Print whole section

Information security guidelines for contractors

Detailed information security guidelines for contractors to the ATO.

Last updated 3 April 2017

Introduction

When the ATO information security guidelines apply to our contractors.

Access to information

The rules about when contractors can access ATO information.

Confidentiality, integrity and availability of information

The procedures and products required to ensure the confidentiality, integrity and availability of ATO information.

Destruction of classified information

Information about the appropriate methos to destroy classified information.

Information security documentation

Information about the key IT security documentation our contractors must have in place.

Information security monitoring

How our contractors must assess, monitor and manage information security risks.

Information technology security

How our contractors must manage the security of their hardware and software.

Access control

Contractors must apply security control measures around access of our information.

QC 17156

Introduction

When the ATO information security guidelines apply to our contractors.

Last updated 13 February 2025

On this page

> Defining and assessing ATO information

These guidelines are effective from 3 April 2017.

The Australian Government expects the ATO to create and maintain a security environment to protect its functions and official resources. The Australian Government Protective Security Policy Framework (PSPF) sets out the policies, practices and procedures that all Australian Government departments and agencies must comply with.

The security of our information is critical. Information security requirements apply to all ATO employees, and similar requirements apply to ATO contractors.

These information security guidelines are derived from the minimum mandatory requirements of the PSPF information security management core policy. They explain the practices and procedures contractors must follow to provide adequate security for the ATO information they access, process or store.

Departure from these guidelines must be authorised in writing by ATO Physical Security Management (or ATO IT Security Branch for electronic systems).

Enquiries about these guidelines, or any security matter involving the ATO, should be directed through the relevant contract manager to ATO Physical Security Management (or for electronic systems, ATO IT Security branch).

Policy

We are committed to preserving the security, privacy, confidentiality, integrity and availability of all information provided to us, or generated from within. This commitment is vital because:

- our reputation as a responsible custodian of sensitive client information is integral to community confidence in our operations
- the proper administration of the tax system depends on our ability to keep information secure
- legislation administered by the Commissioner of Taxation imposes certain information security obligations

- legislation, such as the *Crimes Act 1914* and *Privacy Act 1988*, require us to safeguard information
- Australian Government policies make certain security procedures mandatory for all government agencies.

Applicability

Procedures within these guidelines apply to all contractors (which includes officers, employees, agents and subcontractors) or any other person or entity acting for the ATO and having custody of or access to ATO information. Use of the word 'contractor' within these guidelines applies equally to all such parties, including consultants and service providers.

Scope

These guidelines will support contractors who access, process, store or otherwise handle ATO information that is either unclassified or warrants a Dissemination Limiting Marker (DLM).

Additional protective security measures apply to security-classified material - ATO Physical Security Management and/or IT Security Branch must be consulted if access to information other than unclassified or that bearing a DLM is required.

The contractor must appoint somebody who is responsible for the security of ATO information.

Contractors must deliver a plan that describes the security architecture of systems that will store, access or transmit ATO information before starting services. This plan must be approved by ATO IT Security.

Contractors must establish an IT security review process that measures compliance of IT systems and operations against the ATO IT Security Policy and the ISM and take corrective actions to address areas of non-compliance.

Defining and assessing ATO information

In the context of these guidelines, 'ATO information' includes data from any source and in any form, which is collected, received, stored or

developed by the ATO, or by ATO employees and contractors. Our information may exist in a range of forms, including:

- documents, papers and other printed or written material
- electronic data
- voice communications
- video and audio recordings
- any physical item from which information belonging to the ATO could be derived
- intellectual knowledge.

We assess all of our information according to the degree of harm that may result if it was accessed without authority, lost, damaged, destroyed, altered or otherwise compromised. Based on this assessed degree of harm, or other legislative requirements which restrict the distribution of the information, a protective marking is applied to information. Protective markings include DLMs and security classifications. Authority to downgrade or upgrade the security classification, or remove the protective marking of ATO information, rests exclusively with us.

QC 17156

Access to information

The rules about when contractors can access ATO information.

