Information Security Policy

Introduction

Focal Point Training and Consultancy Ltd is committed to preserving the confidentially, integrity and availability of information (see note below) we hold and to protecting the information from a range of threats, in order to ensure business continuity, minimise business damage or damage to individuals.

Information takes many forms and includes data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video.

Note: *Confidentiality: ensuring that information is accessible only to authorised individuals.*

Integrity: safeguarding the accuracy and completeness of information and processing methods.

Availability: ensuring that authorised users have access to relevant information when required.

We ensure that

- ☑ Regulatory and legislative requirements will be met
- ☑ Our business continuity plan and information asset log are maintained and reviewed on an annual basis
- ☑ Regular information security briefings and updates will be available to all team members
- ☑ All associate team members are clear what processes to follow when handling information and data on behalf of Focal Point
- ☑ All breaches of information security, actual or suspected, will be reported to, and investigated by, the Directors (see data breach management process below)
- ☑ Our information asset log details what type of data is held where, with security levels and access rights
- ☑ We ask for evidence of Data Protection Legislation compliance for all new suppliers
- ☑ We operate a retention policy based on our obligations and outlined in our Data Register

Responsibilities

All consultants and support team members are directly responsible for implementing the Information Security Policy within their sub contracted roles - there is a set of internal guidelines outlining their responsibilities

Data Breach Management Process

If a breach is identified by us or a 3rd party we will take the following steps:

© Focal Point Training and Consultancy Ltd 2020

1. Containment and Recovery

One of the Directors will lead on investigating the breach.

We will

- ☑ immediately deal with the data breach and take steps to prevent further loss of data
- ☑ identify who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment and recovery exercise. This could be finding a lost piece of equipment or recovering files from back up storage for example
- ☑ if appropriate, inform the police

2. Assessing the Risk

We will initially assess the potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

This will include considering the following

- ☑ What type of data is involved?
- ☑ How sensitive is it?
- ☑ If data has been lost or stolen, are there any protections in place such as encryption?
- ☑ What has happened to the data? If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk
- ☑ What could the data tell a third party about the individual? Could it be used in fraud or identity theft for example
- ☑ How many individuals' personal data are affected by the breach?
- ☑ Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach
- ☑ What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- ☑ Are there wider consequences to consider such as a loss of client confidence in an important service we provide?

3. Notification of Breaches

- ☑ If we assess that there is a need to notify individuals affected, we will notify them and the ICO within 72 hours, where feasible
- ☑ This will include details of how and when the breach occurred and what data was involved and what we have already done to respond to the risks posed by the breach
- ☑ We will also try and give clear advice on the steps individuals can take to protect themselves and also what we can do to help

4. Evaluation and Response

© Focal Point Training and Consultancy Ltd 2020

- ☑ We will investigate why the breach occurred and make recommendations as a result
- ☑ We will ensure recommendations are implemented in a timely way
- ☑ We document our response to and handling of a specific breach using our Data Breach Management Log (spreadsheet)
- ☑ We will review this process annually, along with our business continuity plan and our Information asset log

Communicating the Policy

We ensure that all our associate trainers and support staff have a copy of this policy when they first join our team. All staff will attest annually to their compliance with our data protection and IT policies.

Reviewing the Policy

This policy will be monitored and reviewed annually.

© Focal Point Training and Consultancy Ltd 2020