Information Security Strategy

Dated 23 June 2006.

Telstra Corporation Limited (ABN 33 051 775 556) ("**Telstra**")

Disclaimer

This Information Security Strategy is being published in furtherance of Telstra's obligations under the Telecommunications Act 1997. The purpose of this Information Security Strategy is solely to assist in Telstra's compliance with and monitoring of Telstra's performance of the Operational Separation Plan.

The publication of this Information Security Strategy is not intended to confer any rights on any person. In particular, nothing in this Information Security Strategy is to be taken as a representation that Telstra will act or refrain from acting in any particular way.

1 Purpose and scope

1.1 This Information Security Strategy has been developed in accordance with the OSP to outline the measures Telstra will adopt to protect confidential information relating to Telstra's wholesale customers, in order to promote the objective of providing high quality services to wholesale customers and to meet Telstra's obligations under the OSP.

1.2 In addition to the information security requirements under the OSP, Telstra is subject to a range of obligations regarding confidential information relating to wholesale customers. These obligations arise from a number of sources, such as contracts, common law and equitable obligations of confidentiality, the *Telecommunications Act* 1997 (Cth), the *Privacy Act* 1988 (Cth) and telecommunications industry codes. Telstra has separate policies and procedures in place for meeting these general information security obligations, and therefore such obligations are not covered by this Strategy.

2 Obligations

2.1 Telstra will:

(a) ensure that the Wholesale Business Unit does not disclose confidential information relating to a wholesale customer:

(i) to the Retail Business Unit, unless authorised to do so by the wholesale customer; or

(ii) to the Key Network Services Business Unit otherwise than on a need-to-know basis or where authorised to do so by the wholesale customer;

(b) ensure that the Key Network Services Business Unit does not disclose confidential information relating to a wholesale customer to the Retail Business Unit unless authorised to do so by the wholesale customer;

(c) have measures in place to ensure that an employee of the Retail Business Unit or the Key Network Services Business Unit who had been an employee of the Wholesale Business Unit at any time does not disclose or use confidential information relating to a wholesale customer of which the employee had become aware whilst working for the Wholesale Business Unit; and

(d) have security measures in place for Telstra's information storage systems and data systems in order to ensure that there is no disclosure of confidential information relating to a wholesale customer to a member of staff of the:

(i) Retail Business Unit without authorisation to do so by the wholesale customer; and

(ii) Key Network Services Business Unit otherwise than on a need-to-know basis or where authorised by the wholesale customer.

2.2 The obligations set out in clause 2.1 of this Strategy will be satisfied by Telstra implementing the processes set out in clause 5 of this Strategy to give effect to the principles outlined in clauses 3 and 4 of this Strategy.

3 Definition of confidential information and principles

What is confidential information relating to a wholesale customer?

3.1 Confidential information relating to a wholesale customer includes but is not limited to:

(a) information identifying a wholesale customer or an end user to whom a wholesale customer supplies an eligible service, which was provided by the wholesale customer in connection with the supply of an eligible service by the Wholesale Business Unit; and

(b) information derived from information of the kind described in clause 3.1(a), whether or not in an aggregate form, that:

(i) would enable the identity of a wholesale customer to be ascertained; or

(ii) would enable the identity of an end user to whom a wholesale customer provides an eligible service to be ascertained,

but does not include information of the kind described in clause 3.1(b)(i) where the information is aggregated on a national basis.

Examples

3.2 The following are examples of information which, if provided to the Wholesale Business Unit by a wholesale customer, is likely to be considered confidential information relating to that wholesale customer:

(a) forecasts about that wholesale customer's needs;

(b) the wholesale customer's ordering and provisioning details (including details of when and where orders are submitted);

(c) information disclosed by the wholesale customer regarding confirmed plans to purchase a type of product, or products in particular geographical areas;

(d) details of the end users of the wholesale customer, such as name, address, contact details, account and service numbers;

(e) contractual terms which are specific to that wholesale customer (including price terms);

(f) any 'service assurance' arrangements between Telstra and the wholesale customer;

(g) information about the wholesale customer's network or facilities; and

(h) information disclosed about the wholesale customer's business during negotiations.

What is not confidential information relating to a wholesale customer?

3.3 In some circumstances, information will not be confidential information relating to a wholesale customer (even if such information would fall within one of the examples referred to in clause 3.2 or might otherwise appear to be confidential information relating to a wholesale customer). This includes:

(a) information in the public domain;

(b) information obtained by Telstra via a third party;

(c) information about Telstra's own wholesale products that is not disaggregated by customer or is otherwise not customer specific (such as total wholesale ADSL services in operation) or the range of products supplied to wholesale customers;

(d) any information provided by an end user directly to Telstra (for example, where an end user is also a Retail Customer or enquires about services provided by the Retail Business Unit);

(e) any information provided by a wholesale customer directly to a Business Unit other than the Wholesale Business Unit (for example, product orders where the wholesale customer is also a customer of the Retail Business Unit (and therefore is a Retail Customer)).

Common examples of authorised use and disclosure

3.4 Telstra may use or disclose information which could be classified as confidential information relating to a wholesale customer where authorised to do so by the wholesale customer. The most common examples are where the use or disclosure is:

(a) authorised under the supply contract between Telstra and the wholesale customer; or

(b) in accordance with any telecommunications industry code to which Telstra and the wholesale customer are signatories.

4 Principles for access and use of information

General principles: "need-to-know basis"

4.1 In this Strategy, "need-to-know basis" means a principle or policy of disclosing only such information as is necessary in order for a member of staff of the relevant Business Unit to perform his or her duties effectively.

4.2 Where confidential information relating to a wholesale customer is permitted to be used or disclosed for the purposes of the performance of an agreement between Telstra and the wholesale customer, the information is only made available to staff of the Key Network Services Business Unit on a need-to-know basis, unless otherwise authorised by the wholesale customer (as described in clause 3.4).

Telstra Staff - Wholesale Business Unit

4.3 Telstra staff in the Wholesale Business Unit must only disclose confidential information relating to a wholesale customer in accordance with this Strategy and Telstra's obligations of confidentiality to that wholesale customer (which, as outlined in clause 1.2, arise from a number of sources).

4.4 Telstra staff in the Wholesale Business Unit who receive confidential information relating to a wholesale customer (whether directly from the wholesale customer or from Telstra systems or other staff members) are required not to disclose that information to any person in the Retail Business Unit, or to any person in the Key Network Services Business Unit (as relevant), unless the disclosure is permitted under both this Strategy and Telstra's internal policies and procedures regarding confidential information relating to a wholesale customer.

If the disclosure is so permitted, the relevant staff member must only disclose that information on a need-to-know basis.

4.5 Access to confidential information relating to a wholesale customer will be revoked upon a Telstra staff member ceasing their employment in the Wholesale Business Unit. If the staff member is transferring to the Key Network Services Business Unit, future access to confidential information relating to a wholesale customer will be determined in accordance with the need-to-know principle and the process outlined in clause 5. If the staff member is transferring to the Retail Business Unit:

(a) necessary arrangements (including via the security measures outlined in clause 5) will be made to ensure that the relevant staff member will no longer have access to any confidential information relating to a wholesale customer; and

(b) the relevant staff member will not be permitted to use or disclose any confidential information relating to a wholesale customer in their possession or control.

Telstra Staff - Key Network Services Business Unit

4.6 The default position under Telstra's business and information technology systems and processes is that a staff member in the Key Network Services Business Unit will have no access to confidential information relating to a wholesale customer unless they 'need-to-know' the relevant information either for the purposes of performing an agreement with that wholesale customer or otherwise as is necessary for that staff member to perform his or her duties effectively, before the information will be disclosed to that staff member. The following examples illustrate the application of the need-to-know principle in relation to Telstra staff in the Key Network Services Business Unit:

(a) some staff in the Key Network Services Business Unit need-to-know confidential information relating to a wholesale customer on a frequent or ongoing basis in order to provide services and discharge contractual obligations to the customer. These staff are provided with access to the information of the kind that they need; and

(b) other staff in the Key Network Services Business Unit need-to-know confidential information relating to a wholesale customer from time to time, and have access on request, as required for permitted purposes.

4.7 Telstra's staff in the Key Network Services Business Unit who receive confidential information relating to a wholesale customer are required not to disclose that information to any person in the Retail Business Unit or to any other person in the Key Network Services Business Unit, unless the disclosure is permitted under this Strategy and Telstra's internal policies and procedures regarding confidential information relating to a wholesale customer.

If the disclosure is so permitted, the relevant staff member must only disclose such information on a need-to-know basis.

4.8 Access to confidential information relating to a wholesale customer will be revoked upon a Telstra staff member ceasing his or her employment in the Key Network Services Business Unit. If the staff member is transferring to the Retail Business Unit:

(a) necessary arrangements (such as the security controls referred to in clause 5) will be made so that the relevant staff member will no longer have access to any confidential information relating to a wholesale customer; and

(b) the relevant staff member will not be permitted to use or disclose any confidential information relating to a wholesale customer in his or her possession or control.

