

Commonwealth of Australia

*Telecommunications Act 1997*

**Telecommunications (National Broadband Network—  
Restricted Recipients and Storage, Handling and  
Destruction of Protected Carrier Information) Rules  
2008 (No. 1)**

I, ANTHONY NORMAN ALBANESE, Minister for Infrastructure, Transport, Regional Development and Local Government, on behalf of the Minister for Broadband, Communications and the Digital Economy in accordance with an authorisation under section 18C of the *Acts Interpretation Act 1901*, make these Rules under subsections 531N(1) and 531P(1) of the *Telecommunications Act 1997*.

Dated 6 August 2008

ANTHONY NORMAN ALBANESE

Minister for Infrastructure, Transport, Regional Development and Local  
Government

---

**1 Name of Rules**

These Rules are the *Telecommunications (National Broadband Network—Restricted Recipients and Storage, Handling and Destruction of Protected Carrier Information) Rules 2008 (No. 1)*.

**2 Commencement**

These Rules commence on the day after they are registered on the Federal Register of Legislative Instruments.

**3 Definitions**

In these Rules:

2 *Telecommunications (National Broadband Network—Restricted Recipients and Storage, Handling and Destruction of Protected Carrier Information) Rules 2008 (No. 1)*

**Act** means the *Telecommunications Act 1997*.

**authorised entrusted company officer** means an entrusted company officer in relation to whom a receiving officer has given a certification in accordance with subclause 4(2) of these Rules.

**Department** means the Department administered by the Minister.

**Determination** means the *Telecommunications (National Broadband Network) Determination under subsection 531H(4) 2008 (No. 1)*.

**Minister** means the Minister administering the Act.

**relevant company** means a company in relation to which a receiving officer has obtained or will obtain protected carrier information under section 531H of the Act.

**receiving officer** has the meaning given in the Determination and includes an entrusted company officer who has been nominated by a relevant company to replace a receiving officer provided that:

- (a) the relevant company has notified an authorised information officer of the nomination; and
- (b) the nominated entrusted company officer is an entrusted company officer within the meaning of paragraphs (a) or (b) of the definition of ‘entrusted company officer’ in section 531B of the Act; and
- (c) the nominated entrusted company officer has given an authorised officer a signed copy of an undertaking in substantially the form specified in Schedule 1.

*Note 1:* Each of the following expressions used in these Rules has the meaning given by the Act:

- authorised information officer
- entrusted company officer
- protected carrier information.

*Note 2:* Each of the following expressions used in these Rules has the meaning given by the *Acts Interpretation Act 1901*:

3 *Telecommunications (National Broadband Network—Restricted Recipients and Storage, Handling and Destruction of Protected Carrier Information) Rules 2008 (No. 1)*

- document
- record.

**4 Access to protected carrier information**

- (1) Protected carrier information may be disclosed under subsection 531H(1) of the Act to a receiving officer of a company that has given a notice to an authorised information officer under paragraph 531H(1)(b) of the Act.

*Note:* An authorised information officer would need to be satisfied that the conditions specified in the Determination have been met before disclosing protected carrier information under subsection 531H(1).

- (2) Protected carrier information may be disclosed to an entrusted company officer under paragraph 531K(2)(a) of the Act if a receiving officer has certified to an authorised information officer that:

- (a) the duties of the entrusted company officer are directly relevant to the exceptions to the prohibition on use in subsection 531K(1) of the Act set out in subsection 531K(2A) of the Act; and
- (b) the entrusted company officer has signed an undertaking that is substantially in the form specified in Schedule 1.

*Note:* A certification by a receiving officer under subclause 4(2) may relate to more than one entrusted company officer. A receiving officer may make more than one certification.

- (3) For the purposes of subclause (2), the certification must be in the form of a statutory declaration made under the *Statutory Declarations Act 1959* (Cth).

**5 Receiving officer to maintain list of officers who are given access to protected carrier information and relevant company to provide access to premises on request**

- (1) A receiving officer must maintain a list containing details of each authorised entrusted company officer to whom the receiving officer initially gives access to protected carrier information, details of the premises where that information is stored and the overall period during which each authorised entrusted company officer had access to the information, being the period from the date on which the officer first had access until the date on which the officer ceased to have access.
- (2) A receiving officer must keep the original of all undertakings signed by entrusted company officers under paragraph 4(2)(b).

4        *Telecommunications (National Broadband Network—Restricted Recipients and Storage, Handling and Destruction of Protected Carrier Information) Rules 2008 (No. 1)*

- (3) If requested, a receiving officer must, as soon as practicable after the request is made, provide to an authorised information officer details about the matters mentioned in subclauses (1) and (2), including a copy of the undertakings mentioned in subclause (2).
- (4) If requested, a relevant company must, as soon as practicable after the request is made, permit the Commonwealth or an authorised agent of the Commonwealth to inspect the premises mentioned in subclause (1) to ensure that appropriate security arrangements are in place at those premises.