Last updated 13 February 2025

On this page

> Security clearances
>
> Security awareness and training

To reduce information being lost, destroyed, damaged, compromised or misused, access to ATO information by a contractor or other party is authorised only if all the following conditions are met:

- there is a genuine 'need to know' the information
- access will comply with legislative requirements
- there is no conflict of interest regarding the information
- the person has the required level of security clearance.

ATO information must not be given to any third party or transferred to unapproved systems including those overseas unless the contractor has received written approval from the ATO Contract manager prior to the placement or transfer. The contract manager is required to ensure IT security is notified and any required IT security reviews are initiated prior to any transfer.

We must be consulted and provide formal written approval before any outsourcing arrangements are put into effect.

ICT services must not be delivered or managed from overseas. ATO data must not be transmitted, stored or processed overseas.

Please note that all data supplied by or created for and that which is collected, received, stored or developed by the ATO always remains the property of the ATO.

Need-to-know

The 'need-to-know' principle states that the availability of information should be limited to those who need to use or access it to do their work. Contractors are not entitled to access information merely for the sake of convenience, or by virtue of status, position, office, or level of security clearance. The need to know principles must be enforced through the uses of access controls and authorisation procedures.

Systems access

If a contractor processes or stores ATO information on any electronic system and is required to access the ATO information the contractor must provide appropriate documentation such as (an Information Technology (IT) Security Plan and standard operating procedures) which document access requirements as specified in the ISM . These documents must be endorsed by ATO IT Security.

Authorised personnel

All contractors with access to ATO information in any format must satisfy our pre-engagement integrity checking requirements. These requirements include:

- identity verification
- character assessment, including a police records check
- completion of an ATO Declaration of Secrecy.

Pre-engagement integrity checks must be undertaken by us . Contractors may be responsible for costs associated with these requirements. Our contract managers are responsible for ensuring integrity-checking requirements are completed before access commences.

Security clearances

Contractors and their authorised personnel who access systems that store, process or communicate ATO information will be required to obtain and maintain an appropriate government security clearance as per the PSPF and ISM.

Security awareness and training

Contractors must ensure all personnel who have access to ATO information (including systems that store ATO information) undertake ATO mandatory security awareness training (this can be obtained through the contract manager) before accessing ATO information.

You and your authorised personnel must be made aware of the following:

- ATO security classification and protective marking system

- requirements for ATO pre-engagement integrity check
- requirements for obtaining security clearance
- information management requirements, including storage, transmission and destruction of information
- proper use of ATO IT systems, facilities and assets
- appropriate levels of access to systems, facilities, assets and electronic information
- close-of-business security procedures
- the 'need-to-know' principle
- protocols to report security-related incidents
- their responsibilities to notify changes in circumstance relating to service provision (for example, subcontracting out of services, relocation/renovation of premises, changes in key personnel, conflicts of interest)
- privacy and secrecy obligations
- the legitimate use of system accounts, software and information
- the security of accounts, including shared passwords
- how to protect ICT workstations and devices from unauthorised access
- rules and regulations governing the secure operation and authorised use of systems.

QC 17156

Confidentiality, integrity and availability of information

The procedures and products required to ensure the confidentiality, integrity and availability of ATO information.

Last updated 13 February 2025

On this page

To reduce information being lost, destroyed, damaged, compromised or misused, access to ATO information by a contractor or other party is authorised only if all the following conditions are met:

- there is a genuine 'need to know' the information
- access will comply with legislative requirements
- there is no conflict of interest regarding the information
- the person has the required level of security clearance.

ATO information must not be given to any third party or transferred to unapproved systems including those overseas unless the contractor has received written approval from the ATO Contract manager prior to the placement or transfer. The contract manager is required to ensure IT security is notified and any required IT security reviews are initiated prior to any transfer.

We must be consulted and provide formal written approval before any outsourcing arrangements are put into effect.

ICT services must not be delivered or managed from overseas. ATO data must not be transmitted, stored or processed overseas.

Please note that all data supplied by or created for and that which is collected, received, stored or developed by the ATO always remains the property of the ATO.

