audit office
OF NEW SOUTH WALES

Third party security policy

Date: December 2023

INSIGHTS FOR BETTER GOVERNMENT

contents

1.	**Policy statement**	**1**
2.	**Policy objective**	**1**
3.	**Scope**	**1**
3.1	In scope	1
3.2	Out of scope	1
4.	**Roles and responsibilities**	**1**
4.1	Third party responsibilities	1
4.2	Audit Office roles and responsibilities	2
5.	**Third party security management**	**3**
5.1	Principles	3
5.2	Approach to managing third party risk	3
5.3	Inherent and residual third party risk classification	3
5.4	Assessment frequency	4
5.5	Mandatory requirements	4
5.6	Exemptions	5
6.	**Third party risk assessment procedures**	**5**
6.1	Assessment process outline	5
6.2	Minimum contractual requirements	6
6.3	Additional audit service provider mandatory requirements	7
6.4	Recommended contractual considerations	7
6.5	Minimum disclosure requirements	8
7.	**Regulatory context**	**9**
7.1	Legislation	9
7.2	Policy	10
8.	**Data handling**	**10**
9.	**Contact point**	**10**
10.	**Review**	**10**
Appendix A – Standard policy definitions		**11**

1. Policy statement

Third parties may have access to a wide range of Audit Office of New South Wales (Audit Office) systems or information. This access could be either through storing information or technology belonging to the Audit Office at an offsite facility (e.g. as part of a cloud service provider arrangement), or through having remote or physical access to systems or information at Audit Office premises.

As a result, appropriate controls and mitigation processes must be established with all third parties to minimise the risk associated with potential security breaches to within risk appetite. The Audit Office has a low risk appetite for the loss of confidential or sensitive information resulting in compliance breaches, business disruption, financial loss or reputation damage (strategic risk #6). In that context, the purpose of this policy is to ensure that the Audit Office's information and systems that are accessed by external suppliers and service providers are subject to appropriate protection.

2. Policy objective

The Audit Office uses third parties for the delivery of audit, information technology, and other business services to the organisation. The risks associated with the use of those third parties need to be managed, so that the Audit Office can gain assurance that its information, services, and stakeholders are protected within the Audit Office's risk appetite.

3. Scope

3.1 In scope

This third party security policy applies to supplier-side arrangements only i.e. to arrangements in which the Audit Office:

- partners with third parties in the delivery of its audit activities, or
- permits third parties to process, store, collect or transfer Audit Office data, or
- permits third parties to access technology infrastructure, data or applications hosted or managed by the Audit Office, or
- outsources the operation, development or management of technology infrastructure, data or applications to external hosting/outsourcing suppliers.

This policy applies to suppliers and approved sub-contractors of suppliers.

These may include external hosting/outsourcing organisations, outsourced applications development, and process outsourcing service suppliers for services such as payroll.

This policy applies to all vendor agreements entered into after 1 December 2023. Where existing vendor agreements are in place, the Audit Office will work collaboratively with suppliers to transition to the minimum standards and principles during the agreement.

3.2 Out of scope

Contractors and consultants who agree to the Audit Office acceptable use policy and only use Audit Office systems to process, store, collect or transfer Audit Office data, are subject to a police check and do not require to be assessed as part of this assessment program. Systems access must be authorised as per usual business processes.

Contractors and consultants who are not solely using Audit Office systems are still required to be assessed unless an exemption is sought.

4. Roles and responsibilities

4.1 Third party responsibilities

Third parties engaged, or seeking to be engaged by the Audit Office must agree to be assessed against this policy by the Audit Office as part of its assessment program. Both the third party and the Audit Office should work collaboratively and in good faith to address any security concerns and risks identified in this assessment process.

4.2 Audit Office roles and responsibilities

The CIO will notify all staff members when this policy is updated. Delegation holders must consider if existing vendors need to be notified of the updates. When updated the policy will be made available on the Audit Office website.

All staff members who have delegation (delegation holders) to enter into agreements on behalf of the Audit Office should ensure contracts refer to this policy where the third party meets the scope requirements as outlined in section 3.

Vendor Risk Management Group (VRMG)

This policy refers to a group called the Vendor Risk Management Group (VRMG); in relation the Audit Office, this consists of the Chief Information Officer (CIO), the Executive Director Finance and Performance and the Director Governance (Risk and Ethics), each role of the group may delegate the responsibility, but remain accountable.

