THIRD PARTY SECURITY POLICY

Responsible Position:	Chief Information Officer	HP RM Reference:	D1828570
Approved By:	Office Executive	Version:	2
Date Approved:	23/09/2019	Next Review Date:	23/09/2020

Table of Contents

1 Introduction

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 infrastructure belonging to 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. In that context, the purpose of this document 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 Purpose

The Audit Office uses third parties for the delivery of Audit, ICT 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

This Third Party Security policy applies to supplier-side arrangements only i.e. to arrangements in which the Audit Office:

- outsources its audit activities, or
- permits third parties to access ICT infrastructure, data or applications hosted within Audit Office premises, or
- outsources the operation, development or management of ICT infrastructure, data or applications to external hosting/outsourcing suppliers.

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

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

It is the responsibility of the Vendor Risk Management Group to update, review and maintain this policy. The Vendor Risk Management Group consists of the Chief Information Officer, the Chief Financial Officer and the Chief Risk Officer.

Roles and responsibilities relating to the various stages of the third party security management process are outlined in the Audit Office's Vendor Management RACI matrix (D1920336).

This policy comes into effect for all new vendor agreements entered into after approval on 1 November 2019. Where existing vendor agreements are in place best efforts should be made to request compliance with the assurance program.

4 Third Party Security Management

4.1 Assurance process

The following flowchart defines the process for third party security assessment.
The characteristics of the third party vendors that will be assessed are listed in the rest of this policy.

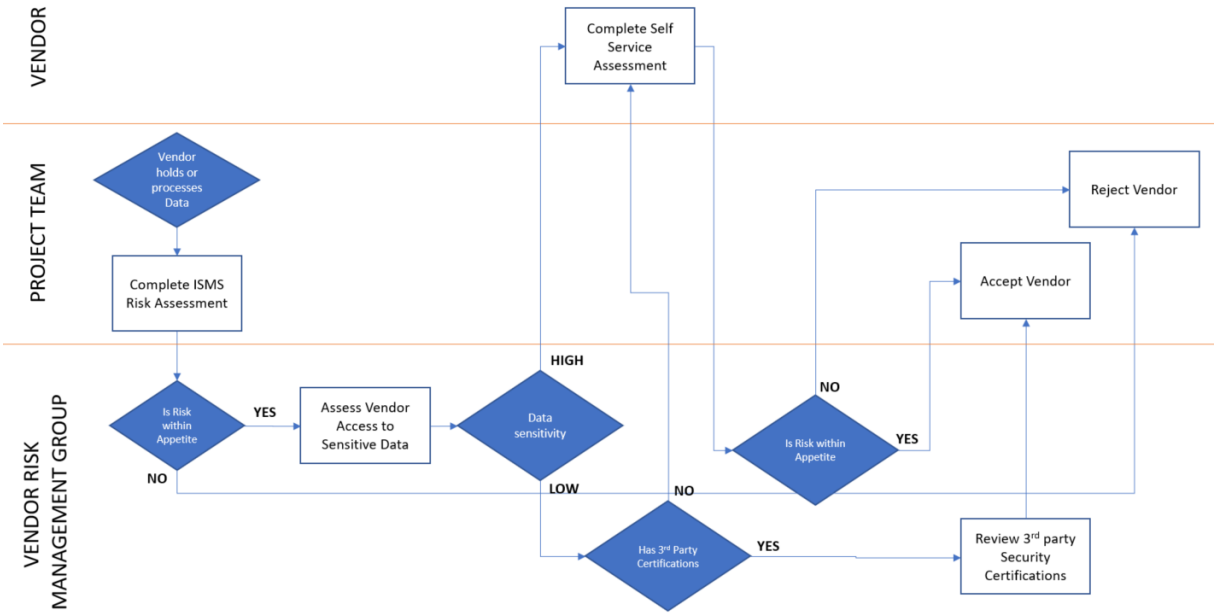

Figure 1 - Third party security assessment

4.2 Third Party security incident notification process

Audit Office vendors must agree to notify the Audit Office of NSW in the event of a cyber incident or breach that relates to any data, systems infrastructure or processes used in its arrangement with the Audit Office.
Such notifications should be addressed to governance@audit.nsw.gov.au

4.3 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 vendors to prevent re-occurrence.

4.4 Data exchange

Data transfer methods between vendors and 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 attachements
- password protected physical file transfers (USB Storage).

5 Third Party Security Requirements

5.1 Principles

The following principles are recognised as fundamental to ensuring relationships 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
- 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.

The following sections provide a suite of controls that apply as general requirements and conditions, as relevant to the third-party environments. These controls will be used to assess third party vendors and the outcomes of these assessments will be evaluated in line with the risk appetite of the Audit Office. Best efforts should be made to apply all controls were relevant.

5.2 Engagement requirements

Engagement requirements are to be considered prior to, and during, the process of engaging a vendor or third party organisation.

i) Due diligence

Requirement	**Third parties shall be assessed using an approved, defined process.**
Rationale	A poorly defined or inconsistent approach to assessing third parties may result in unidentified risks, and loss of availability, loss of services, and/or loss of confidentiality of sensitive information. Additionally, once a supplier has been engaged, it may be difficult to retrospectively apply security controls.

Approach	• A third party due diligence program will be implemented to assess all third parties for solvency and security prior to engagement.
	• Diligence undertaken will be proportionate to the risk posed to the organisation.
	• The due diligence program may include:
	  ○ verification of certification (PSPF, ISM, ISO27001/2, DISP, SOC2)
	  ○ self-assessment questionnaires
	  ○ security controls audit
	  ○ Audit Office manual assessment.
	• Confirmation of data breach notification and privacy requirements should be included in the due diligence process.

ii) Risk assessment

Requirement	**The risks associated with the use of third parties shall be assessed.**
Rationale	Outsourcing critical business processes potentially reduces the Audit Office's ability to effectively manage and maintain an acceptable risk profile within the environment.

	The reduced ability to manage risks and control effectiveness may result in the compromise of Audit Office information or loss of service availability. This may cause downstream impacts to Audit Office stakeholders, individuals and the community.
Approach	• Outsourcing arrangements and third party providers handling Audit Office Data shall be assessed for risk in accordance with the Audit Office Risk Management Framework. • Security risk assessments should be conducted prior to engagement of the third party, at least annually thereafter, and upon any changes in the risk profile of the third party.

iii) Contractual obligations

Requirement	**Security obligations shall be defined and included in contracts.**
Rationale	Security requirements not explicitly included in agreements with third parties may not be implemented or enforceable, and may put Audit Office information and services at risk.

Approach	• Compliance with relevant laws and obligations will be included in contracts where relevant. These may include:
	  ○ *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.*
	• An obligation to comply with the Information Protection Principles in Part 2 of the *Privacy and Personal Information Protection Act 1998* (as if the third party were a "public sector agency" within the meaning of that Act) to the extent that those Information Protection Principles are not inconsistent with any legal obligations (if any) that the third party otherwise has under or arising pursuant to the *Privacy Act 1988* (Cth) or other legislation relating to privacy to the extent such legislation is relevant to the Agreement
	• The obligation to comply with Audit Office security policies and standards, or demonstrate compliance with industry standards will be included in contracts. These may include:
	  ○ Australian Government Protective Security Policy Framework (PSPF)
	  ○ Australian Government Information Security Manual (ISM)
	  ○ ISO 27001.
	• The right to audit the third party will be included in new contracts.
	• The right for the Audit Office, or obligation for the third party, to conduct security testing such as vulnerability scanning and penetration testing, will be included in new contracts.
	• 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.

	• The obligation to report a security breach to the Audit Office within a mandated time frame will be included in contracts. • 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.

iv) Service obligations

Requirement	Service obligations will be defined and included in contracts
Rationale	Where security controls, obligations and service levels are not defined, or poorly defined, the Audit Office may have no recourse in the event of a service failure.

Approach	• The scope of required services, expected security controls, and service levels will be clearly defined for all contracted services.
	• A register of controls will be documented, along with responsible party and service level expectations.
	• The service levels defined may include the availability of the hosting itself, any information technology services provided, incident response or breach notification, contract changes or cancellation, or the like.
	• Service levels will meet Audit Office requirements for security.
	• The allocation of responsibilities between the Audit Office and the third party will be explicitly defined, in particular for:
	  ○ logging and monitoring
	  ○ incident handling
	  ○ business continuity
	  ○ disaster recovery.
	• Consideration for loss of availability or unmet service levels should be included in contracts.
	• Obligations for service providers downstream from the contracted party should be included in defined security obligations.
	• Contract terms should include the obligation to report to the Audit Office on compliance with security controls, service levels, and agreed metrics, at a defined interval.

5.3 Management requirements

Management requirements are generally applicable to the ongoing management and assurance of the services provided by, or the operation of, a vendor or third-party organisation.

i) Stakeholder management

Requirement	A designated Audit Office employee or delegate will govern each relationship.
Rationale	Having a single Audit Office point of contact for each relationship shall ensure the Audit Office gets the best outcomes from the relationship.

Approach	• Assign a relevant Audit Office employee or delegate to each third party who has ultimate responsibility and accountability for the relationship and the activities undertaken by the third party. • The designated employee or delegate shall be informed of the risks associated with the third party. • The designated employee or delegate shall be responsible for ensuring the third party is monitored and evaluated against the agreed service levels.

ii) Assurance program

Requirement	**A program of third party assurance activities will be implemented.**
Rationale	In order to have an understanding of the risks associated with the use of third parties, and assurance that those third parties are fulfilling their obligations, the Audit Office may validate third party compliance with their security obligations.

Approach	• Third parties must be assessed for risk in accordance with the Audit Office Risk Management Framework and the ISMS Risk Assessment Framework.
	• Should the risk associated with the third party be outside of the Audit Office's acceptable risk level/posture, further assessment of security controls may be warranted.
	• Security testing must be conducted from time to time, to verify security controls have been implemented as asserted by the third party. This may include:
	  ○ penetration testing and vulnerability reporting
	  ○ security control audits.
	• Security audits and testing must be conducted by a qualified party independent of the party or environment tested.

iii) Human security

Requirement	**Third party providers shall screen employees for their suitability for employment.**
Rationale	Where providers have access with elevated privileges to environments hosting the Audit Office's systems or information, a breach by that provider may materially affect the Audit Office and its operations.
Approach	• The Audit Office will request evidence of policy and procedures supporting screening of employees at the third party. • This evidence may include a review of relevant certifications or directly obtaining supporting documentation. • The policies and procedures must include either police checks, reference checks, or other checks to ascertain the suitability of applicants to work in sensitive positions.

iv) Security awareness and training

Requirement	**Third party personnel accessing Audit Office information and environments shall understand and agree to their responsibilities.**
Rationale	Enforcing compliance with Audit Office security policies and standards will not be possible without third parties understanding and acknowledging their responsibilities to comply with those policies and standards.
Approach	• Third parties must acknowledge in writing that they have read and comply with the Information Security Policy and related standards and detail to the Audit Office areas where they are not compliant.

5.4 Third party access requirements

Third party access requirements define how and where access to Audit Office systems and information is to be granted to a third-party organisation.

i) Business requirements

Requirement	**Third party access and privileges shall not exceed business requirements.**
Rationale	Access by third parties to Audit Office environments, systems, and information may result in loss or unauthorised disclosure of that information.
Approach	• Third party access to Audit Office information shall be provided based upon the minimum access levels, time periods, and privileges required to perform their duties. • Access reviews shall be performed in line with the Identity and Access Management policy to verify that the provisioned access is authorised, is the minimum required, and ensure that unnecessary access is removed. • Should access need to be extended beyond the original time frame requested, a new request for access should be submitted.

ii) Authorisation

Requirement	**All third-party access shall be formally requested and authorised.**
Rationale	Third party access to systems and environments must be authorised based on a legitimate business need and restricted to only that access required.
Approach	• A formal registration and de-registration process must be documented and implemented, with approval provided by a relevant Audit Office employee or delegate. • A record must be maintained of all third-party access requests, approvals, and organisations and persons provided access, including: ○ business justification for access

	○ explicit resource requirements ○ duration of access required.

iii) Access control

Requirement	Access and traffic shall be restricted to those necessary for business.
Rationale	Overly permissive access may result in compromise of the environment and unauthorised disclosure of sensitive information.
Approach	• Where required, access must be provided in accordance with the following standards: ○ Audit Office Identity and Access Management Policy. • Enable only required ports, protocols, and services for the host or application. • All content must be scanned for malicious files or egress or sensitive data.

5.5 Termination of service

Termination of Service requirements define how the Audit Office disengages from a third-party organisation.

i) Service termination

Requirement	Services posing an unacceptable level of risk shall be terminated.
Rationale	Services provided can change over time and change the level of risk to the Audit Office, or the Audit Office's appetite for risk may change. Should a third-party risk eventuate, the Audit Office may incur reputational damage or experience an impact to the service it provides to its stakeholders.
Approach	• Third parties must be risk assessed as per the Audit Office risk assessment process. • Where control deficiencies or unacceptable risks are identified which are unable to be corrected or mitigated, best efforts should be made to amend or terminate the contract. • The costs for contract termination must be understood and captured in the contract to prevent punitive termination actions taken by the provider.

ii) Access termination

Requirement	Access shall be terminated upon contract termination.
Rationale	There is a risk of third parties committing malicious activities should they retain access beyond their contract term.

Approach	• Disable or remove third party physical and logical access to Audit Office systems and environments upon contract termination, or where required, upon completion of handover. • All artefacts, such as computers, 2FA tokens, access passes and identification must be returned upon contract termination. • Where contracts are terminated prematurely (e.g. due to breach of contract provisions), removal of access shall be undertaken immediately.

iii) Service continuity

Requirement	**Handover processes shall ensure the continuity of Audit Office business processes.**
Rationale	The availability of business processes which have been outsourced may be at risk should handover not occur smoothly, causing impact to Audit Office stakeholders.
Approach	• Disengagement agreements shall be included in contracts. • Information under the control of the service provider shall be returned to the Audit Office, and any remaining copies destroyed. • A handover plan shall be documented and agreed with the third party prior to termination of the contract. • Handover must be conducted within a reasonable time frame defined by the Audit Office, and those timeframes included in the contract agreement.

iv) Information recovery

Requirement	**Information held by third parties shall be repatriated by the Audit Office, or destroyed.**
Rationale	Audit Office information held by third parties may be subject to unauthorised disclosure should it be stored for longer than necessary. The Audit Office may need to retain the information for statutory or regulatory purposes, even though the service is terminated.
Approach	• Audit Office information shall meet legal requirements for storage and retention, regardless of storage location or custodianship. • The information to be returned and format of that information shall be included in contracts. • All information shall be returned to the Audit Office using the agreed medium and format. • Liability for lost or corrupt data should be included in contracts where possible.

6 Hosted/Cloud Service Security Requirements

6.1 Principles

Service providers who make use of third party hosted and/or managed infrastructure and systems, including Cloud services, present additional risk to the Audit Office and are subject to additional requirements.

These controls apply in addition to the general requirements and conditions outlined in section 5, and as relevant to a hosted/SaaS/cloud environment.

These controls will be used to assess third party vendors and the outcomes of these assessments will be evaluated in line with the risk appetite of the Audit Office. Best efforts should be made to apply all controls were relevant. The CIO may offer guidance as to what controls are relevant to hosted/SaaS or other cloud service vendors.

