Policy Documents

Data Security Breach Policy

Purpose & Aim

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

By adopting a standardised and consistent approach to all reported incidents, this policy aims to ensure that:

- Incidents are reported in a timely manner and can be properly investigated
- Incidents are handled by appropriately authorised and skilled members of staff
- Appropriate levels of 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.

Definition

A data security breach is considered to be "any loss of, or unauthorised access to the company's 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 data
- Equipment failure
- Human error
- Hacking attack
- 'Blagging' offences where information is obtained by deceit

For the purposes of this policy data security breaches include both confirmed and suspected incidents.

Scope

This policy applies to all information connected to the DMC Group, regardless of format. It is applicable to all staff, visitors, contractors and data processors acting on behalf of the company. It is to be read in conjunction with the DMC Group's Information Technology (IT) Policy, as well as the Data Protection Policy.

Responsibilities

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.

Heads of Department

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

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 organisation has the ability to quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner. In order for assessment of risk to be conducted, all reported incidents will need to include the appropriate data classification. Data classification referred to in this policy means the following approved data categories:

Public Data

Information intended for public use, or information which can be made public without any negative impact for the DMC Group.

Internal Data

Information regarding the day-to-day business and operations of the group. Primarily for staff to use, though some information may be useful to third parties who work with the group.

Confidential Data

Information of a more sensitive nature for the business and operations of the Group, 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 Group.

Highly Confidential Data

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

Data Security Breach Reporting

Confirmed or suspected data security breaches should be reported promptly to the Human Resources (HR) and IT department, whichever is more relevant. 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 process. 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.**

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 four elements will need to be conducted in accordance with the checklist for Data Security Breaches. An activity log recording the timeline of the incident management should also be completed. See **Appendix 4.**

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.

References

Information Commissioner:

https://ico.org.uk/media/1562/guidanceondatasecuritybreachmanagement.pdf

Appendix 1 – Incident Report Form:

Description of the Data Breach:	
Time, date & by whom breach was identified:	
Who is reporting the breach: Name, Job Role, Department	
Contact details: Telephone & E-mail	
Classification of data breached: ➢ Public Data ➢ Internal Data ➢ Confidential Data ➢ 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 the IT Service and advise the analyst that a Data Security Breach report form is being sent.

Received by:	
Time & Date:	

Appendix 2 - Evaluation of Incident Severity

Assessment would be made based upon the following criteria:

High Criticality: Major Incident
➢ Highly Confidential/Confidential Data ➢ Personal data breach involves > 1000 individuals ➢ External third party data involved ➢ Significant or irreversible consequences ➢ Likely media coverage ➢ Immediate response required regardless of whether it is contained or not ➢ Requires significant response beyond normal operating procedures
Moderate Criticality: Serious Incident
➢ Confidential Data ➢ 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 not require immediate response ➢ Incident response may require notification to Groups's senior managers
Low Criticality: Minor Incident
➢ Internal or Confidential Data ➢ Small number of individuals involved ➢ Risk to company is low ➢ Inconvenience may be suffered by individuals impacted ➢ Loss of data is contained/encrypted ➢ Incident can be responded to during working hours ➢ Example: e-mail sent to the wrong recipient or loss of encrypted mobile device

Appendix 3 - Data Breach Checklists

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

Step	Action	Notes
A	**Containment & Recovery:**	**To contain any breach, to limit further damage & to seek to recover any lost data.**
1	IT Department to ascertain the severity of the breach and determine if any personal data is involved.	See Appendix 2
2	IT department 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. If personal data has been breached, also contact Br-Data-Protection. If the event is severe, the company's 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 & assess the ongoing risks that may be associated with the breach.**
7	What type & 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 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.
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' personal data are affected by breach?	

13	Who are the individuals whose data has been compromised?	Staff, customers, clients 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 or 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 identifiers) 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 unauthorised 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 Information Commissioner's Office (through the Director of Information).	Contact and liaise with the Director of Legal Services or the Governance and Information Compliance Team.
22	Consider the dangers of 'over notifying'.	Not every incident will warrant notification "and notifying a whole 2 million strong customer-base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work".
23	Consult the ICO 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 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.

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 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,
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, trade unions, website/system owners, bank/credit card companies.
D	**Evaluation & Response**	**To evaluate the effectiveness of the DMC Group's 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 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.
29	Consider and identify any weak points in levels of security awareness/training.	Fill any gaps through training or tailored advice.

Appendix 4 - Timeline of Incident Management

Date	Time	Activity	Decision	Authority

Document Policy Change

This policy can be changed at any time and will be reviewed periodically.

Latest Revisions

Revision 1.1 - 25/01/18

Understanding this Document

If an employee is unsure about any of the terms listed within this document and needs clarity on any aspect, they should raise a private query to their line Manager, Department Head or the Human Resources team.