- Developing and maintaining the Audit Office's third party security framework.
- Issuing third party security questionnaire.
- Reviewing security assessment responses to identify risks and making recommendations on their management.
- Notifying the delegation holder of risks identified in the third party security questionnaire and any mitigations recommended for inclusion in contracts.

Delegation Holder / Buyer

A delegation holder is an employee defined in the delegation register. A buyer is an employee who is operating on behalf of a delegation holder, but does not have authorisation to accept the risk on behalf of the delegation holder.

- Notifying the VRMG as early as possible of any intent to procure services in scope of this policy.
- Reviewing risks and mitigations identified by the VRMG, and ensuring these mitigations are put in place and accepting residual risk.
- The delegation holder may defer to a more senior delegation holder when there is concern about accepting a risk or mitigating control.

Chief Information Officer (CIO)

- Maintenance of this policy and providing guidance on its application.
- Ensuring in scope third parties (except for Audit Service Providers) are assessed regularly as determined and required by the assessment frequency section 5.4.

Senior Procurements and Contracts Officer

- Promoting an awareness of this policy to delegation holders.
- Ensuring procurement policy, Request for Information, Quote and Tender notifications refer to this policy.
- Ensuring the Audit Office's standard agreements appropriately reference the requirements of this policy.
- Monitoring that audit service providers are assessed regularly as determined and required by the assessment program.

Governance Team

To assist in coordinating responses to data breaches or cyber incidents consistent with the Data Breach Management Policy, and supporting the Auditor-General to meet mandatory reporting obligations.

5. Third party security management

5.1 Principles

The following principles are recognised as fundamental to ensuring procurement with third parties support the Audit Office requirements for the security of its data:

- Audit Office information shall be protected in accordance with applicable laws and NSW Government directives.
- Formal agreements shall be used to manage all third party arrangements.
- Responsibility for protecting Audit Office information ultimately resides with the Audit Office.
- Third Party management is an ongoing process throughout the relationship.

5.2 Approach to managing third party risk

Area	Control
Due diligence	Third parties shall be assessed using an approved, defined process.
Risk assessment	The risks associated with the use of third parties shall be assessed in accordance with the Audit Office risk management framework.
Contractual obligations	Agreed mitigations that are identified as part of the assessment program will be defined and included in contracts as clauses. Security obligations shall be defined and included in contracts.
Stakeholder management	Where appropriate, a designated Audit Office staff or delegate will govern each relationship.
Assessment program	An assessment program will provide a framework for and guidance on assessing third party security risk.
Business requirements	Third party access and privileges shall not exceed business requirements.
Authorisation	All third party access to Audit Office systems and data shall be formally requested via Service Desk and authorised by the CIO or their delegate.
Access termination	Third party access to Audit Office systems and facilities shall be terminated upon contract termination.
Necessary traffic	The Audit Office shall restrict connectivity to the minimum required to enable data transfer with Third Parties and/or access of their systems.

5.3 Inherent and residual third party risk classification

Third parties are classified with an initial inherent risk classification and a residual risk classification after an assessment is completed. The inherent risk classification is completed at the beginning of the assessment process and used to tailor the third party risk assessment questions related to the identified risk. The residual risk classification is assessed based on the responses to the questions from the third party and considers any mitigating controls agreed.

All assessments are completed by the VRMG against a risk scale which determines the impact and likelihood of a risk event including but not limited to:

- Loss of confidential or sensitive information resulting in compliance breaches, business disruption ore reputational damage
- Loss of availability or interruption to normal business activities resulting in lost productivity or being unable to continue normal business activities
- Loss of integrity such as corruption of information, resulting in the inability to deliver business activities.
- Financial/reputational damage to the Audit Office through cyber fraud.
- ASP's, suppliers, consultants or 4th parties are enablers of cyber-events

Factors that contribute to the risk assessment (where applicable) include:

- the sensitivity of the data,
- the level of access that is required,
- value of the agreement,
- the type of service being offered,
- prior assessments having been completed,
- other contributing factors the Audit Office deem appropriate.

Guidance for Audit Office staff is provided in Alfie.

5.4 Assessment frequency

Third party security assessments must take place prior to execution of a contract. Frequency of assessments after the execution contract are based on materiality which considers the residual risk classification (section 5.3) and factors that contribute to materiality such as strategic importance, criticality, contract value, length of commitment.

All material third parties should be assessed as part of the procurement process on an annual basis. All non-material third parties should be assessed as part of an ongoing assessment once every two years.

The materiality rating is stored in a register, links to the register and guidance for Audit Office staff are provided in Alfie.

