Guidance for Scottish Water on Network and Information Systems (NIS) Regulations 2018

Incident Reporting

Final Version 1.0

04/12/2018

1. Purpose

1.1. The purpose of this Guidance Document is to set out the incident reporting thresholds and the criteria for Scottish Water to be compliant with the NIS Regulations 2018.

1.2. This Guidance has been issued by the Drinking Water Quality Regulator for Scotland in compliance with regulation 3 of the NIS Regulations 2018.

2. Background

2.1. The Network and Information Systems (NIS) Regulations 2018 came into effect on 10 May 2018. These Regulations designate drinking water supply and distribution as an essential service, and as such, Scottish Water has been designated as an Operator of Essential Services (OES).

2.2. These Regulations implement the NIS Directive (EU 2016/1148). They are designed to boost the overall level of security of network and information systems that support the delivery of essential services within the EU.

2.3. The Competent Authority (CA) for the water sector in Scotland is the Drinking Water Quality Regulator for Scotland (DWQR).

2.4. This guidance has been developed by DWQR to set out the process and reporting thresholds that apply to Scottish Water in relation to NIS Incident Reporting. It is the first of a series of guidance notes which will be developed during 2018/19 in relation to the NIS Regulations. The incident thresholds set out in this guidance will be reviewed as required to ensure that they are appropriate and proportionate.

3. NIS Incidents

3.1. A NIS incident is any event that has an actual **adverse effect** on the security of network or information systems and that has resulted in a **significant impact** on the continuity of the essential service. In relation to the provision of drinking water, this means any incident that has resulted in a **significant impact** on the wholesomeness of drinking water and/or the continuity of the supply.

3.2. A NIS incident can be a cyber (e.g. hacking or malware) or non-cyber (fire, flood, hardware related) incident.

3.3. Network and information systems are defined in the NIS Regulations, and 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. They include operational Technology (OT) systems and Information Technology (IT) systems.

3.4. A significant impact on the continuity of the services provided to users is where there is a loss, reduction or impairment in the sufficiency or quality of the drinking water supply that meets specific incident reporting thresholds which are set by DWQR.

3.5. Early notification is strongly encouraged. Where an incident has not yet met the threshold but it is likely or expected that it might meet the threshold at a future point, it should be reported as soon as possible.

3.6. The UK makes a distinction between reporting of incidents affecting network and information systems for incident management purposes which will continue on a **voluntary** basis and **mandatory** notifications under NIS Regulations which meet the defined thresholds. This distinction has been made to ensure that Scottish Water does not wait until an incident reaches the 'significant impact' thresholds before seeking support from National Cyber Security Centre (NCSC) and the Scottish Government in containing and mitigating incidents that risk affecting the supply of drinking water.

3.7. The mandatory incident notifications under the NIS Regulations will sit alongside any voluntary or existing reporting requirements. In general it is expected that Scottish Water will voluntarily report any cyber incidents to the NCSC and the Scottish Government so that they can obtain support and assistance on managing the incident.

4. Incident thresholds

4.1. The Incident thresholds for the water sector in Scotland have been set considering the population affected and the duration of an incident. A significant incident for NIS reporting purposes will include: unauthorised, malicious or suspicious interference with a network or information system ; an operational failure of network or information system which result in:

- the loss of drinking water supply to more than 10,000 consumers lasting for 12 hours or more.
- a reduction in the quality of the drinking water supply to more than 10,000 consumers lasting for 12 hours or more.
- the requirement to issue restrictions over the use of the drinking water supply to more than 100 consumers lasting for 24 hours or more.
- the quality or sufficiency of the drinking water supply to another essential service, such as a hospital.

3.2 If Scottish Water are concerned that a NIS related incident which does not meet these thresholds but should be considered as significant due to specific local circumstances, for example the drinking water supply to a Scottish island or carries the likelihood of media interest, then this should be also reported to DWQR.

3.3 These thresholds do not replace the existing requirement to report all drinking water quality events to DWQR or those that should be reported in accordance with the

Scottish Government's Policy, Guidance and Reporting Framework for Security and Resilience to Scottish Water.

5. Mandatory NIS Incident Notification Requirements to DWQR

4.1. The NIS Regulations require incidents notifications to be reported to DWQR without undue delay and no later than 72 hours after Scottish Water is aware that a reportable incident has occurred.

4.2. Early notification is strongly encouraged. Where an incident has not yet met the threshold but it is likely or expected that it might meet the threshold at a future point, it should be reported as soon as possible.

4.3. The flow chart shown at Annex A sets out the process for both (i) mandatory NIS notifications and (ii) voluntary reporting for incident response/management.

4.4. An incident notification template can be found in Annex B which details the information that should be submitted to the DWQR. Incident reports should be sent to the DWQR at Sue.Petch@gov.scot copied to Rosemary.Greenhill@gov.scot .

