**Information Security Incident Reporting Form**

**How to complete this form**

# This form should be used by members of NDORMS when reporting any actual or potential information security incidents. It should be completed by the individual who discovered the incident.

This form can be used alongside [IG03: NDORMS Information Security Incident Reporting Procedures](https://intranet.ndorms.ox.ac.uk/information-governance/information-governance-policies/ig03-ndorms-information-security-incident-reporting-procedures).

Once this form is complete, send as an attachment to [infogov@ndorms.ox.ac.uk](mailto:infogov@ndorms.ox.ac.uk) and CC’ in

* Information asset owner (e.g. OCTRU management team, PI, group lead)
* Relevant IT Team ([it@ndorms.ox.ac.uk](mailto:it@ndorms.ox.ac.uk) or [it-support@kennedy.ox.ac.uk](mailto:kirit@kennedy.ox.ac.uk))
* Relevant tech team (e.g. server admin, programmer etc.)
* OXCERT ([oxcert@it.ox.ac.uk](mailto:oxcert@it.ox.ac.uk))

We will review, triage and get back to you in a timely manner. Please be available to answer any questions.

**Reporting timelines**

# It is vital that incidents are reported as soon as possible.

# All data breaches need to be reported within 72 hours under UK GDPR. The sooner a suspected incident is reported, the better we can

|  |  |
| --- | --- |
| **Your Details:** | |
| Name |  |
| Email address |  |

|  |  |
| --- | --- |
| **Incident Details –** *please provide as much detail as possible, but leave blank anything that you are not sure of or you think not applicable to the event.* | |
| Date and time (where possible) incident occurred |  |
| Date and time (where possible) incident discovered |  |
| Do you know if the incident relates to processing of personal data (identified or identifiable)?  *If relating to research data, include project name and name of PI* |  |
| If incident relates to personal data, it should be reported to the University data breach team [data.breach@admin.ox.ac.uk](mailto:data.breach@admin.ox.ac.uk)  *Please confirm time and date of reporting.* |  |
| If incident relates to a server or machine, please provide details including name of any technical staff managing it |  |
| Whydid the security incident happen?  *Please include all details known at the time of completion. e.g. Was the incident accidental or deliberate?* |  |
| Howdid the security incident happen?  *Please include all details known at the time of completion.**e.g. How did the security incident happen? Is there evidence that existing controls failed or were bypassed or that there was a gap.* |  |
| Please provide information about any activity already taken to manage or contain this incident. |  |

As well as completing this form, please keep 'contemporaneous' notes. This will help with providing an account for actions during the incident.