DATA BREACH POLICY

VERSION: MAY 2021

www.oneway.co.uk

Data Security Background

Data security breaches are increasingly common occurrences, whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more ways in which data can be breached. One Way need to have in place; a robust and efficient process for responding to any reported data security breaches, to ensure it can act responsibly in reporting data breaches to the ICO and protecting One Way's data as much as possible.

Aim

The aim of this policy is to standardise business wide the response to any reported data breach incident and ensure that each incident is appropriately logged and managed in accordance with the ICO.

By adopting a standardised consistent approach to all reported incidents, it aims to ensure that:

- All incidents are recorded and documented
- The impact of the incident is understood and action is taken to prevent further damage
- That any external bodies or data subjects are notified if their data has been breached
- All incidents are dealt with in a timely manner and normal operations restored
- If an incident occurs, each incident is reviewed to identify if improvements need to be made in our policies and procedures
- All incidents that include a breach of personal data must be reported to the ICO within 72 hours of finding out that they have happened

Definition

A data security breach is considered to be "any loss of, or unauthorised access to data". Examples of data security breaches may include:

- Loss or theft of data or equipment which data is stored
- Unauthorised access to confidential or highly confidential data
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' offences
- Sending personal data to an incorrect recipient
- Loss of availability of personal data.

Scope

This policy applies to all One Way information, regardless of format and is applicable to all staff, visitors, contractors and third parties acting on behalf of One Way.

Containment and Recovery

As soon as a data security breach has been detected or is suspected the following steps should be taken:

1. Identify who should lead on investigating and managing the breach. In most cases this should be directed to the Executive Office to be dealt with

2. Establish who within One Way, any third parties and if data subjects should be aware of the breach. Nasstar, our IT provider must also be notified immediately

3. Identify and implement any steps required to contain the breach. For example, isolating of/closing a compromised section of the network, finding a lost piece of equipment or simply changing a password

4. Identify and implement any steps required to recover any losses and limit the damage of the breach. Establish whether there is anything that can be done to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of backups to restore lost or damaged data

5. If appropriate inform the police

Assessing the Risks

Some data security breaches will not lead to risks beyond possible inconvenience and may not stop One Way team members from doing their job. An example might be where a server has been damaged beyond repair, but all files have been backed up and can be recovered. While these types of incidents can still have significant consequences, these risks are very different from those posed by, for example, the theft of the database, the data on which may be used to commit identity fraud.

Before deciding on what steps are necessary to contain the breach, assess the risks which would most be associated with the breach, for example:

- What type of data is involved?
- How sensitive is the data that has been breached?
- If data has been lost or stolen, is there any protection in place such as encryption?
- If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relates to
- If the data has been damaged. this poses a different type and level of risk, for example unforeseen circumstances such as flood, fire or power failures etc.
- What could the data that has either been lost or stolen tell a third party about the individual?
- How many individual's personal data have been affected?
- Who are the individuals whose data has been breached? Whether they are team members, candidate or clients.
- What harm can come to this individuals? Are there risks to physical safety, reputation, financial loss or a combination of these?
- If individuals' bank details have been lost, consider contacting the individuals bank themselves for advice on anything the can do to help prevent fraudulent use.

Notification of Breaches

When a breach occurs One Way will need to assess the situation to see who needs to be informed about the breach. Just because a breach has happened, doesn't mean that all persons need to be notified. Notifications should have a clear purpose, whether is to notify individuals or third parties that have been affected.

The list below identifies who should be notified depending on what type of breach One Way has had.

Type of Breach	Who to Notify	Contact	Contact Details
A breach that does not affect an individual's data.	Operations Assistant	Abbie McMahon-Smith	023 8098 1605 AbbieMcmahon-Smith@oneway.co.uk
	Operations Director	Duncan Bartlett	023 8098 1605 DuncanBartlett@oneway.co.uk
Loss of data (loss of laptop, mobile phone)	Operations Assistant	Abbie McMahon-Smith	023 8098 1605 abbieMcmahon-Smith@oneway.co.uk
	Operations Director	Duncan Bartlett	023 8098 1605 AbbieMcmahon-Smith@oneway.co.uk
	Nasstar	Nasstar	01604 826580 itsupport@nasstar.co.uk
	Onecom (Vodafone)	Onecom	0330 0240000
Human Error	Operations Assistant	Abbie McMahon-Smith	023 8098 1605 AbbieMcmahon-Smith@oneway.co.uk
	Operations Director	Duncan Bartlett	023 8098 1605 DuncanBartlett@oneway.co.uk
Unforeseen circumstances such as fire or flood	Executive Office	Executive Team	023 8098 1605 exective@oneway.co.uk
Hacking attack	Operations Assistant	Abbie McMahon-Smith	023 8098 1605 AbbieMcmahon-Smith@oneway.co.uk
	Operations Director	Duncan Bartlett	023 8098 1605 DuncanBartlett@oneway.co.uk
	Nasstar	Nasstar IT Support	01604 826580 itsupport@nasstar.co.uk
	Mercury1	Support Team Stew Ward	023 8000 7008 support@mercury1.co.uk stew@mercury1.co.uk
Breaches that we need to notify the ICO about	ICO (Information Commissioner' Office)	ICO Helpline	0303 123 1113

Each situation needs to be assessed to see if we need to notify the ICO and if an individual is affected. For example, if we have had a breach that affects a large amount of individuals then we need to notify the ICO within 72 hours; however, if we had a breach that didn't affect an individual's data then we still need to document this, but we don't need to notify the ICO and just need to document why we have not decided to notify them.

Evaluation and Response

After a breach One Way must evaluate the breach to make sure that One Way's data breach policy is effective, depending on security, staff awareness, business continuity and the people that are being notified about the breach.

Each breach must be evaluated on:

- The risks of the data that was breached, for example, do we need it?
- Are there any weak points in our security that could have been fixed to prevent the breach?
- Is there enough staff awareness about data breaches and what to do if one occurs?
- Could anything of been done to prevent the breach?
- Are the recommended persons to notify about breaches the relevant people and are the efficient enough?

Documenting Breaches

All breaches that occur must be documented even if they do not affect an individual's data. Please report all breaches to the executive team. The executive team will then need to fill out the 'Data Breach Incident Report'. In the report the following things will need to be stated:

- The date of when the breach occurred
- The time the breach occurred
- Activity – The type of breach and the description
- The severity of the breach – Low, Medium, High and Severe with an explanation of why the decision was made to give that breach the ranking it was given.
- Evaluation and Response
- Authority – The name and job title of who made the decision of what to do with the breach and signed off that they were happy with the evaluation and decision.
- Who was notified of the breach.

Signed Date: May 2021

Duncan Bartlett

Operations Director