ISO 27001 Defined Process for Security / Data Breach

Version	Updated By	Date	Change Description
1.0	JPH	01/06/2021	First Release

Introduction

Montgomery and Coupers supplies “SOTERweb” a CAFM / Contractor and Supplier Facilities Management System as a platform for Organisations to Store, Manage and Monitor Organisation, Contractor, Contacts and Estate information and operational requirements and responsibilities.

Purpose

This document sets the Defined Process for Security / Data Breach within the scope of the **SOTER**web System.

Applicability

This document applies to staff who are involved with building and testing of the following areas of **SOTER**web

SDB01 SYSTEM SECURITY / DATA BREACH

SDB01.1 INTRODUCTION.

The General Data Protection Regulation (GDPR) sets out in Article 33 the requirements for notifying the supervisory authority of a personal data breach, and in Article 34 the requirements for communicating a data breach to affected data subjects. The relevant supervisory authority is the Information Commissioner’s Office (ICO).

SDB01.2 DEFINITIONS.

Personal data is defined as “any information relating to an identified or identifiable natural person”. This means information that is about a specific person who can be identified, either from the data or by combining the data with other information.

A breach of personal data is any security incident that results in personal data being accidentally or unlawfully:

- Destroyed, Lost or Altered.
- Disclosed to an unauthorised person.
- Accessed by an unauthorised person.

SDB01.3 BREACH IN THE SOTERweb SYSTEM.

A data breach is an incident where information is stolen or taken from a SOTERweb system without the knowledge or authorisation of the system's owner.

Stolen data may involve sensitive, proprietary, or confidential information, Generally, SOTERweb only stores Name and Email address (Mainly Work Contact email) of people and does not store credit card, bank details etc.

Note: It is under the end user’s responsibility to ensure that no data is entered without the persons permission. It is assumed that majority of data is to be obtained from the Employing Company or Person while attending an Induction or entering the information directly into the system etc.

SDB01.4 PROCESS.

1) REPORT INCIDENT

Report Incident Internally
All SOTERweb staff must report all suspected or possible breaches immediately they learn of them.
The incident is to be reported to a Director of Montgomery and Coupers Ltd.

We must record the details of all breaches in the internal breach register.

The register should include:

- what happened
- what data was affected
- what individuals were affected
- what caused the breach
- the effects and consequences
- what we plan to do to mitigate these effects and consequences
- a timeline of the breach, including when we first became aware of the incident and when we determined that it was a breach
- our decisions regarding notification

2) CONTAIN

Minimise Harm and Secure Data.
The breach is to be secured without delay.

3) ASSESS

Assess Risk to determine any further containment and response.

We will make an assessment of the level of risk posed to the data subjects by the breach. The assessment will consider:

- The type of breach.
- The type of personal data.
- The sensitivity of the personal data.
- The volume of the personal data.
- The number of affected individuals.
- The nature of the processing.
- The ease of identifying individuals.
- The severity of consequences for the individuals.
- The permanence of consequences for the individuals.
- Where there is a breach of confidentiality, the intentions of the persons who have accessed the data. The assessment should conclude that the beach is either:
    - Unlikely to result in a risk to the rights and freedoms of natural persons.
    - Likely to result in a risk to the rights and freedoms of natural persons.
    - Likely to result in a high risk to the rights and freedoms of natural persons.

4) NOTIFY

The following internal parties are to be notified if required upon a Security or Data breach.

Montgomery & Coupers Ltd Internal Staff
T3 Network Solutions Ltd
Easyspace Ltd.
Client SOTERweb system Administrator(s).

Note: the SOTERweb Mass Communication tool can be used to notify users by the end user if required..

5) EVALUATE

Evaluate any improvements to mitigate risk in the future