Need-to-know

The 'need-to-know' principle states that the availability of information should be limited to those who need to use or access it to do their work. Contractors are not entitled to access information merely for the sake of convenience, or by virtue of status, position, office, or level of security clearance. The need to know principles must be enforced through the uses of access controls and authorisation procedures.

Systems access

If a contractor processes or stores ATO information on any electronic system and is required to access the ATO information the contractor must provide appropriate documentation such as (an Information Technology (IT) Security Plan and standard operating procedures) which document access requirements as specified in the ISM . These documents must be endorsed by ATO IT Security.

Authorised personnel

All contractors with access to ATO information in any format must satisfy our pre-engagement integrity checking requirements. These requirements include:

- identity verification
- character assessment, including a police records check
- completion of an ATO Declaration of Secrecy.

Pre-engagement integrity checks must be undertaken by us . Contractors may be responsible for costs associated with these requirements. Our contract managers are responsible for ensuring integrity-checking requirements are completed before access commences.

Security clearances

Contractors and their authorised personnel who access systems that store, process or communicate ATO information will be required to obtain and maintain an appropriate government security clearance as per the PSPF and ISM.

Security awareness and training

Contractors must ensure all personnel who have access to ATO information (including systems that store ATO information) undertake ATO mandatory security awareness training (this can be obtained through the contract manager) before accessing ATO information.

You and your authorised personnel must be made aware of the following:

- ATO security classification and protective marking system
- requirements for ATO pre-engagement integrity check
- requirements for obtaining security clearance
- information management requirements, including storage, transmission and destruction of information
- proper use of ATO IT systems, facilities and assets
- appropriate levels of access to systems, facilities, assets and electronic information
- close-of-business security procedures
- the 'need-to-know' principle
- protocols to report security-related incidents
- their responsibilities to notify changes in circumstance relating to service provision (for example, subcontracting out of services, relocation/renovation of premises, changes in key personnel, conflicts of interest)
- privacy and secrecy obligations
- the legitimate use of system accounts, software and information
- the security of accounts, including shared passwords
- how to protect ICT workstations and devices from unauthorised access
- rules and regulations governing the secure operation and authorised use of systems.

Destruction of classified information

Information about the appropriate methos to destroy classified information.

Last updated 13 February 2025

On this page

Contractors must apply the appropriate destructions methods to paper-based and electronic classified information.

Additionally contractors must obtain written approval from the ATO data owner prior to destruction.

Paper-based resources

Careless disposal of information increases the likelihood of unauthorised disclosure. Contractors must ensure waste ATO information is destroyed in accordance with government standards, which requires mutilation to the extent that it would be impossible to recognise or use the content. Approved methods include:

- shredding
- wet pulping
- burning
- pulverisation
- disintegration.

Destruction of our information may occur through:

- an ATO-approved classified waster destruction facility
- the contractor's premises using an ATO-approved destruction method

- return of the classified waste to an ATO site.

Contractors proposing to destroy ATO information either at their premises or using a commercial service provider must first consult ATO Physical Security Management.

ATO information pending destruction must be safeguarded in an appropriately secure environment. Recycling of waste ATO information is only permitted for material which has already been destroyed by approved methods.

The ATO and Australian Archives have records disposal schedules which detail retention periods and other requirements relating to particular types of documents. These requirements must be adhered to when preparing to destroy ATO information. When in doubt, you should contact your contract manager.

Electronic media and equipment

Information can still be retrieved from IT equipment and electronic storage media which has either failed or outlived its purpose. It is essential for computing media which has carried ATO information to be disposed of appropriately. Contractors must provide destruction plans for electronic media and equipment before starting services and these must be endorsed by ATO IT Security, Contractors must develop asset registers which include a unique register for the media; if the media is in storage or in use, where it is in use, and if the media has been sanitised or destroyed (if used to store or communicate ATO information)

QC 17156

Information security documentation

Information about the key IT security documentation our contractors must have in place.

Last updated 13 February 2025

On this page

Contractors must apply governance measures to maintain the security of our information, including a documentation framework and system audits.

