New Zealand Telecommunications Forum

Code for Vulnerable End Users of Telecommunication Services

("Vulnerable End User Code")

Code Status:	**For Public Consultation**
Code Classification:	Voluntary Code
Date:	No yet endorsed
Review Status:	First version

CONTENTS

A. PURPOSE

1. The purpose of this Self-Regulated Code (the Code) is to ensure that Vulnerable End Users are not unduly placed at risk through the provisioning process or subsequent failure of Telecommunications Services and that there is a standard definition for identifying a Customer as a Vulnerable End User dependent on a fixed line Telecommunications Service at their premises for their wellbeing in New Zealand.

2. This Code sets out the minimum requirements a Retail Service Provider (RSP) and Network Operator should adhere to when providing fixed line Telecommunications service to a Vulnerable End User.

3. The Code will be updated from time to time to reflect changes in technology and End User requirements.

4. This Code will take effect [3 months from the final approval by the TCF Board].

5. The Code is applicable to the Code signatories.

B. DEFINED TERMS

Bilateral Agreement	Means an agreement between a Party who is obliged to comply with the terms of this Code and another party (who might or might not also be a party to this Code).
Billing Relationship	Means a relationship where the Service Provider has a bona fide right to charge the Customer for any chargeable activity relating to the provision of Telecommunications Services.
Business Day	Means a day on which registered banks are open for normal banking business, excluding Saturdays, Sundays and nation-wide public holidays. Regional public holidays are Business Days.
CCF or **Code Compliance Framework**	Means the overarching compliance and enforcement regime for TCF codes as set out in the TCF Code Compliance Framework.
Code Signatory	Means a person who agrees to comply with a nominated TCF Code or Codes and be legally bound by the code requirements which includes compliance with the framework.
Compliance Officer	Means the person appointed by the TCF as the compliance officer under the Code Compliance Framework.
Customer	Means a person who has a bona fide Billing Relationship with a Service Provider in respect of a Telecommunications Service. The Customer may also be referred to in this Code as a Vulnerable End User.
Network Operator	A term defined in section 5 of the Telecommunications Act 2001, and may also be referred to as a Local Fibre Company.
New Zealand Telecommunications Forum or **TCF**	Means the New Zealand Telecommunication Forum Incorporated Society registered in New Zealand.
Party	Means a Person bound by this Code under the Telecommunications Act or a Person signed up to this Code.

Person	Means a legal person and includes a company and any other legal entity.
Retail Service Provider or **RSP**	Means any person providing a Telecommunication Service to a Customer and who has the bona fide Billing Relationship with the Customer for that service. An RSP may also be referred to as an Access Seeker or a Service Provider. The term is defined in section 5 of the Telecommunications Act 2001.
Self-Regulated Code	As described in the TCF Rules section 20, the obligations set under this Code are either voluntary or obligatory as approved by the TCF Board.
Telecommunication(s)	Is the conveyance by electromagnetic means from one device to another of any encrypted or non-encrypted sign, signal, impulse, writing, image, sound, instruction, information, or intelligence of any nature, whether for the information of any person using the device or not; but excluding any conveyance that constitutes broadcasting.
Telecommunication(s) Service	Means any goods, service, equipment and/or facility that enables or facilitates Telecommunication.
Voluntary Code	A Voluntary Code is a Self-Regulated Code which TCF Members and other Parties may choose to sign up to. Compliance is through self-certification and monitored through the CCF.
Vulnerable End User or **VEU**	A Vulnerable End User is a Customer or a prospective Customer, who has demonstrated to the satisfaction of their RSP that for reasons of, health, disability or safety they, or a member of their household, are dependent on a Telecommunications Service for their wellbeing.

C. OBJECTIVES AND SCOPE

6. Objectives

6.1. The objective of this Code is to ensure that the Telecommunications industry acts in a responsible manner when dealing with Customers who have an identified vulnerability and a dependency on connection to a fixed line Telecommunications Service. This objective will be achieved by:

6.1.1 Identifying a Customer against the Vulnerable End User definition.

6.1.2 In general terms set out operational guidelines for when a Vulnerable End User requests a new connection or reports a fault.

