NetFM UK

DATA SECURITY BREACH MANAGEMENT POLICY

May 2021
Version 2.0

DATA SECURITY BREACH MANAGEMENT POLICY

CONTENTS:

DATA SECURITY BREACH MANAGEMENT POLICY

1. INTRODUCTION

1.1 NetFM UK Ltd is committed to ensuring that the data it processes is done so in a secure and appropriate way in line with data protection legislation. However, NetFM recognises that data security breaches may occur for a number of reasons, including:

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances (e.g. fire or flood)
- Hacking attacks
- "Blagging" offences (e.g. information is obtained by deceit)

1.2 This policy ensures that NetFM responds to and manages data security breaches responsibly, systematically and effectively.

2. SCOPE

2.1 This policy is applicable to all members of NetFM who process and use data ("Information users") who should implement this policy when they identify a suspected or confirmed data security breach.

2.2 This policy applies to all information processed by NetFM (regardless of format) and should be read in conjunction with NetFM's Information Security Policy.

3. RESPONSIBILITIES

3.1 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.

3.2 The Chief Technical Officer (CTO) / Directors / Lead Developers are responsible for ensuring that staff within their area of the business act in compliance with this policy and assist with investigations as required.

3.3 The CTO will be responsible for overseeing management of data security breaches in line with the Data Security Breach Management Plan delegation may be appropriate in some circumstances.

3.4 The CTO shall work with Directors / Lead Developers to respond appropriately to data breach incidents.

4. WHAT IS A DATA SECURITY BREACH?

4.1 A data security breach in this context means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

4.2 Data security breaches involving personal data include:

- Access to personal data by an unauthorised third party
- Deliberate or accidental action (or inaction) by a data controller or processor.
- Sending personal data to an incorrect recipient

- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss, destruction, corruption or unauthorised disclosure of personal data
- All of the above if it has a significant negative impact on individuals

4.3 In addition, and as stated within Recital 5 of the GDPR, a personal data breach:

"... may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

5. REPORTING A DATA SECURITY BREACH

5.1 Confirmed or suspected data security breaches should be reported immediately to the CTO (dave@netfm.org) using the Data Security Breach Incident Report Form. The CTO may be contacted to advise on containing the breach and any next steps depending on the extent and urgency of the breach.

5.2 The report should include full and accurate details of the incident including who is reporting the incident and what classification of data is involved according to the Information Asset Classification System contained within the Information Security Policy by completing the Data Security Breach Incident Report Form and submitting this to the CTO.

5.3 Once a potential, suspected or confirmed data breach has been reported an initial assessment will be undertaken by the CTO to establish the severity of the breach in accordance with Table 1 and the Data Security Breach Management Plan shall be initiated.

5.4 The CTO shall keep a Personal Data Security Breach Log to record all reports of confirmed data security breaches to ensure appropriate oversight in the types and frequency of these incidents for management and reporting purposes in line with guidance published by the Information Commissioner's Office (ICO).

DATA SECURITY BREACH MANAGEMENT POLICY

BREACH TYPE	CRITERIA (ONE OF THE FOLLOWING)
MAJOR BREACH	• The breach involves data classified as Highly Restricted / Restricted • The breach involves more than 1000 individuals • External third-party data is involved • There are significant or irreversible consequences • The breach is likely to result in media coverage • An immediate response is required regardless of whether it is contained or not • The breach requires a significant response beyond normal operating procedures
SERIOUS BREACH	• The breach involves data classified as Restricted • The breach is not contained within NetFM • The breach involves personal data of more than 100 individuals • A significant inconvenience will be experienced by individuals impacted • The breach may not yet be contained • The breach does not require an immediate response • The response to the breach may require notification to NetFM's CTO / Directors / Lead Developer
MINOR BREACH	• The breach involves data classified as Internal Use or Restricted • The breach involves a small number of individuals (less than 100) • The breach incurs a low risk to NetFM • Inconvenience may be suffered by individuals impacted • The breach involves data that is contained / encrypted / password protected • The breach can be responded to during working hours **EXAMPLES:** An email being sent to a wrong recipient Loss of an encrypted mobile device