Security documentation framework

Contractors must have an established security documentation framework including a hierarchical listing of all information security documentation and their relationships, or adopt the documentation structure and naming conventions of the Australian Government Information Security Manual (ISM).

Contractors must develop documentation to effectively manage the IT security framework for systems that store, process or communicate ATO information.

Key IT security documentation includes:

- information security policy
- security risk management plan (SRMP)
- system security plan (SSP)
- incident response plan (IRP)
- standard operating procedures (SOPs)
- security architecture design
- audit logging plans.

Security documentation should be maintained appropriately and should be:

- formally approved by an authorised person
- reviewed at least annually and after significant changes to the system.

System audits

Contractors must conduct audits every 18 months of their systems that store, process or communicate ATO information, and provide a report of results to us. A summary of the results and treatment of any identified risks are to be included in the security risk management plan.

You need to conduct audits on a regular basis that:

- compare the approved system documentation with the actual implementation
- determine the effectiveness of the implemented controls
- identify ineffective controls for remediation.

We reserve the right to require evidence of compliance to this cyber security requirement, and to inspect contractor process.

Contractors shall permit nominated ATO personnel to perform an IT security compliance review of contractor IT systems and operations as required. Contractors must provide suitable contacts and resources at the start of the contract so that nominated ATO personnel can verify your IT systems that store, process or communicate ATO information are operating securely.

Evidence collected may include documentation such as architecture diagrams, procedures and system output, and behaviour such as systems settings and log output.

QC 17156

Information security monitoring

How our contractors must assess, monitor and manage information security risks.

Last updated 13 February 2025

On this page

Vulnerability management

We recommend that contractors conduct vulnerability assessments on the systems that hold ATO information, particularly in the following situations:

- as a result of a specific cyber security incident
- after a change to a system or its environment that significantly impacts on the approved and implemented system architecture and information security policy
- as part of a regular scheduled assessment.

Contractors should also subscribe to a security alert service that provides up-to-date notifications on vulnerabilities that exist with the products they use.

Change and release management

Contractors must maintain change and release management processes to ensure that changes affecting information security are reviewed and have authorisation.

Types of system changes include:

- an upgrade to, or introduction of, ICT equipment
- an upgrade to, or introduction of, software
- major changes to access controls.

Business continuity and disaster recovery

Contractors must ensure that business continuity plans are established to recover from disasters and prevent a loss or degradation of an ATO service. Contractors should conduct annual tests of their business continuity plan, covering systems that store, process or communicate ATO information, and provide evidence to us of test results.

Cyber security incidents

Contractors must have a process to identify, report and contain any cyber security incident that could affect ATO information. Contractors must deploy and manage tools in such a way that they are capable of detecting and responding to information security incidents. Regular system integrity checks must be performed to detect deviation from the expected configuration.

Contractors may consider some of the following tools for detecting potential cyber security incidents:

- anomaly detection system
- intruder prevention system
- log analysis
- network and host-intrusion detection systems
- system integrity verification.

Contractors must report cyber security incidents to the ATO for any system which stores, processes or communicates ATO information., The report must include the cause of the incident and what remediation has occurred. Reporting must occur within 4 hours, a preliminary report provided to the ATO within 3 business days and a final report within 5 business days of the incident occurring.

It is recommended the cyber security incidents are recorded in a register. At a minimum, the register should include:

- the date the incident was discovered
- the date the incident occurred
- a description of the incident, including the personnel and locations involved
- the action taken

- the date reported
- the file reference.

Contractors must:

- configure IT systems and environments in response to the latest threats and maintain associated information security documentation
- detect, contain and remove malware by maintaining malicious code protection software.

QC 17156

Information technology security

How our contractors must manage the security of their hardware and software.

Last updated 13 February 2025

Contractors must classify all information and communication technology (ICT) equipment that stores, processes or communicates ATO information, based on the highest classification of information they manage. You must clearly label all ICT equipment capable of storing ATO information.

Contractors must prevent attackers from exploiting known vulnerabilities in products by implementing robust patch-management processes. You must ensure all critical security patches are applied as soon as possible and ensure security patches are applied through a vendor-recommended patch or upgrade process.

