Table of Contents

Introduction

Data Security Breaches are increasingly common occurrences whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached. CIOL Qualifications (CIOLQ) is duty bound to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect its information assets as far as possible.

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation of the European Parliament, the Council of the European Union and the European Commission intended to strengthen and unify data protection for all individuals within the European Union (EU). It requires that all organisations publish and maintain a policy on data protection and how personal data is handled.

Scope

This company-wide policy applies to all CIOL Qualifications information, regardless of format, and is applicable to all staff and stakeholders associated with the CIOLQ and data processors acting on behalf of the CIOLQ. It is to be read by all members of staff and 3rd

Responsibility

CIOLQ staff, associates and 3rd parties who have access to data are responsible for reporting actual, suspected, threatened or potential information security breach incidents and for assisting with investigations as required; particularly if urgent action must be taken to prevent further damage.

Departmental Heads are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

The GDPR data team will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan. Suitable delegation may be appropriate in some circumstances.

Data Classification

Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore, it is important to identify quickly, the classification of the data and respond to all reported incidents in a timely and thorough manner.

All reported incidents will need to include the appropriate data classification in order for assessment of risk to be conducted.

The severity and risk associated with a data breach can be found in Appendix C: Evaluation of Incident Severity

Data Security Breach Reporting

External identification

Confirmed or suspected data security breaches should be reported promptly to CIOLQ Head of Qualifications +44 020 7940 3100 or email qualifications@ciol.org.uk The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. Where possible the incident report form should be completed as part of the reporting process.

Once a data breach has been reported an initial assessment will be made to establish the severity of the breach and who the responsible officer to lead should be.

All data security breaches will be centrally logged on the data breach document to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

Internal identification

As External identification with regard to the initial assessment and severity rating. Whether the identification is act

Data Breach Management Plan

The response to any reported data security breach will involve the following four elements:

See Appendix A

1.

Appendix D: Example Format of Timeline of Breach

Actual format is a spreadsheet log stored on the shared drive

Date	Time	Activity	Decision	Authority	Date Authorised
	[redacted]				