the use and re-use of this information resource should be sent to: [psi@nationalarchives.gsi.gov.uk](mailto:psi@nationalarchives.gsi.gov.uk)

|  |  |  |
| --- | --- | --- |
| Version number | Date Published | Summary of amendments |
| Version 1 | Issued on 4 October 2021, Call for Input only | Not Applicable. |
| Version 2 | 01 April 2022 | Post consultation closure on 01 Dec 2021 with DGE sector incorporating the responses. |
| Version 2 | Issued on 14 Feb 2023, Call for Input only | Section 1, clause 1.3 added; clause 4.4 embedded document updated; Section 5 clause 5.2 embedded document updated;  Section 7, clause 7.1 added. |
| Version 3 | 28 April 2023 | Section 7 updated. |

**Contents**

[1. Summary of Changes 4](#_Toc131063041)

[2. NIS Reporting Requirement Part A: Overview and Scope Updates 5](#_Toc131063042)

[Scope Declaration 5](#_Toc131063043)

[Scope Change 5](#_Toc131063044)

[NIS Scope 5](#_Toc131063045)

[3. NIS Reporting Requirement Part B: Risk Management Updates 6](#_Toc131063046)

[Risk Management Process Changes 6](#_Toc131063047)

[Risk Tolerance Level Changes 6](#_Toc131063048)

[Risk Assessment Results 6](#_Toc131063049)

[4. NIS Reporting Requirement Part C: NCSC Cyber Assessment Framework Updates 7](#_Toc131063050)

[Target Profile Achievement Date 7](#_Toc131063051)

[CAF Gap Assessment Update 7](#_Toc131063052)

[Other Framework Data 7](#_Toc131063053)

[5. NIS Reporting Requirement Part D: Improvement Plan Updates 8](#_Toc131063054)

[6. NIS Incident Reporting 9](#_Toc131063055)

[7. NIS Annual Report Approval 10](#_Toc131063056)

[8. References 12](#_Toc131063057)

[A. Roles and Responsibilities 13](#_Toc131063058)

1. Summary of Changes
   1. Ofgem’s ‘NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain’ (“the Guidance”) [1] should be used to guide the completion of this template.
   2. **Reporting period:** April [YEAR] to March [YEAR]
   3. [Provide an overview of any major changes that will be detailed within this report. For example, if there is an update on scope, state it here at a high level]. [Also provide a statement for each part of report whether a change has been made for any section when compared to the last submission, please declare the report name and submission date post which no further changes have been made for this current submission for all the following four parts.]

Part A: Overview and Scope Updates –[Declaration statement]

Part B: Risk Management Updates –[Declaration statement]

Part C: NCSC Cyber Assessment Framework Updates –[Declaration statement]

Part D: Improvement Plan Updates –[Declaration statement]

1. NIS Reporting Requirement Part A: Overview and Scope Updates

Scope Declaration

* 1. [Confirm whether i) there have, ii) will be, or iii) have not been a change to scope. Where there has been or will be changes to scope, complete the relevant section below. Otherwise, state N/A for each section.

Scope Change

* 1. The below section details changes in NIS scope since the last reporting period.
  2. [Include changes to scope e.g., from acquisition or merger, sale, addition, decommissioning, descoping. Provide the timelines associated with the change, any impact to capacity, consumers service, rationale for change to scope and any further supporting information.]

NIS Scope

* 1. [Provide your current NIS scope. You should utilise the essential service, functional, system, site and dependencies viewpoints that were developed for the self-assessment. Include full details of any new sites and network and information systems on which the essential service relies, or which are used for the provision of an essential service;

1. NIS Reporting Requirement Part B: Risk Management Updates

Risk Management Process Changes

* 1. [Confirm whether i) there have or ii) have not been any changes to your Risk Management process as described in your self-assessment or previous annual report. Where there is a change, provide details of what this is, the rationale, and state what the impact has been on previous risk assessments performed.]