Contractors must harden IT systems during installation. Examples of hardening processes include:

- developing standard operating environments (SOEs)
- developing security configuration baselines
- removing unnecessary software or system services

- changing default system authentication settings (for example, passwords)
- applying security software and patches
- testing the system security controls for vulnerabilities.

Implement secure software testing and development procedures where required.

Contractors must have a documented process for the disposal of ICT equipment that holds ATO information. They must maintain a register for disposal of ICT equipment.

QC 17156

Access control

Contractors must apply security control measures around access of our information.

Last updated 13 February 2025

On this page

Identification and authentication

Contractors must implement an authentication mechanism to identify users who access ATO information. Contractors must:

- develop and maintain user identification, authentication and authorisation policies and procedures; for example, password policy
- record sufficient audit-logging information to determine user/system access to ATO information. This information must be regularly reviewed to identify any security breaches
- develop as part of the implementation of services an audit-logging plan that covers the events that are recorded for any system that stores, processes or communicates our information
- preserve the integrity of logs used to record information security incidents. The contractor must develop processes and procedures to ensure the integrity of logs that record access to all systems that store, process or communicate ATO information
- regularly assess tests of the log collection processes and integrity of logs.

The contractor must restrict and minimise the allocation of privileged and system accounts according to the principle of least privilege. The contractor must control access by using a delegated rights model to form an access matrix. The matrix is used as definition where privileges are granted according to the specific requirements of the role staff perform. The matrix and the number of staff in each role are to be reported to the ATO when requested.

Systems access

Where the contractor processes or stores ATO information on any electronic system, an information technology (IT) security plan must be in place before starting services to ensure access to ATO information is available only to authorised persons. IT security plans must be endorsed by ATO IT Security.

Remote access

The ATO recommends prohibiting remote access for administration to contractor systems which store, process or communicate ATO information. Where there is a business requirement, the contractor must implement remote access as per the ISM and in a secure manner

that will not compromise ATO information stored on the contractor's IT systems. The contractor must provide documentation to assure us that remote access to our information is securely implemented.

The contractor must use multi-factor authentication for remote access to systems that process, store or communicate ATO information.

Cryptography

Encryption of data in transit must be used to provide protection for classified information being communicated over unclassified or public networks.

The contractor must use cryptographic algorithms approved by the Defence Signals Directorate (DSD), and DSD-approved cryptographic protocols, to transfer ATO information across untrusted networks.

Where encryption is being used, contractors must develop a key management plan to document all cryptographic information transfer methods for ATO information.

Network security

For each network that is used to communicate ATO information, the contractor must have:

- a high-level diagram showing all connections into the network
- a logical network diagram showing all network devices.

The contractor must restrict and control the connection of peripheral devices to IT systems that store, process or communicate ATO information.

Gateway security

Where connections from one security domain to another occur, the contractor must deploy controls commonly understood as a gateway - for example, between a private contractor network processing, storing or transmitting sensitive ATO information, and the internet.

The Australian Government Information Security Manual is the authoritative reference for ATO gateway requirements. The contractor must ensure gateway IT security controls protect connections from the

contractor's network storing or processing ATO information to other untrusted networks such as the internet.

Gateway security controls can include but are not limited to:

- firewall devices
- routers with security access lists enabled
- gateway security appliances
- maintained and monitored security logs
- annual security risk assessments on gateways
- security training for system administrators, including limiting administration functions
- irregular testing on gateways.

Perimeter defence measures must be implemented. They must be effective in detecting and preventing intrusions from all connected networks while controlling the approved information flows between internal and external systems.

QC 17156

Our commitment to you

We are committed to providing you with accurate, consistent and clear information to help you understand your rights and entitlements and meet your obligations.

If you follow our information and it turns out to be incorrect, or it is misleading and you make a mistake as a result, we will take that into account when determining what action, if any, we should take.

Some of the information on this website applies to a specific financial year. This is clearly marked. Make sure you have the information for the right year before making decisions based on that information.

If you feel that our information does not fully cover your circumstances, or you are unsure how it applies to you, contact us or seek professional

advice.

Copyright notice