# 1. RESPONSIBILITIES

|  |  |
| --- | --- |
| Received phishing emails targeting University accounts | phishing@it.ox.ac.uk |
| Responded to a phishing email | 1. Your line manager 2. itadmin@servicedesk.medsci.ox.ac.uk*Incidents should be reported directly to the Information Security Team if your local IT Support team does not respond within four working hours.* |
| Opened an attachment which turned out to be malicious or caused suspicious behaviour |
| Malware infection on your work machine  |
| Loss or theft of mobile devices or storage media, e.g. laptops, tablets, mobile phones or USB drives |

* **Head of Administration** is responsible for: ensuring that specific requirements for particular categories of data are recorded in section 3; ensuring that incidents and activities to resolve them are recorded; ensuring that incidents are subsequently reviewed; and implementing improvements to policies and procedures to prevent re-occurrence.
* **Line Managers** are responsible for ensuring staff are aware of these requirements and for escalating incidents as required.
* **IT Support** are responsible for confirming received reports, investigating them, and reporting confirmed incidents to the Information Security Team within 4 working hours.
* **Everyone** is responsible for reporting incidents as per these requirements.
* **The University Information Security Team** is responsible for coordinating the response to, including the escalation of, any breaches of information security.

# 2. Incident response processes

* All suspected information security incidents must be reported in a timely fashion so that they are dealt with effectively and efficiently. If in doubt – report!
* In all cases, if IT support confirm that an information security incident has occurred they are responsible for reporting this to the University Information Security Team via oxcert@it.ox.ac.uk or in urgent cases via phone to (01865 2)82222.
* Should you need out of hours support, the central university IT Service Desk is available 24/7 via (01865 6)12345.

Here are some examples of suspected incidents and who to report them to:

# 3. legal and regulatory requirements

Where incidents may affect the security of particular categories of data, the relevant stakeholders should also be informed. Examples of who to notify in each case are listed below:

|  |  |
| --- | --- |
| Personally identifiable information covered under the Data Protection Act | data.protection@admin.ox.ac.uk  |
| Cardholder Data covered under PCI DSS | cashiers@admin.ox.ac.uk  |