5.5 Mandatory requirements

The following requirements are deemed to be mandatory for all in scope (as per section 3) third parties engaged by the Audit Office. Third Parties must acknowledge compliance with them as part of a formal procurement response.

Area	Requirement
Participation in the assessment program	Third parties must agree to be assessed in line with the assessment program.
Contractual and disclosure requirements	Third parties must agree to work with the Audit Office in good faith on minimum disclosure requirements and contractual commitments defined in section 6 Minimum disclosure requirements are expected to be continuous during the lifetime of the product or service where any change emerges.
Data exchange	Exchange of sensitive data (refer section • Regulatory context

5.6 Legislation

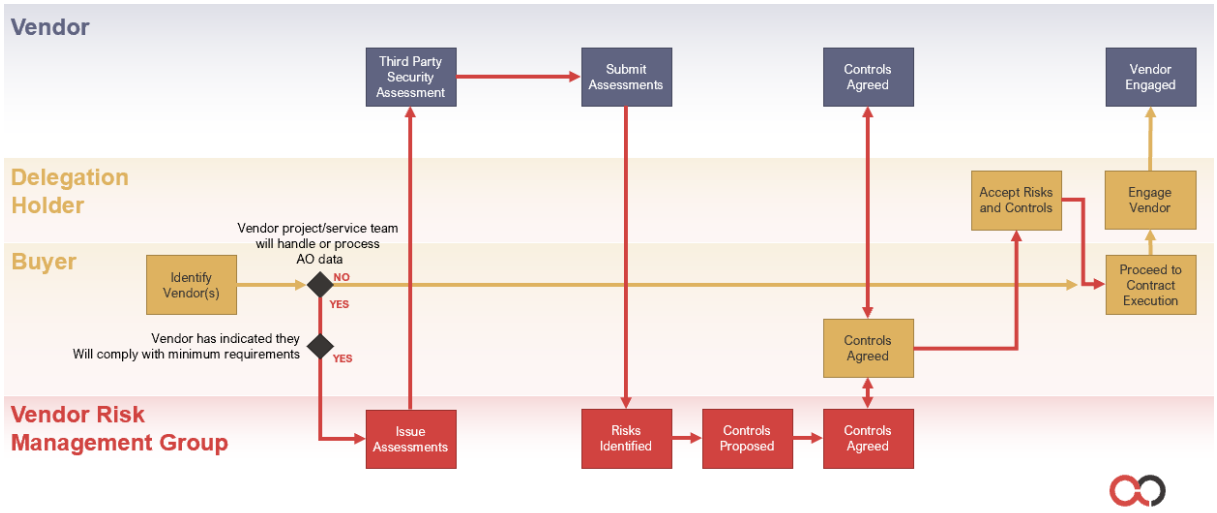
	• Privacy and Personal Information Protection Act 1998 (NSW) • Privacy Act 1988 (Commonwealth) • Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) • Corporations Act 2001 • Australian Securities and Investments Commission (ASIC) Act 2001. **5.7 Policy** • Data breach management policy • Procurement and contract management policy • Risk Management Policy • Information security management framework • Procurement framework (NSW) • NSW cyber security policy Data) between Third Parties and the Audit Office must be mutually agreed and may only be one of the following methods: • encrypted data transfer through a secure application platform (direct entry into a system) • encrypted and protected file share platforms (e.g. ShareFile file transfer) • password protected email attachments • password protected physical file transfers (USB Storage).
Cyber Incident or breach notification	Third parties engaged by the Audit Office must immediately notify the Audit Office of a suspected or actual data breach including a cyber security incident that relates to any data, systems infrastructure or processes used in this arrangement with the Audit Office. Such notifications should be addressed to Our contact person listed in the agreement, and to the Audit Office's data breach response team at databreach.notification@audit.nsw.gov.au. Third parties must follow reasonable directions from the Audit Office to assist in containing and responding to a data breach, including by providing information to the Audit Office for our mandatory reporting obligations, and reasonable directions that arise from incident investigations.
Shared awareness around cyber resilience	The Audit Office may conduct lessons learned exercises into an incident or breach and where agreed by both the Audit Office and the affected party, share this information with other Third Parties to prevent re-occurrence.

5.8 Exemptions

Exemptions to the assessment process may be approved by the Chief Information Officer.

Where exemption is sought third parties must comply with the mandatory requirements in section 5.5, minimum contractual requirements in section 6.2 and minimum disclosure requirements in section 6.5. Not being able to comply with these requirement requires approval from the Deputy Audit General.

6. Third party risk assessment procedures



6.1 Assessment process outline

The buyer and the delegation holder may be the same person.