Risk Tolerance Level Changes

* 1. [Confirm whether i) there have or ii) have not been any changes to the risk tolerance levels. Provide details of what these changes are and supporting rationale for these changes and how this impacts any identified risks]

Risk Assessment Results

* 1. [Confirm whether i) there have or ii) have not been any new risks identified. Where new risks have been identified provide a high-level explanation of these and any recommended treatment plans.]
  2. Use the attached spreadsheet to detail the risks relating to the security of the network and information systems on which your essential service relies, or which are used for the provision of an essential service, together with details of any risk response decisions. All cyber or physical security risks which are being treated as per OES’s risk appetite and are relevant for the reporting period must be included. This should include newly identified risks, and all previously identified risks.]



1. NIS Reporting Requirement Part C: NCSC Cyber Assessment Framework Updates

Target Profile Achievement Date

* 1. The original target date for reaching the target profile was [ENTER DATE].
  2. We are on track for meeting the target date / The new target date is: [ENTER DATE].
  3. The target date has changed because [enter reason for change in date or delete].

CAF Gap Assessment Update

* 1. [Use the attached to provide an assessment against the CAF target profile.]



Other Framework Data

* 1. [Add in any comparable outcome-based frameworks such as the National Institute of Standards and Technology (NIST) Cyber Security Framework if utilised.]

1. NIS Reporting Requirement Part D: Improvement Plan Updates
   1. Provide an update on your improvement plan, clearly highlighting any new or additional initiatives that have been identified since the last report.
   2. See attachment for suggested improvement plan and Gantt chart formats.



1. NIS Incident Reporting
   1. [Confirm whether i) there have or ii) have not been any NIS incidents since the last reporting period.
   2. Please also refer to the relevant Annex of BEIS’s Policy Guidance on the Implementation of the Network and Information Systems Regulations [2], for the Incident Reporting Template.]
2. NIS Annual Report Approval
   1. This condition requires the licensee to send to the Authority an annual assurance statement in relation to the NIS Reporting template and sets out the form of that statement.
      1. The OES must by 31 July in each Year starting from 1 April 2023, send to the Authority an assurance statement that NIS Self-Assessment and/or NIS Annual report:

(a) has been approved by resolution of the OES’s board of directors or, where it is appropriate, by the OES’s most relevant senior management body;

(b) is signed by a director of the OES, or, where it has none, by its appropriate senior manager, pursuant to that resolution in sub-paragraph (a);

* 1. The prescribed form for the assurance statement is as follows:
     1. In accordance with the NIS reporting requirements, the Directors of [OES] ("the designated operator”) hereby certify that for NIS Reporting Year YYYY, in their opinion:

(a) the submitted report represents a fair interpretation of the OES’s NIS obligation as shown in the in the OES’s Self-Assessment/Annual Report;

(b) [OES] have met the Basic Profile or commit to Basic Profile attainment by [DD/MM/YYYY] as set out in section 4.5 of this NIS Self-Assessment and Improvement Report submission.

| **Board Member or Director of the OES** | | | |
| --- | --- | --- | --- |
| **Name** | **Position** | **Signature** | **Date** |
|  |  |  |  |

* 1. The NIS Responsible Officer (NRO) named below confirm that:
* all guidance released by BEIS, NCSC and Ofgem, relating to the NIS Regulations has been circulated and made available to the relevant individuals and third parties involved in the delivery of the essential service.
* the details in this self-assessment have been reviewed and approved by the relevant responsible individuals including the NIS Responsible Officer (NRO).

| **NIS Responsible Officer** | | |
| --- | --- | --- |
| **Name** | **Signature** | **Date** |
|  |  |  |

1. References

[1] Office of Gas and Electricity Markets (2021), NIS Guidance for Downstream Gas and Electricity Operators of Essential Services in Great Britain.

[2] Department for Business, Energy and Industrial Strategy (2018), Security of Network and Information Systems Regulation 2018 Implementation in the Energy Sector for GB (current version), <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721357/FINAL_NIS_Policy_Document_to_the_Energy_Sector_.pdf>

1. Roles and Responsibilities

|  |  |
| --- | --- |
| **Role** | **Named Contact** |
| CEO |  |
| CIO |  |
| CISO |  |
| NIS Responsible Officer (NRO) |  |
| Deputy NIS Responsible Officer (DNRO) |  |
| Cyber Operational Lead (IT) |  |
| Cyber Operational Lead (OT) |  |