6.1.3 Set out expectations when communicating with a Customer or a prospective Customer who has identified themselves as a Vulnerable End User and communication of the status of that Vulnerable End User to appropriate parties.

7. Scope

7.1. The scope of this Code includes the following:

7.1.1 A process for identifying a Vulnerable End User;

7.1.2 Communication of that status to appropriate parties;

7.1.3 Impact of a Vulnerable End User's request on various Telecommunication

Industry processes, including:

- Fault management process;
- Ordering and installation process; and
- Informing Vulnerable End Users of the impact of power loss on equipment connected to Telecommunications Services.

7.2. In the instances that RSPs and Network Operators cannot guarantee uninterrupted connectivity they will assist their Customers by encouraging resilience and back up plans.

8. Exclusions from Scope

8.1. This Code does not apply to:

8.1.1 Business Customers – unless identified by a Network Operator or RSP as being a residential Customer, consuming a residential product in a business campus like environment and their Telecommunications Services are not connected to that business.

8.1.2 VoIP Interoperability is covered by the TCF SIP ATA Technical Requirements Standard 2015 and the TCF IP Interconnection for Voice Technical Standard 2012.

8.1.3 111 Calling covered by the TCF Emergency Services Calling Code 2015.

8.1.4 Disconnection of services is covered by the TCF Disconnection Code 2013.

8.1.5 Customer complaints process is covered by the TCF Customer Complaints Code 2016.

8.1.6 Any regulations or industry codes that govern the use or installation of medical equipment.

8.1.7 The communication to Vulnerable End Users on an individual level of planned and unplanned outages.

D. VULNERABLE END USERS

9. RSPs and Network Operators must act in a socially responsible manner by meeting the obligations set out in this Code, when dealing with Vulnerable End Users who have identified their reliance on fixed line Telecommunications Services.

10. A Vulnerable End User is a Customer or a prospective Customer, who has demonstrated to the satisfaction of their RSP that for reasons of, health, disability or safety they, or a member of their household, are dependent on a Telecommunications Service for their wellbeing.

10.1. The following are examples of Customers who should be considered Vulnerable End Users. This list is for guidance only and RSPs should use their discretion to determine the status of a Customer based on their individual circumstances:

10.1.1 Customers who have a monitored medical alarm that are reliant on fixed network access for their continued operation;

10.1.2 Customers with medical conditions where their medical practitioner has certified that they require access to a fixed network access to manage their condition (e.g. to be able to make calls to emergency services);

10.1.3 Customers who are able to provide a protection order that is issued from the Family Court and rely on their fixed line Telecommunications Service for their

safety rather than the use of an alternative service such as a mobile phone; and

10.1.4 Customers who have a family violence safety alarm which is reliant on fixed network access for continued operation.

11. The RSP and Network Operator will:

11.1. Ensure a process is in place for dealing with Vulnerable End Users, and

11.2. Ensure a socially responsible approach is taken when considering a Vulnerable End User's dependency on fixed line Telecommunications Services.

E. IDENTIFYING AND RECORDING VULNERABLE END USERS

12. RSPs will determine whether a Customer or a member of their household, has a genuine dependence on fixed line Telecommunications Services, described in Section D.

13. RSPs will use information provided by a Vulnerable End User regarding their status or the status of someone living in their home in accordance with the RSP's privacy policy.

14. RSPs and Network Operators will ensure that information relating to the definition of Vulnerable End Users and how to identify as a Vulnerable End User is available either online or in written material that is easily accessible by Customers.

15. Identification of a Vulnerable End User

15.1. RSPs will adopt a process which requires the Customer or the prospective Customer requesting to be identified as a Vulnerable End User to provide documentation as to their vulnerability.

15.2. If a Customer identifies themselves as a Vulnerable End User (for example when placing an order or reporting a fault), the RSP may decide to accept their word initially until they have completed the validation process outlined in clause **Error! Reference source not found.**.

