**Report to the *Information Security Manager***

This report should be completed in MS Word, then PDF’d and sent to the Information Security by email, unless the email system is compromised in which case it should be printed, signed and sent as a paper copy.

**TYPES of Information security events**

* Loss of service, functionality, equipment or other facilities
* System, software or hardware malfunctions, unscheduled shutdowns, unexpected system errors or overloads
* Human errors
* Non-compliances with requirements of the ISMS (including uncontrolled system changes)
* Breaches of physical security arrangements
* Access violations

Note: this is not a conclusive list of information security events.

**warning:**

Do not investigate what appears to be an information security event.

Do not attempt to prove an information security weakness.

Do not continue working after observing an information security event or weakness.

Failure to report information security weaknesses or events, and failures to comply with the information security reporting procedure (ISMS-C DOC 16.1.2-3) will be treated as disciplinary offences.

**Name of person making report:**

**Position/role/status:**

**Name and title of line manager:**

**Date and time of report:**

**This report concerns:**

System/information asset description:

*Identifying serial number/asset number/other mark*

**Weakness or event:**

Date and time weakness or event observed:

Observed by whom (if not person making the report):

Description of weakness or event:

[*Please provide as much detailed information as possible: what malfunctioned, what (sequence of) actions you were executing at the time, what messages came up on your screen, what precise things or strange behaviour occurred, what appeared to be the breach or other issue, what services, facilities or equipment ceased to be available, awareness of any human errors or non-compliance with organisational policies, procedures or Work Instructions, or breaches of physical security.*]

**EVENT ASSESSMENT**

Initial analysis:

Event Incident Vulnerability Unknown

Reasons for assessment:

Final analysis

Event Incident Vulnerability Unknown

Reasons for assessment:

Signed: Date:

*(Person making this report)*

The box below is for use by the Information Security Manager.

***Document Owner and Approval***

The Information Security Manager is the owner of this document and is responsible for ensuring that it is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff on the corporate intranet.

This reporting form was approved by the Chief Information Security Officer (CISO (DIRECTOR)) on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature:

Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |