Data Breach Policy

1. Introduction

Amco FM Limited Ltd holds and processes small amounts of personal data, information that may include personal or confidential information that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security.

Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on service provision, legislative non-compliance, and/or financial costs.

In the event of a data breach or an information security incident, it is vital that appropriate actions are taken to minimise associated risks.

2. Purpose

AMCO FM LIMITED Ltd is obliged under the GDPR to have in place an institutional framework designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility. This Policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across Amco FM Limited.

3. Scope

This Policy relates to all personal and sensitive data held by Amco FM Limited regardless of format.

This Policy applies to all Amco FM Limited staff, students and contractors at Amco FM Limited. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of Amco FM Limited.

The objective of this Policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

4. Responsibilities

All users of Amco FM Limited information assets are required to familiarise themselves and comply with this policy.

All individuals who access, use or manage Amco FM Limited information are responsible for reporting data breach and information security incidents immediately to one of the Directors of the company.

Failure to adhere to this policy will be addressed by necessary disciplinary actions in accordance with Amco FM Limited Staff Disciplinary Procedures and relevant contractor and third party contractual clauses relating to data security.

4. Definition / Types of Breach

For the purpose of this Policy, data security breaches include both confirmed and suspected incidents.

An incident in the context of this Policy is an event or action, which may compromise the confidentiality, integrity or availability of systems or data, accidentally or deliberately, and has caused or has the potential to cause damage to the Amco FM Limited's information assets and/or reputation.

An incident includes but is not restricted to, the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
- Equipment theft or failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system(s)
- Unauthorised disclosure of sensitive / confidential data (e.g. email sent to an incorrect recipient or document posted to an incorrect address or addressee)
- Unauthorised use, access to or modification of data or information systems e.g. sharing of user login details (deliberately or accidentally) to gain unauthorised access or make unauthorised changes to data or information systems.
- Compromised user account (e.g. accidental disclosure of user login details)
- Website defacement
- Hacking attack
- Disruption to or denial of IT services
- Unforeseen circumstances such as a fire or flood
- Human error
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

5. Reporting an incident

Any individual who accesses, uses or manages Amco FM Limited information is responsible for reporting data breach and information security incidents immediately to one of the Directors of the company; martin@amcofm.co.uk or ami@amcofm.co.uk.

If the breach occurs, or is discovered, outside normal working hours, it must be reported as soon as is practicable.

The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information, and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process. See Appendix 1

All staff should be aware that any breach of the GDPR may result in the Amco FM Limited Disciplinary Procedures being instigated.

6. Containment and Recovery

The Director will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

An initial assessment will be made by the Director in liaison with relevant members of staff to establish the severity of the breach and who will take the lead investigating the breach, this will depend on the nature of the breach in some cases it could be the Director.

The Lead Investigation Officer (LIO) will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The LIO will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

The LIO, in liaison with the relevant officer(s) will determine the suitable course of action to be taken to ensure a resolution to the incident.

7. Investigation and Risk Assessment

An investigation will be undertaken by the LIO immediately and wherever possible within 24 hours of the breach being discovered / reported.

The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will take into account the following:

- the nature of the incident
- the type of data involved
- its sensitivity
- the protections are in place (e.g. encryptions)
- what's happened to the data, has it been lost or stolen
- whether the data could be put to any illegal or inappropriate use
- who the individuals are, number of individuals involved and the potential effects on those data subject(s)
- whether there are wider consequences to the breach, e.g. IT services being disrupted or unavailable.

8. Notification

The LIO and the Director will determine who needs to be notified of the breach. The LIO and or the Director must consider notifying third parties such as the police, insurers, bank or credit card companies. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

Every incident will be assessed on a case-by-case basis; however, the following will need to be considered:

- Whether there are any legal/contractual notification requirements
- Whether notification would assist the individual affected, e.g. could they act on the information to mitigate risks?
- Whether notification would help prevent the unauthorised or unlawful use of personal data
- If a large number of people are affected, or there are very serious consequences, whether the Information Commissioner's Office (ICO) should be notified. The ICO will only be notified if personal data is involved. Guidance on when and how to notify ICO is available from their website at: https://ico.org.uk/media/1536/breach_reporting.pdf
- The dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been

taken to mitigate the risks. Individuals will also be provided with a way in which they can contact the AMCO FM LIMITED for further information or to ask questions on what has occurred.

The LIO and or the Director will consider whether a press release is required and to be ready to handle any incoming press enquiries.

All actions will be recorded by the Director.

9. Evaluation and response

Once the initial incident is contained, the Director will carry out a thorough review of the causes of the breach. The report will detail the root cause of the incident and contributory factors, the chronology of events, response actions, recommendations and lessons learned to identify areas that require improvement.

Existing controls will be reviewed to determine if they are adequate and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- Where and how personal data is held and where and how it is stored
- Where the biggest risks lie, and will identify any further potential weak points within its existing measures
- Whether methods of transmission are secure; sharing minimum amount of data necessary
- Identifying weak points within existing security measures
- Staff awareness
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security

Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.

Appendix 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify your line manager immediately, complete Section 1 of this form and email it to one of the directors – martin@amcofm.co.uk or ami@amcofm.co.uk

Section 1: Notification of Data Security Breach	
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details:	
Brief description of any action taken at the time of discovery:	
For use by the Data Protection Officer (Director)	
Received (date):	
Forwarded for action to:	
On (date):	

Section 2: Assessment of Severity	To be completed by the Lead Investigation Officer in consultation with the head of area affected by the breach and if appropriate IT where applicable
Details of the IT systems, equipment, devices, records involved in the security breach:	
Details of information loss:	
What is the nature of the information lost?	
How much data has been lost?	
Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the AMCO FM LIMITED or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	
What is the nature of the sensitivity of the data? Please provide details of any types of information that fall into any of the following categories:	
HIGH RISK personal data	

• Sensitive personal data (as defined in the GDPR) relating to a living, identifiable individual's a) racial or ethnic origin; b) political opinions or religious or philosophical beliefs; c) membership of a trade union; d) physical or mental health or condition or sexual life; e) commission or alleged commission of any offence, or f) Proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.	
• Information that could be used to commit identity fraud such as; personal bank account and other financial information; national identifiers, such as National Insurance Number and copies of passports and visas;	
• Personal information relating to vulnerable adults and children;	
• Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed;	
Security information that would compromise the safety of individuals if disclosed.	

Section 3: Action taken	To be completed by Director and/or Lead Investigation Officer
Incident number: (e.g. year/001)	
Report received by:	
On (date):	
Action taken by LIO/Director:	
Was incident reported to Police?	YES/NO
If YES, notified on (date):	
Follow up action required/recommended:	
Notification to ICO	YES/NO
If YES, notified on (date):	
Details:	
Notification to data subjects	YES/NO
If YES, notified on (date):	
Details:	