

# INTOWORK AUSTRALIA AND SUBCONTRACTORS NOTIFIABLE DATA BREACH POLICY

The objective of this policy is to have arrangements in place at IntoWork Australia and businesses in the Group, to protect data and procedures to respond to any data breach that occurs.

IntoWork recognises its obligations and reporting responsibilities under privacy legislation, including its obligation to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm.

For the purpose of this policy, a data breach occurs when personal information held by IntoWork Australia or businesses in the Group, is lost or subjected to unauthorized access or disclosure. Data breaches may occur in the following circumstances:

- a device containing customers' personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person.

IntoWork is committed to ensuring that it minimises the threat of data loss and responds in the event that it occurs by:

1. Implementing a Privacy Policy for the effective management of personal information at IntoWork Australia and the IntoWork Group of businesses
2. Providing relevant information on key responsibilities under privacy legislation to all employees
3. Maintaining a Data Breach Response Plan

Implementation of this policy at each IntoWork business is the responsibility of their senior management. The maintenance and review of this policy is the responsibility of the Executive Manager People and Performance. The review will be conducted in consultation with Senior Management of the IntoWork businesses.

This policy has been developed in consultation with interested parties and with consideration to access and equity principles and legislative requirements.

Reference: *Privacy Amendment (Notifiable Data Breaches) Act 2017.*

*Victorian Protective Data Security Standards (VPDSS)*

*South Australian Information and Security Management Framework*


*Queensland Government Information Security Policy*

*Tasmanian Government Information Security Framework*

*New South Wales Digital Information Security Policy*

*Western Australia Digital Security Policy*

*Australian Government Information Security Core Policy*

A handwritten signature in black ink, appearing to read "Paul Botkin", positioned above a horizontal line.

Poul Bottern  
IntoWork Australia Group CEO  
Date: 27 June 2018  
Review: June 2021

## GUIDANCE NOTES

These Guidance Notes accompany the IntoWork Notifiable Data Breach Policy. They are provided to assist in achieving the objective of the Policy at each IntoWork business. They are not part of the Policy and are guidance for compliance only. Additional information and assistance with the development and implementation of the required management systems is available by contacting IntoWork.

### 1. Providing Information on key responsibilities under privacy legislation to all employees

There is a legal requirement to provide information, instruction and training on notifiable data breaches. The statement applies to all employees. The information contained in the policy must be provided. Relevant information should be determined and provided. The business should be able to demonstrate that the policy statement is being implemented. An example could be including a copy of the policy and relevant information in an employee induction program.

### 2. Maintaining a Data Breach Response Plan

There is a legal requirement to maintain a Data Breach Response Plan. A Data Breach Response Plan is a framework to help manage a data breach. It sets out the roles, responsibilities and steps to be taken for managing the breach as well as internal and external reporting requirements. The plan is to be reviewed regularly in line with any changes to privacy legislation.

### 3. Victorian Protective Data Security Standards (VPDSS) compliance and reporting obligations.

There is a requirement for Victorian contracted service providers to comply and report to funding bodies under the Victorian Protective Data Security Standards (VPDSS). The VPDSS categorises funded organisations as contracted service providers. The information security compliance and reporting obligations between the department and funded organisations is defined by VPDSS Standard 9. According to VPDSS Standard 9, it is the department's responsibility to ensure that contracted service providers "do not do or act or engage in a practice that contravenes the Victorian Protective Data Security Standards (VPDSS)."

Further information on the VPDSS can be accessed at:

<https://fac.dhhs.vic.gov.au/news/victorian-protective-data-security-standards>

### 4. South Australian Information and Security Management Framework.

There is a requirement in South Australia that suppliers must comply with the South Australian Government Information Security Management Framework to the extent to which their contractual conditions with Agencies require them to do so. Suppliers may also be subject to contractual conditions requiring compliance to the ISMF by way of across government purchasing agreements. The Framework can be accessed at:

<https://digital.sa.gov.au/resources/topic/policies-guidelines-and-standards/security/information-security-management-framework>

### 5. Queensland Government Information Security Policy

There is a requirement in Queensland that suppliers must comply with the Queensland Government Information security policy (IS18:2018) to the extent to which their contractual conditions with Agencies require them to do so.

The Information Security Policy (IS18:2018) can be accessed at:

<https://www.qgcio.qld.gov.au/documents/information-security-policy>

## 6. Tasmanian Government Information Security Framework

There is a requirement in Tasmania that suppliers must comply with the Tasmanian Government Information Security Framework to the extent to which their contractual conditions with Agencies require them to do so.

The Information Security Framework can be accessed at:

[http://www.egovernment.tas.gov.au/information\\_security\\_and\\_sharing/tasmanian\\_government\\_information\\_security\\_framework/the\\_tasmanian\\_government\\_information\\_security\\_policy](http://www.egovernment.tas.gov.au/information_security_and_sharing/tasmanian_government_information_security_framework/the_tasmanian_government_information_security_policy)

## 7. New South Wales Digital Information Security Policy

There is a requirement in New South Wales that suppliers must comply with the New South Wales Government Digital Information Security Policy to the extent to which their contractual conditions with Agencies require them to do so. The Digital Information Security Policy can be accessed at:

<https://www.finance.nsw.gov.au/ict/sites/default/files/Digital%20Information%20Security%20Policy%202015.pdf>

## 8. Western Australia Digital Security Policy

There is a requirement in Western Australia that suppliers must comply with the Western Australian Digital Security Policy to the extent to which their contractual conditions with Agencies require them to do so. The Digital Security Policy can be accessed at: <https://www.wa.gov.au/government/publications/digital-security-policy>

## 9. Australian Government

The Australian Government requires suppliers to implement Information Security measures which are outlined in program DEEDs and Contracts. For further information, the Australian Government Information Security Core Policy can be assessed at: <https://www.protectivesecurity.gov.au/informationsecurity/Pages/Information-security-core-policy.aspx>

## 10. Related IntoWork Australia Frameworks, Policies and Procedures

The IntoWork Australia Notifiable Data Breach Policy should be read in conjunction with the following IntoWork Australia frameworks, policies and procedures:

- IntoWork Australia Privacy Policy
- IntoWork Australia IT Security Framework
- IntoWork Australia Incident Escalation of Reporting (Medium/Large Businesses) Procedure
- IntoWork Australia Incident Escalation of Reporting (Small Businesses) Procedure

Rev.	Date	Nature of Changes	Approved By
0	[Date of Issue]	Original Issue	[Policy Approver Name]