PS LA 2002/19 (Withdrawn) - Security of Taxpayer Data (Written Binding Advice)

This law administration practice statement is withdrawn with effect from 30 June 2009. Tax officers must comply with the access and security provisions set out in Corporate Management Procedures and Instructions (2006/07/06) - Security Assessed Client Information
.

This document has changed over time. This version was published on *30 June 2009*

Australian Government
Australian Taxation Office

Practice Statement Law Administration

PS LA 2002/19

This law administration practice statement is withdrawn with effect from 30 June 2009. Tax officers must comply with the access and security provisions set out in Corporate Management Procedures and Instructions (2006/07/06) - Security Assessed Client Information.

FOI status: may be released

This practice statement is issued under the authority of the Commissioner of Taxation and must be read in conjunction with Law Administration Practice Statement PS LA 1998/1. It must be followed by Tax Office staff unless doing so creates unintended consequences or is considered incorrect. Where this occurs Tax Office staff must follow their business line's escalation process.

SUBJECT: **Security of Taxpayer Data (Written Binding Advice)**

PURPOSE: **To provide direction as to the application of security policy to written binding advice data records**

Table of contents **Paragraph**

STATEMENT

Applicability

1. This practice statement applies to all Tax Office employees who provide written binding advice as defined in Law Administration Practice Statement PS LA 2008/3.

2. This practice statement is consistent with Australian Government and Tax Office security policies and principles embodied in the *Australian Government Protective Security Manual 2005* (PSM) and in the *ATO Guide to Information Security*. A link to the *ATO Guide to Information Security* (available to Tax Office staff only) is

available in the Other References section at the conclusion of this practice statement.

Classification of data records

3. Written binding advice data records (referred to in this practice statement as 'relevant data records') must be assigned a security classification level in accordance with the PSM and the *ATO Guide to Information Security.* That is, IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED.

4. In addition to the Australian Government Standards, the Tax Office provides enhanced protection to information relating to particular clients that may be potentially exposed to heightened risk of privacy and security breach, or fraud. This information can be comprised of details in clients' primary records or their dealings with the Tax Office in 'case' records, that is referred to as 'security assessed client' information. Security assessed client information can be classified as IN-CONFIDENCE, PROTECTED or HIGHLY PROTECTED.

5. Relevant data records may be reclassified where it is determined that the existing level of classification is inappropriate. Instructions for reclassifying information are contained in the *ATO Guide to Information Security.*

Storage of data records

6. Relevant data records classified as IN-CONFIDENCE may be stored on ATOnet.

7. Relevant data records classified as PROTECTED must not be stored on ATOnet. An appropriately secure Information Technology (IT) environment, ***ATO Protect***, has been developed to accommodate data records classified at the PROTECTED level. Written binding advice classified at this level is stored and actioned in ***ATO Protect***. Most of the data of these cases will not be in the Technical Decision Making System (TDMS). However, a shell of the case is in TDMS for integrity purposes and to allow normal authorisation processes and reporting to be carried out.

8. Records classified as HIGHLY PROTECTED are not permitted on ATOnet or ***ATO Protect***. In situations where an assessment of a client's situation may warrant classification at the HIGHLY PROTECTED level, risk treatments will be dealt with outside mainstream systems and operations (offline), in accordance with the 'High Risk Client Procedures' as detailed in *CMPI 2006/07/06 Security Assessed Client Information*. These procedures are not available for general distribution. The National SAC Coordinator will act as the intermediate liaison point through which line staff must escalate potential 'high risk client' issues. Again a shell of a case is in TDMS – see paragraph 7. A link to the *CMPI 2006/07/06* (available to Tax Office staff only) is available in the Other References section at the conclusion of this practice statement.

9. A TDMS Quick Reference Guide detailing the processes to be followed when actioning PROTECTED and HIGHLY PROTECTED written binding advice can be found on the Tax Office intranet. It is titled 'How to record protected cases on TDMS'.

10. TDMS utilises certain 'caveats' to restrict access to specific categories of client information within that system. The access caveats are 'High Wealth Individual' and 'COMMERCIAL-IN-CONFIDENCE'. These caveats operate in addition to, but do not override, primary IT systems access controls in respect of the AIS Client Register, or records pertaining to security assessed client information.

Access to data records

11. All Tax Office employees must comply with the 'need-to-know' principle whereby, without access to relevant data records, they would be hindered in the performance of their duties. Employees are not to access data records merely because it would be convenient for them to know, or by virtue of status, position, office or level of security clearance.

12. All case officers and authorising officers who deal with relevant data records will be provided access to appropriate IT client information systems at the IN-CONFIDENCE level as a base requirement, in accordance with the 'need-to-know' principle.

13. TDMS work classifiers (and mail-handlers), are exempt from obtaining a security clearance in respect of their specific classifying (or mail-handling) duties only.

14. Managers are responsible for ensuring that Tax Office staff are in possession of an appropriate level of security clearance before being assigned access to relevant data records classified above IN-CONFIDENCE. Procedures for obtaining a security clearance are set out in '*Security Clearances in the Tax Office'*. Provision of access is to be in strict accordance with details contained in *CMPI 2006/07/06 – Security Assessed Client Information*. Access to ***ATO Protect*** requires a security clearance at a minimum level of PROTECTED. A link to *Security Clearances in the Tax Office* (available to Tax Office staff only) is available in the Other References section at the conclusion of this practice statement.

15. Each business or service line (BSL) must have in place appropriate contingency arrangements and succession plans to ensure that sufficient numbers of security cleared personnel are available at all times to process cases involving security assessed client information.

Positions of trust

16. Persons assigned access to sensitive security information above IN-CONFIDENCE, or whose duties may have wide ranging, highly discretional access or authorities which, if mishandled, may cause considerable harm, are deemed to occupy a 'position of trust' (PoT). Included in this category are individuals with systems access to security assessed client information.who are required to hold an Australian Government security clearance, in accordance with the level of access provided.

Assuring conformance

17. Security Policy and Services (ATOPP) and ATO Trusted Access (ICT) conduct periodic assurance reviews in respect of *CMPI 2006/07/06 – Security Assessed Client Information*.

18. CAS (Plan and Manage) through the National Security Assessed Client Coordinator is responsible for operational issues detailed in *CMPI 2006/07/06 – Security Assessed Client Information* and the coordination of line network support staff. Identified non-compliance issues are reported to National Program Managers for appropriate review and follow-up action as required.

19. As prescribed in clause 5.3 of the *ATO Guide to Information Security*, 'Managers must ensure reviews of HIGHLY PROTECTED information are conducted at irregular intervals within their area of control. The purpose of these checks is to verify material is accounted for, classifications are still valid and that handling and storage procedures meet the standards as set out in this Guide. It is also good practice to conduct reviews of PROTECTED information on a periodic basis.'

EXPLANATION

Classification of data records

20. The PSM places all official information handled by Government agencies into two main categories: Non-National Security and National Security. Nearly all sensitive information handled by the Tax Office falls within the Non-National Security category.

21. Within the Non-National Security category there are two types of non-sensitive official information (UNCLASSIFIED and its subset UNCLASSIFIED-Public) and three levels of security classification (IN-CONFIDENCE, PROTECTED and HIGHLY PROTECTED).

22. Security classifications are used to indicate the level of damage that could result if the information was subject to unauthorised disclosure, loss, theft, damage, misuse or other compromise. These include:

- The IN-CONFIDENCE security classification is used when compromise of the information could cause limited damage to the Australian Government, commercial entities, or members of the public. The majority of taxpayer/client data falls within this security classification and must be kept secure.
- The PROTECTED security classification is used when compromise of the information could cause damage to the Australian Government, commercial entities, or members of the public. The amount of PROTECTED information held should be limited and must be provided with a higher level of security than IN-CONFIDENCE material.
- The HIGHLY PROTECTED security classification is used when compromise of the information could cause serious damage to the Australian Government, commercial entities, or members of the public. The amount of HIGHLY PROTECTED information held should be very limited and must be provided with a higher level of security than PROTECTED material.

23. Confirmation is required by an area manager when assigning a PROTECTED classification and an EL2 equivalent (or higher) when assigning a HIGHLY PROTECTED classification.

24. Further information regarding security classifications is available in the *ATO Guide to Information Security.*

Additional client categories

25. COMMERCIAL-IN-CONFIDENCE is a subset of the IN-CONFIDENCE security classification and is information that, if compromised by unauthorised access or disclosure, loss, theft or damage, could cause harm to the business to which the information relates, or provide an unfair advantage to competitors of that business.

26. 'High Wealth Individual' (HWI) status is defined on the Small to Medium Enterprise Tax Office intranet site 'High Wealth Individual Taskforce Overview'. Further information is available through the HWI Taskforce. A link to this definition

(available to Tax Office staff only) is available in the Other References section at the conclusion of this practice statement.

Restricted access clients

27. In addition to Australian Government security classification levels, the Tax Office provides enhanced protection to particular categories of client information, referred to as security assessed client information, where there is an increased likelihood that the compromise of that information could:

- cause personal harm or result in a significant breach of privacy to an individual
- damage the reputation of individuals who, by virtue of their community profile, generate a high level of interest in their affairs
- cause severe financial loss or significantly affect business viability
- significantly damage or impair the business operations of the Tax Office
- severely damage the reputation of the Tax Office resulting in loss of community confidence, or
- provide opportunity for individuals or other entities to commit fraud at the Tax Office

Included in the category of security assessed client information are:

- 'special interest clients'
- 'staff clients', and
- cases pertaining to special interest clients whose classification is at a minimum level of PROTECTED.

Only a small proportion of client records will possess a security classification above IN-CONFIDENCE that include 'special interest clients' within the following categories:

- Personal risk
- Tax sensitive
- High community profile, and
- Government officials.

Decisions concerning the security classification level of client records are determined by the National Security Assessed Client Coordinator CAS (Plan and Manage).

Storage of data records

28. The *ATO Guide to Information Security* specifies minimum storage standards for the protection of official information. All Tax Office employees who deal with relevant data records must adhere to these standards.

29. Information stored electronically and in hard copy form are subject to equivalent levels of protective security measures.

Access to data records

30. Access to data records held by the Tax Office is authorised only if the conditions described in the *ATO Guide to Information Security* are met. These conditions address the 'need-to-know' principle, legislative requirements, conflict of interest and appropriate levels of security clearance for employees.

Subject references	commercial-in-confidence highly protected in-confidence information security protected public domain security assessed client security of taxpayer data unclassified written binding advice
Related Practice Statements	PS LA 2003/10 PS LA 2008/3
Other references	Australian Government Protective Security Manual 2005 (PSM) (Part C) Note: following links available internally only High Wealth Individual Taskforce Overview ATO Guide to Information Security PS CM 2004/04 Proper use of IT facilities CM PI 2006/07/06 – Security Assessed Client Information Security Clearances in the Tax Office
Amendment history	14 July 2004: To update references and clarify contents 1 September 2004: Update paragraph 13 - TDMS classifiers not required to have security clearances for duties as classifier 28 February 2008: To update references and contents to reflect updates to security policy documents
File reference	2002/019493
Date issued	**13 July 2004**
Date of effect	**13 July 2004**