DATA SECURITY BREACH MANAGEMENT POLICY

6. DATA SECURITY BREACH MANAGEMENT PLAN

6.1 NetFM shall take appropriate action to handle a data security breach efficiently utilising its data security breach management plan which consists of the following four elements:

a) Containment and recovery, whereby:
- Action is taken to contain and investigate the breach.
- Action is taken to recover data and limit the damage the breach can cause.
- The police are informed if appropriate.

b) Assessment of ongoing risk, whereby:
- A risk assessment is undertaken of the breach and the potential adverse consequences for individuals concerned to determine next steps necessary further to immediate containment.

c) Notification of a breach, whereby:
- Individuals concerned, the Information Commissioner's Office (ICO) and third parties are notified of the breach as appropriate depending on the nature of the breach.

d) Evaluation and response, whereby:
- The effectiveness of NetFM's response to the breach is considered through action planning and monitoring.
- Improvements to existing procedures are identified to enhance data security.

A) Containment and recovery

6.2 Following the reporting and initial assessment of a data security breach the CTO shall:

a) Identify a member of the Senior Management Team who is independent of the department where the breach occurred to take the lead on investigating the breach.
b) Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise, e.g. isolate or close a compromised section of the network, find a lost piece of equipment or change access codes of doors or IT equipment.
c) Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause, e.g. as well as the physical recovery of equipment, this could involve the use of back-up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
d) Where appropriate, inform the police.

6.3 All actions and decisions should be recorded on the Data Security Breach Management Timeline of the *Data Security Breach Incident Report* form.

DATA SECURITY BREACH MANAGEMENT POLICY

B) Assessment of ongoing risk

6.4 The lead investigating the data security breach shall undertake a risk assessment associated with the breach to assess potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen using the *Data Security Breach Management – Assessment of Ongoing Risk* form to carry out this assessment and to record their findings.

C) Notification of a data breach

6.5 The CTO and lead investigating the data security breach shall determine whether data subjects or other organisations should be informed of the breach to enable those whose data has been compromised to take steps to protect themselves, to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints using the *Notification of a Data Breach Checklist* to determine this.

6.6 If the risk to individuals' rights and freedoms is unlikely, the breach does not have to be reported to the individual or the ICO but shall still be documented in the *Personal Data Security Breach Log* by the CTO.

i. Notifying individuals affected

6.7 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, they shall be informed without undue delay. This shall normally by the responsibility of the CTO who shall provide individuals affected with the following information using the *Notification of a Data Breach to User* template.

a) The name and contact details of the CTO or other contact point where more information can be obtained.
b) A description of the likely consequences of the personal data breach.
c) A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

6.8 The CTO shall record this in the *Personal Data Security Breach Log*.

ii. Notifying the ICO

6.9 If a personal data breach has occurred and it has been determined that there is a risk to individuals' rights and freedoms the CTO must inform the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach, even if all the details have not yet been obtained. This shall normally be the responsibility of the CTO who shall follow the ICOs reporting process described here: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

6.10 The CTO shall record this in the *Personal Data Security Breach Log*.

iii. Notifying other regulatory bodies

6.11 If any other regulatory body needs to be informed of a data breach, the CTO shall be responsible for providing them with the Notification of a Data Breach.

iv. Notifying third parties

6.12 If third parties (e.g. the police or banks) need to be informed of a data breach, the CTO shall be responsible for providing them with the Notification of a Data Breach.

v. Notifying the media

6.13 If the data breach is likely to come to the attention of the media, the CTO shall liaise with Marketing to draft a press release.

D) EVALUATION AND RESPONSE

6.14 Further to the investigation of the data breach, the lead member of staff shall identify any enhancements to policies or practices to prevent a similar incident from happening in the future and complete Section 7 of the *Data Breach Incident Report Form* and provide this to the CTO.