4.5. DWQR will inform the NCSC and the Scottish Government of any incident that is notified under the NIS Regulations.

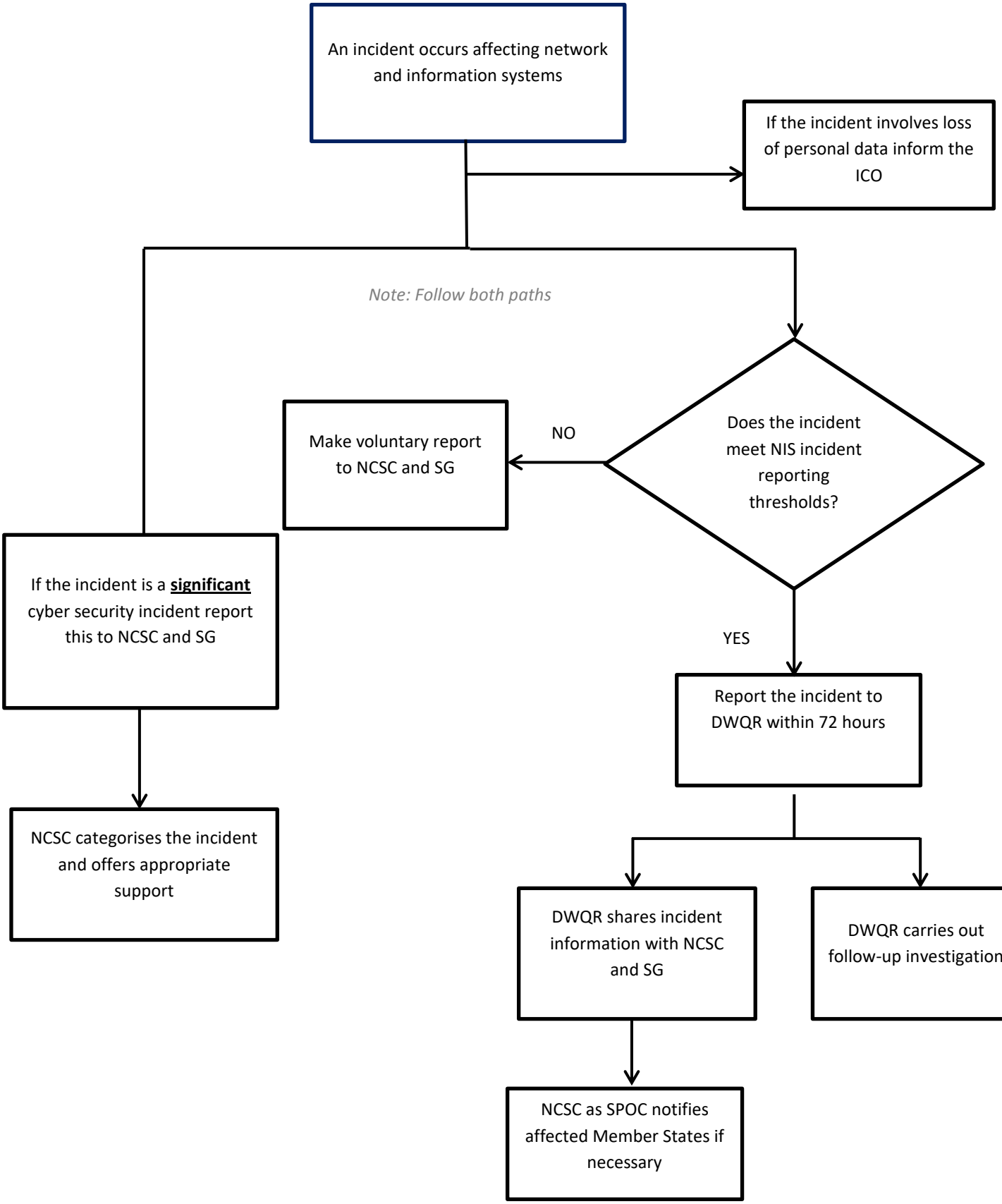
4.6. DWQR will log the incident and decide what follow-up investigation is required. DWQR will also provide an annual report to the Single Point of Contact (SPOC) outlining the number and nature of NIS incidents. The first report was submitted on the I July 2018.

6. Voluntary Reporting for Cyber Incidents

5.1. The NCSC is the national technical authority for cyber related incidents. To ensure the NCSC can fulfil its function as the UK's Computer Security Incident Response Team (CSIRT) and SPOC under the NIS Regulations, Scottish Water should provide voluntary notification to NCSC of any cyber-security incident, even if this falls below the thresholds set out in section 3 of this guidance.

5.2. Scottish Water should also follow existing reporting guidelines produced by the Scottish Government for cyber-security or resilience incidents.

Annex A – NIS Incident notification flowchart



Annex B – NIS Incident Notification Template

NIS Incident Notification	
Contact Details	
Business Details Company Name Internal incident ID number or name	
Date and time incident detected and duration	
Type of incident Cyber/non-cyber/both	
Incident status Detected incident/suspected incident	
Incident stage Ongoing/ended/ongoing but managed	
Summary of Incident, including: Impact to services and/or users Description of the incident How was the incident discovered Location of the incident Services/systems affected Impact on those services/systems Any other relevant information	
What investigations/mitigations have been carried out?	
Who else has been informed?	
What are the planned next steps?	