GUIDANCE ON THE IMPLEMENTATION OF THE NETWORK AND INFORMATION SYSTEMS (NIS) REGULATIONS 2018

INCIDENT REPORTING REQUIREMENTS

DOCUMENT CONTROL
The only controlled version of this document can be accessed on the DWI Website

Printed copies of this document, together with electronic copies held on local computers and other storage devices are uncontrolled.

CONTENTS

1. INTRODUCTION AND PURPOSE

1.1 The purpose of this Guidance Document is to outline the requirements on water companies, designated as an Operator of Essential Service (OES), to report incidents under the NIS Regulations.

1.2 This includes setting the incident reporting thresholds, defining a significant impact against the essential service, the process to notify a NIS incident and the process to voluntarily report cyber incidents to the NCSC.

1.3 This Guidance has been issued by the Drinking Water Inspectorate (DWI), who undertake the operational responsibilities of the competent authority function, for the sector on behalf of the Secretary of State for Environment, Food and Rural Affairs and Welsh Ministers, and in compliance with regulation 3 of the NIS Regulations 2018.

1.4 Further Guidance Documents are available on the DWI website on the following topics:

- Roles and Responsibilities
- The Cyber Assessment Framework (CAF)
- Inspections (Audits)
- Enforcement

1.5 These Guidance Documents will be amended as required to ensure they remain accurate and up to date. Additional guidance may be added to these documents if necessary or within another individual document if required.

2. NIS DEFINITIONS FOR THE WATER SECTOR

2.1 Regulation 1(2) outlines the following definitions:

- A “NIS incident” is any event having an actual adverse effect on the security of network and information systems. For the water sector an actual adverse effect is defined as a **loss, reduction or impairment** of that system.

- “Network and information systems” are considered to include, electronic communications networks; any device or group of interconnected or related devices which perform automatic processing of digital data; or digital data stored processed, retrieved or transmitted by an electronic network or device. For the water sector this applies to both **Operational Technology (OT) systems and Information Technology (IT)** systems.

- The “essential service” means a service which is essential for the maintenance of critical societal or economic activities. For the water sector the essential service is defined as the **production and delivery of wholesome water**

3. NIS INCIDENT THRESHOLDS FOR MANDATORY REPORTING

3.1 The requirements for an OES to notify a NIS incident to the Competent Authority are outlined in regulation 11(1).

3.2 A NIS incident is any event that has an actual adverse effect on the security of network or information systems that has resulted in a significant impact on the production and delivery of wholesome water.

3.3 A **significant impact** is defined as meeting one of the following thresholds:

- Any unauthorised, malicious or suspicious action (external, internal or otherwise) on a network or information system that directly impacts on the production and delivery of wholesome water, irrespective of whether or not customers are directly affected;

- An operational failure of a network or information system that directly impacts on the production and delivery of wholesome water which leads to a direct effect on customers.

3.4 A direct effect on customers is defined as a direct loss of supply and/or pressure, or a breach of regulation 4 of the Water Supply (Water Quality) Regulations 2016 (as amended) or the Water Supply (Water Quality) Regulations 2018 (Wales)

3.5 It is DWI's intention to capture major disruption on network systems and not routine Business as Usual (BAU) events or brief unplanned outages. A water company may still experience impacts on the essential service, however if it doesn't meet the above thresholds then, where required, these incidents should be reported voluntarily to the NCSC (Section 4).

4. VOLUNTARY REPORTING OF CYBER INCIDENTS

4.1 The NCSC is the national technical authority for cyber related incidents and is the UK's Computer Security Incident Response Team (CSIRT) and the Single Point of Contact (SPOC) under the NIS Regulations.

4.2 To ensure the NCSC can fulfil these functions, water companies should actively report cyber security incidents, to the NCSC even if that incident falls below or hasn't met the NIS incident notification thresholds outlined in Section 3.

4.3 Whilst it is the decision of the company to determine which incidents are notified to NCSC, DWI expects that an OES should not wait until an incident reaches the 'significant impact' threshold before seeking support from the NCSC and other parts of Government in containing and mitigating an incident that could risk affecting the production and delivery of wholesome water.

4.4 The process to notify cyber incidents to NCSC is outlined in Annex 1.

4.5 Whilst there is no regulatory requirement to notifying DWI of cyber incidents that have not met the NIS incident reporting thresholds outlined in Section 3, water companies are actively encouraged to voluntarily report any of the following incident examples to DWI:

- Any Telemetry issue across multiple sites where the company are unable to monitor site information either remotely and locally

- The identification of unauthorised access (external, internal or otherwise) on a network or information system, or physical security assets (including, if applicable, waste water assets) that the company deem to be suspicious but there was no impact on the production and delivery of wholesome water.