6.2 Engagement requirements

Engagement requirements are to be considered prior to, and during, the process of engaging a vendor or third-party organisation.

i) Hosting jurisdiction

Requirement	**Information shall be hosted in jurisdictions whose laws are not a risk to the Audit Office, or to persons about whom information is stored.**
Rationale	Where information is hosted in jurisdictions other than Australia, the Audit Office (or supplier) may be subject to a lawful requirement to disclose information that would pose an operational or reputational risk. Additionally, once a supplier has been engaged, it may be difficult to retrospectively apply security controls.
Approach	• If data is hosted outside Australia, the laws of countries in which the Audit Office's information is hosted (relating to the classification of information) must be evaluated for the risk to the Audit Office's operations and reputational, including: ○ loss of control of the information ○ discoverability of the information by governments and other unauthorised third parties ○ record retention time-frames ○ ability to meet local laws for safekeeping of records ○ backups must be considered in the assessment of risk ○ the Audit Office must select a jurisdiction acceptable to the Audit Office Governance team and Privacy Officer for hosting sensitive information a register of jurisdictions that have been evaluated and found suitable should be documented and maintained.

ii) System architecture

Requirement	**A designated Audit Office employee or delegate will govern each relationship.**

Rationale	Without an understanding of the systems hosting the Audit Office information, the Audit Office may not have a complete understanding of the risks associated with those systems, and the likelihood of compromise.
Approach	• Develop a system design document, including all hosts supporting the system, ports and protocols used to transmit information, and services available on the hosts. • The information types and their classification used within the system shall be included in design documents. • All controls within the hosting environment should be documented, including firewalls, logging and monitoring, proxies, breach detection, file integrity monitoring, etc. • Include hosting locations in design documents. • System architecture documentation must be maintained ongoing.

iii) Customer segregation

Requirement	**Audit Office data, processing, and traffic shall be isolated from the provider management zones and other tenants.**
Rationale	Lack of controls to segregate the Audit Office's information and traffic from other tenants and service providers may result in compromise of Audit Office data.
Approach	• Ensure the hosting provider has logical controls to segregate the Audit Office's data from other tenants where infrastructure or the application stack is shared with other tenants. • Ensure a separate database and storage solution is used for the Audit Office's data, so that deletion can be assured when required. • Ensure that the architecture and implementation of software isolation techniques such as virtualisation and containers is security reviewed.

iv) Availability

Requirement	**Hosted systems shall be measured against defined availability requirements.**
Rationale	Ultimately, where a system is hosted should not impact whether the delivery of the service meets business requirements or not. Services should be selected to ensure those requirements are met.
Approach	• Define availability requirements for systems as part of system design processes in accordance with service and deployment tiering as defined by service management. • Availability requirements may be based on an assessment of the risks associated with the system, or business process supported by the system. • Select hosted load balancing, backup, and recovery services to meet availability requirements.

	• Ensure use of those services considers dual sites for redundancy of the hosting environment in the event of a disaster affecting a region. • Ensure that security controls are in place to protect the hosted service from a denial-of-service (DoS) attack on its externally facing infrastructure and applications. • Computing resources must support scaling on-demand. However, auto-scaling must be limited to avoid DoS attacks, and to control over utilisation of resources over contractual agreements. • Ensure that contractually the hosting provider provides sufficient notice to the Audit Office's point of contact of any upcoming temporary service outages. • Engagement with another hosting provider must be evaluated in case the primary hosting provider is affected by a prolonged outage.

v) Backup and recovery

Requirement	**Backup and recovery measures must be implemented in accordance with the Audit Office's business function requirements.**
Rationale	Lack of backup and recovery measures defined in accordance with the Audit Office's business requirements could lead to unavailability of critical data at the time of a disaster.
Approach	• Ensure that backup, recovery, business continuity and disaster recovery processes have been defined, documented in service agreements and are implemented in the hosted environment, in accordance with the Audit Office's requirements. • Ensure that the process to operate the service in case of a disaster has been documented in a Business Continuity and a Disaster Recovery Plan (BCP and DRP), and tested to ensure that there is minimal downtime to the service. • The BCP and DRP must clearly document and implement alternate methods to utilise the services of the affected application in case of prolonged outages.

vi) Incident management

Requirement	**Division of incident management responsibilities and procedures shall be defined and communicated.**
Rationale	Where multiple parties are needed to be involved in the event of an incident, lack of defined responsibilities will cause delays to incident resolution, and potentially exacerbate the impact of an incident.
Approach	• Define responsibilities and handover points for incident response between the hosting provider and the tenant. • Logging and monitoring data, including the information of assets affected, must be promptly made available by the hosting provider to the Audit Office to carry out investigation of how the data breach occurred.

	• Hosting providers must have defined responsibilities for notifying the Audit Office in the event of an incident or data breach.

vii) Physical security

Requirement	**Physical security shall be enforced at premises housing the Audit Office information systems.**
Rationale	Insufficiently secured premises that house Audit Office information systems may lead to accidental or deliberate business disruption through damage, theft or unauthorised access or modification to the ICT assets contained.
Approach	• Access to the Audit Office information assets stored within the hosting providers' premises must only occur with appropriate authorisation from the Audit Office, and only where access is necessary for an individual to complete their employment duties in accordance with the Audit Office Physical Security Policy. • The hosting provider must make access logs of the premises hosting Audit Office information assets available for review by the Audit Office, if required. • In the case of Software as a Service providers appropriate assurances should be obtained by the Audit Office around physical data security.

6.3 Management requirements

Management requirements are generally applicable to the ongoing management and assurance of the services provided by, or the operation of, a vendor or third party organisation.

i) Ownership of access

Requirement	**The Audit Office shall retain ownership of access control to its environments.**
Rationale	Complexities may arise with access control infrastructure and processes controlled by external providers. For example, the impact of security incidents may be exacerbated should the Audit Office not have control over removing unauthorised access by malicious actors.
Approach	• Ensure that Audit Office access control functions are not delegated or outsourced to Cloud providers. • Systems controlling access to Audit Office systems or environments must be owned, or controlled and managed, by the Audit Office

ii) Security operations

Requirement	**Information assets within the hosted environment shall be securely operated and maintained.**
Rationale	Information assets if not adequately configured, operated and maintained within the Cloud could result in compromise, disclosure or modification of data, and unauthorised access to, the Audit Office.

Approach	• Deploy servers (physical and virtual machine images) within the hosted environment which are monitored for configuration compliance in line with best practices.
	• All the deployed servers must have implemented at a minimum, but not limited to, the following:
	  ○ disable unnecessary services, ports and protocols
	  ○ disable or rename vendor default passwords
	  ○ system patches installed prior to, and periodically upon, system roll-out in accordance with the 'Patch and Vulnerability Management Policy'
	  ○ servers deployed within the hosted environment must utilise 'Disk Encryption', where possible.
	• Core changes to the hosted environment, especially those impacting the server and network infrastructure, must be subject to a controlled change management process in accordance with the Audit Office Change Management Policy.

iii) Secure connections

Requirement	**Data in transmission shall be protected from eavesdropping or modification.**
Rationale	Data sent over unencrypted connections may be intercepted or modified, which may result in theft of credentials, disclosure or modification of data, and unauthorised access to the Audit Office's networks and systems.
Approach	• Use encrypted connections for all transmissions between hosts within the hosted environment, and to users of the systems. • Secure protocols and algorithms must be used for all connections, and insecure protocols and algorithms explicitly denied in configurations. • SSLv3, and TLS 1.0 and 1.1 are known to be insecure. TLSv1.2 should be used for connections.

iv) Necessary traffic

Requirement	**The Audit Office shall restrict connectivity to the minimum required to operate.**
Rationale	Overly permissive access may result in compromise of the environment and unauthorised exfiltration of sensitive information.
Approach	• Allow only the required ports and protocols to the relevant hosts, components or applications. • Only the protocols each application tier requires to interface shall be exposed. • Restrict ingress and egress of files to only the required file and data types.

