

# Network and Information Systems Regulations 2018 (NIS) Incident Notification Form

## What is the purpose of this form?

This form is for **Relevant Digital Service Providers** (RDSPs) to notify the ICO of a NIS incident. We will use the information you provide to record the incident and, if necessary, investigate further. You are only required to complete this form if you have access to sufficient information that allows you to assess whether the incident’s impact is substantial.

If you are **not** an RDSP (eg, if you are an operator of essential services/OES), you must report the incident to your competent authority.

If you are an OES that wants to report a personal data breach resulting from a NIS incident, please contact our helpline on **0303 123 1113**.

## Will the information we provide be shared with anyone else?

Under Regulation 12(8) of NIS, the ICO is required to share incident notifications with the [National Cyber Security Centre](https://www.ncsc.gov.uk/) (NCSC) in support of its role as the UK’s computer security incident response team (CSIRT). This also supports the UK’s strategy to prevent cybercrime and to protect organisations and individuals from such crime. We may also share information with law enforcement agencies such as the [National Crime Agency](http://www.nationalcrimeagency.gov.uk/), the [National Fraud Intelligence Bureau](https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/nfib/Pages/default.aspx) and [Regional Cyber Crime Units](https://www.ncsc.gov.uk/information/regional-organised-crime-units-rocus) as appropriate.

Where an incident has a cross-border impact on two or more EU Member States, the ICO may share information with relevant authorities within those States.

As stated by Regulation 12(12), if we (or the NCSC) are of the view that public awareness about the incident is necessary to prevent and/or manage it, or such awareness is in the public interest, we (or the NCSC) may inform the public about the incident or direct you to do so. However, we will consult with you before taking such a decision.

## How do we complete this form?

You should complete and submit this form as soon as possible once an incident has occurred. NIS requires you to notify us without undue delay and no later than 72 hours of becoming aware of an incident. You should provide as much detail as you can, based on the information available to you at the time you notify.

If you don’t know the answer to a question, or you are waiting on the completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant supporting information, eg incident or third party forensic reports.

Before completing this form, you should read the section of our [Guide to NIS on incident reporting](https://ico.org.uk/for-organisations/the-guide-to-nis#reporting).

**You must complete all fields marked with an asterisk (\*) where you have information that allows you to do so.**

## Section A: Your contact details

\* Your name:

\* Your role in the RDSP:

\* Work phone:

\* E-mail Address:

Other useful contact information:

## Section B: Your digital service details

\* Name of your digital service:

\* Address of your head office (or UK nominated representative, if applicable):

\* Your digital service type:

 Online search engine [ ]

 Online marketplace [ ]

 Cloud computing service [ ]

 Multiple digital services (please specify):

Internal incident ID number or name (if applicable):

\* Companies House Registration number:

## Section C: Nature of the incident

\* Date and time the NIS incident occurred:

\* Duration of the NIS incident:

\* Type of incident:

[ ] Cyber (if so, please also complete Section H)

[ ] Non-cyber (if so, please also complete Section I)

[ ] Both (if so, please also complete Sections H and I)

\* Brief description of the incident:

\* Have you identified the root cause of the incident?

[ ] Yes [ ]  No

\* If yes, please describe the cause:

\* How did you discover the incident?

\* What is the current status of the incident?

[ ] Ongoing

[ ] Ended

[ ] Ongoing but managed

\* Please describe the network and information systems affected by the incident and outline the high level function of such systems:

## Section D: Impact of the incident

**Please refer to the incident notification section of the Guide to NIS, as well as the DSP Regulation, if you are uncertain how to complete this section.**

\* Number of users affected:

\* Geographical area affected:

\* Extent of the disruption to the functioning of your service:

\* Extent of the impact on economic and societal activities:

\* Number of user hours your service was unavailable:

\* Has the incident resulted in a loss of integrity, authenticity or confidentiality of stored, transmitted or processed data?

[ ] Yes [ ] No

If yes, please specify:

If yes, how many users were affected by this loss?