**6        Storage of protected carrier information**

- (1) If protected carrier information is in electronic form, a relevant company must ensure that this information is stored such that it is quarantined from the company's business information system on a stand-alone computer system which has no connectivity to the company's business system or other external systems including the Internet. Additionally, no one other than an authorised entrusted company officer must be able to access the stand-alone computer system.
- (2) A relevant company must ensure that electronic access to protected carrier information is by way of a system that requires users to be uniquely identifiable and authenticated on each occasion of access. User authentication can be achieved by a variety of means including passwords, passphrases, cryptographic tokens, smartcards or biometrics, or a combination of these.
- (3) A hard copy of protected carrier information or a CD, DVD, USB thumb drive or other electronic storage device (other than a hard drive of a computer forming part of a stand-alone computer system referred to in subclause (1)) containing protected carrier information must be securely stored in at least a Class 'C' container that is accessible only to an authorised entrusted company officer.

*Note:* Class 'B', Class 'C' and Class 'D' containers are all made from sheet steel of at least 1.6 mm thickness, Class 'D' containers being the less secure. Class 'B' containers are fitted with a SCEC (Security Construction & Equipment Committee) endorsed combination lock, Class 'C' containers are fitted with a SCEC endorsed bi-lock and Class 'D' containers are fitted with a commercially available lock.

## **7        Handling of protected carrier information**

- (1) A relevant company must ensure that protected carrier information is marked ‘Strictly Private & Confidential’.
- (2) This marking is to be applied to the top and bottom of each page of a hard copy of the information and in the title and body of the information if it is in electronic form.
- (3) A relevant company must maintain a record containing details of:
  - (a) each authorised entrusted company officer who had access to the protected carrier information following the initial disclosure under subclause 4(2); and
  - (b) the premises where the protected carrier information is stored; and
  - (c) the overall period during which that officer had access to the information, being the period from the date on which the officer first had access until the date on which the officer ceased to have access.
- (4) A relevant company must maintain a record containing details of any copies (including screen prints) and extracts of protected carrier information.
- (5) A record under subclause (4) must include details of:
  - (a) the person who made the copy or extract;
  - (b) the time and date on which the copy or extract was made;
  - (c) the time and date on which the copy or extract was destroyed.
- (6) Subject to subclause 7(8), a relevant company must ensure that a copy or extract of protected carrier information is marked with the name or identifiable code of the authorised entrusted company officer who produced it.
- (7) A relevant company that incorporates into a database or document material qualities of the whole or part of protected carrier information must ensure that the incorporated information is subsequently destroyed or otherwise dealt with in accordance with clause 8.
- (8) A relevant company must maintain a record of any database or document into which protected carrier information has been incorporated and the name of the authorised entrusted company officer who incorporated the protected carrier information into the database or document. This database or document must contain notes or markings to identify where the information has been incorporated.

6        *Telecommunications (National Broadband Network—Restricted Recipients and Storage, Handling and Destruction of Protected Carrier Information) Rules 2008 (No. 1)*

- (9) If protected carrier information in electronic form is to be transferred or sent electronically from one authorised entrusted company officer to another, the information must be encrypted in accordance with a cryptographic protocol that meets the requirements of ACSI 33 when in transit.

*Note:* For the purpose of using ACSI 33, protected carrier information is considered to be classified as 'IN-CONFIDENCE'. Further information about ACSI 33 (the Australian Government Information and Communications Technology Security Manual) can be found at [www.dsd.gov.au](http://www.dsd.gov.au).

- (10) Subclause (9) does not apply where protected carrier information in electronic form is transferred or sent between authorised entrusted company officers using the same stand-alone computer system referred to in subclause 6(1).
- (11) If protected carrier information in hard copy form or contained in a CD, DVD, USB thumb drive or other electronic storage device is to be transferred or transported from one authorised entrusted company officer to another:
- (a) where the other authorised entrusted company officer is not located at the same premises at which the protected carrier information is stored, it must be double bagged and sent by registered courier or passed by hand; and
  - (b) where the other authorised entrusted company officer is located at the same premises at which the protected carrier information is stored, it must be passed by hand.

*Note:* Subclause 7(9) would also apply in addition to this subclause and, in the case of paragraph 7(11)(a), prior notification of different premises, and inspection of the premises if requested by the Commonwealth, must have occurred in accordance and with subclauses 7(12) and (13) prior to the information being transferred or transported.

