Central Scotland Valuation Joint Board

Data Security Breach Procedure

Version Control ***Table* Version**	**Maintained by**	**Amendment date**	**History of changes**
0.1	J Wandless	07/06/2017	1st Draft
1.0	J Wandless	07/07/2017	Approved MT
2.0	J Wandless	24/05/2018	
Review Frequency		Annual	
Next Review Date		May 2019	
Reviewer		Assistant Assessor	

Overview
In terms of the Data Protection Act 1998 (DPA) organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data. This procedure, which is based on the Information Commissioners guidance on data security breach management, outlines what action should be taken in the event of a data security breach.

This Procedure applies to data breaches involving Central Scotland Valuation Joint Board, Assessors and Electoral Registration Officer data (referred to below collectively as CSVJB)

A data security breach can happen 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 such as a fire or flood
- Hacking attack
- Blagging offence where information is obtained by deceiving the organisation who holds it

1. Reporting

All data security breaches or suspected data security breaches should be reported immediately to your line manager and the Principle Administration Officer (PAO). In their absence this should be any member of the management team and the Assistant Assessor. The Data Protection Officer (DPO) should immediately be informed by the Principle Administration Officer or in his absence the Assistant Assessor of the breach or suspected breach. The DPO is currently Stephen Coulter, Head of Resources and Governance Officer.at Clackmannanshire Council.

Details of the breach should also be recorded on the Data Security Breach log on the Management Team folder. The log should record the date of the breach, date of notification of the breach, nature of breach and action taken.

2. Containment and Recovery

The Principle Administration Officer or delegated investigating officer should:

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 etc.) 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 cooperate fully with any investigation. It is essential for staff involved in any data loss to be completely frank so that the PAO can assess the risks and take appropriate mitigating action.

The PAO or investigating officer 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 and reporting the loss to the Information Commissioner.

3. Assessing the Risks

The PAO 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, e.g. 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.

The assessment will be immediately communicated to the Assessor or Assistant Assessor and the DPO

4. Notification of breach

Informing people and organisations that CSVJB has experienced a data security breach is an important part of CSVJB's breach management procedure.

Consideration will be given to:

- Who will be notified (police, banks etc),
- 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 CSVJB to respond to the breach. The decision to notify individuals will normally be taken by the PAO or, for large scale notifications, by the Assessor or Assistant Assessor. Decisions on notifying the Information Commissioner will be taken by the PAO in conjunction with the Assessor or Assistant Assessor.

If the Information Commissioner requires to be notified, the DPO will do this as soon as possible following notification of the breach but certainly within 72 hours via the following link: https://ico.org.uk/for-organisations/report-a-breach/

5. Evaluation and response

Part of the overall breach response will be to investigate the causes of the breach and also the effectiveness of CSVJB'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 the PAO and reported to the Management Team. A report on the review must be made available to the Assessor and Assistant Assessor 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-curing.

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 meeting of the Management Team