INFORMATION SECURITY DETECTION OR WEAKNESSES AND EVENTS CHECKLIST

REPORT TO THE *Data Protection Officer / GDPR Owner*

TYPES OF INFORMATION SECURITY EVENTS

Loss of service, functionality, equipment or other facilities
System, software or hardware malfunctions, unscheduled shut downs, 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 (GDPR-C DOC 16.1.2-3) will be treated as disciplinary offences.

Name of person making report:

Position/role:

Name and title of line manager:

[Office/location]

Date and time of report:

This report concerns:

System/information asset description:
[Identifying serial number/asset number/system name/other mark if applicable]

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.]

Signed:

(Person making this report)

EVENT ASSESSMENT

Initial analysis:

Event Incident Vulnerability Unknown

Reasons for assessment:

Final analysis
Event Incident Vulnerability Unknown
Reasons for assessment:

Document owner and approver

The Luminate Director of IT is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the GDPR.

A current version of this document is available to all members of the Luminate Education Group.

This procedure is issued on a version controlled basis.

Change History Record

Issue	Description of Change	Date of Policy
1.0	Initial issue	14/11/2017
1.1	Amendment to Luminate Form	12/05/2021
1.2	Annual Review	02/05/2022
1.3	Reviewed – no amendments	12/09/2023
1.4	Annual Review	17/10/2024