DATA

BREACH

POLICY

January 2018

ISM OP15

Version 1.0

CONTENTS

1. Background

Data security breaches are increasingly common occurrences whether these are caused through human error or via malicious intent. As technology changes and the creation of data and information grows, there are more emerging ways by which data can be breached. Shift F7 needs to have in place a robust and systematic process for responding to any reported data security breach, to ensure it can act responsibly and protect its information assets as far as possible. This policy should be read in conjunction with the Information Security Incident Procedure (ISO27001:2013).

2. Aim

The aim of this policy is to standardise Shift F7's response to any reported data breach incident, and to ensure that they are appropriately logged and managed in accordance with best practice guidelines.

By adopting a standardised consistent approach to all reported incidents it aims to ensure that:

- Incidents are reported in a timely manner and can be properly investigated.
- Incidents are handled by appropriately authorised and skilled personnel
- Appropriate levels of Shift F7 management are involved in response management.
- Incidents are recorded and documented.
- The impact of the incidents are understood and action is taken to prevent further damage
- Evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny.
- External bodies or data subjects are informed as required.
- The incidents are dealt with in a timely manner and normal operations restored
- The incidents are reviewed to identify improvements in policies and procedures.

3. Definition

A data security breach is considered to be "any loss or unauthorised access to Shift F7 data" Examples of data security breaches may include:

- Loss or theft of data or equipment on which data is stored
- Unauthorised access to confidential or highly confidential Shift F7 data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- Blagging offences where information is obtained by deceit

4. Scope

This Shift F7 policy applies to all Shift F7 information, regardless of format, and is applicable to all staff, visitors and contractors acting on behalf of the company. It is to be read in conjunction with the IS Security Policy and the Information Security Incident Management Procedure.

5. Responsibilities

5.1 Information users

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

5.2 Line Managers

Line Mangers are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

5.3 Directors

The Directors will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan. Suitable delegation may be appropriate in some circumstances.

6. Data Classification

Data Security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that the company is able to quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.

All reported incidents will need to include the appropriate data classification in order for assessment of risk to be conducted. Data classification referred to in this policy means the following approved company Data Categories:

6.1 Public Data:

Information intended for public use, or information which can be made public without any negative impact on Shift F7.

6.2 Internal Data:

Information regarding the day to day business and operation of Shift F7. Primarily for staff use, though some information may be useful to third parties who work with the company.

6.3 Confidential Data:

Information of a more sensitive nature for the business and operations of Shift F7, representing the basic intellectual capital and knowledge. Access should be

limited to only those people that need to know as part of their role within the company.

6.4 Highly Confidential Data:

Information that, if released, will cause significant damage to the company's business activities or reputation, or would lead to a breach of the Data Protection Act. Access to this information should be highly restricted.

7. Data Security Breach Reporting

Confirmed or suspected data security breaches should be reported promptly to the IT Service Desk as the primary point of contact by email. The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved. Where possible the incident report form should be completed as part of the reporting purposes. See **Appendix 1.**

Once a data breach has been reported an initial assessment will be made to establish the severity of the breach and who the lead responsible officer to lead should be. See **Appendix 2.**

All data security breaches will be centrally logged to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes.

8. Data Breach Management Plan

The management response to any reported data security breach will involve the following four elements. See **Appendix 3** for suggested checklist.

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Each of these for elements will need to be conducted in accordance with the check list re: Data Security Breaches. An activity log recording the timeline of the incident management should also be completed. See **Appendix 4.**

9. Authority

Staff, contractors, consultants, 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.

10. Review

The IS Management Team will monitor the effectiveness of this policy and carry out regular reviews of all reported breaches.

Appendix 1: Incident Report Form

Description of the Data breach:	
Time and Date breach was identified and by whom	
Who is reporting the breach: Name/post/Dept	
Contact details: Telephone/Email	
Classification of data breached (in accordance with company security policy) i. Public Data ii. Internal Data iii. Confidential Data iv. Highly confidential Data	
Volume of data involved	
Confirmed or suspected breach?	
Is the breach contained or ongoing?	
If ongoing what actions are being taken to recover the data?	
Who has been informed of the breach?	
Any other relevant information	

Email form to IT Service Desk: help@shiftf7.com

Call 03106 873900 and advise the Information Security Manager or Security Officer.

