Information Security Incident Reporting Procedure

Introduction

The majority of data security breaches are innocent and unintentional such as the user not 'logging out' of their desktop or laptop computer at the end of the day. However, 'near misses' where no actual harm results from the incident, should still be reported and analysed to look for possible ways of preventing an actual incident occurring in the future and also to ensure that all incidents are identified, reported and monitored

Process

In order to accurately estimate the actual and consequential damage to ABCA Systems if a security breach occurs it is essential that a proper investigation be carried out. This is to establish both the cause of the incident and, if possible, the individual(s) responsible

An incident would indicate one or more of the following:

- Weakness in ABCA Systems Information Security Policy
- non-compliance with company policies and procedures
- weakness in hardware and software controls
- that a new threat has emerged or there are changed risks

It is, therefore, important that every incident is reported.

Any member of staff who observes, becomes aware of, or suspects that a breach of the company Information Security Policy has taken place must immediately report the incident to the Company's DPO.

Definition of an Incident

A security incident may be defined as an event such as a security breach, threat, weakness, vulnerability or malfunction that has, or could have, resulted in the loss or damage of company information assets, including:

E-mail misuse

- Emailing information to a non-secure address (e.g. Hotmail etc.)
- Sending inappropriate content.
- Emailing personal data that isn't secure by password protection or encryption

ID Cards/Warrants/Keys

- Lost, missing, stolen and not returned
- Sharing of ID card with colleagues

Physical security

Wide ranging but consider the following:

- Failed locks
- Windows left open
- Doors wedged open
- Alarms not set
- Not using the shutters on doors and windows

Procedural

- Failure to comply with policy and procedure through lack of awareness
- Deliberate attempts to circumvent security measures

Unauthorised Disclosure

- GDPR breaches

- Unauthorised disclosure of information
- Insecure disposal of personal data

Malicious software

- Unusual or unexplained activity at a system boundary (e.g. potential Denial of Service Attack) should be reported.

NB – successful and regular identification and quarantine of Malware at, or near, a system boundary is not counted as an incident.

Unauthorised access to systems or data

- Access rights incorrectly granted
- Clear Desk/Clear Screen Procedure breached
- Unattended equipment left logged on

Internet misuse

- Breaches of company E-mail and Internet Procedure
- Excessive personal use
- Disclosures on personal social networking sites

Unauthorised person(s) on ABCA premises

- Failure in technical access controls
- Failure in physical access procedures/controls

Account sharing

- Password sharing
- Logged on account used by others
- Non-standard accounts

Loss or theft of assets

Assets can include the following:

- Laptop
- PDA
- Mobile phone
- USB memory stick

Paper Documents

- Loss, including non-delivery by Royal Mail, courier or internal post
- Documents found where they should not have been
- Left insecure on desks, vehicles, public transport etc.

Data Storage

- Where data (including backup material) is not stored within its correct file/network path

Vetting/Personnel

- New employee, contractor or volunteer allowed access to premises, data or systems without the appropriate security clearance

USB related incidents

- Use of private USB memory stick to transfer data
- Unauthorised download/upload of data via USB ports

Unauthorised equipment

- Use of equipment that has not been approved by the DPO e.g. items generally brought from home or bought by the individual or Department without approval from DPO

Unauthorised software

- Commercial software installed without authority/licence
- Use of a cloud based storage system, where date can be transferred from the company network to the cloud, then removed from the cloud to a non-company device

Insecure disposal of non-paper information

Reporting of Incidents

All staff must adopt the following procedure when reporting incidents:

- as an immediate measure a verbal report of the incident must be made to the line manager
- the incident must be recorded via the Incident Reporting form on the Staff Intranet located at https://www.abcaintranet.co.uk/incident-reporting

Reporting of Security Weaknesses

There is a need for every staff member of the company to be vigilant and report any suspected security weaknesses as per the above section.

However, employees are reminded that they should not, under any circumstances, attempt to prove a suspected weakness, particularly those in response of computer systems. This is for their own protection because their action in testing the weakness may be interpreted as a potential misuse of the system.

Reporting of Software/Malfunction/Virus

If it is suspected that a malfunction is due to a malicious piece of computer software, such as a computer virus, the user should:

- note the symptoms and any message appearing on the screen
- stop using the computer and isolate if possible
- inform line manager and SmartIT
- CDs/DVD/USB/Cameras/Card Readers or any other peripherals must not be used on any other computer
- users must not attempt to remove the suspected software
- recovery procedures must only be carried out by SmartIT

Finalisation of Incidents

Before any incident may be finalised all required actions shall be completed or delegated to the appropriate Department as some incidents may highlight the need to review existing procedures. Recommendations shall be made to address all reported incidents.

All incidents will be documented in line with ITP31 Incident Reporting Procedure.

Any breaches must be reported immediately, do not delay in reporting hoping that the breach will go un-noticed, delay in reporting any breaches to the DPR may be classed as a disciplinary offence.