1. As part of the procurement process the buyer must determine if the third party needs to be assessed as per section 3.
2. In scope third parties should review the minimum third party security requirements (see section 6.2) to confirm they wish to continue with the procurement process and the following assessment.
3. The VRMG complete an inherent risk assessment (section 5.3) which is used to tailor the questions that form the third party security questionnaire.
4. A third party security assessment is issued in the form of a self-assessment questionnaire.
5. The questionnaire helps the Audit Office build an understanding of security controls and risk with regards to a third party organisation. Assessments can be shared with other members of your organisation to assist in completing.
6. Third parties are encouraged to add justifications to their answers where they believe it will help create a better understanding of the risk and control landscape.
7. The buyer will need to review and negotiate any potential mitigation with the vendor until the delegation holder responsible for the procurement is satisfied to accept the risks and mitigations.
8. The VRMG will need to approve any mitigating controls and will rate the third party vendor with a residual risk classification.
9. Contract execution may then take place.

The full process for Audit Office staff can be found on Alfie.

6.2 Minimum contractual requirements

The following table outlines the requirements that must be addressed in formal agreements with a third party.

Area	Potential Requirement
Service termination	Changes to the nature of an engagement and/or agreement that pose an unacceptable level of security risk must be prevented or allow for the agreement to be terminated.
Service continuity	Handover/Transition-out processes must be defined to ensure the continuity of Audit Office business processes.
Data jurisdiction	Third Party and their sub-contractors will **NOT**, without requesting and seeking express permission of the Audit Office store, process, access, or transfer Audit Office data outside of Australia. Audit Office data shall be only transferred, stored and processed in jurisdictions, considered to be of an acceptable risk level to the Audit Office subject to the data in question. Data jurisdictions relevant to the agreement should be listed in the contract.
Access to data	Audit Office data must only be accessed on a 'need to know' basis in providing services to the Audit Office. Access to our data must be defined in the contract.
Compliance with relevant laws	Compliance with relevant laws and obligations will be included in contracts where relevant. These may include: • *Privacy and Personal Information Protection Act 1998 (NSW)* including the privacy principles under the Act • *Health Records and Information Privacy Act 2002 (NSW)* including the health privacy principles under the Act • *Privacy Act 1988 (Commonwealth)Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) • *Corporations Act 2001* • *Australian Securities and Investments Commission (ASIC) Act 2001*.
Compliance with Audit Office policies	The obligation to comply with Audit Office Information Security Management System (ISMS) policies and standards that are relevant to the engagement. These will be added to the contract as needed.
Data offboarding	The obligation to return to the Audit Office information, or destroy information which cannot be returned, upon termination of the contract will be included in contracts.
Cyber Incident or Breach Notification	Third parties engaged by the Audit Office must immediately notify the Audit Office of a suspected or actual data breach including a cyber security incident that relates to any data, systems infrastructure or processes used in this arrangement with the Audit Office. Such notifications should be addressed to Our contact person listed in the agreement, and to the Audit Office's data breach response team at databreach.notification@audit.nsw.gov.au. Third parties must follow reasonable directions from the Audit Office to assist in containing and responding to a data breach, including by providing information to the Audit Office for our mandatory reporting obligations, and reasonable directions that arise from incident investigations.
Data jurisdiction change	The obligation to report to the Audit Office on any substantive changes to data handling and storage procedures (such as change of country where

	data is being stored) within a mandated timeframe will be included in contracts.

6.3 Additional audit service provider mandatory requirements

Staff Awareness	Third parties must ensure their staff working with Audit Office data will be briefed on cyber risk and their responsibilities at least annually.
Staff Screening	Third parties must ensure their staff working with Audit Office data have been subject to a criminal record check.

6.4 Recommended contractual considerations

The following table outlines the requirements that should be considered and addressed, as required or not, when forming an agreement with a third party.

Ideally these requirements if relevant to an engagement should be flagged as part of a Request for Information, Quote or Tender.

Area	Potential Requirement
System architecture	Architecture of systems developed on behalf of the Audit Office must be clearly documented and provided to the Audit Office to ensure continuity of service. Third parties and the Audit Office must put appropriate security safeguards around this information.
Availability	Hosted systems shall be measured against defined availability requirements.
Backup and recovery	Backup and recovery measures of Audit Office data handled by the third party must be implemented in accordance with the Audit Office's business requirements.
Ownership of access	The Audit Office must retain ownership of access control to systems, technology infrastructure and platforms it procures from third parties.
Source code	The Audit Office shall have rights to source code developed on its behalf.
Right to audit	The right for the Audit Office, to audit the third party with relation to systems and/or security processes.
Security testing	Obligation for the third party, to conduct security testing such as vulnerability scanning and penetration testing, will be included in new contracts

6.5 Minimum disclosure requirements

The following disclosure requirements should be reviewed by the Third Party, and if disclosure is required, should be addressed with some contextual detail in the response to a formal procurement process. Disclosures will be considered as part of the evaluation process. Any change impacting one of the disclosures during the lifetime of the product and/or service should be communicated promptly.

Area	Disclose if…

Jurisdiction	Any Audit Office data related to this engagement or otherwise will be stored, processed, accessed, or transferred outside of Australia by the Third Party or one of Third Party's contractors. If so, please list the countries and what Audit Office data related to this engagement will be handled in them.
Multi factor	Any remote access to the third party's systems (including email) where Audit Office data related to this engagement will be stored is not protected by Multi-Factor Authentication If so, please list the systems and what Audit Office data will be stored in them.
Sub-processors and sub-contractors	Any Audit Office data related to this engagement or otherwise will be stored, processed, accessed, or transferred by one of the third party's suppliers or contractors. If so, please list the parties.
Third party systems	The third party intends to store, process or transfer Audit Office data, related to this engagement or otherwise, in another third party system that is not fully owned, operated and managed by your organisation. If so, please list the systems. E.g. you propose to use file sharing service x, online email service y, or collect data using system z. For each system confirm: • The system and data hosted in Australia. • Access protected by multi-factor authentication
New technology or services	If the third party introduces or intends to introduce new technology including applications or services which handle Audit Office data they will notify the Audit Office promptly
Artificial intelligence technology	Third Parties must inform Audit Office if any part of the solution or service being offered uses Artificial Intelligence technologies.
Critical Vulnerabilities	Advise the Audit Office of any critical vulnerability promptly. The third party should disclose: • an explanation of the vulnerability, including its impact • applications, products or services affected • potential end users affected • potential mitigation steps to take • ongoing remediation and security arrangements • target timelines and periodic updates • confirmation of remediation
Security program	The third party organisation is not covered by a security program that is based on industry standards (e.g. PCI, ISO27001/2, SOC2 etc)
Business continuity	Your organisation does not have a formal business continuity plan to continue providing services to the Audit Office in the event of a disruption. If not please outline if there is a plan to develop one or explain how you will ensure operational consistency during a major disruption.
Assurance	Your organisation does not have an annual internal or independent audit covering your security program.

	If not please list how regularly this does occur and when it is next planned.
Staff awareness	Your organisation does not provide annual cyber awareness training to your staff. If not please confirm how you will ensure your staff working with Audit Office data will be briefed on cyber risk.
Staff screening	Your staff on-boarding process does not include a criminal record check. If not please confirm how you will ensure your staff working with Audit Office data will be covered by a criminal record check.

7. Regulatory context

7.1 Legislation

- Privacy and Personal Information Protection Act 1998 (NSW)
- Privacy Act 1988 (Commonwealth)
- Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act)
- Corporations Act 2001
- Australian Securities and Investments Commission (ASIC) Act 2001.

7.2 Policy

- Data breach management policy
- Procurement and contract management policy
- Risk Management Policy
- Information security management framework
- Procurement framework (NSW)
- NSW cyber security policy

8. Data handling

This policy refers to sensitive data. Sensitive data should be considered any data that if compromised can be considered to cause damage to an individual, organisation, New South Wales local or state government entities, the Audit Office of NSW, or Australian government in general.

9. Contact point

If staff or third parties have question about this policy, they should contact the Chief Information Office, cio@audit.nsw.gov.au.

10. Review

This policy is to be reviewed every two year and whenever changes are made to maintaining third party security processes.

Changes to this policy will be notified to impacted vendors of the Audit Office of NSW.

Changes to this policy will be notified to staff members of the Audit Office who have delegation to enter into agreement.

Appendix A – Standard policy definitions

Audit Office of NSW used for initial reference in document, thereafter referred to as the Audit Office.

Manager is an employee who is responsible for the supervision of workers.

Staff or staff member includes all employees of the Audit Office, including contractors and temporary staff.

Visitor means a member of the public who visits the Audit Office premises.

Worker includes all members who are directly or indirectly engaged by the Audit Office to conduct work in the interest of the organisation, paid or unpaid.

Workplace means premises where work is usually conducted, including client sites, working from home and where permission has been given to conduct work from.