4.6 These voluntary notifications will be treated as Information Reports and will assist DWI in building up the level of activity within the sector.

4.7 Water companies will not be penalised under the NIS Regulations for voluntarily submitting an Information Report to DWI.

5. INCIDENT SUPPORT FOR NON CYBER (RESILIENCE) INCIDENTS

5.1 The Secretary of State for Environment, Food and Rural Affairs and/or the Welsh Government will provide support through their existing contingency structures for non-cyber incidents and broader resilience incidents.

5.2 If incident support is required for these types of incidents then the water company should make direct contact with the Secretary of State for Environment, Food and Rural Affairs and/or the Welsh Government to ensure the correct level of response can be provided.

6. NIS REPORTING PROCESS TO THE COMPETENT AUTHORITY

6.1 Notification of a NIS incident should be made **without undue delay and unless it is not feasible, no later than 72 hours** after the OES has been made aware that the incident has occurred. Annex 2 outlines the reporting process for both NIS incidents and voluntary reporting to NCSC.

6.2 Should a NIS incident occur that affects multiple companies, all impacted companies, in scope of the Regulations, is required to individually notify the incident to DWI.

6.3 An OES should use the following procedure to notify a NIS incident:

1. Contact the Inspectorate via telephone, following the order specified in the cascade system (Annex 3)
2. Submit a completed Initial NIS Incident Report (Annex 4), which should be sent via email to dwi.NIS@defra.gsi.gov.uk following this phone call

6.4 Notification of Information Reports do not require companies to make contact via phone but will require a completed Initial NIS Incident Report to be sent via email to dwi.NIS@defra.gsi.gov.uk.

7. COMPLETING THE INITIAL NIS INCIDENT REPORT

7.1 It is recognised that at the time of the incident, the company may not have all the required information to hand. It is also recognised that some of the information, as listed, may not be applicable to every notifiable incident. A company should therefore aim to complete the Initial NIS Incident Report using the knowledge best available at the time.

7.2 Examples of the type of information OES should include is outlined below:

Detail	Required Information in Report
Company Name	Name of notifying company
Incident Type	Whether the incident is a Reportable Incident or an Information Report
Date and Time	Date and Time when incident was identified
Incident Duration	Duration or estimated duration (hours/days)
Description of Incident	Brief outline of the incident and the possible cause - Unauthorised Use/Access, Malicious Code, Internal issue
Impact of the Incident	Information around what systems have been impacted, what is the impact within company, have back-up systems been affected
Company Mitigation	Outline initial mitigation measures, running on back up data, moved to DR site, removed asset from supply
Customer Impact	Will customers be affected, if so please provide rough estimate of numbers
Any, or any likely, cross-border impact	Company only, Sector only, Wider impact
Media Interest	Has the incident attracted any local/national media attention
Other Agencies notified	Please specify e.g. NCSC, police
Has this triggered a Water Quality event notification	Yes/No

8. FURTHER REPORTING REQUIREMENTS

8.1 DWI will notify the Secretary of State for Environment, Food and Rural Affairs and/or the Welsh Government of any incident that is notified under the NIS Regulations. DWI will also notify other Devolved Administrations if the incident has the potential to significantly impact on the continuity of the essential service within that Devolved Administration.

8.2 DWI also has a duty under regulation (11)(5)(b) to share the information provided by the OES during a NIS incident with the CSIRT (NCSC) as soon as reasonably practicable.

8.3 If, after notification to the CSIRT, the incident has the potential to significantly impact on the continuity of the essential service of other Member States then the CSIRT will inform the relevant authorities in that Member State. However the CSIRT is not required to inform other Member States in this way if the information submitted is deemed confidential by the OES and/or prejudice the security or commercial interests of the OES.

8.4 After receipt of the notification, DWI and/or the CSIRT will inform the public about the NIS incident only if it is of the view that public awareness is necessary in order to handle that incident or prevent a future incident. In this instance the DWI and/or the CSIRT will consult each other, and the OES who provided the notification, before making a final decision to undertake this action.

8.5 Under regulation 11(9), DWI will provide a report to the SPOC (NCSC) outlining the number and nature of NIS incidents notified on an annual basis.

8.6 For the purpose of the NIS Regulations, the NCSC will be undertaking the role of both the SPOC and the CSIRT.

9. ASSESSMENT OF NIS INCIDENTS AFTER THE INITIAL NOTIFICATION

9.1 The Initial Notification is designed to ensure the OES meets the requirements under regulation 11(3b) however DWI has duties under regulation 11(5) to assess what further action, if any, is required regarding the incident.