Received by:	
Date/Time:	

Appendix 2: Evaluation of Incident Severity

The severity of the incident will be assessed per the standard IS Incident Management Procedure (by the IS Service Management team during office hours OR the IS Manager outside office hours). Assessment would be made based upon the following criteria:

High Criticality: Major Incident	**Contact:**
• Highly Confidential/Confidential Data • Personal data breach • External third party data involved • Significant or irreversible consequences • Immediate response required regardless of whether it is contained or not • Requires significant response beyond normal operating procedures	<u>Lead Responsible Officer</u> • Directors <u>Other relevant contacts</u> • Governance and information Compliance • Internal senior managers as required • Contact external parties as required i.e. police/ICO/individuals impacted
Moderate Criticality: Serious Incident	**Contact:**
• Confidential Data • Not contained within Shift F7 • Breach involves personal data of more than 100 individuals • Significant inconvenience will be experienced by individuals impacted • Incident may not yet be contained • Incident does now require notification to company's senior managers /Directors	<u>Lead Responsible Officer</u> • On call IS Manager or Security Officer <u>Other relevant contacts</u> • Registrar • Directors
Low Criticality: Minor Incident	**Contact:**
• Internal or Confidential Data • Small number of individuals involved • Risk to company low • Inconvenience may be suffered by individuals impacted • Loss of data is contained/encrypted • Incident can be responded to during working hours Example: Email sent to wrong recipient Loss of encrypted mobile device	<u>Lead Responsible Officer</u> • IS Manager or Security Officer <u>Other relevant contacts</u> • Directors

Appendix 3: Data Breach Checklist

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Step	Action	Notes
A	**Containment and Recovery:**	**To contain the breach, to limit further damage as far as possible and to seek and recover any lost data.**
1	IS Manager to ascertain the severity of the breach and determine if any personal data is involved.	See Appendix 2
2	IS Manager to identify Lead Responsible Officer for investigating breach and forward a copy of the data breach report	To oversee full investigation and produce report. Ensure lead has appropriate resources including sufficient time and authority. In the event that the breach is severe, the Incident Management Team will be contacted to lead the initial response.
3	Identify the cause of the breach and whether the breach has been contained. Ensure that any possibility of further data loss is removed or mitigated as far as possible.	Establish what steps can or need to be taken to contain the breach from further data loss. Contact all relevant departments who may be able to assist in this process. 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.
4	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.
5	Where appropriate, the Lead Responsible Officer or nominee to inform the police	E.g. stolen property, fraudulent activity, offence under Computer Misuse Act.
6	Ensure all key actions and decisions are logged and recorded on the timeline.	
B	**Assessment of Risks**	**To identify and assess the ongoing risks that may be associated with the breach.**
7	What type and volume of data is involved?	Data Classification/volume of individual data etc.
8	How sensitive is the data?	Sensitive personal data? By virtue of definition within Data Protection Act (e.g. health record) or sensitive because of

		what might happen if misused (banking details).
9	What has happened to the data?	E.g. if data had been stolen, it could be used for purposes which are harmful to the individuals to whom the data relates; if it has been damaged, this poses a different type and level of risk.
10	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of data/device.
11	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
12	How many individuals whose data are affected by breach	
13	Who are the individuals whose data has been compromised?	Staff, customers or suppliers?
14	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.
15	Is there actual/potential harm that could come to any individuals?	E.g. are there risks to : • Physical safety; • Emotional wellbeing; • Reputation; • Finances; • Identify (theft/fraud from release of non-public identifier); • Or a combination of these and other private aspects of their life?
16	Are there wider consequences to consider?	E.g. a risk to public health or loss of public confidence in an important service we provide?
17	Are there others who might advise on risks/courses of action?	E.g. If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.
C	**Consideration of Further Notification**	**Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions.**
18	Are there any legal, contractual or regulatory requirements to notify?	E.g. terms of funding, contractual obligations

19	Can notification help the company meet its security obligations under the seventh data protection principle?	E.g. prevent any unauthorized access, use or damage to the information or loss of it.
20	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?
21	If a large number of people are affected, or there are very serious consequences, inform the police.	Contact and liaise with a Director or a member of the IS Management Team.
22	Consider the dangers of 'over notifying'	Not every incident will warrant notification "and notifying a whole 2 million strong customer base on an issue affecting only 2,000 customers may well cause disproportionate enquiries and work" (example)
23	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 give specific and clear advice on the steps they can take to protect themselves and also what the institution 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).
24	Consult the ISO guidance on when and how to notify it about breaches.	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 IS Team 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.

25	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
D	**Evaluation and Response**	**To evaluate the effectiveness of the Companies response to the breach.**
26	Establish where any present or future risks lie.	
27	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.
28	Consider and identify and 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, system/network protections.
29	Consider and identify and weak points in levels of security awareness/training.	Fill any gaps through training or tailored advice.
30	Report on findings and implement recommendations.	Report to Information Security Management Team.

Appendix 4: Timeline of Incident Management

Date	Time	Activity	Decision	Authority