iagre.org

Agriculture ■ Forestry ■ Horticulture ■ Environment ■ Amenity

IAgrE

Institution of Agricultural Engineers

Data Security Breach Policy

Author **Alastair Taylor**

Approved Date **10th January 2018**

Approved by the Executive board

1. Background

What is a Data Security Breach?

A data security breach is considered to be any loss of, or unauthorized access to, IAgrE data, normally involving IAgrE Personal or Confidential information. Data security breaches include the loss or theft of data or equipment on which data is stored, inappropriate access controls allowing unauthorized use, human error (e.g. information sent to the incorrect recipient), hacking attacks and 'blagging' where information is obtained by deception.

Managing a Data Security Breach

Data security breaches will vary in impact and risk depending on the content and quantity of data involved, the circumstances of the loss and the speed of response to the incident. Breaches can result in fines of up to £500,000 for loss of personal information and significant reputational damage, and may require substantial time and resources to rectify the breach. The following procedure outlines the main steps in managing a breach and will help ensure that all breaches are dealt with effectively and efficiently.

This procedure outlines the four stages which should be completed following the initial containment of the breach. The individual stages may run concurrently.

2. Record Keeping

Throughout the breach management process records should be kept of what action has been taken and by whom.

3. Security Breach Procedure

Containment & recovery

As soon as a data security breach has been detected or is suspected the following steps should be taken:

- Identify who should lead on investigating and managing the breach
- Establish who (within the Institution) should be aware of the breach.
- Identify and implement any steps required to contain the breach
- Identify and implement any steps required to recover any losses and limit the damage of the breach
- If appropriate inform the police/insurance office

Assessment of risk

All data security breaches must be managed according to their risk. Following the immediate containment of the breach, the risks associated with the breach should be assessed in order to identify an appropriate response.

The checklist in ***Appendix A*** should be used to help identify the exact nature of the breach and the potential severity, this information can then be used to establish the action required.

Notification of breach

Consideration is required as to whether any individuals, third parties or other members should be notified of the breach. This will depend on the nature of the breach, any notification must be carefully managed. Don't be too quick to disclose information before the full extent of the breach is understood; when disclosure is required ensure that it is clear, complete and serves a purpose.

The checklist in ***Appendix B***: Notification of breach checklist should be used to identify potential members who should be notified and to establish what information should be disclosed.

The CEO must be involved in the notification process and no message sent without approval. The Information Commissioner's Office may be notified only after liaison with the University Data Protection Officer.

Evaluation and response

It is important to investigate the causes of the breach and evaluate IAgrE's response to the breach. A brief report on the breach, how it was dealt with and recommendations on how to prevent the breach reoccurring and similar risks should be written. All significant breaches must be reported.

Finally if there are recommended changes to this procedure, such as additional information that would have been helpful or further explanation required these should be communicated to IT Governance and Compliance.

4. Further Resources and Contact Details

Resources

ICO guidance on Data Security Breach Management
Notification of Data Security Breaches to the ICO

Contacts

To report an urgent security breach please contact the IAgrE Secretariat immediately at:

Data Protection Officer
The Institution of Agricultural Engineers
The Bullock Building (Building 53)
University Way
Cranfield
Bedford
MK42 0GH

APPENDIX A: SECURITY BREACH RISK ASSESSMENT CHECKLIST

- What is the nature of the breach? (This information should be as detailed as possible covering what has happened e.g. theft/unauthorised access)
- How did the breach occur?
- What type of Data is involved? (The individual data fields should be identified e.g. name, address, bank account number, commercially sensitive contracts)
- How many individuals or records are involved?
- If the breach involved personal data, who are the individuals? (Students, staff, members etc)?
- What has happened to the data?
- Establish a timeline? (when did the breach occur, when was it detected, who detected the breach, when was the breach isolated? etc)
- Were there any protections in place? (e.g. Encryption)
- What are the potential adverse consequences for individuals or the IAgrE? How serious or substantial are they and how likely are they to occur?
- What could the data tell a third party about an individual, what harm could this cause? What commercial value does the information have?
- What processes/systems are affected and how? (e.g. web page taken off line, access to database restricted)

APPENDIX B: NOTIFICATION OF BREACH CHECKLIST

WHO TO NOTIFY

There should be a purpose to notifying individuals of a breach, it may be that there are steps they need to take to protect themselves, we may be legally or contractually obliged to report breaches to members or we may need to manage potential reputational damage. The following (non exhaustive) list identifies key external stakeholders who may require notification.

- Police – in the case of criminal activity
- Individuals whose data has been compromised
- Information Commissioner's Office (ICO) - There is no legal obligation to inform the
- ICO, but serious breaches should be reported.
- Regulatory bodies
- Others – e.g. banks where steps may be required to protect accounts, press

WHAT TO SAY

Communication and Marketing Services will be able to advise on the content of any message sent. Any notification message should not be sent too quickly, it is important that we understand the extent of the breach and are able to provide useful information, whilst at the same time if there are important steps that individuals need to take this should be communicated promptly.

You should consider including the following:

- Details of what happened and when the breach occurred
- What data was involved
- What steps have been taken to contain the breach and prevent reoccurrence
- Advice on what steps they should take e.g. contact banks
- How will you help and keep them informed (if necessary)
- Provide a way to be contacted