Telstra Staff - Retail Business Unit

4.9 Confidential information relating to a wholesale customer is not to be disclosed to staff of the Retail Business Unit unless authorised by the wholesale customer (as described in clause 3.4).

Wholesale customers dealing with multiple Business Units

4.10 The application of the general principles set out above regarding use and disclosure of confidential information relating to a wholesale customer, may be varied as a result of arrangements or dealings between Telstra and a wholesale customer. For example, if a wholesale customer provides information to, or acquires services from, a Business Unit other than the Wholesale Business Unit (for example, the Retail Business Unit) or where the relevant services are being supplied as contemplated by clause 3.7 of the OSP. In each case the other Business Unit may share such information with the Wholesale Business Unit, and the Wholesale Business Unit may share information with the other Business Unit, to the extent required by the other Business Unit to perform that other Business Unit's obligations to the wholesale customer.

4.11 However, Telstra recognises the importance of maintaining the division of responsibilities between the Wholesale Business Unit and the Retail Business Unit in order to promote transparency and equivalence in the supply by Telstra of wholesale and retail services. Accordingly, while wholesale customers may elect to receive services from the Retail Business Unit, Telstra will continue to promote the availability of the wholesale channel as the preferred avenue for Telstra

dealing with all carriers and carriage service providers in order to maintain the separation of wholesale and retail operations.

5 Security Measures

Information storage systems and data systems

Overview

5.1 Telstra's security measures for protecting confidential information relating to wholesale customers held in Telstra's information storage systems and data systems consist of the following:

(a) internal policies and procedures regulating information practices within Telstra, which include detailed procedures for upholding security of Telstra's information storage systems and data systems. Compliance with these policies and procedures is monitored by Telstra and any breaches by Telstra staff are regarded as a serious matter, with the possibility of performance management action in appropriate cases; and

(b) IT security controls.

In this clause 5, a reference to "security measures" is a reference to either Telstra's internal policies and procedures or the IT security controls employed by Telstra.

5.2 Under these security measures, Telstra staff are only entitled to a level of access appropriate for their duties. For each Telstra staff member, access to any information system containing, or likely to contain, confidential information relating to a wholesale customer is allowed only if that staff member's role requires access to that system or if the staff member is otherwise entitled to access the system according to the principles set out in this Strategy. The application of these principles to the relevant Telstra systems is discussed below in clauses 5.3 to 5.9.

Information in the Wholesale Business Unit's systems

5.3 For systems which exclusively relate to the Wholesale Business Unit (for example, the Wholesale Business Unit's 'Front of House (FoH)' systems) and contain confidential information relating to a wholesale customer ("**Wholesale Systems**"), access to both data storage systems and live systems is only permitted by staff in the Wholesale Business Unit, or staff in the Key Network Services Business Unit who need-to-know the information contained in those systems in order to perform their duties effectively or are entitled to access such information in accordance with the authorisation of a wholesale customer (as described in clause 3.4). Staff in the Retail Business Unit are not authorised to access Wholesale Systems, except where this is in accordance with the authorisation of a wholesale customer (as described in clause 3.4) or in circumstances described in clause 4.10.

Information in shared systems

5.4 Information relating to the Wholesale Business Unit, the Retail Business Unit and the Key Network Services Business Unit may be maintained in shared systems. In this case, staff in each Business Unit have access to the system, but are not

authorised to access those parts of the system which contain, or are likely to contain, confidential information relating to a wholesale customer ("**Wholesale Areas**") without the permission of Telstra. Telstra will:

(a) permit access to Wholesale Areas by staff in the Wholesale Business Unit and those staff in the Key Network Services Business Unit who (having regard to clause 4) need-to-know the information contained in those systems or are entitled to access such information in accordance with the authorisation of a wholesale customer (as described in clause 3.4);

(b) not permit access to Wholesale Areas by staff in the Retail Business Unit, except where this is in accordance with the authorisation of that wholesale customer (as described in clause 3.4) or in circumstances described in clause 4.10.

Approval process

5.5 As outlined in clause 4.6(a), a limited set of staff positions within the Key Network Services Business Unit are pre-approved for access to relevant confidential information relating to wholesale customers (on the grounds that such persons need-to-know that information on a frequent or ongoing basis). These staff members are entitled to access that information by virtue of their position and do not need to apply for specific approval from Telstra.