\* Has the incident created a risk to public safety, public security or loss of life?

[ ] Yes [ ] No

If yes, please specify:

\* Has the incident caused material damage to at least one user in the EU, where such damage exceeds €1 million?

[ ] Yes [ ] No

If yes, please specify:

\* Do any operators of essential services rely upon your digital service?

[ ] Yes [ ] No

If yes, please specify:

\* Did the incident have a significant impact on the continuity of the essential service(s)?

[ ] Yes [ ] No

 If yes, please provide a description of the impact:

\* Please describe the actions already taken to mitigate the impact of the incident:

\* Please outline any additional steps you intend to take:

## Section E: Cross-border incidents

**You only need to complete this section if the incident affected users in two or more EU Member States.**

\* Do you operate in two or more Member States?

[ ] Yes [ ] No

Please specify:

\* Has the incident had a significant impact on services in another Member State?

[ ] Yes [ ] No [ ] Unknown at time of notification

If yes, please describe the impact:

## Section F: Personal data

\* Did the incident result in, or lead to, a personal data breach?

[ ] Yes [ ] No [ ] Unknown at time of notification

\* If yes, please provide a brief description:

\* If yes, have you reported this as a personal data breach under the GDPR?

[ ] Yes [ ] No

## Section G: Other agencies and external support

\* Have you notified the NCSC of the incident?

[ ] Yes [ ] No

\* If yes, have you requested the NCSC’s support to manage the incident?

[ ] Yes [ ] No

\* Please describe any other external support you have in place:

\* Have you notified any other agencies (eg, National Crime Agency, etc.)?

[ ] Yes [ ] No

\* If the incident was attributable to a malicious actor, has a suspected perpetrator been identified?

[ ] Yes [ ] No

\* If yes, please provide additional details about the type of perpetrator:

## Section H: Additional information – cyber incidents

**NIS requires you to provide any other information that may be useful to us in our investigation. Please complete as much of this section as possible.**

\* Classification of the incident (please indicate all that apply):

[ ] Denial of service attack

[ ] Malware: malware distribution via email (including phishing)

[ ] Malware: malware distribution via websites

[ ] Malware: malware infiltration via mobile devices and/or USB media

[ ] Malware: malware intrusion via network infiltration

[ ] Malware: malware distribution over other or unknown infection vector (if other, please specify):

[ ] Malware: ransomware infection

[ ] Malware: Trojans

[ ] Man-in-the-Middle attack

[ ] Identity theft: phishing

[ ] Identify theft: spoofing

[ ] Identify theft: pharming

[ ] Identify theft: other – please specify:

[ ] Hacking: injection attack

[ ] Hacking: security misconfiguration

[ ] Hacking: broken authentication

[ ] Hacking: other – please specify:

[ ] Exploitation of a known vulnerability or vulnerabilities in components, services and/or applications (please provide an appropriate reference, eg CVE number):

[ ] Cryptographic flaw

[ ] Software malfunction

[ ] Interference with hardware

[ ] Hardware malfunction

[ ] Physical damage

[ ] Loss or theft of equipment

[ ] Other (please specify):

## Section I: Additional information – non-cyber incidents

**NIS requires you to provide any other information that may be useful to us in our investigation. Please complete as much of this section as possible.**

\* Classification of the incident (please indicate all that apply):

[ ] Flood

[ ] Fire

[ ] Equipment failure

[ ] Power failure

[ ] Human error

[ ] Criminal Damage

[ ] Natural disaster – please specify:

[ ] Other – please specify:

## Section J: Any other relevant information

If you have any further information that would be useful to us, please provide it here:

## Next steps

### Sending this form

Please send your completed form to icocasework@ico.org.uk, with ‘NIS incident notification form’ in the subject field. Please note that we cannot guarantee security of forms or any attachments sent by email.

### What happens next?

When we receive this form, we will contact you within seven calendar days to provide:

* a case reference number; and
* information about our next steps.

If you need any help in completing this form, please contact our helpline on
0303 123 1113 (operates 9am to 5pm Monday to Friday).