15.3. RSPs will accept a Customer's application as determined by the RSP's Vulnerable End User identification process.

15.4. The RSP will advise the Network Operator whenever they request a transaction impacting a Vulnerable End User.

16. Vulnerable End User Identification Process

16.1. RSPs may choose to obtain the following information, signed (or equivalent) by the account holder:

16.1.1 The account holder's contact details and details of an alternative contact;

16.1.2 Details of the vulnerable person who lives at the premises, if this is different to the account holder;

16.1.3 Permission from the account holder to share the vulnerable person's name and other essential details required for supporting the Vulnerable End User process,

between the RSP, the Network Operator; including those parties who have been contracted to do work on their behalf and, if required, the medical equipment service providers; and

16.1.4 Reason why the loss of the fixed line Telecommunications Service would be a threat to the health, disability or safety of the Vulnerable End User who lives at the premises provided by their medical practitioner.

16.2. The RSP will then record the Customer as a Vulnerable End User for the duration of the transaction.

16.3. The requirement for the Customer to provide a medical certificate will be at the discretion of their RSP.

16.4. The Network Operator will accept RSPs on their word that a genuine Vulnerable End User exists. The Network Operator may require the RSP to provide evidence if it is suspected that the process is being abused, subject to the Privacy Act 1993, the RSP's privacy policy and any terms and conditions.

16.5. If the Network Operator becomes aware of a potential Vulnerable End User during an installation or fault and they have not previously been informed by the RSP, they will act as if they had been advised that they were a Vulnerable End User by the RSP and should advise the Customer to contact their RSP directly to initiate their validation process.

F. OPERATIONAL GUIDELINES

17. On each occasion when the RSP requests the Network Operator to connect a Customer, or repair a Customer's connection, the RSP will advise the Network Operator if the Customer is a Vulnerable End User. The Network Operator will take appropriate action in each of the following scenarios if advised that the Customer is a Vulnerable End User.

18. Connections

18.1. When connecting Telecommunication Services the RSP should encourage the Vulnerable End User to discuss their request with their medical equipment service provider if they have medical alarms or equipment installed at the premises, and if necessary, get them to contact the RSP directly to discuss any installation requirements.

18.2. The RSP will record the vulnerable dependency as per section D when the new service request is received from the Customer.

18.3. When placing an order, the RSP will advise the Network Operator of the Vulnerable End User and any relevant information regarding the Customer's vulnerability by:

18.3.1 capturing the information in the order noting that a dependency exists;

18.3.2 including in the notes any vital details regarding technical requirements (which the RSP has knowledge of), if the order involves a physical installation; and

18.4. The Network Operator will pass this information onto field contractors in the details of the service request transactional record.

18.5. The Network Operator will ensure that the installing technicians are made aware the

Customer is a Vulnerable End User and should check before installation that the Vulnerable End User has confirmed that he/she has taken steps to ensure the continued operation of their medical equipment. Installation may be deferred if any party has concerns.

18.6. The Vulnerable End User is responsible for ensuring any medical equipment or apparatus is working after the connection is completed (this maybe done through their medical equipment service provider).

18.7. Where appropriate the Network Operator will use all reasonable commercial endeavours to prioritise the installation.

19. Fault reported by Vulnerable End User

19.1. The following section outlines the process for reporting a fault for a Vulnerable End User. The response service levels are addressed in section 20.

19.2. The RSP will follow its trouble shooting processes to validate the fault and resolve the issue if possible.

19.3. If required the RSP will pass the fault/s to the Network Operator having identified the fault is a network fault advising the existence of a Vulnerable End User and escalate to Network Operator service manager if deemed necessary, refer to section 20.

19.4. The Network Operator fault process must capture details of the Vulnerable End User, as advised by the RSP, and gives the fault appropriate priority within the Network Operator's NOC and field contractor.

19.5. The Network Operator will provide regular updates to the RSP in accordance with its existing BAU fault management process.

19.6. The RSP will confirm with its Vulnerable End User that their service is restored and is no longer compromised.

20. On site response service levels

20.1. Where a fault is proven in a RSP's network, the RSP will respond by endeavouring to give priority to the analysis and repair of the fault and will use all reasonable commercial endeavours to restore service as soon as practically possible.

20.2. Where a fault is proven into the Network Operator's network by the RSP, the Network Operator will endeavour to treat the fault as a priority for on-site response at the location of the fault and will use all reasonable commercial endeavours to restore service as soon as practically possible.

Note: On-site refers to the location of the fault. The response time may vary depending on the location i.e. a fault recorded by a Vulnerable End User located at an outlying candidate area may take longer to reach.

