Data Breach Process Form

A data breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

Section 1 Informed of Potential Breach

Date of Breach:	
Time of Breach:	
Description of breach:	
Cause of breach:	
Which system(s),if any, are affected?	
Has corrective action occurred to remediate the breach or potential breach?	
Person who informed of breach:	

Section 2 Assessment and Determination

Information received by:	
Date of receipt of information:	
Is personal information involved?	
Is the information sensitive in nature?	
Has there been unauthorised access, disclosure, loss of personal information in circumstances where access to the information is likely to occur?	
Describe the type and extent of personal information involved	
Does the breach include multiple individuals?	

Provide details of people or type of people who now have access	
Determine where there is (or could be) a real risk of serious harm to affected individuals	
Determine whether there could be media or stakeholder attention as a result of the breach or potential breach	

Section 3 Data Breach managed internally

Complete when data breach is the managed by local level or relevant staff member within 48 hours

Description of breach:	
Action taken:	
Outcome of action:	
Prevention processes implemented:	
Relevant information:	
Recommendations:	
Signature:	
Date:	