MARSTON'S PLC

INCIDENT RESPONSE PLAN

Policy for dealing with Data Security Breaches

Version 1

16 September 2014

The Company must take appropriate measures against data security breaches (including loss or damage to personal information). This Plan, and the effective implementation of it, will help the Company ensure that we are compliant with those obligations. It will also help you understand your obligations and who you should notify if you become aware, or suspect, a data security breach.

Marston's PLC (the "Company")
Incident Response Plan (the "Plan")

CONTENTS

This Plan is split into numbered sections helping you to quickly decide who to report a data security breach to, and what steps that person should then take in relation to that breach.

To help you navigate your way around the Plan, you can <CTRL + click> on the relevant section of the above contents summary. Also, when a page number, or section, is quoted in this Plan, all numbers are also a hyperlinks and you can navigate to the page, or section, referred to by hovering over the number and clicking <CTRL + click>.

Alternatively, please contact any member of the Incident Response Team or your local member of the Data Security Committee for assistance (see section 2b).

1. INTRODUCTION

A data security breach can happen for a number of reasons including:

- Loss or theft of data or equipment on which data is stored
- Computer viruses
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

A data security breach is defined as unauthorised acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by us. Good faith acquisition of personal information by an employee or agent of the Company for business purposes is not a breach, provided that the personal information is not then compromised or subject to unauthorised disclosure.

The Company must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. This Plan, and the effective implementation of it, will help the Company ensure that it is compliant with those obligations. In this Plan, such incidents will be collectively referred to as a "**breach**".

This Plan also outlines the key steps to follow in the event of a breach (whether actual or suspected) and identifies and describes the roles and responsibilities of the Incident Response Team. The Incident Response Team (or relevant team members) is responsible for putting an Incident Management Plan into action.

The Information Commissioners Office (the "**ICO**") is the authority responsible for overseeing data privacy and protection in the UK. The ICO's guidance on data security breach management can be found by clicking HERE.

If you have any queries or comments regarding this Plan, please contact Company Secretariat (Ext 1163) or the IT Service Desk (Ext 1500).

2. INCIDENT RESPONSE TEAM

a) Purpose and remit of the Incident Response Team

The Incident Response Team has been established to provide a quick, effective and orderly response to all breaches. The Team is made up of members of the Data Security Committee who are responsible for helping to raise awareness of data protection and promote good practice throughout the Company.

The Incident Response Team is authorised to take all appropriate steps deemed necessary to contain, mitigate or resolve the breach.

The Incident Response Team is responsible for formulating an Incident Management Plan. This is discussed in more detail below (see section 3) but, in accordance with the ICO's guidance, an Incident Management Plan will involve the following FOUR key stages:

1) **Containment and recovery**
2) **Assessment of ongoing risk**
3) **Notification of breach**
4) **Evaluation and response**

b) Members of the Incident Response Team – WHO SHOULD I CONTACT?

Each of the following members on the next page will have a primary role in any incident response and you should contact ANY named representative, or their alternative contact, IMMEDIATELY after becoming aware of a breach, or you suspect a breach has taken place.

Department	Name and Job Title	Contact Details	Alternative Contact; Name and Job Title	Alternative Contact's contact details
IT	**Richard Cockbill;** Head of Technology Services	IT Service Desk: 1500 or 01902 329500 * **OR** 07971 899003	**Mike McMinn**; Group IT Director	07971 899001
Compliance & Risk	**Jonathan Moore;** Corporate Risk Director	07814 731857	**Gareth Edwards;** Head of Risk, Audit and Compliance	07976382473
Company Secretariat	**Anne-Marie Brennan;** Company Secretary	07976 532348	**Bethan Raybould;** In-house lawyer **Michelle Woodall;** Assistant Company Secretary	07814 213588 07814857653
Human Resources	**Catherine Taylor;** Group HR Director	07581170410	**Alison Shaw** Head of Shared Services	07813695571
Group Finance	**Warwick Congrave;** Group Finance Systems Manager	01902 329549	**Bill Whittaker;** Director of Group Finance	07973 285647

* **NOTE:** The IT Service Desk are open 24/7 therefore to ensure a timely response, the IT Service Desk will act as a central point of contact for reaching the Head of Technology Services. All computer-related incidents or incidents which occur out of hours should be reported to the IT Service Desk in the first instance.

