Information Security Incident Management Policy

Document Type: Policy (Internal)

Version: 1.0

Issue Date: 25th October 2019

Author: Lee Thompson

Contents

1. Context and Overview

Policy prepared by: Lee Thompson
Approved by: Lee Gregson
Policy became operational on: 1st November 2018
Next review date: 30th March 2020

Introduction

This policy explains how information about reporting incidents is provided, who is responsible for reporting, responding and investigating and how these are handled. It applies to everyone who is involved in an actual, suspected, threatened or potential incident which involves data loss or a breach of information security.

Why this policy exists

It is the policy of the company that Information Security incidents will be handled properly, effectively and in a manner that minimises the adverse impact to the company and the risk of data loss to any and all stakeholders.

Scope

This policy applies to all information under the company's control and to all methods of accessing that information.

Oversight

The Quality Assurance Steering Group, chaired by the Managing Director, will monitor the effectiveness of this policy and carry out regular reviews.

Information security incident management principles

The company has adopted the following principles as the foundations of this policy:

1. Incidents are reported in a timely manner and can be properly investigated.
2. Incidents are handled by appropriately authorised and skilled personnel.
3. Appropriate levels of management are involved in the determination of response actions.
4. Incidents are recorded and documented.
5. The impact of the incidents are understood and action is taken to prevent further damage.
6. Evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny.
7. External bodies or data subjects are informed as required.
8. The incidents are dealt with in a timely manner and normal operations restored.
9. The incidents are reviewed to identify improvements in policies and procedures.

The company will provide information on its website, and through other training and communications channels, which explains how information security incidents should be reported and will encourage the reporting of all incidents whether they are actual, suspected, threatened or potential.

2. Responsibilities

Staff who have specific responsibility for receiving information security incident reports and for initiating investigations are:

- The Managing Director
- Members of the Quality Assurance Steering Group
- Nominated members of the Network and Infrastructure Team
- Data Protection Officer (DPO)

Incident reports may be received and escalated by any Head of Department.

All information users are responsible for reporting actual, suspected, threatened and potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

Directors and Heads of Departments are responsible for ensuring that staff in their area act in compliance with this policy and for assisting with investigations as required.

Staff, suppliers, visitors and guests who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

Any breach of information security or violation of this policy must be reported to the Managing Director who will take appropriate action and inform the relevant authorities.

3. Implementation

This policy explains how information about reporting incidents is provided, who is responsible for reporting, responding and investigating and how these are handled. It applies to everyone who is involved in an actual, suspected, threatened or potential incident which involves data loss or a breach of information security.

This potentially includes all staff, associates and anyone else authorised to use company IT facilities and information.

Method Statement

This method statement describes elements to consider and address in the event of data loss or an information security breach. It will assist the company in determining appropriate courses of action if a security breach involving personal or confidential data occurs and dealing with any security breach effectively. It forms part of the company's Information Security and Data Protection policies.

Data loss and security breaches can happen for a number of reasons and occur in different contexts. They may encompass more than personally identifiable information (e.g. trade secrets or intellectual property, denial of service, technical malfunctions).

The company must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal information. A breach management policy constitutes one of these measures and supports the company's obligations under the seven data protection principles where personal information is involved.

Breaches of information security, duties of care, confidentiality and integrity (including inappropriate access to or loss of research and development data) constitute unacceptable conduct. All Employees are to sign a contract binding them to comply with the Rules of Conduct for members of staff and the Terms and Conditions of Employment which stipulates adherence to the company's Data Management and Information Security policies.

Breach Management

Breaches of information security must be reported as soon as discovered and notified in accordance with the reporting protocols and principles detailed in the company's Incident Management Guidance document (below)

Breaches of information security must be reported to the Data Protection Officer who will take appropriate action and inform the relevant authorities (dpo@fulfilmentcrowd.com).

Breach management has four important strategic elements. When a security breach is discovered the priorities are:

1. Containment and recovery, to limit as far as possible any damage.
2. Assess the risks associated with the breach. A risk assessment will help inform decisions about remedial actions and notification.
3. Notifying the appropriate people/organisations that a breach has occurred.
4. Understand the causes and evaluate the effectiveness of its response to the incident, revising as necessary its information security measures in the light of any findings.

Directors and Heads of Departments will work with relevant stakeholders, data protection and security specialists and the Quality Assurance Steering Group to investigate any reported breach in their area of responsibility. They will assist in the timely reporting of breaches and remedial actions to the Managing Director.

Departments holding data supplied by a third-party organisation (e.g. customer), where there is a contractual duty to report an incident to that organisation within a particular timeframe, must respect the reporting timescales and guidelines agreed in the governing agreement or terms of use, having first alerted and (wherever possible) consulted the Managing Director.

The Quality Assurance Steering Group will monitor and review information security incidents to identify recurring incidents and areas of risk. The review process will be used to identify requirements for new or changed policies, to update the company risk register and to identify any other relevant controls. The Managing Director will determine notification to the Information Commissioner's Office (ICO).

Precautions, in the form of a contract, should be taken to protect the information security interests of the company where external organisations or individuals are employed to work on company information systems or provided with or given access to confidential information.

4. Appendix 1 – Definitions

An information security incident

This is defined as an adverse event in relation to the security of company information or IT systems which has already occurred, is suspected, has been threatened or has the potential to occur.

