Information Security Data Policy

Scope

The scope of this Policy applies to all Mimoto employees and members. Subcontractors who are required to work on Mimoto's information systems will also be made aware and expected to abide by this policy.

Purpose

To have a clear policies and procedures in place in the event of a serious security incident or data breach.

To ensure that damage done by security incidents is kept to a minimum.

To reduce the likelihood of occurance of security incidents.

Introduction

Mimoto is responsible for the processing, security, and integrity of all information it holds. The Mimoto protects this information using all means necessary by ensuring at all times that any incident which could cause damage/distress to the data subjects, damage to Mimoto's assets/reputation, damage to it's clients, is prevented or minimized.

An incident or breach is defined as any event, any suspicion that an event has occurred, or any discovery or suspicion that vulnerability has been exploited to pose a threat to the confidentiality, integrity, or availability of information assets.

Classes of threat are listed below.

- **Threats to confidentiality.** These events may include attempts to gain access to an information asset for the purposes of obtaining information that the individual would not be authorised to have. The reverse may also occur if restricted information were placed in a publicly accessible location, either inadvertently or purposely, thus constituting a threat to confidentiality and a possible violation of the law. *Incident classes: Disclosure, Unauthorised access, Password sharing.*
- **Threats to integrity.** These are errors, intentional acts, and natural or accidental events that can result in the corruption or loss of information stored in, processed on, or transmitted by Mimoto and its data processors. Corruption may be caused by fraud or associated with a disruption of service resulting from unauthorised modification, system failure or procedural error, even though the intent of such incidents may not have been deliberate. Misuse is a growing concern because it covers email, Internet, image files or even individuals doing private work. *Incident classes: Fraud, Unauthorised modification, Power failure, Procedural errors and Misuse.*

- **Threats to availability** These are events that may be caused deliberately or accidentally by individuals who cause disruptions in processing or loss of stored or transmitted information. Examples include wilful damage, power failure, procedural errors or theft. Malicious software is now taking many forms including denial-of-service attacks utilising some operating system or network exploit, viruses, worms, spoofing and email spamming. *Incident classes: Theft; Malicious Software; Wilful damage; System failure*

Types of security incident

An incident is classifed as serious when the incident:

- Involved actual or potential failure to meet the legislation to protect information, such as GDPR.
- Potentially involves, or could lead to a data breach.

Reporting Security incidents

Security incidents must be reported to Mimoto's directors as soon as they have been identified.

Details of security incidents can be very sensitive and sensitive information should be handled with discretion and communicated via secure means to just those who need to be informed.

The Mimoto's directors will determine whether it is a security incident or data breach and will allocate it in accordance with the appropriate plan.

Where the potential for a data breach is discovered Mimoto will inform potentially implicated clients within 24 hours.

Public reporting

Mimoto advertises and monitors the abuse@mimoto.co.uk email account for the purposes of reporting security concerns. An associated GPG encryption key is also advertised to support the reporting on sensitive matters.

Training

All staff and members need to be introduced to their basic responsibilities under GDPR in regards to protecting the data we hold and the systems we use. This includes understanding what is an incident and how to report it. To ensure that they are aware, they will need to complete mandatory training in Information Security and Data Protection in addition to reading this policy.

Monitoring and review

This policy will be reviewed when there are changes to the legislation.

Data breach procedure

Purpose

This breach procedure sets out the course of action to be followed if a data protection breach takes place.

Immediate containment/recovery.

1. The person who discovers the data breach must inform the directors of Mimoto.
2. Mimoto will determine whether the breach is still occuring and if so immediately take steps to minimise the effect of the breach. Eg: shutdown a system, heavily restrict access to a web site, etc.
3. Mimoto will consider whether the Police need to be informed.
4. Mimoto will consider whether credentials have been compromised. If so it will arrange their reset or notify affected parties.
5. Mimoto will use backup data to restore lost/damaged data.
6. Mimoto will consider if the breach affects client data, if so it will inform the client within 24 hours.
7. Mimoto will consider if this breach needs to be reported to the ICO. If so it must be done within 72 hours of the breach.

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. Recital 85 of the GDPR explains that:

"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."

This means that a breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors

Investigation

The next stage is for Mimoto to fully investigate the breach. The investigation should ascertain:

- whose data was involved in the breach.
- the potential effect on the data subject.
- what further steps need to be taken to remedy the situation.

The investigation will also identify any potential security improvements that can be made in light of the breach

The investigation should consider:

- The type of data
- Its sensitivity
- What protections are in place (eg: encryption)
- What has happened to the data
- Whether the data could be put to any illegal or inappropriate use
- How many people are affected