c) Incident Response Team's next steps

Once the relevant member of the Incident Response Team becomes aware, or is notified of a breach, they are responsible for escalating to all other appropriate members of the Incident Response Team and/or the Data Security Committee and/or Executive Management or Board. They should also consider whether it is appropriate to engage external advisors. The current members of the Data Security Committee can be found HERE

The Incident Response Team will, together with all appropriate colleagues, prepare an Incident Management Plan. See the next section for guidance. A template can be found in **SCHEDULE 1.**

3. INCIDENT MANAGEMENT PLAN

Data security breaches will vary in impact and risk depending on the content and quantity of data involved. The implementation of an Incident Management Plan and following the four steps below will help ensure that all breaches are dealt with effectively and efficiently. A template Incident Management Plan can be found in **SCHEDULE 1.**

a) STEP 1 – Containment & Recovery

As soon as a data breach is detected, or reported, immediate steps should be taken to try and contain the situation. The Incident Management Plan at **SCHEDULE 1** includes a Step 1 checklist which will help to establish the following:

- **Who needs to be made aware of the breach** – if you haven't already done so, the appropriate members of the Incident Response Team and, if necessary, the Data Security Committee should be contacted. Consider if specialist legal or technical advice is required.
- **Who should take the lead in investigating the breach** and project managing the investigation. This is likely to be a member of the Incident Response Team or the Data Security Committee. Ensure that person has the appropriate resources and support.
- **Identify and implement any steps required to contain the breach**. This will depend on the nature of the breach and could range from closing a compromised section of the Company's infrastructure or network to changing an alarm code.
- If the breach is an internal computer related incident, or it involves the loss, or compromise, of cardholder/payment data, you should also refer to the Company's PCI Policy (please ask the IT Support Desk or the relevant member of the Data Security Committee for advice).
- Whether there is anything you can do to **recover any losses and limit the damage a breach can cause**.

b) STEP 2 - Assessing the Risks

All breaches must be managed according to the risk that they pose. Following the immediate containment of the breach (Step 1) the risks associated with the breach should be assessed in order to identify and take any appropriate action.

The Incident Management Plan at **SCHEDULE 1** includes a Step 2 checklist which should help identify the exact nature of the breach and the potential adverse consequences for individuals or for the Company. Not all questions on the checklist will be appropriate to every type of breach, but answers to all questions (even if that answer is "not applicable") should be recorded.

c) STEP 3 – Notification

Considering whether or not to inform other Company employees and stakeholders, individuals and other organisations (such as the ICO or our PR Agency) that the Company has experienced a breach is an important element of the Incident Management Plan. This will depend on the nature of the breach and the risks identified in Step 2. In relation to affected individuals, the ICO warns against "over-notification" so the Company should not make a decision until the full extent of the breach is understood.

Informing people 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 and their personal information or to allow the ICO to perform their regulatory functions and deal with complaints.

Answering the questions in Step 3 of the Incident Response Plan at **SCHEDULE 1**should assist the Incident Response Team when determining whether to notify and if so who should be notified.

If notifying affected individuals, there are a number of different ways in which to do this so the Company will need to consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation. Any notification should, at the very least, include a description of how and when the breach occurred, what data was involved, details of what steps the Company has taken to address any risks posed by the breach and advice on the steps an affected individual can take to protect themselves.

If the breach involves personal data and a large number of individuals are affected, or there are very serious consequences, the Company should notify the ICO. The ICO has produced guidance on what information they expect to receive as part of a breach notification and this can be accessed by clicking HERE.

d) STEP 4 – Evaluation & Response

It is important not only to investigate causes of the breach but also to evaluate the effectiveness of the Company's response to it. If the breach was caused, or the response to it hampered by, inadequate policies and procedures, or systematic problems, then containing the breach alone is not acceptable - it is important to review any weaknesses revealed and take all appropriate action.

Communicating and/or sharing lessons learnt will also help to encourage ongoing staff awareness of data security and drive best practice.

To help achieve this, the appropriate person from the Incident Response Team should complete a post-incident report form and this should be communicated to the Data Security Committee. A template post-incident report form appears at **SCHEDULE 2.** The Committee will then have the opportunity to discuss any risks and weaknesses identified, as well as having the opportunity to suggest any solutions. Any "lessons learnt" should be taken away by the individuals on the Data Security Committee and communicated to the part(s) of the Company they are "Data Protection

Champions" for. The Chairman of the Committee should also consider whether it is appropriate to report to the Executive and/or the Board.

4. PCI COMPLIANCE

"PCI" compliance relates to the protection of "Payment Card Information" which the Company's customers may provide to us to pay for goods and services.