Examples of information security incidents include:

- Data loss due to any cause
- Attempts (either failed or successful) to gain unauthorised access to a system or its data
- Theft or other loss of a laptop, desktop, PDA, or other device that stores company information, whether or not the device is owned by the company.
- Unwanted disruption or denial of service
- Unauthorised use of a system for the processing or storage of data
- Uncontrolled system changes
- Malfunctions of software or hardware
- Noncompliance with information security and acceptable use policies

5. Appendix 2 – Guidance for Information Security Incidents

The guidance outlines important actions and considerations for the investigator(s) when addressing an information security breach that involves personally identifiable information. It supports the method statement on data loss and information security breach management.

Step	Action points	Notes
Containment and recovery		**To contain any breach, to limit further damage as far as possible and to seek to recover any lost data.**
1	Establish lead for investigating breach	To investigate extent and nature of breach, to contact and co-ordinate with specialists and stakeholders (e.g. Data Protection specialist, IT Services, system owners, External Relations).
2	Ensure lead has appropriate resources	Including sufficient time and authority.
3	Ascertain the scope of the breach and if any personal data is involved.	See 'Risk assessment' below.
4	Establish who needs to be made aware of the incident and inform them of what they are expected to do to assist in the containment/recovery exercise.	E.g. Finding lost piece of equipment, changing passwords or access codes, isolating/closing part of network, pulling webpages, informing police, checking any contractual obligations to act/report where data has been supplied under contract (see #19). If you have any reason to suspect that there is computer misuse ("hacking"), contact the Computer Emergency Response Team who will provide advice on actions to take and how to preserve evidence.
5	Ensure that any possibility of further data loss is removed or mitigated as far as possible	As above. This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident.
6	Determine whether anything can be done to recover any losses and limit any damage that may be caused	E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups.
7	Where appropriate, inform the police.	E.g. stolen property, fraudulent activity, offence under Computer Misuse Act.
Risk assessment		**To identify and assess the ongoing risks that may be associated with the breach. In particular: an assessment of (a) potential adverse consequences for individuals, (b) their likelihood, extent and seriousness. Determining the level of risk will help define actions in attempting to mitigate those risks.**
8	What type and volume of data is involved?	Identify the data types (e.g. addresses), record volume and interested third parties
9	How sensitive is the data?	Sensitive personal data? Of a personal nature (e.g. address) or sensitive because of what might happen if misused (e.g. authorised data capture fields).

10	What has happened to the data?	E.g. 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.
11	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of the data and/or device.
12	If the data was damaged/corrupted /lost, were there protections in place to mitigate the impact of the loss?	E.g. back-up tapes/copies, event logs.
Additional assessment for breaches involving personal data		
13	How many individuals' personal data are affected by the breach?	An initial estimation of the record volume should be followed by an empirical analysis or cross-referencing to confirm.
14	Who are the individuals whose data has been compromised?	Customers, prospects, suppliers or staff?
15	What could the data tell a third party about the individual? Could it be misused?	Consider this regardless of what has happened to the data. Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
16	Is there actual/potential harm that could come to any individuals?	E.g. are there risks to: physical safety emotional wellbeing and mental health professional and/or personal reputation finances identity (theft/fraud from release of non-public identifiers) or a combination of these and other private aspects of their life?
17	Are there wider consequences to consider?	E.g. a risk to health or loss of consumer confidence in the services we provide?
18	Are there others who might advise on risks/courses of action?	E.g. If a server has been fraudulently accessed, request guidance from hosting provider or infosec advisors
Notification		**To consider any necessary notification of people and organisations. "Informing interested parties about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions"**
19	Are there any legal, contractual or regulatory requirements to notify?	E.g.: contractual obligations; reporting responsibilities, service provider obligations under Privacy and Electronic Communications Regulations?

20	Can notification help the company meet its security obligations under the seven data protection principles (lawfulness, purpose limitation, data minimisation, accuracy, storage limitation, integrity, accoutability)?	E.g. prevent any unauthorised access, use or damage to the information or loss of it.
21	Can notification help the interested parties?	Could individuals or organisations act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?
22	If a large number of people are affected, or there are very serious consequences, inform the Information Commissioner's Office (through the Data Protection Officer).	Contact and liaise with the DPO.
23	Consider the dangers of 'over notifying'.	Not every incident will warrant notification. For example, notifying a 250,000 customer database of an issue affecting only 500 records may well cause disproportionate enquiries and rectification works.
24	Consider whom to notify, what you will tell them and how you will communicate the message.	There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation. Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach. When notifying individuals or organisations, offer specific and clear advice on the steps they can take to protect themselves and also what the company is willing to do to help them. Provide a way in which they can contact us for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page).
25	Consider how notification can be made appropriate for particular groups of individuals or organisations.	E.g. vulnerable adults, international customers
26	Consult the ICO guidance on when and how to notify it about breaches.	There is not a legal requirement to report security breaches which result in the loss, release or corruption of personal data to the Information Commissioner. Serious breaches should be brought to their attention however. Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the ICO where a large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Cases must be considered on their own merits and there is no precise rule as to what constitutes a large volume of personal data.

27	Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.	E.g. police, insurers, professional bodies, funders, website/system owners, bank/credit card companies.
Evaluation and response		**To evaluate the effectiveness of the company's response to the breach. To learn and apply any lessons or remedies in the light of findings or experience.**
28	Establish where any present or future risks lie.	Within department, platform instance, supplier (e.g. host), infrastructure cell
29	Consider the data and contexts involved.	E.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept.
30	Consider and identify any weak points in existing security measures and procedures.	E.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections.
31	Consider and identify any weak points in levels of security awareness/training.	Raise a Corrective Action that specifies the issue, root cause and rectification that may include training, revised process, disciplinary action, investment or tailored advice.
32	Report on findings and implement recommendations.	Report to Quality Assurance Steering Group.