Veritau Group

Data Security Incident Management Procedure

Contents

PURPOSE 2

SCOPE 2

DEFINITIONS 2

INITIAL REPORTING 3

CONTAINMENT AND RECOVERY - IMMEDIATE ACTION 3

INVESTIGATION AND SUBSEQUENT ACTION 4

Investigation 4

Notification of individuals or other parties affected by the breach 4

The Information Commissioner's Office 5

EVALUATION AND RESPONSE 5

Follow-up 6

ANNEX 1

Risk Assessment Matrix 7

Veritau Group

Data Security Incident Management Procedure

PURPOSE

1 This procedure is intended to help the Veritau group to respond to data security incidents and to minimise the possible impact of any such security breach.

SCOPE

2 This procedure relates to information held by Veritau in its own right, including personal data of which Veritau is the data controller.

3 Incidents relating to information held on behalf of client organisations should be reported in accordance with the relevant policies and response plans of the client in question. It is likely that this will nevertheless require Veritau staff to complete the emergency response, manage and contain the incident, and investigate the circumstances as below, but to report to the client's SIRO rather than the Chief Executive.

4 This procedure must be followed for both actual and potential (near miss) data security incidents. The procedure applies to all employees of Veritau, and any other person working for or engaged by the group.

DEFINITIONS

5 An **Information Asset** is as defined in the Information Governance Policy.

6 An **information security incident** is one that occurs within Veritau or in the course of its operations and causes or introduces a risk to any information asset in whole or in part. That asset may belong to a client or to Veritau. A part of an asset may be as small as a single document or item of data. An incident may either actually cause, or risk causing:

- Unauthorised disclosure of data or information
- Loss or corruption of data or information, or other degradation of an information asset.

7 **Loss** means that the data or information is no longer available. This can be caused by failures in data storage, processing or transmission.

8 **Compromise** means that a security control has been left less effective, so the risk of actual disclosure, data loss or corruption is greater. Any event which could compromise an information asset is an information security incident. Compromise may follow a breach of policy, procedure, legislation or regulation.

9 **Personal data** is data, either on its own or by reference to other information, which identifies a living individual, as defined by the Data Protection Act 2018. An Information Asset may or may not include personal data.

INITIAL REPORTING

To be done on the day the incident occurs or is identified.

10 An employee must report any incident to the Information Governance Team (IGT) as soon as possible. Notification should preferably be done by email to information.governance@veritau.co.uk and the email should be copied to relevant managers, Chief Executive and Deputy Chief Executive.

11 Members of the public might also report an incident, perhaps as part of a complaint. If so the person receiving the complaint should apply this procedure as well as the applicable complaints or customer service procedures.

12 If illegal activity is suspected the Chief Executive or Deputy Chief Executive may decide to refer the matter to the police and/or the Information Commissioner's Office (ICO).

13 The incident will be recorded on the IGT case management system and on the incidents spreadsheet list

CONTAINMENT AND RECOVERY - IMMEDIATE ACTION

To be completed on discovery of the incident, or within no more than two days

14 Managers who have been informed of the incident will liaise with each other to take immediate remedial action to limit the negative consequences for the Group and for the data subject. Actions (which of course may be delegated to others) may include:

- Retrieving the information. Where it is not possible to retrieve the information (for example, the information has been sent by email) assurances should be obtained from an unauthorised recipient that the information has been deleted. The unauthorised recipient should also be requested not to forward the information to anyone else.
- Informing the data subjects. This should be done where the data subject may need to take immediate action to limit further damage (for example where bank account details have been disclosed).
- Implementing immediate actions necessary to prevent further unauthorised disclosures - eg locking storage cupboards and offices.

15 Managers should also consult the Information Governance Team who can offer advice on actions, and help draft messages or requests.

INVESTIGATION AND SUBSEQUENT ACTION

To be completed within two weeks of the occurrence or discovery of the incident

16 Information security incidents will be assessed to determine what further action should be taken. The rating can be changed as the investigation proceeds. See the assessment matrix at Annex 1.

