**Managing Data Breach Procedure**

|  |  |
| --- | --- |
| **Related Policy:** | Managing Breach Data Policy |
| **Related Section:** |  |
| **Authorised By:** |  |
| **Prepared By:** |  |
| **Issue Date:** |  |
| **Review Date:** |  |
| **Version:** |  |

|  |  |
| --- | --- |
| **Purpose** | The purpose of this procedure is to enable Your Association to identify and manage a breach or attempted breach of the Your Association database or general IT system. This procedure is to reduce the risk to Your Association when a breach of data has been identified and to ensure Your Association complies with the requirements of the Privacy Act and the Office of the Australian Information Commissioner. |
| **Scope** | All Your Association Staff and Volunteers |
| **Definitions** | Eligible Breach of Data |
| **Procedure** | When a member of Your Association suspects a breach of data the following process will occur:1. Determine if there has been a breach of the Your Association information system – see definition of attached support notes detailing examples of a data breach.
2. Immediately confer or consult with President to assess the type of breach if the breach is an eligible breach of data for reporting purposes?
3. Identify and take note of characteristics of the data breach – example spyware, unlawful downloads, information sent to other parties accidently.
4. Upon confirmation of a nominated person of a data breach or potential data breach. Ensure any association computers and internet connections are shut down or takes steps to contain the breach.
5. The CEO or delegated person will have the overall responsibility for containing, assessing and managing any data breaches.
6. The President or CEO will be responsible for the implementation of the
7. Data Breach Plan which would cover the following:
* Identify the data breach
* Confirm if the data breach can be contained immediately
* Assess if the data breach is an eligible data breach- for reporting purposes see flow chart.
* Upon confirmation of an eligible data breach, alert the Senior Management Team or Data Recovery Response Team
* Contact external information technology contractor who will consult with the Data Recovery Response team
* The response team will undertake immediate steps to contain, assess the data breach and review what actions should be taken to limit any further breach.
* Implement communication strategy to notify impacted individuals there has been a breach of data and how Your Association is managing the data breaches
* CEO will direct staff to contact members, families and other staff members, advising them that there has been a breach of data and criminals could use their personal information. Refer to Victoria Police to report any evidence of the illegal use of personal data
* CEO or designated person to adhere to the Privacy Act requirements if there is a notifiable breach of data and report the matter to the Office of the Australian Information Commissioner
* Notify Insurance Broker of any breach of data
* Keep an ongoing record of data breaches for annual review.
 |
| **Responsibilities** | Be specific and insert responsibilities in relation to this procedure, not just generic responsibilitiesGoverning Committee is responsible for:1. Will have overall responsibility for the containing, assessing and managing any data breaches
2. Ensuring the Data Breach Plan is activated and coordinating the activities of the Data Recovery Response Team and to help identify any reportable breaches of data. The appointed service manager is responsible for all recording of breaches and preparation of information for the purposes of reporting
3. Employees are responsible for:
* Ensuring proper due diligence to prevent any breach of data
* Insert
 |
| **References – Internal** |  |
| **References – External**  | * Office of the Australian Information Commissioner
* Private Act 1988
 |
| **Review** | Your Association at its own discretion reserves the right to change the policy and procedure in line with relevant legislation and organisational needs. |