Information Breach Assessment and Resolution Form

To be completed by the Director/Manager of the DTMI business unit where the breach originated and addressed to the Director Information Governance via pris@transport.wa.gov.au .

Details of the individual undertaking the assessment of the breach incident.			
Full name			
Position title		Location and Business Unit	
E-mail		Phone number	

Assessment			
Date received		Date commenced	

Potential breach of discipline/code of conduct	☐ Yes ☐ No	*If yes, immediately notify the Executive Director People and Culture, and comply with further instructions.*
Cyber security breach?	☐ Yes ☐ No	*If yes, immediately contact DTMI IT Service desk: 16999 or 1800216222 or Report an Incident on TRANSPORTA via ServiceNow and comply with their instructions.*
The breach is an assessed notifiable information breach	☐ Yes ☐ No	Provide reasons that justify the assessment.
The breach is likely to cause serious harm to an individual	☐ Yes ☐ No	Explain the basis on which this conclusion is made.
Who is affected by the information breach?	*E.g. Authorised Users, members of the public, other government agencies, third party stakeholders.* *The assessment may include reviewing whether individuals/organisations have been affected by the breach.*	
Who has been notified of the breach?	*Record who and date notified.*	
What immediate actions were taken to contain the breach?	*What was done to manage the risk of further damage/harm?* • *Has the information been recovered?* • *Security measures taken.*	
What caused it? Identify the causal factors and underlying causal circumstances.	*The assessment may include reviewing:* • *How did the current controls fail to mitigate the risk of breach?* • *Whether the breach occurred as part of a deliberate act or negligence.* • *Was it a one-off incident or does it expose a more systemic vulnerability?*	

Assessment	
What is the potential harm to the affected individuals or the organisation?	*Consider the level of sensitivity of the information and what possible use there is for the information. For example, could it be used for identity theft, threats to physical safety, financial loss, or damage to reputation?* *Is it official information that could result in damage to individuals, organisations or government if released* *Whether any individuals have personal circumstances which may put them at particular risk of harm.*
What controls were in place to mitigate the risk of this information breach?	*For example: Policy, Procedures, Restricted Access, Monitoring, Security etc.*

Review and Risk Management	
Is further investigation considered necessary and if so, how will this be undertaken?	*Will the breach need to be escalated or transferred to another authority?*
Risk Assessment. Refer to DTMI risk reference tables	*Consider: Individual harm, financial loss, service interruption, reputational damage. Assess:* • *The likelihood and consequence should the breach recur.* • *The controls managing the risk.* • *Risk acceptance/tolerance.*
After looking at the DTMI risk reference tables, what is the level of risk for the most impacted category?	• *1 Insignificant* • *2 Minor* • *3 Moderate* • *4 Major* • *5 Catastrophic*
Mitigation Action Plan - What is required to prevent the breach from occurring again?	*The mitigation action plan may include:* • *Strengthening the current controls and any additional controls that have been developed/implemented.* • *Improving security and access.* • *Education and training.* • *Changing the environment or location.*
Are PRIS Act assessment and notification timeframes on track to be met?	*If at risk, specify:* • *Which timeframe(s) are at risk (assessment / notification)* • *Date and details of escalation to Director Information Governance / Director General (or delegate)* • *Any engagement with the Information Commissioner regarding extensions*

Assessment Status and Closure	
Assessment status	☐ Assessment ongoing ☐ Assessment complete
Notifications (if applicable)	☐ Information Commissioner notified (if required) ☐ Affected individuals notified (if required) ☐ Notifications not required *(explain basis for rationale)*
Mitigations actions	☐ Mitigation actions identified ☐ Mitigation actions assigned to responsible owner(s) ☐ Mitigation actions completed ☐ Ongoing mitigation actions *(provide details and expected completion date)*
Assessment closure	Assessment closed on: ___ / ___ / _____ Approved by: Name: _____ Position / Role: _____

For additional information go to the PRIS page: Managing Privacy Risks > Information Breaches.

On completion, please forward this form to pris@transport.wa.gov.au