In addition to the Company's Incident Management Plan credit card companies may require us to immediately report a security breach that relates to the suspected or confirmed loss or theft of any material or records that contain cardholder data or bank details (please ask the IT Support Desk or the relevant member of the Data Security Committee for advice).

SCHEDULE 1

INCIDENT MANAGEMENT PLAN TEMPLATE

STEP 1 – CONTAINMENT & RECOVERY	
Who should be made aware of the breach and who should project manage the investigation.	
Consider any Company policies or procedures for dealing with the type of breach – e.g. those relating to our internal computer systems or to PCI compliance.	
Identify and implement any steps to contain the breach, preserve any evidence and limit damage.	
Identify all relevant sources of evidence (including hard drives, lap tops, memory sticks, paper files of relevant employees etc.) and if appropriate, quarantine.	
Is it appropriate to notify the police or our insurers?	
What steps are being taken to try and ensure documents which are created during the course of the investigation are subject to “legal privilege”?	

STEP 2 - ASSESSING THE RISKS	
What type of data is involved?	
Are living individuals identified in the data?	
How “sensitive” is the data? (Bank details, health records etc.)	
If data has been lost or stolen, are there any protections in place such as encryption?	
What has happened to the data? If data has been stolen, this poses a different level of risk to if it has been damaged	

Establish a timeline wherever possible covering: • When the breach occurred • When was it detected • How was it detected and by whom • When was the breach contained	
What steps could the data tell a third party about the individual? **NB:** Sensitive data could mean very little to an opportunistic laptop thief while the loss of a marketing database could help a fraudster build up a detailed profile of a person.	
How many individuals are affected by the breach?	
Who are the affect individuals – staff, customers etc.?	
What harm could come to those individuals affected or to the Company? For example, physical safety or financial loss.	
Are any processes or systems likely to be affected and if so what is the impact? For example, could restricted access cause operational problems or lead to customer complaints.	
Are there wider consequences, such as a risk to the public?	
If individuals' bank details have been lost, consider contacting the relevant banks or card companies for advice on helping to prevent fraud.	
Are there any contracts in place governing the use or processing of the data, particularly if the compromised of data is held by a third party (i.e. a marketing partner or service provider)? This is a mandatory requirement of the Data Protection Act 1998. All contracts should be collated and reviewed as a matter of urgency. In particular consider whether we have rights of audit or if there are clauses dealing with providing assistance following a breach.	
Any other relevant concerns raised by the Incident Response Team?	

STEP 3 - NOTIFICATION	
NOTIFYING AFFECTED INDIVIDUALS	
Can notification help the Company meet its obligations with regard to the seventh data protection principle? (i.e. "personal information must be kept secure")	
Would notification help individuals? For example, bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks by cancelling a credit card or changing a password?	
Consider how any notification can be made appropriate for particular groups of individuals. The Company must consider what it is going to tell those affected and how it is going to communicate the message.	
Notifying the ICO	
If the breach involves the compromise of personal data, consider if the ICO should be notified. There is no legal obligation to do so, however serious breaches affecting large numbers of individuals should always be notified.	
Internal communications/notifications	
Have all staff who could make potentially damaging admissions or statements concerning the loss been identified and briefed?	
Is it likely that customers affected by the breach may make contact as a result of press coverage or any notification? If so, consider briefing customer facing staff, such as reception and customer services.	
Has a dedicated point of contact been established to deal with any press enquiries?	
Consider whether in the circumstances, it would be advisable to set up a dedicated enquiry number or email address.	
Establish systems to deal with adverse comments on social media, websites and other chat rooms.	

Consider the appropriateness of a statement for public release.	
Third party notifications	
The ICO should only be notified when the breach involves personal data. Are there any other regulatory authorities who may take an interest in the loss – for example, the Financial Services Authority?	
What notification requirements are there in connection with any PCI compliance or any other accreditation scheme?	

SCHEDULE 2

DATA BREACH INCIDENT – POST INCIDENT REPORT

Incident date:

Nature of incident:

Report by:

(1) Details of Incident

Please give details such as time of incident, extent of breach etc.

(2) Response to Incident

Please describe how the incident was handled including how it was communicated to the business and beyond

(3) Issues Raised

Please highlight any issues that were raised as a result of the incident and planned actions to deal with them? How robust are/were the Company's policies and procedures in connection with the breach; how extensive is compliance with those policies and procedures and should any changes be made/recommended?

	Issue	**Response**
1		
2		
3		.
4		
5		