	• Scan all content for malicious files or egress of sensitive data. • Access must be provided in accordance with the Mobile and Remote Working policy and Identity and Access Management Policy. • Data inputs and outputs must be controlled by an API or similar.

v) Interface security

Requirement	**Interfaces shall be exposed only to those systems and users authorised to transact with that interface.**
Rationale	In a normal hosting environment, traffic may be explicitly controlled by a firewall between the application tiers. In a Cloud hosted environment, traffic flows must be specifically defined, for example, to prevent databases being presented directly to the internet.
Approach	• Ensure each endpoint for a connection is defined and configured. • Where traffic to an interface is allowed from any address, it must still allow only traffic in accordance with Necessary Traffic requirements (see section 6.3.iv). • In Microsoft Azure, define the input endpoints, instance input endpoints, and internal endpoints allowed to interact with each system. • In AWS, define security groups for your server instances to allow only the required traffic to your instances.

vi) Cryptographic key management

Requirement	**Defined processes and technologies shall protect cryptographic keys from unauthorised access.**
Rationale	Compromise of cryptographic keys may result in compromise of sensitive information, or complete loss of encrypted information should the key be unavailable.
Approach	• Implement key management practices in accordance with the Cryptography and Key Management Policy. • Ensure cryptographic keys are protected from unauthorised access, loss, or disclosure using either a Cloud based service, a hardware security module (HSM), or manual processes.

vii) Logging and monitoring

Requirement	**Logging and monitoring must be implemented on the hosted environment for effective detection and management of cyber-attacks.**
Rationale	Lack of logging and monitoring could impede the Audit Office's ability to detect suspicious/malicious activities, which could lead to disruption of business-critical services. Furthermore, unavailability of log information could also restrict the Audit Office's ability to justify its position during incident investigation and legal proceedings, when required.

Approach	• Logging and monitoring security controls must be implemented within the hosted environment in accordance with the Logging and Monitoring Policy, to aid in Security Incident Management requirements, and meet legal and regulatory requirements. • Logs from the hosted environment must be immediately accessible to authorised Audit Office personnel.

viii) Intrusion detection

Requirement	**The Audit Office shall have the means to identify and prevent intrusion attempts.**
Rationale	Events which may affect the availability of, or indicate a compromise or attempt to compromise, Cloud hosted systems must be detectable so that they can be acted upon to protect the Audit Office's information and business processes.

Approach	• Ensure an intrusion detection or prevention system is implemented for hosted systems.
	• The following events should be logged and identifiable:
	  ○ all access and access attempts
	  ○ all modifications to system software or configuration
	  ○ system usage, including spikes in usage
	  ○ system and user inputs and outputs
	  ○ changes to virtual machine configuration settings.
	• Intrusion attempts and malware should be able to be detected and their execution prevented.

7 Outsourced Development Security Requirements

7.1 Principles

Outsourced services that make use of third party development of software or systems present additional risk to the Audit Office, and are subject to additional requirements.

These controls apply in addition to the general requirements and conditions outlined in section 5 and as relevant to a development environment.

These controls will be used to assess third party vendors and the outcomes of these assessments will be evaluated in line with the risk appetite of the Audit Office. Best efforts should be made to apply all controls were relevant. The CIO may offer guidance as to what controls are relevant to development vendors.

7.2 Engagement requirements

Engagement requirements are to be considered prior to, and during, the process of engaging a vendor or third-party organisation.

i) Source code

Requirement	**The Audit Office shall have rights to source code developed on its behalf.**
Rationale	Where the Audit Office has outsourced development, it may be at risk should a third party become insolvent, or should the Audit Office wish to change development providers.
Approach	• Ownership clauses for code developed on behalf of the Audit Office shall be included in contracts. • Where possible, ensure that the source code is developed and stored in an Audit Office controlled repository, or backed up to Audit Office environments. • Where the above is not possible, a source code escrow facility should be included in contracts and used.

ii) Secure coding practices

Requirement	**Third party secure coding methodologies shall be defined and documented.**
Rationale	Where the Audit Office utilises software coded by third parties to store, process, or transmit sensitive information, assurance must be gained that their development practices ensure that the systems developed are secure.
Approach	• Contracts must include a requirement for the third party to follow a formal development practice and utilise secure coding standards. • Third party development practices should be verified for compliance to Audit Office Secure Application Development Policy. • The risks associated with the vendor's development practices should be included in annual risk assessments.

	• For high risk applications or systems, contractual requirements should include the requirement to verify security through vulnerability and penetration testing.

8 Review

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

Changes to this policy will be notified to 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 agreements, as agreements with vendors must refer to this policy if data is being processed, stored, collected or transferred.