5.6 All other staff members of the Key Network Services Business Unit or the Retail Business Unit must submit access requests to be authorised to access information systems which contain, or are likely to contain, confidential information relating to a wholesale customer subject to Telstra's internal policies and procedures regulating information practices.

Access monitoring

5.7 Telstra maintains a log of all approved requests for authorised access to information systems which contain, or are likely to contain, confidential information relating to a wholesale customer by staff in the Key Network Services Business Unit and by staff in the Retail Business Unit (who are entitled to access such information in accordance with the authorisation of the wholesale customer (as described in clause 3.4) or in circumstances described in clause 4.10). The log generally includes the approval date, approving manager, type of access, the reason it is required and a unique reference number that is manually added to the user's access profile in the application systems during provisioning to facilitate access auditing and profile management.

5.8 Telstra performs annual audits to ensure that individuals with information systems access are still entitled to have such access on the basis of the principles set out in this Strategy. Telstra is also introducing an automated process whereby a notification is generated for systems administrators when individuals move between the various Business Units in order to modify their access (if necessary) according to their new role.

Management of system control issues

5.9 Each Wholesale Business Unit system is managed by specific 'System Owners' who are responsible for maintaining a database of the relevant systems and the corresponding 'System Owners' which is accessible in read-only format by Telstra staff.

Physical security of information

5.10 The physical security of the information held by Telstra is an integral component of Telstra's measures to protect confidential information relating to wholesale customers. Telstra maintains a number of policies and practices to ensure general physical security of information. Nominated Telstra representatives manage various aspects of physical security.

5.11 Telstra specifically protects confidential information relating to wholesale customers in accordance with this Strategy by ensuring physical separation between the Wholesale Business Unit and Retail Business Unit as described below.

Physical Separation of Wholesale and Retail Premises

5.12 To ensure that confidential information relating to wholesale customers is protected, Telstra ensures physical separation is maintained between the premises occupied by the Wholesale Business Unit and the Retail Business Unit.

5.13 This separation is achieved in a number of ways. The primary method used by Telstra is maintaining separate premises for staff in the Wholesale Business Unit and the Retail Business Unit (although not necessarily in separate buildings). Telstra's premises are secured by doors operated by security cards or other access control devices, with access being allowed only to authorised staff.

Private locations for customer meetings

5.14 At each Telstra business place where Telstra holds meetings with wholesale customers, Telstra provides private and secure locations for meetings.

Data collection, storage and archiving security

5.15 Telstra has established records management practices, policies and procedures to assist the corporation and its staff to comply with:

(a) the International and Australian Standard on Records Management (AS ISO 15489);

(b) industry codes and legislative provisions relating to recordkeeping (such as the *Archives Act* 1983 (Cth), the *Telecommunications Act* 1997 (Cth), the *Corporations Act* 2001 (Cth) and various legislation relating to tax, accounting and staff activities); and

(c) records management initiatives and standards issued by the National Archives of Australia.

5.16 Archiving security is maintained through supervision by the Director Business and Finance Services and the National Corporate Records Manager.

5.17 Telstra also has internal policies for the maintenance of documentation to assist in managing record storage.

6 Implementation

6.1 In accordance with clause 4.3 of the OSP, Telstra will comply with this Information Security Strategy from 30 November 2006.

6.2 As outlined in clause 5.1, to promote compliance by Telstra staff with this Information Security Strategy, Telstra has developed internal policies and

procedures setting out the various responsibilities of Telstra staff in each Business Unit in relation to the access and use of confidential information relating to wholesale customers. These internal policies and procedures will be available online to all Telstra staff and must be followed by all affected Telstra staff.

6.3 Telstra will also provide mandatory training for affected Telstra staff in relation to this Information Security Strategy. This training will be provided both as part of the induction of new Telstra staff and regularly for all affected Telstra staff.

6.4 Telstra will monitor and report on its compliance with this Information Security Strategy in the manner set out in the OSP.

7 Definitions

7.1 In this Information Security Strategy, the following words have the following meanings:

"**ADSL**" means Asynchronous Digital Subscriber Line.

"**Business Unit**" means the Wholesale Business Unit, the Retail Business Unit or the Key Network Services Business Unit.

"**OSP**" means the operational separation plan approved by the Minister under clause 55(1) of Schedule 1 to the *Telecommunications Act* 1997 (Cth) on 23 June 2006.

"**Wholesale Areas**" has the meaning given in clause 5.4.

"**Wholesale Systems**" has the meaning given in clause 5.3.

All other capitalised terms have the meaning given to those terms in the OSP.