Breach Policy

Document Control
Reference: Breach Policy
Issue No: 1
Issue Date: 21/09/2018

1. Purpose

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant Supervisory Authority. The current Supervisory Authority for the UK is the ICO (Information Commissioners Office https://ico.org.uk/). Organisations must do this within 72 hours of becoming aware of the breach, where required.

If a breach is likely to result in a high risk of adversely affecting the individuals' rights and freedoms, those individuals must also be notified without undue delay.

Under GDPR, each organisation is required to have data breach reporting procedures in place.

All breaches, regardless of whether reported to the ICO or not, need to be recorded.

As with any security incident, we are required investigate whether a breach was a result of human error or a systemic issue and how a recurrence can be prevented – whether this is through better processes, further training or other corrective steps.

This document covers the breach policy and procedure for iSAMS Ltd.

For the Breach Procedure please see section 5 in conjunction with the Data Breach Form

2. What is a breach?

A personal data breach 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. It also means that a breach is more than just about losing personal data.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever.

- any personal data is lost, destroyed, corrupted or disclosed;
- if someone accesses the data or passes it on without proper authorisation;

- or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

The GDPR makes clear that when a security incident takes place, we should quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

3. Types of Breach

Personal data breaches can include:

- Theft of data or equipment on which data is stored
- Loss of data or equipment on which data is stored
- Destruction or damage to personal data
- Loss of availability of personal data.
- Unlawful disclosure of personal data to a 3rd party
- Sending personal data to an incorrect recipient
- Access by an unauthorised third party
- Phishing, social engineering or similar where information is obtained through deceit
- Alteration of personal data without permission

4. What breach should the ICO be informed of?

When a personal data breach has occurred, we 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 the ICO must be notified; if it's unlikely then the ICO do not need to be notified. However, all breaches should be documented.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. 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. We need to assess this case by case, looking at all relevant factors.

As an example, from the ICO:

"The theft of a customer database, the data of which may be used to commit identity fraud, would need to be notified, given the impact this is likely to have on those

individuals who could suffer financial loss or other consequences. On the other hand, you would not normally need to notify the ICO, for example, about the loss or inappropriate alteration of a staff telephone list."

5. Breach Procedure – What should you do?

If you discover that data has been lost or that that there has been breach you must notify the iSAMS Information Security Team within 24 hours of becoming aware.

The person discovering the breach notifies and returns the completed form to the DPO within 24 hours

Forms need to be completed with as much information as possible but don't have to be 100% completed prior to submission.

DO NOT contact the ICO directly

Should you discover a breach, carry out the following steps:

Step 1 – Immediately aim to minimise the risks and contain the breach.
For example:

- Disconnect from the network
- Find lost equipment
- Change password

Our priority will be to contain the breach and minimise the risks to those affected by it.

Step 2 – Inform the iSAMS Information Security Team

- Depending on the severity, contact the iSAMS Information Security Team by email or phone giving your name, the data/time of the breach and basic information about the breach
- For all breaches, complete the Data Breach Reporting Form as thoroughly as possible and send to the iSAMS Information Security Team copying in the Service Desk no later than 24 hours after becoming aware of the breach
- Forms are available within the Information Security Section on SharePoint
- Should you be unable to access the form, a member of the iSAMS Information Security Team will start the form
- The form should take no longer than 15 minutes to complete
- The Data Protection Officer can be contacted directly for urgent advice

Step 3 – Evaluate

- It is important to evaluate the causes of the breach to prevent further breaches
- Simply contain a breach and continuing as normal is not acceptable

Step 4 – Follow guidance

- Once you have reported a breach, minimised any further risks and evaluated the cause, please wait for further guidance from either:

- The iSAMS Information Security Team
- The Data Protection Officer
- The ICO

6. Breach Procedure – What will the iSAMS Information Security Team and DPO do?

The Data Protection Officer within the Information Security Team will follow the ICO guidelines on notification and recording of the breach.

Upon becoming aware of a breach, the Data Protection Officer will

- Assess the severity of the breach
- Consider whether it is appropriate to inform the ICO
- Advise the relevant iSAMS business units of the breach
- Advise Network Support

If the breach is deemed low risk

- The ICO will not be notified
- A record of the breach will be recorded in the Data Breach Log
- The person/team who notified the breach will be provided guidance on what to do next
- If required, an action plan will be created to prevent similar breaches occurring and shared with the relevant business units
- The Data Protection Officer will then follow up with the relevant Department Heads to confirm action has been taken.

If the breach is deemed high risk

- The ICO will be notified within 72 hours (See Appendix A)
- A record of the breach will be recorded in the Data Breach Log
- The Information Security Team will notify individuals(s) concerned without undue delay
- The ICO will assess the breach and contact the iSAMS DPO
- The ICO will advise the DPO of the verdict and provide support in mitigating the breach
- The DPO will create an action plan and share with the relevant business units
- The DPO will follow up with the relevant Department Heads to confirm action taken.
- The DPO liaises with the ICO on next steps

Other Information

What happens if we fail to notify?
Failing to notify a breach when required to do so can result in a significant fine up to 10 million euros or 2 per cent of global turnover.

How much time do we have to report a breach?
We must report a notifiable breach to the ICO without undue delay, but no later than 72 hours after becoming aware of it. If we take longer than this, we must give reasons for the delay.
What if we don't have all the required information available yet to notify?

The GDPR recognises that it will not always be possible to investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. GDPR allows us to provide the required information in phases, if this is done without undue further delay. We must still notify the ICO of the breach when we become aware of it, and submit further information as soon as possible.

7. Appendix A

Contacting the ICO
To report a breach to the ICO, call the ICO helpline 0303 123 1113
The ICO will then provide guidance and advice on what to do next
Use the iSAMS Data Breach Reporting Form to answer the questions about the breach

How to report a Data Breach to the ICO
https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

Change History Record

Issue	Description of Change	Approval	Date of Issue
0.1	Draft	Head of Service and Operations	21/09/2018