# GDPR Security Breach Strategy

| | |
|---|---|
| **Title** | **GDPR Security Breach Strategy** |
| **Who should use this** | All Staff |
| **Author** | Assessor & ERO/HOVS |
| **Approved by Management Team** | Approved at 23/04/18<br>Corporate Governance Forum |
| **Approved by Joint Board** | |
| **Reviewer** | **Assessor & ERO/HOVS** |
| **Review Date** | **June 2021/as required** |

Review History

| REVIEW NO. | DETAILS | RELEASE DATE |
|---|---|---|
| 1 | NEW STRATEGY | |
| 2 | MINOR AMENDMENTS APRIL 2018 | JUNE 2018 |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |

**Data Security Breach Strategy**

As the Board processes personal data it must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of, or damage to personal data.

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

- **loss or theft of data or equipment on which data is stored**
- **loss or theft of paper based information**
- **inappropriate access controls allowing unauthorised use**
- **equipment failure**
- **human error for example, a mis-sent email**
- **unforeseen circumstances such as fire or flood**
- **fraudulent representation for example, someone claiming to be someone who they are not**
- **cybercrime attacks including hacking, malware, ransomware, phishing and spear-phishing**
- **deliberate acts carried out by individuals from inside the organisation.**

## 1. Containment and Recovery

Every loss of Board information or equipment, whether stolen or accidental, **must be reported immediately**.

Equipment losses must be reported to the Assessor and Electoral Registration Officer (Assessor & ERO) or the Head of Valuation Services & Assistant ERO (HOVS).

The loss of information must be reported to your Line Manager and the HOVS straight away regardless of whether or not the information is deemed to be personal, sensitive or confidential. Where a member of staff receives information sent in error they should report it straight away to the sender, but it is the responsibility of the sender to formally report the incident.

Advice will be provided on next steps, including possible recovery of the information.

All investigations into the loss of Board information or equipment will be conducted under the guidance of the Assessor & ERO and or the HOVS. The primary objectives of the initial investigation are:

1. **Confirm the nature of the information lost**, and in particular whether the information consists of sensitive personal data (medical information, details of convictions or alleged criminality for example, or information of use in carrying out identity theft (such as bank account details).

2. **Prevent any further loss of information** and if possible any further dissemination of the information which has been lost or compromised.

All staff must co-operate fully with any such investigation. It is essential for staff involved in any data loss to be completely frank with the investigation so we can assess the risks and take appropriate mitigating action.

The Assessor & ERO will determine who needs to be made aware of the breach and what they need to do to contain the breach; this may include notifying affected individuals; the Chair and Depute Chair of the Board and reporting the loss to the Information Commissioner within 72 hours of the organisation becoming aware of the breach.

Individual members of staff must not notify affected individuals directly; the decision to notify individuals and external organisations will be taken by the Assessor & ERO and or the HOVS.

## 2. Assessing the Risks

An Assessment Team will be established and will include – the HOVS, Principal Administration Officer (PAO), and a member of South Ayrshire Councils Communications Team. This team will determine the risks associated with the loss.

The risks associated will be dependent on:

- the type of data involved
- how sensitive the information is
- whether there were any protections in place, for example, encryption of a portable device
- what has happened to the data, if known
- how many individuals' personal data are affected by the breach
- what harm can come to those individuals whose data has been lost
- whether there are any wider consequences to the loss of the data
- if individual's bank details have been lost, consideration will be given to contacting the banks for advice on preventing fraudulent use.

A checklist of actions in the event of a security breach can be found in **Appendix 1**.

The assessment will be immediately communicated to the Assessor & ERO.

## 3. Notification of Breaches

Informing people and organisations that the Board has experienced a data security breach is an important part of our breach management strategy.

Consideration will be given to:

- who will be notified (police, banks for example
- what we will be notifying them of, and
- how we are going to notify them.

If a decision is taken to notify individuals of the breach, the notification will tell them how and when the breach occurred and what data was involved. The notification will also tell the individual what has and is being done by the council to respond to the breach. The decision to notify individuals will normally be taken by the Assessor & ERO. Decisions on notifying the Information Commissioner will be taken by the Assessment Team in conjunction with the Assessor & ERO.

If the Information Commissioner requires to be notified, the Assessor and Electoral Registration Officer and or the HOVS will do this within 72 hours of the breach being discovered.

## 4. Evaluation and Response

Part of the overall breach response strategy will be to investigate the causes of the breach and also the effectiveness of the Board's response to the breach.

Simply containing the breach is not acceptable, particularly if the breach was caused (even in part) by a systematic or ongoing problem. Action must be taken to rectify the underlying problem. A review will be conducted by members of the Assessment Team. A report on the review must be made available to the Board and the Assessor and Electoral Registration Officer within three weeks of the incident and must address issues which caused the incident and make recommendations as to the steps necessary to prevent or minimise such an incident re-occurring.

Based on 'lessons learned' policies and procedures will be reviewed and updated if required.

Any data loss reported to the Information Commissioner will be reported to the next Management Team Meeting. All data losses will be reported to the next Board Meeting or before if required. The Board will also consider the terms of the response plan produced by the Assessor & ERO and or the HOVS following any data loss.

**Appendix 1**

## Checklist of Actions

| | | Yes/No Comments | Responsible Post Holder |
|---|---|---|---|
| 1. | Reported to Line Manager | | Person who discovered the breach |
| 2. | Reported to Assessor and ERO and or HOVS | | Line Manager of Team who discovered the breach |
| 3. | Reported to Assessor and ERO and or HOVS if device is lost or stolen | | Line Manager of Team who discovered the breach |
| 4. | Nature of information lost confirmed | | Type/Information Risk Owner |
| 5. | Identify steps taken to recover information | | Assessment Team Leader |
| 6. | Decision taken on whether to notify individuals affected by the loss | | Assessment Team Leader |
| 7. | Information Commissioner's Office notified | | Assessor and ERO |
| 8. | Police notified | | Assessor and ERO |
| 9. | Banks notified | | Assessor and ERO |
| 10. | Board Notified | | Assessor & ERO |
| 11. | Risk assessment of the loss carried out, including determining how the loss occurred | | Assessment Team Leader |
| 12. | Actions identified to minimise further losses | | Assessment Team Leader |

| | |
|---|---|
| **Checklist completed by** | |
| **Job Title/Role** | |
| **Date** | |