Investigation

17 The purpose of the investigation is to establish all the relevant facts of the case and make recommendations for further action. The Veritau pro-forma report should be used to ensure all aspects are covered. It must be saved as a new document with the appropriate reference number inserted into the header. Issues to consider include (non-exhaustive list) whether:

- equipment was faulty
- information (eg an address) was inaccurate
- procedures or instructions were incorrect, misleading or ambiguous;
- anyone has failed to follow company policy, procedure or instructions, or has acted unreasonably or irrationally
- disciplinary measures are required
- or is there any other fault or error

18 It will be investigated by the manager or AD within whose area of responsibility the incident has occurred. He or she will be supported by the IGT.

19 The investigating officer will consult IT, HR and/or legal specialists as necessary and if necessary also external stakeholders, suppliers and other agencies.

Notification of individuals or other parties affected by the breach

20 Depending on the nature and severity of the breach or incident, data subjects or others affected by the incident may be notified that a breach has occurred. However, notification will only occur where it has a clear purpose. This purpose may be to enable those individuals affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

21 When considering whether to notify those affected, the following should be taken into account:

- Any legal or contractual requirements to notify.
- Whether notification will help the individuals concerned to mitigate the risks.
- How particular groups of individuals, for example, children or vulnerable adults should be notified.
- The dangers associated with notifying those affected. Notification may cause unnecessary anxiety and stress for those affected or may present a health and safety risk for Veritau's employees.

22 Consideration will need to be given as to who to notify, what to tell them and how the notification will be communicated. The decision to notify individuals (or not) should be made by the investigating officer.

23 That person will provide those officers tasked with notifying with clear guidance as to

- what information they are to provide to help reassure the individuals
- how to enable those individuals to take any necessary protective action
- how Veritau will assist them
- who to contact within Veritau for further information.

The Information Commissioner's Office

24 The company has a duty to report serious breaches of security, which may result in the loss, release or corruption of personal data, to the ICO. The ICO has the power to impose fines on organisations that have experienced significant data security breaches.

25 The Chief Executive and/or Deputy Chief Executive are responsible for ensuring security breaches are notified to the ICO. Breaches which satisfy the conditions set out in ICO guidance must be reported to the ICO:

- Where the information is of a particularly sensitive or confidential nature and substantial actual harm, or substantial potential harm, either because of volume of data (5 or more records), its sensitivity or a combination of the two, could result
- Where a particularly large number of individuals are affected (ICO guidance cites in excess of 1,000 individuals as a guide where the data is not particularly sensitive.)
- Where the contravention could have been prevented with appropriate technical and organisational measures, particularly if the risk of a breach had been previously recognised by the company.

26 Other external bodies such as the police, insurers, professional bodies, bank or credit card companies, or trade unions may also need to be informed. The decision on who, if anyone, to inform will be taken by the Chief Executive and/or Deputy Chief Executive.

EVALUATION AND RESPONSE

This stage to be completed within four weeks of the occurrence or discovery of the incident

27 Following the completion of the investigation the investigating manager should report the findings to the Chief Executive.

28 The Chief Executive will consider whether the breach has further implications for the company and what procedural or other actions, if any, could be implemented to improve the security of the information the company holds and to reduce the possibility of a similar breach in the future.

Follow-up

29 The Data Protection Officer will report annually to VMT and include relevant statistics about incidents.

ANNEX 1

Risk Assessment Matrix

This matrix is designed to assess the risk associated with a data breach. Following a breach, please complete the steps below by ticking the boxes that apply.

Step 1

How many individuals' personal information is at risk?	Number of data subjects affected	Score	Selection
	0-10	+0	☐
	11 -50	+1	☐
	51-100	+2	☐
	101 -500	+3	☐
	500 -1000	+4	☐
	1000 or more	+5	☐

Step 2

Sensitivity factors – select each that apply		Score	Selection
Low	Contained no sensitive or confidential personal data.	-1	☐
	The information is already easily accessible or in the public domain, or it would have been published or released under FOI anyway.	-1	☐
	The information is encrypted, and it is therefore unlikely to be viewed.	-1	☐
	It was only disclosed internally, to a trusted professional who is bound by a code of confidentiality and has no personal relationship with the data subject.	-2	☐
	It was disclosed to an external trusted professional (e.g. the police or an NHS trust) which is bound by a code of confidentiality, or to a trusted individual such as a professional colleague who has no relationship with the data subject.	-1	☐
	Individuals identified are in different geographical locations or are unlikely to be known to each other and/or the recipient of the data.	-1	☐
	The information is unlikely to actually identify any individual(s).	-1	☐
High	Breach involves detailed profile information, e.g. work/school performance, salaries or personal life including social media activity, even if no special category data is involved.	+1	☐
	Breach involves high risk confidential or special category information e.g. SEND case or	+1	☐

