Information security – checklists

This document contains three checklists:

* Contract development checklist;
* Information and Supplier Security Checklist; and
* Procurement Security Compliance Checklist.

This document supports the [Information security - goods and services procurement guide](https://www.buyingfor.vic.gov.au/information-security-goods-and-services-procurement-guide).

Contract development checklist

# What is the contract development checklist?

This checklist ensures contracts include appropriate security related clauses. The clauses within contracts increase protections to public sector information and assets.

# How to apply the contract development checklist?

 Use this checklist when creating the contract management plan. The checklist helps project managers and contract manages ensure the protection of:

* public sector data,
* information and
* assets

through the legal agreement with the supplier.

|  |  |  |
| --- | --- | --- |
| Item | Item description | Yes/No/NA |
| 1 | Has the contract included clauses related to the requirement to maintain a security program aligned to an industry standard (e.g. ISO 27001)? |  |
| 2 | Has the contract included clauses related to limitation of liability? |  |
| 3 | Has the contract included clauses related to confidentiality of government data? |  |
| 4 | Has the contract included clauses related to Service Level Agreements (SLAs) and penalties? |  |
| 5 | Has the contract included clauses related to supplier financial reporting? |  |
| 6 | Has the contract included clauses related to preventing data loss? |  |
| 7 | Has the contract included clauses related to the supplier being insured? |  |
| 8 | Has the contract included clauses related to the supplier’s requirements to maintain and provide access to business continuity/disaster recovery plans?  |  |
| 9 | Has the contract included clauses related to backup guarantees? |  |
| 10 | Has the contract included clauses related to warranties?  |  |
| 11 | Has the contract included clauses related to breach notification? |  |
| 12 | Has the contract included clauses related to the supplier’s requirements on termination? |  |
| 13 | Has the contract included clauses related to privacy? |  |
| 14 | Has contract included clauses related to:* Security functional requirements
* Security strength requirements
* Security-related documentation?
 |  |
| 15 | Has the contract included clauses related to assurance requirements?* E.g. Penetration testing, iRAP (for cloud services), etc.
 |  |
| 16 | Has the contract included clauses related to acceptance criteria? |  |
| 17 | The contracted can be terminated if the provider fails to comply with provision of the contract? |  |

Information and Supplier Security Checklist

# What is the information and supplier security checklist?

This checklist helps evaluation panels to assess the goods and services for public sector bodies which:

* store, transmit, process or
* have access to Victoria Public Sector data or networks.

The panels assess the suitability of goods and services.

# How to apply the information and supplier security checklist?

Use this checklist when evaluating a supplier’s response to a market approach where the goods or services:

store, transmit, process or

have access to Victoria Government information or networks.

To reduce the burden on project teams:

* information and supplier security assessments should only be undertaken for competitive offers.

|  |  |  |
| --- | --- | --- |
| Item  | Item description | Yes/No/NA |
| 1 | The supplier has agreed to meet the security functional, strength and assurance requirements detailed in the contract? |  |
| 2 | The supplier has provided information security documentation (e.g. frameworks, strategies, policies, procedures, etc.) and/or demonstrated an industry recognised approach to security? |  |
| 3 | The supplier has provided third party security assurance reports (e.g. SOC2, penetration testing, ISO27001 Certification, iRAP assessment or another independent audit)? |  |
| 4 | The supplier has sufficient personnel security controls in place? |  |
| 5 | The supplier has sufficient physical security controls in place? |  |
| 6 | The supplier has sufficient information security controls in place? |  |
| 7 | The supplier has sufficient ICT security controls in place? |  |
| 8 | The supplier has a security incident management plan? |  |
| 9 | Is a governance arrangement in place to managing ongoing security requirements? |  |
| 10 | An organisationally defined appropriate person (e.g. ICT manager, cyber security lead, risk committee, etc.) has accepted any residual risk? |  |

Procurement Security Compliance Checklist

# What is the procurement security compliance checklist?

This checklist supports buyers compliance with risk management requirements. Buyers ensure management of supply chain risks to the public when:

* buying goods and services for public sector bodies, which
* store, transmit, process or have access to Victoria Public Sector data or networks.

# How to apply the procurement security compliance checklist?

Use this checklist when buying goods and services before signing contracts.

|  |  |  |
| --- | --- | --- |
| Item  | Item description | Yes/No/NA |
| 1 | The project team have included security clauses within the contract? See Contract development security checklist |  |
| 2 | Information and supplier security residual risk has been accepted by an appropriate person? See Information and Supplier Security Checklist |  |

© State of Victoria 2020 (Victorian Government Purchasing Board)



This work is licensed under a [Creative Commons Attribution 4.0 licence](http://creativecommons.org/licenses/by/4.0/). You are free to re-use the work under that licence, on the condition that you credit the State of Victoria as author. The licence does not apply to any images, photographs or branding, including the Victorian Coat of Arms, the Victorian Government logo and the Department of Treasury and Finance logo.

Copyright queries may be directed to IPpolicy@dtf.vic.gov.au