G. COMMUNICATION TO VULNERABLE END USERS

21. Change in the Customer's Broadband Plans

21.1. RSPs will communicate to Vulnerable End Users any impact on their fixed line Telecommunications Services when they change their broadband plans. This may also

include information that should be passed onto their medical equipment service provider if necessary.

22. Service Interruption

22.1. When an RSP provides a voice or broadband service and where that service relies on the underlying telecommunications connection to function, the Vulnerable End User must be informed by the RSP that the service will not be available in the event of a service interruption or power outage, unless the Customer has a battery back-up service in their home. This includes an explicit statement that they will not be able to make calls to emergency services if the voice service is not available.

22.2. The Vulnerable End User must also be informed that an RSP cannot guarantee uninterrupted voice or broadband connectivity. Therefore, customers who rely on voice or broadband must take this into consideration and take the necessary steps to ensure they have a robust backup plan in place should connectivity fail.

23. Encourage Resilience

23.1. The RSP will encourage Vulnerable End Users to consider the resilience of their fixed line Telecommunications equipment to minimise the impact of a loss of service. End Users who rely on voice or broadband connectivity must take this into consideration and take the necessary steps to ensure they have a robust backup plan in place should connectivity fail. For example, it may be appropriate to encourage the Vulnerable End User to ensure a mobile phone is available as a backup service in case their fixed line service is lost and need to contact emergency services. Their backup plan could also include Vulnerable End User's ensuring they have access to third party support which could be neighbours, DHB or local support services.

24. Medical Services and Equipment Service Providers

24.1. The RSP will inform the Vulnerable End User that it is their responsibility to inform their medical equipment service provider that they are transferring their voice services and/or broadband services to fibre. The medical equipment service provider should ensure that the medical equipment installed at the premises is able to be connected to the telecommunications network and connectivity remains.

24.2. When there is a new connection the RSP will encourage the Vulnerable End User to discuss their request with their medical equipment service provider and if required get them to contact the RSP directly to discuss any installation requirements.

H. COMPLIANCE

25. The TCF Code Compliance Framework (CCF) applies to the ongoing monitoring and compliance of this Code. By becoming a Code Signatory, Code Signatories agree to comply with and are bound by the terms of the CCF and obligations set out in this Code.

26. For the purposes of the self-certification requirements under the CCF, the key metrics of this Code that Code Signatories are required to report against are set out in Clause I of this Code.

27. In the event of any inconsistency between this Code, any relevant legislation, any Bilateral Agreement and any Commerce Commission determinations, this inconsistency will be resolved in the following (descending) order of precedence:

27.1. Legislation;

27.2. Commerce Commission determinations;

27.3. Bilateral Agreements;

27.4. This Code.

I. SELF-CERTIFICATION AND MONITORING REQUIREMENTS FOR THIS CODE

28. Each signatory to this Code must keep information they deem necessary to show their compliance with this Code, should it be required.

29. In accordance with the CCF, Code Signatories must file initial and annual self-certification forms with the Compliance Officer to demonstrate their initial and ongoing compliance with this Code. The key metrics that Code Signatories must stipulate they comply with in relation to this Code are set out below:

    29.1. RSPs and Network Operators will communicate the status of a Vulnerable End User when necessary (clause 18.3);

    29.2. Network Operators will operate in an appropriate manner when notified by an RSP of a Vulnerable End User status (clause 16.4);

    29.3. Parties will ensure adequate information is provided to Vulnerable End Users on service interruption (clause 22).

30. The CCF's complaints management procedures will apply to any allegations of a breach of this Code, made by one Code Signatory about another to the Compliance Officer. By signing up to this Code, Code Signatories agree to abide by the terms of the CCF and will always cooperate in a full and frank manner with the Compliance Officer, participate in good faith in any investigations they may be involved in and adhere to any sanctions levied against them under the CCF in relation to this Code.

J. EXPIRY, REVOCATION AND AMENDMENT OF THE CODE

31. The expiry, revocation or amendment of this Code will be in accordance with the New Zealand Telecommunications Forum's Operating Procedures Manual 'The Handbook', any TCF Member may put a Project Proposal to the Forum Board (at any time) for the amendment or revocation of the Code.