Sensitivity factors – select each that apply		Score	Selection
	safeguarding notes, spreadsheets of marks or grades obtained, information about individual student discipline or sensitive disclosures, staff health information.		
	The individuals affected are already known to be vulnerable, e.g. victims of a harassment or crime, a child, or family under social service support.	+1	☐
	The individuals affected are likely to be placed at risk of physical harm.	+1	☐
	Wider consequences are envisaged, e.g. embarrassment to the individual, reputational damage or similar effects. They may withdraw from engaging with a public authority's services or other professionals.	+1	☐
	The incident is likely to attract media interest and/or a complaint has been made directly by a member of the public, another organisation or external individual.	+1	☐
	The incident is due to a failure to implement, enforce or follow appropriate organisational or technical safeguards to protect the information.	+1	☐
	There have been one or more previous incidents of a similar type in the last 12 months.	+1	☐
	The breach was a result of targeted malicious/criminal activity such as physical theft or a cyber-attack.	+2	☐

Step 3

Effect of the breach on individuals (select one)		Score	Selection
No negative effects	There is absolute certainty that no negative effects will arise from the breach.	+0	☐
Low	Individuals are unaffected or may experience a few inconveniencies, which they will overcome easily (e.g. time spent re-entering information/changing passwords, annoyances or irritations).	+1	☐
Medium	Individuals may encounter inconveniences, which they will be able to overcome despite a few difficulties (eg inability to access business services, lack of understanding or stress).	+2	☐

Effect of the breach on individuals (select one)		Score	Selection
High	Individuals may encounter significant consequences, which they should be able to overcome but with difficulties (e.g. recoverable or minor financial loss, property damage, factors affecting employment, health issues; risk of harassment, bullying or violence).	+3	☐
Very high	Individuals may encounter significant or even irreversible consequences, which they may not overcome (eg substantial debt or inability to work, loss of employment, long-term psychological or physical ill health, death or death threats).	+4	☐

Step 4

Likelihood that negative effects will occur (select one)			
Likelihood	**Description**	**Score**	**Selection**
Will not occur	There is absolute certainty of no negative effects. This rarely applies, and never applies to breaches involving vulnerable groups. If using this, provide evidence.	-2	☐
Not likely	There is a small possibility of a negative effect, but no evidence to rule out negative effects altogether.	+1	☐
Likely	It is fairly likely that a negative effect could occur as a result of the breach.	+2	☐
Highly likely	There is reasonable certainty that a negative effect will occur either shortly or at some point in the future.	+3	☐
Occurred	The negative effect arising from the breach has already occurred and is known.	+4	☐

Step 5

This step is only relevant if an employee obtained, accessed, edited or destroyed data when they do not have authorisation to do so.

If this is step not relevant, continue to the next section.

Staff actions and behaviour			
Factor	**Description**	**Score**	**Selection**
Intentional	The individual was not authorised to view the information but deliberately opened or searched for the data.	+3	☐
Accidental	The individual was not authorised to view the information, but accidentally opened the data in the course of their duties.	+1	☐
No pre-existing knowledge of or relationship	The employee does not know the data subject(s) through their work or personal life.	+0	☐
Pre-existing knowledge of or relationship	The employee knows the data subject(s) either through their work or personal life.	+2	☐

Step 6: Risk scoring and rating

Please calculate the total from all the steps above, and record the risk score:

Risk Score	

Based on this score use the table below to identify the risk rating for the incident.

Score	**Risk Rating**
< 2 (including < 0)	**Very Low**
3-5	**Low**
6-8	**Moderate**
9-10	**High**
11+	**Very High**

Step 7: Reporting to individuals and ICO

Below is a table of the suggested reporting requirements indicated for each risk rating.

Risk Rating	Mandatory to inform the data subjects*	Reportable to ICO
Very Low	No	No
Low	No	No
Moderate	No	No
High	No	Yes
Very High	Yes	Yes