9.2 The purpose of the assessment is to: i) establish the cause of the incident and whether the incident was preventable; ii) assess whether effective and reasonable risk management was in place; iii) to determine whether the operator had in place appropriate security measures; and iv) assess how the OES responded to and managed the incident.

9.3 An OES must submit to DWI, a Final Report within 20 working days of the date of notification. The Final Report should build on the information submitted in the Initial Notification and include as a minimum:

- A complete overview of the incident including any additional company investigations into the cause, impact and nature of the incident
- Details of any lessons learnt from the event and actions taken or being taken to prevent a recurrence of the event
- Estimated timescales of the completion of any mitigating actions
- Any further relevant information that the company feel would aid the assessment of the incident

9.4 Once the investigation has concluded, the DWI will decide on any appropriate next steps, be it no action, advice or formal enforcement action.

9.5 It should be noted that simply having an incident is not in itself an infringement of the NIS Regulations and therefore does not automatically mean enforcement action will be taken. The key factor for determining whether enforcement action should be taken as a result of an incident, is whether or not **appropriate and proportionate** security measures and procedures were in place and being followed. This will come from the post-incident investigation conducted by the DWI.

9.6 Not notifying DWI of an incident that meets the incident notification thresholds would be an infringement of the NIS Regulations.

10. EVENT NOTIFICATIONS UNDER THE WATER SUPPLY (WATER QUALITY) REGULATIONS 2016 (AS AMENDED) OR THE WATER SUPPLY (WATER QUALITY) REGULATIONS 2018 (WALES)

10.1 Water companies, in England and Wales, already notify DWI of any event which, by its nature has, or is likely to adversely affect the quality or sufficiency of the water supplied. This requirement is set out in paragraph 9(1) of the Water Industry (Suppliers' Information) Direction 2017.

10.2 DWI expects that in some cases a reportable incident under the NIS Regulations will also be notified under the requirements outlined in Section 10.1. However, due to the complexity around some NIS related incidents it is recognised that in most cases the first notification will be related to the Water Supply (Water Quality) Regulations

10.3 Both the NIS incident and Water Quality event will be assessed separately and information around actions taken, mitigation required and whether any further action is needed will be outlined in individual assessment letters focusing on the respective Regulations.

10.4 DWI expects that companies should have a clear understanding of when each notification is required and that clear communication channels are set up internally so that the relevant information is included in the respective reporting requirements to ensure compliance with both sets of Regulations

Annex 1: Incident Reporting to NCSC

To ensure the NCSC can fulfil its function as the UK's CSIRT and SPOC under NIS, and provide support with incident response, OES should provide notification of a NIS cyber-security incident to the NCSC at the earliest opportunity.

This will ensure that the NCSC can, if necessary, respond promptly to help mitigate a serious incident, provide technical guidance, issue advice, and provide cross-Government co-ordination of the response. OES should also provide notification of cyber-security incidents to the NCSC that fall below or haven't reached the NIS thresholds. OES should use the following instructions as a guide.

Companies should notify the NCSC when facing a cyber incident which:

A. Requires NCSC's support to manage (in communications this should be marked '**FOR ACTION**'); OR
B. Is of wider interest (in communications this should be marked '**FOR INFORMATION**')

'**FOR ACTION**': The NCSC will provide advice, guidance and where resources allow, support for cyber incidents that:

- Disrupt UK essential services or critical national infrastructure (including any that meet or are likely to meet NIS reporting thresholds); or
- Result in a significant loss of data important to the ongoing operation of the company, including loss of sensitive information or intellectual property; or
- Indicate unauthorised access or malicious software on key IT systems which the company are unable to resolve yourselves.

'**FOR INFORMATION'**: The NCSC is keen to receive notification of incidents that OES (or wider CNI organisations) assess are noteworthy, either at the time or post-investigation. This includes incidents that could:

- Add to NCSC's understanding of adversary activity;
- Inform the advice and guidance that NCSC provide;
- Help to protect other organisations.

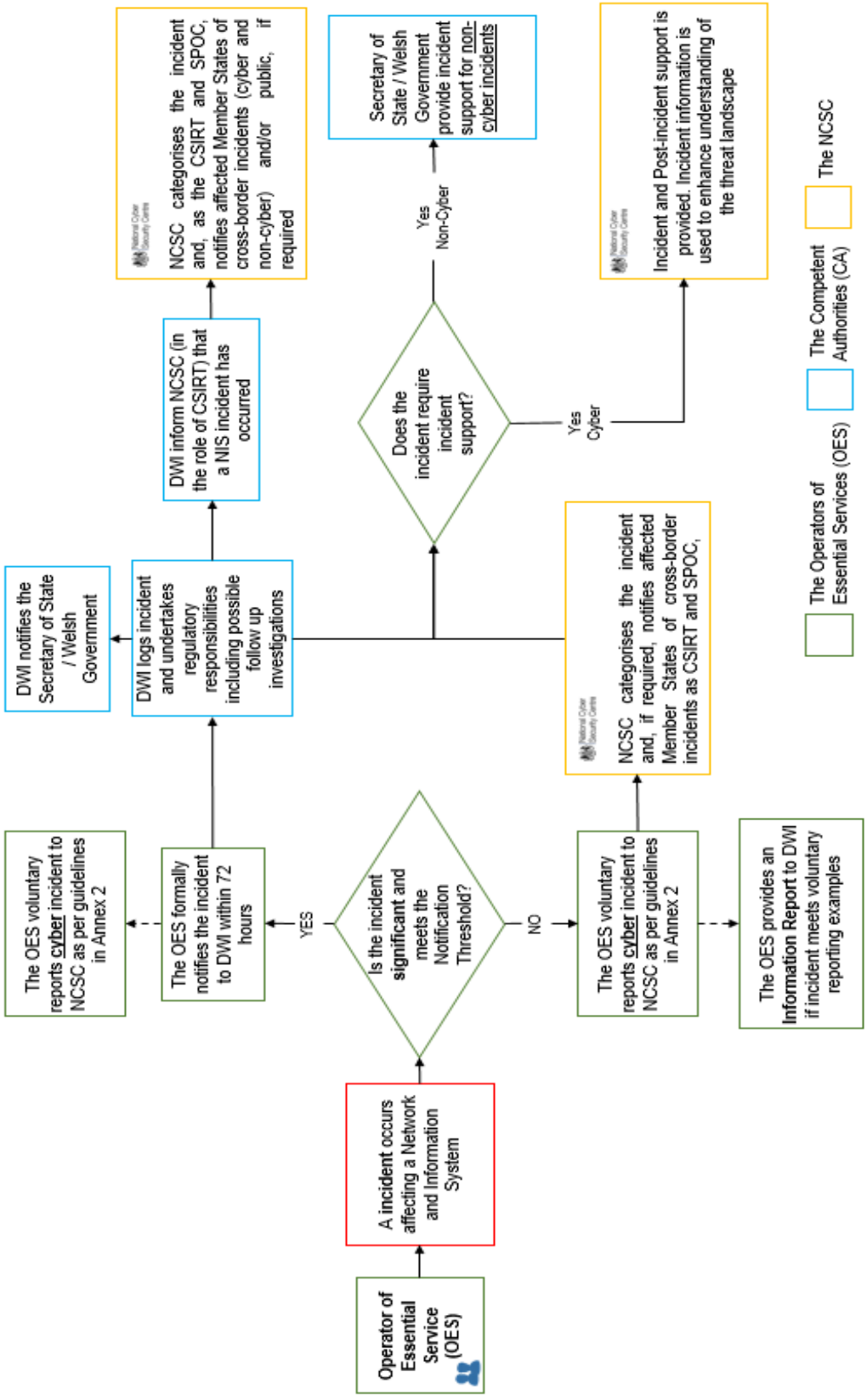
When contacting the NCSC:

1. The NCSC's Incident Management team are contactable on a 24/7 basis (on 0300 020 0973, or incidents@ncsc.gov.uk.)

2. Please put in the header of any messages to NCSC whether the message is '**FOR ACTION**' or '**FOR INFORMATION**'. This will assist with triage and, when appropriate, help to expedite support from the NCSC.

3. Recognising resource constraints, NCSC may only send back an automated response to 'FOR INFORMATION' submissions, but the information will be gratefully received and analysed to help NCSC mitigate threats against the UK.

Annex 2: Reporting Flowchart



Annex 3: Call Cascade for NIS Notifications

Name	Contact Number
Steve Youell	07880 473237
Simon Benton	07909 007356
Mike Turrell	07909 007248
Laura Moss	07747 455889

Annex 4: Initial NIS Incident Report

Initial NIS Incident Report: Required Information	
Company Name	
Incident Type	
Date and Time	
Incident Duration	
Description of Incident	
Impact of the Incident	
Company Mitigation	
Customer Impact	
Any, or any likely, cross-border impact	
Media Interest	
Other Agencies notified	
Has this triggered a Water Quality event notification	