UCL Incident Reporting Form

# Report author

|  |  |
| --- | --- |
| 1. Name
 |  |
| 1. Department
 |  |
| 1. Organisation
 |  |
| 1. Email address
 |  |
| 1. Telephone number
 |  |
| 1. Date
 |  |

# Description of the incident

## Basic details

|  |  |
| --- | --- |
| 1. Give a brief description of the incident
 |  |
| 1. Who is/was managing the incident? Give name, role, and contact details
 |  |
| 1. How would you categorise the incident? Pick the primary category.
 | [ ]  Spam[ ]  Phishing[ ]  Brute force attack[ ]  Malware[ ]  Denial of service attack[ ]  User damaged information[ ]  User leaked information (including copyright infringement)[ ]  User misused UCL resources[ ]  Theft/loss of mobile devices (USB sticks, mobile phones, laptops, tablets etc)[ ]  Theft/loss of non-mobile devices (servers etc)[ ]  Theft/loss of paper based information[ ]  Software failure[ ]  Power failure[ ]  Hardware failure[ ]  Network failure[ ]  Premises break-in[ ]  Act of deity, vandals, or terrorists |
| 1. How many people were affected?
 |  |
| 1. Total time spent investigating/resolving incident (person-hours)
 |  |
| 1. Overall impact of the incident on UCL
 | Very High / High / Medium / Low / Very Low(see Likelihood and Impact Ratings <https://www.ucl.ac.uk/informationsecurity/risk-management>) |

## Timeline

## **Initial investigation and response**

|  |  |
| --- | --- |
| 1. How was the incident discovered?
 |  |
| 1. When?
 |  |
| 1. By whom?
 |  |
| 1. What initial actions were carried out to assess the issue?
 |  |
| * 1. Who carried out these activities?
 |  |
| * 1. When?
 |  |
| 1. Who was informed of the incident?
 |  |
| 1. What immediate response activities have been carried out to limit the impact of the incident?
 |  |
| * 1. Who carried out these activities?
 |  |
| * 1. When?
 |  |
| 1. Were any third parties involved in the investigation or response?
 |  |
| * 1. Who?
 |  |
| * 1. What did they do?
 |  |

## **Current situation**

|  |  |
| --- | --- |
| 1. What is the current status of the incident?
 |  |
| 1. What further investigative/resolving actions are planned, and when?
 |  |

## **Resolution and follow-up**

|  |  |
| --- | --- |
| 1. When was the incident fully resolved?
 |  |
| 1. How was the incident fully resolved?
 |  |
| 1. What is thought to have caused the incident?
 |  |
| 1. What changes can be made to prevent recurrence?
 |  |
| * 1. Have these changes been approved? By whom?
 |  |
| * 1. When will they be implemented?
 |  |

# **Technical details (fill in if relevant)**

## Affected machine(s) (duplicate for each host)

|  |  |
| --- | --- |
| 1. Host name and IP address
 |  |
| 1. Time zone
 |  |
| 1. Function or role of the system (e.g. mail server, desktop pc)
 |  |

## Source(s) of attack if known (duplicate for each host)

|  |  |
| --- | --- |
| 1. Host name and IP address
 |  |
| 1. Time zone
 |  |

**Please return completed form to the UCL Information Security Group at isg(at)ucl.ac.uk.**

# FOR UCL-CERT INTERNAL USE

|  |  |
| --- | --- |
| Timestamp |  |
| Incident reference  |  |