- (12) If a relevant company proposes to store or handle protected carrier information in a location different from the premises mentioned in subclause 5(1) or paragraph 7(3)(b) or subparagraph 4(1)(a)(i) of the Determination, the company must notify the Commonwealth.
- (13) If the Commonwealth receives a notice under subclause (12) from a relevant company, the company must, if requested, permit the Commonwealth or an authorised agent of the Commonwealth to inspect the proposed location to ensure that appropriate security arrangements are in place at that location before protected carrier information is moved to that location.
- (14) If requested, a receiving officer must, as soon as practicable after the request is made, provide an authorised information officer with details of the records mentioned in subclauses (3), (4) and (8).

7        *Telecommunications (National Broadband Network—Restricted Recipients and Storage, Handling and Destruction of Protected Carrier Information) Rules 2008 (No. 1)*

- (15) If requested, a relevant company must, as soon as practicable after the request is made, permit the Commonwealth or an authorised agent of the Commonwealth to inspect the premises mentioned in subclause 5(1) or paragraph (3)(b) or subparagraph 4(1)(a)(i) of the Determination to ensure that appropriate security arrangements are in place at those premises.

**8        Destruction of protected carrier information**

- (1) Within 1 month of receiving a notice from the Commonwealth in relation to the destruction of protected carrier information, a relevant company must, subject to subclause (2), ensure that:

- (a) all hard copies of protected carrier information (including any copies or extracts of protected carrier information) and documents into which such information has been incorporated are shredded in a Class ‘B’ cross-cut paper shredder or disposed of by an ‘ASIO endorsed’ waste disposal company; and

*Note 1:* There are two types of cross-cut shredders, Class ‘A’ and Class ‘B’ shredders. Class ‘A’ shredders reduce waste to particle sizes of 1mm x 20mm or less; Class ‘B’ shredders reduce waste to particle sizes of 2.3mm x 25mm or less.

*Note 2:* Details of ‘ASIO endorsed’ waste disposal companies can be obtained from an authorised information officer.

- (b) all CDs or DVDs containing protected carrier information are returned to the Department for secure destruction; and
- (c) all electronic storage devices (including hard drives and USB thumb drives) on which protected carrier information has been stored have been sanitised in accordance with ACSI 33.

*Note:* For the purpose of using ACSI 33, protected carrier information is considered to be classified as ‘IN-CONFIDENCE’. Further information about ACSI 33 (the Australian Government Information and Communications Technology Security Manual) can be found at [www.dsd.gov.au](http://www.dsd.gov.au).

- (2) A relevant company may retain board minutes and any reports or documents containing protected carrier information to the extent that the company is required to do so by law or any professional standard applicable to the company.
- (3) A receiving officer must provide a certification to an authorised information officer to the effect that the company has complied with subclause (1).
- (4) For the purposes of subclause (3), the certification must be in the form of a statutory declaration made under the *Statutory Declarations Act 1959* (Cth).

8 *Telecommunications (National Broadband Network—Restricted Recipients and Storage, Handling and Destruction of Protected Carrier Information) Rules 2008 (No. 1)*

- (5) If requested, a relevant company must, as soon as practicable after the request is made, permit the Commonwealth or an authorised agent of the Commonwealth to inspect any premises where protected carrier information was stored to ensure that the information has been destroyed or otherwise dealt with in accordance with subclause (1).

**9 Notification and assistance**

- (1) A receiving officer must notify the Commonwealth in writing (with full details) as soon as practicable after he or she becomes aware of any breach of these Rules by a relevant company or by an entrusted company officer or any breach of an undertaking referred to in paragraph 4(2)(b) of the Determination by the receiving officer or an undertaking referred to in paragraph 4(2)(b) by an authorised entrusted company officer.
- (2) If requested, a receiving officer and an entrusted company officer must, give the Commonwealth or an authorised agent of the Commonwealth all reasonable assistance, including by way of signing and producing documents (at no cost to the Commonwealth) to ensure that the intention and the requirements of these Rules are being duly met.

## SCHEDULE 1

### Undertaking

This Undertaking is given by [ *insert name and address*] for the purposes of paragraph 4(2)(b) of the *Telecommunications (National Broadband Network – Restricted Recipients and Storage, Handling and Destruction of Protected Carrier Information) Rules 2008 (No. 1)* (**Rules No. 1**).

Words defined in Rules No. 1 have the same meanings when used in this Undertaking.

I am an employee/director/partner/consultant of [ *insert name of company*].

I irrevocably and unconditionally undertake to:

1. not use or disclose any protected carrier information that is in my possession or control, except as permitted by the Act;
2. not copy or duplicate any protected carrier information that is in my possession or control, except as permitted by Rules No. 1; and
3. duly and punctually comply with the Act and to perform any obligation imposed on me by Rules No. 1.

This Undertaking is governed by the laws of the Australian Capital Territory.

.....

Name:

Date: