

Operations and Support Manual for the Emergency Calling Code

July 2022

© 2022 The New Zealand Telecommunications Forum Inc. All rights reserved. Copyright in the material contained in this document belongs to the New Zealand Telecommunications Forum Inc. No part of the material may be reproduced, distributed or published for any purpose and by any means, including electronic, photocopying, recording or otherwise, without the New Zealand Telecommunications Forum Inc written consent.

Table Of Contents

1.	Explanatory Statement	3
2.	Background	3
3.	Purpose of the Manual	3
4.	Document Precedence	3
5.	Procedures for changes to the Manual	4
6.	Definitions and Interpretation	4
7.	Schedules	5
Sche	dule 1: Arrangements for providing a 111 capable voice service	6
Sche	dule 2: Emergency Calling Code Compliance Template	7
Sche	dule 3: Resale Providers Compliance Notification	14
Sche	dule 4: Calling Party Number	15
Sche	dule 5: Template Emergency Services Calling Mobile arrangements	17
Sche	dule 6: Emergency services calls interconnect link test plan	20
Sche	dule 7: TESA database specification for the provision of customer information	22

1. Explanatory Statement

- 1.1 The purpose of this Operations and Support Manual (**the Manual**) for the Emergency Calling Code (**the Code**) is to provide Voice Service Providers (**VSP's**) with procedural guidance and definition with regards to the delivery of the requirements of the Code.
- 1.2 Its intent is to ensure that the consumers of the New Zealand Emergency Calling Service are provided with a consistent experience that meets the requirements of the Code.
- 1.3 It is intended to provide detailed procedures for operational management of emergency service calling, such that the public expectations of the service are set and managed as are appropriate to the scope of the VSP's responsibilities as defined in the Code.
- 1.4 The Manual provides VSPs with the details for how to comply with the Code, but it does not replace the obligations set out in the Code. Where a VSP meets its obligations in a manner consistent with guidance set out in the manual, this shall be considered by the Compliance Officer as evidence of compliance with the Code.
- 1.5 This document should be read in conjunction with the Emergency Calling Code. A copy of this document can be found on the TCF Website https://www.tcf.org.nz/industry/standards-compliance/public-services/emergency-calling/

2. Background

2.1 The TCF Emergency Calling Code which sets out service performance and customer information standards for Emergency calls made via voice telephony services.

3. Purpose of the Manual

- 3.1 Government Officials, Emergency Service Organisations (ESO's) representatives and VSPs continue to meet to discuss the operation and enhancements to the Code and emergency calling system (members of the Emergency Services Calling Working Party (ESCWP). The ESCWP agreed that an operations manual would:
 - a) Promote Code membership and compliance by capturing obligations and "how to" collateral in a single document. ESCWP members have shared experiences relating to how best to comply and we would seek to capture these findings in the Manual;
 - b) Promote collaboration amongst the parties; and
 - c) Promote consistent implementation of the Code.
- 3.2 The Code sets the high level required outcomes. This approach recognises that VSPs deploy a number of different technologies and systems and must be free to meet the obligations in the most effective way for that particular operator.
- 3.3 Accordingly, while the Manual sets out and promotes consistency within the industry, it does not override the Code obligations nor limit VSPs from complying with those obligations in a way that best reflects the characteristics of its service.

4. Document Precedence

- **4.1** The Code sets out VSP obligations.
- 4.2 The Manual provides VSPs guidance on how best to comply with its Code obligations.

4.3 If a VSP applies the processes and approach set out in the Manual, this shall be taken by the Compliance Officer as evidence of compliance with the Code.

5. Procedures for changes to the Manual

- 5.1 The TCF is the owner of the Manual, with exception to particular reference documents attached to the Schedules.
- 5.2 The ESCWP may recommend a change/s to the Manual from time to time.
- 5.3 The change/s will require approval from the ESCWP and consultation with the Code signatories. The change/s will be submitted to the TCF Board for approval.
- 5.4 Once approval of the change/s is achieved the TCF will notify the Code signatories and Emergency Service Organisations of the approved changes.
- 5.5 Any proposed changes must be in-line with the obligations set out in clause 1.4.

6. Definitions and Interpretation

- **6.1** Terms defined in the Code have the same meaning in this Manual.
- **6.2** This section is intended to provide examples of the common expressions used for operational purposes.

Expression	Clarification Explanatory Note	
BAU	Means business as usual.	
Code	Means the Code for Emergency Voice Calling Services ("Emergency Calling Code.")	
ESCWP	TCF Emergency Services Code Working Party	
Manual	Means the Operations and Support Manual for Emergency Calling Code	
ESO	Emergency Service Organisation i.e., Police, Fire and Ambulance.	
Restricted Means a Telecommunication Service restriction in the form of a compound (inbound/outbound) or access to a Telecommunication Service applied by a Service Provider to confine or limit a Customer's absolute incur additional debt or charges on their account.		
Suspension Means a Service Provider rendering a customer's Telecommunication Services or similar inoperable. This is usu to enforce collections actions due to non-payment of the accounts, where other forms of reminder have been igno customer up to the time of application. NB: Suspend and Susp a similar meaning to 'Suspension'.		
TESA	Telephone Emergency Subscriber Access system used by the Police Emergency Communications Centres as part of the call management process. This is the National Location Register that is referred to in the Code.	

7. Schedules

Sch.	Schedule	Code reference
1	Arrangements for providing a 111 capable voice service	This is for information only.
2	Emergency Calling Code Compliance Template (Checklist sets out code obligations for initial and ongoing compliance review.)	Code compliance (Section M and Annexure 1)
3	Resale Providers Compliance Notification (This sets out the recommended compliance approach to resale services where key characteristics of the service are determined by the wholesale provider.)	Code compliance (Section M and Annexure 1)
4	Calling Party Number	Procedural information regarding calling party numbers (c23)
5	Template Emergency Services Calling Mobile arrangements (Provides for 111 calls to be carried by other mobile providers when technically possible when service from the host provider is not available.)	This template is for information only. Mobile network roaming arrangements sit parallel to the code.
6	Emergency services calls interconnect link test plan	Interconnect link testing (c18.4)
7	TESA database specification for the provision of customer information	Provision of customer information (c24.2)

END

Schedule 1: Arrangements for providing a 111 capable voice service

The following lists the various arrangements that a new voice provider should consider as part of providing a 111 capable voice services:

- TCF Emergency Calling Code (TCF).
- Provision of fixed line caller location information (TESA specification through the Police peter.livesey@police.govt.nz).
- Provision of mobile emergency calling location information (ECLI arrangements through MBIE ECLI Director phil.parker@mbie.govt.nz).
- Mobile 111 calling roaming MOU (arrangement to accept emergency calls of customers from other networks, contact any mobile network operator).
- Interconnection agreement (directly with Spark Wholesale as the current ICAP provider or a Spark NZ interconnected telecommunications provider).
- Telecommunications Information Privacy Code 2020 (check compliance, particularly Schedule 4 of the Code as it relates to the provision of Emergency Location Information).

Schedule 2: Emergency Calling Code Compliance Template

This template sets out the relevant considerations for VSPs considering Code compliance notification.

- 1. This sheet relates to services that are intended to meet the performance standards set out in the Code. It records how the service complies with the Code. It does not include, for example, definitions or service provider obligations.
 - The Code provides for voice services that do not meet the performance standards in the Code. However, for these services, there are customer disclosure and information requirements. A separate sheet would be used for services that are not intended to meet the performance standards set out in the Code.
- 2. Service providers must notify the TCF where a service complies with Code and retain supporting documentation for its initial notification.

Ref.	Clause	Comments/Explanatory Notes	Compliance/Partial-Compliance/Non-Compliance
	Voice Service name: PSTN Local Service; and Cellular Mobile Service		
F	Obligations of the Parties		
14	Where a VSP supplies a Non-Compliant Voice Service, the VSP must: 1. not call this a "Code Standard Voice Service"; and 2. comply with Clause 29.		
G	Availability and Quality of Emergency Calls		
17	Emergency Calling		
17.1	VSPs will ensure that Customers using a Voice Service are still able to make Emergency Calls using that Voice Service where: (a) the Voice Service has been withheld, suspended or restricted for any reason, but has not been disconnected; or (b) the Voice Service has been disconnected but can still be used to contact the		
	VSP Customer service representative.		
17.2	Where there is a technical issue relating to the availability of Emergency Calls for suspended services (for example, where service has been suspended for network fault conditions, abusive callers, temporary disconnect for credit control purposes, or other		

Ref.	Clause	Comments/Explanatory Notes	Compliance/Partial-Compliance/Non-Compliance
	similar scenarios), the VSP will make best endeavours to notify the Customer of the suspended service, and the implications for Emergency Calling. Any such notification can be made by any means (e.g., website, SMS, email) as the VSP considers reasonable and appropriate in the given circumstances of the suspended service.		
17.3	For the purposes of Clause 17.1, a service is disconnected when there has been the final termination of the Voice Service between the VSP and the Customer.		
18	Handling Emergency Calls		
18.1	Subject to Clauses 15 and 20, VSPs will ensure that the Voice Service provided to a Customer allows any end user to make an Emergency Call by using the Emergency Call number "111".	This can only be achieved if their Network recognises the call is a 111 call	
18.2	The parties acknowledge that each VSP may currently have active overseas Emergency Service numbers (for example, "000", "112", "911", "999") in a network which would allow any end user to make an Emergency Call. Any change to those active related Emergency Service numbers can only be done by agreement between the affected VSPs and the Emergency Service Organisations, taking into account any reasonable technical or network restrictions that may exist to give effect to that change. A VSP may activate a new related Emergency Service number in a network, but only with the agreement, and on conditions with the Emergency Service Organisations.	If you are going to use a number that is not 111 then the VSP must ensure it is consistent with NAD and other obligations.	Set out numbers open for emergency service calling, i.e. "customers are able to dial 111, 911, etc to access Emergency Services".
18.3	VSPs will carry (or procure the carriage of) Emergency Calls to the ICAP using the most efficient call routing possible given the handover links and handover arrangements that have been established in accordance with any relevant interconnection agreement between Carriers.		
18.4	VSPs will test handover arrangements relating to Emergency Calls on a regular basis as agreed by the parties to the interconnect agreement governing the provision and operation of the handover link.	See schedule 6 of the Manual.	Refer to testing standard in manual or other arrangements.
19	Priority for Emergency Calls		
19.1	VSPs will manage their networks in such a way that Emergency Calls have priority in the network, and where the Voice Service is provided wholly or partly over another person's network, the VSP shall ensure to the extent practical that the other person's network prioritises Emergency Calls.	Refer to comments under 18.1	For example, 111 calls have their own trunk routes – no other traffic can use.
20	Voice Quality and Availability		
20.1	Where a Voice Service is available to Customers with differing grades of service, the VSP will use the highest quality service available on that Voice Service for Emergency	This clause is to apply to the extent where VSP's are able to offer "differential grades	

Ref.	Clause	Comments/Explanatory Notes	Compliance/Partial-Compliance/Non-Compliance
	Calls.	of service". Where CPE technology is provided by the customer, VSP's are not liable for any degraded Emergency Service access as a result of CPE configuration errors or equipment failures.	
20.2	In any event, VSPs will design and manage the Voice Service so that in normal operating conditions: (a) The Voice Service supports a Voice Quality for Emergency Calls of R≥65 for 95% of calls, and R≥50 for 99% of calls or a similar relevant measure (disregarding in all cases the effect of any Customer Equipment that does not comply with the VSPs published standard), where R is the Transmission Rating Factor as defined in ITU-T G.107 (including any relevant advantage factor for wireless and satellite-based providers); (b) On average each Customer access line will have less than 50 minutes downtime per year due to Core Network outages. This excludes, in all cases, the impact of: I. downtime arising from a Matter Outside the VSP's Reasonable Control; II. downtime arising from a planned or unplanned outage in an access or backhaul network, or satellite gateway. Access and backhaul networks are predominantly subject to existing regulation; or III. partial outages (for example, failure of part of a telephone exchange or voice application server) that do not affect the delivery of Emergency Calls. (c) The probability of an Emergency Call under normal operating conditions being blocked due to insufficient resources being provided between the point at which the call is received by the VSP through to where the call is handed off to the ICAP, does not exceed 1% of total call attempts excluding: I. an event or force majeure or a specified Matter Outside a VSPs Reasonable Control; or II. an outage in a network.	This section was intended to be outcomes rather than measures. What these outcomes mean for different network design and technologies will also differ. Therefore, has been left to RSPs to determine what design and measures to track which will demonstrate compliance with the Code.	
20.3	For the purposes of Clause 20.2, normal operating conditions are the conditions that Emergency Calls made using the relevant Voice Service will generally experience when operating within the network's design specification. In the case of a Voice Service provided over a mobile network, normal operating conditions require that adequate coverage is present.		

Ref.	Clause	Comments/Explanatory Notes	Compliance/Partial-Compliance/Non-Compliance
21	Reliability		
21.1	VSPs will take all reasonable steps to ensure the Voice Service can reliably be used to make Emergency Calls.		
21.2	VSPs will develop plans that will minimise disruption to Emergency Calls made using the Voice Service in peak traffic and disaster conditions.		
21.3	VSPs that operate a mobile network in New Zealand will take all reasonable steps to enter into arrangements whereby they enable their mobile networks to receive, as far as is practically possible, Emergency Calls from Customers of other parties when the Customer's home network is unavailable, and route those Emergency Calls to the Emergency Services.		
Н	Caller Information		
23	Number Identification		
23.1	VSPs will provide the ICAP Provider with the Calling Party Number, to the extent known by the VSP, for all Emergency Calls made using the Voice Service in the signalling format agreed between the VSP and the ICAP Provider (as specified in the Operations Manual).	For example, VSP provides calling number information, as received or generated by its switching systems, to the ICAP Refer to Schedule 4 of this manual for details.	
24	Location and Caller Information		
24.1	The obligations set out in this clause are based on the current systems for providing location information, under which location information is provided to Emergency Service Organisations separately to the delivery of the Emergency Calls. Under these current systems the frequency and format for this information is separately agreed between the VSP's and the Emergency Service Organisations.		
24.2	Unless otherwise agreed between the VSP and Emergency Service Organisations, VSPs will provide the National Location Register an extract containing Customer billing name and address details that can be correlated with the Calling Party Number, in accordance with Clauses 24.2 (a) and 24.2 (b).		
	(a) Where the service is supplied to a Customer at a fixed location, the VSP will provide the National Location Register an extract containing the Customer's name and the physical address at which the service is supplied.		
	(b) Where the service is: I. marketed and expected to be used primarily as a fixed service, but		

Ref.	Clause	Comments/Explanatory Notes	Compliance/Partial-Compliance/Non-Compliance
	capable of mobile or nomadic use; or II. a mobile service; the VSP will provide the National Location Register an extract indicating: i. the Customer's name where known; ii. the Customer's registered service address where known; and iii. advice that the service is capable of mobile or nomadic use, and that the location of calls made using that service may be uncertain.		
24.3	VSPs will as soon as reasonably practicable after a request by an Emergency Service Organisation, provide the Emergency Service Organisation with other information as reasonably requested for the purposes of handling an Emergency Call.	This refers to the process by which emergency services are able to request additional information in accordance with the Privacy Act.	
24.4	VSPs will take all reasonable steps to ensure that the information provided under Clauses 24.2 and 24.3 is in an agreed format and correct at all times.		
24.5	In addition to providing information in accordance with Clause 24.2, in the case of Emergency Calls originating in a mobile cellular network, the VSP will ensure that the ICAP Provider is provided with information on a per call, real time basis in a format agreed between the VSP and the ICAP Provider, which permits identification of the geographic region of the originating cell site.		
24.6	Unless otherwise agreed between the VSP and Emergency Service Organisations, VSPs delivering mobile services will provide mobile location information through the Emergency Location Information System (ELIS), as defined by Schedule 4 of the Telecommunications Information Privacy Code, that is operated by MBIE (or any relevant Government Agency becoming responsible for ELIS). This will be performed in accordance with the VSP's terms and conditions of contract with the relevant Government Agency responsible for ELIS, and consistent with the Telecommunications Information Privacy Code. Where a new VSP commences delivery of mobile services it will use all reasonable efforts to contract with the relevant Government Agency responsible for ELIS to ensure timely delivery of mobile location information through ELIS.		

Ref.	Clause	Comments/Explanatory Notes	Compliance/Partial-Compliance/Non-Compliance
I	Customer information standards		
26	Visibility of the Code Standard Voice Service		
26.1	In relation to a Code Standard Voice Service, the VSP will take reasonable and appropriate steps to provide the following information in an easily discernible manner and easily accessible to all Customers on the VSP's website:		
	(a) the ability to make a 111 Emergency Call as part of the Code Standard Voice Service;		
	(b) the Emergency Service Organisations to which the 111 Emergency Call number provides access;		
	(c) that Emergency Calls should only be used when seeking a response from an Emergency Service Organisation to deal with an emergency to which the organisation is established to respond; and		
	(d) what information VSPs will disclose to Emergency Service Organisations when Emergency Calls are made (including Calling Party Number and caller location information).		
26.2	VSPs will use reasonable endeavours to minimise the impact of non-genuine Emergency Calls on the system.		
27	Customer Information Standards about Service Reliability		
27.1	Customers must be provided with the information required by the 111 Contact Code, where a Code Standard Voice Service is reliant on mains power at the Customer premises and will be unable to make 111 Emergency Calls in a power failure.		
28	Voice Service Provider Contact Information		
28.1	VSPs must provide the Emergency Service Organisations with contact details for the appropriate personnel and keep these details up to date at all times in the event of a fault or problem occurring which requires the Emergency Services Organisation to contact the VSP.		
J	Customer information standards about non-compliant voice services		
29	If a VSP provides a Non-Compliant Voice Service the VSP will:		
29.1	Not promote, describe or represent the service as being a Code Standard Voice Service.		

Ref.	Clause	Comments/Explanatory Notes	Compliance/Partial-Compliance/Non-Compliance
29.2	Advise its Customers, during the sales process, in the terms and conditions of use, and in any user guide that: (a) Emergency Calls cannot be made using that service; or (b) Emergency Calls can be made using that service but that the performance of the Emergency Calls will not meet the service standards of this Code; (as the case may be).		
29.3	During the sales process, offer its Customers (at no extra charge other than reasonable postage and packaging if applicable) equipment labels which state that: (c) Emergency Calls cannot be made using that service; or (d) Emergency Calls can be made using that service but that the performance of the Emergency Calls will not meet the service standards of this Code; (as the case may be).		
К	Customer complaints		
30	Customers must be informed by their VSP about the Customer Complaints process available to them for prompt resolution of any issues under the Code, this must include: (a) Providing Customers with clear information on either how to raise a complaint or where the Customer can find the VSP's complaint process. (b) VSPs must make available information to Customers on how they can access the Telecommunications Disputes Resolution Scheme (TDRS). (c) VSPs must inform Customers of the existence of the Code and what Customers must expect from their VSP under it. This may be by providing a link to the relevant page on the TCF website.		

Schedule 3: Resale Providers Compliance Notification

Introduction

The Code is based on VSPs ensuring compliance with the Code obligations. However, when VSPs are reselling voice services that are subject to the provisions of the Code, aspects of these voice services may not be controllable by the VSP and instead be set by that VSP's wholesale provider.

This schedule sets out a recommended approach for how wholesale providers can certify the aspects of the resale service that comply with the Code.

For the avoidance of doubt, nothing in this Schedule absolves VSPs from their responsibility to certify their compliance with this Code. VSPs are primarily responsible for ensuring that the underlying wholesale or network products are compliant, or able to be made compliant, with this Code. However, the Compliance Officer, will take the certificate in to account in any compliance action.

Process

The wholesale provider may certify it has joined the Code and that its voice complies with the Code. For example, a statement that:

Voice Service Providers (VSPs) may join the TCF Emergency Calling Code (the Code). The Code defines a VSP as the service provider who maintains a direct relationship with the end consumers and this means Reseller customers may also join the Code.

The [wholesale provider] has joined the Code and certifies that its [name] services comply with the Code. However, the Code covers network and end user customer related aspects of the emergency services calling system. Therefore, overall compliance is likely to be a mix of network related functionality provided by [wholesale provider] and reseller provider functionality.

The Code does not provide for the splitting of obligations - the VSP is responsible for ensuring overall compliance with the Code. Set out below are the Code obligations whereby the service provider can rely on [wholesale providers] certification and the obligations where compliance is not related to the resale service that [the wholesale provider] provides.

This purpose of this statement is to support VSPs compliance with the Code.

In the event that a Code Compliance Framework review is required of the VSP, the VSP may refer that aspect of the review or investigation to the underlying wholesale provider.

Schedule 4: Calling Party Number

- The Calling Party Number sent with an Emergency Call must, wherever practical, be a New Zealand Mobile Number or Geographic Number as classified by the New Zealand Numbering Plan (REF ITU-T https://www.itu.int/oth/T0202000099/en). Other types of number such as Toll Free or Special Services should not be used.
- Where any Emergency Call is delivered to the ICAP Provider with a non-compliant Calling Party Number (i.e. of incorrect format or type), the VSP responsible for delivering the Emergency Call to the ICAP Provider must take reasonable steps to detect such events and correct any associated configuration defects in a timely manner.
- Where it is impractical or not technically feasible to provide a Calling Party Number in accordance
 with the above (for example: Mobile phone without active SIM), a suitable workaround must be
 agreed between the VSP and the ICAP Provider and implemented in a timely manner.
- Notwithstanding, the obligations in this Clause, any Emergency Calls provided to the ICAP Provider
 with a non-compliant Calling Party <u>must not</u> be deliberately prevented from reaching the relevant
 Emergency Services Call Taker.
- In the case of a non-registered (U)SIM Emergency Call from a mobile, the VSP will be unable to
 identify the caller's number. The VSP should use reasonable efforts to insert a non-dialable Calling
 Party Number to uniquely identify the caller, in accordance with the standard agreed with ICAP
 provider and emergency services.

The following shows an example of how to deal with 111 calls from unregistered mobile phones. It is not intended to form an obligation on how to implement this.

SPARK POLICY FOR WHAT CLI TO USE FOR 111 CALLS FROM UNREGISTERED MOBILE PHONES

On the Spark network we have based our implementation on section 6.4.3 of 3GPP TS 23.271.

In case of a SIM-less emergency call, or in case of a non-registered (U)SIM emergency call, a non-dialable callback number shall be used to identify the target UE. The format and structure of the non-dialable callback number is according to national or regional regulations. The non-dialable callback number in North America shall, according to J-STD-036 [32], be the digits 911 + the last 7 digits of IMEI expressed in decimal numbers.

NOTE: The use of non-dialable callback numbers in other parts of the world is for further study. The non-dialable callback number should adopt random numbering, if not otherwise unique.

The only difference is we use +64911+the last 7 digits of the IMEI

This has several benefits:

- 1. Easier caller identification as the number is (largely) unique and can be referred back to the serving MNO for investigation.
- ICAP and ESAP staff can identify that it is a device making an unregistered emergency call and follow a SOP if required to identify the actual caller.
- 3. Nuisance calls can be blocked at ICAP
- 4. Potentially compatible with ECLI
- 5. Follows guidelines in 3GPP (i.e. if vendors supply the North American market they should be able to handle this)

We have implemented this in VoLTE via a SMM on our SBGs. The SMM logic similar to the pseudo code below

```
IF SIP:priority exisits THEN
      IF <u>SIP:priority</u> == \"emergency\" THEN
                                                                                IF <u>SIP:from.sip uri.user</u> ~= '(A|a)nonymous' THEN
                                                                                                                         IF <u>SIP:contact;+sip.instance</u> ~= '\\<urn:gsma:imei:([0-9]{7})([0-9])-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9]{6})-([0-9](
9])\\>' THEN
                                                                                                                                                                    <u>SIP:from.sip uri.user</u> = \"+64911\" + $2.2 + $2.3
                                                                                                                                                                    SIP:from.sip uri.host = \"spark.co.nz\"\n
                                                                                                                                                                     SIP:P-Asserted-Identity = \langle sip:+64911 \rangle + 2.2 + 2.3 + \@spark.co.nz \rangle
                                                                                                                          ELSE
                                                                                                                                                                    <u>SIP:from.sip_uri.user</u> = \"+649111234567\"
                                                                                                                                                                    SIP:from.sip uri.host = \"spark.co.nz\"\n
                                                                                                                                                                     SIP:P-Asserted-Identity = \sip:+649111234567\@spark.co.nz\"
                                                                                                                           END IF
                                                                                  END IF
                                       END IF
END IF
```

AUGUST 2021 Spark

Schedule 5: Template Emergency Services Calling Mobile arrangements

Introduction

This schedule is for the information only of mobile network operators.

It sets out a suggested template arrangement for emergency services calling roaming – where technically possible – when customers are unable to use the host network.



111 call roaming scenarios

The information in the table below is intended to be a reference for consumer awareness so that users can be advised, as appropriate, of the circumstances when an emergency call will not proceed, recognising that automatic roaming for emergency calls is not universally available for all locations, times, networks, handsets, and emergency numbers dialled.

Question	2degrees	Spark	Vodafone
What are the main scenarios in which automatic roaming for emergency calls is generally activated? For example, when the handset is outside the coverage of its home network or when the home network has a system failure.	It is entirely handset driven, based on loss of home network RF coverage. That is the only condition, and this coverage loss may be caused by the user leaving the coverage area or by the network failing to broadcast. Issues within the network such as faults preventing any calls from being made, will not trigger this roaming to happen as long as RF coverage is still available.	Emergency call roaming will occur when: • The caller dials a number that the handset recognises as an emergency call, and • The handset cannot attach to the "home" network provider. Emergency roaming relies on: • The handset not being able to attach to the home network. Therefore, under rare network failure scenarios where the device is attached to a network, but calls can't be made, emergency roaming will not occur. • There being an alternative network available to connect to. For example, there is no alternative network. The Spark network will accept emergency calls presented from other network customers.	Emergency call roaming onto Vodafone will occur when: The caller dials a number that the handset recognises as an emergency call, and The handset cannot attach to the "home" network provider, and The handset is in coverage of Vodafone Radio network. Emergency roaming relies on: The handset not being able to attach to the home network. Therefore, under rare network failure scenarios where the device is attached to a network, but calls can't be made, emergency roaming will not occur. There being an alternative network available to connect to. The Vodafone network will accept emergency calls presented from all other network customers

Question	2degrees	Spark	Vodafone
What are the known	See above. Also, being handset driven	Emergency roaming is largely	Emergency roaming is largely controlled
conditions in which	there could be scenarios when the UE	controlled by the handset and won't	by the handset and won't occur where
emergency calls from a	might not choose to camp on another	occur where the handset:	the handset:
mobile handset device will	network e.g. if user has manually	Does not have a SIM in it.	Does not have a SIM in it.
not automatically roam to	selected their home network rather	Does not recognise 111 as an	• Does not recognise 111 as an
another mobile network?	than just relying on automatic network	emergency call because, for example,	emergency call because, for example,
	selection. There may be specifications	the handset is configured for an	the handset is configured for an
This could be because of the	that govern how the UE should behave	overseas market. An Australian	overseas market. An Australian handset
way the handset device	in these types of scenarios but I am not	handset my not recognise 111 as an	my not recognise 111 as an emergency
"locks on" to its home	familiar with the details. Obviously the	emergency call for which roaming is	call for which roaming is possible.
network, the technical	UE also needs to support the 'roaming'	possible.	• Uses incompatible bands (or
compatibility with spectrum	networks' broadcast frequencies in that	Uses incompatible bands (or	frequencies) to those supported by
bands, or other reasons.	location, and for a 4G only (& VoLTE	frequencies) to those supported by	other networks.
	enabled) location the UE would need to	other networks.	Manually selected their home network
	support VoLTE to be able to make an	Is a VoLTE handset connected to a	only
	emergency call.	small number of RCG with no	
		underlying 3G coverage.	Note: Vodafone Handsets that have
			selected 2G only, will not be able to
		Spark sourced/supplied handsets are	roam onto Spark and 2Degrees
		tested to ensure they support	network.
		emergency roaming.	

Schedule 6: Emergency services calls interconnect link test plan

Introduction

This schedule sets out the recommended test plan for interconnect links. Interconnect links are the links between the VSP and Spark's network.

Spark provides the 111 initial call answering service. VSPs intending to hand over 111 calls to Spark will need to enter into an Interconnection Agreement. Contact Spark Wholesale for more information on handovers.

Test plan

Part 1 is the testing of the 111 Service Protect (SP) routes- functionality, voice quality (subjective) and origination phone number.

Part A- Where there are small and infrequently used SP routes, mainly from the smaller exchanges in the network, there is a Monthly Test to ensure that when 111 is dialled the exchange will switch this call to the ICAP and display the correct origination telephone number.

No attempt is made to test large well utilised 111 SP routes between major nodes or the ICAP. The normal monitoring of these routes to detect failures is sufficient to identify failures.

Part B- When a new CellSite is being commissioned, a test call is made from the site to the 111 Emergency Service ICAP and confirmed that the correct originating number is displayed.

Part 2 is the testing of the failure scenarios.

It is normal practice to offer the 111 Emergency Service traffic to one or two nodes, Points of Interconnect (POI), under normal conditions. In the event that the "normal routing" is compromised, the traffic will be routed to other POIs.

This re-routing, if the normal routing is compromised may be:

- · Automatic; or
- Manual

Further the re-routing may be effected by-

- Manual intervention i.e., preceding a planned outage to move traffic to another node; or
- Automatic in the event of a failure of the VSP equipment or the ICAP providers POI.

It is proposed that there be a test schedule set-up between the VSP and the ICAP Provider to test the fail-over configuration of the 111 Emergency Service SP Routing.

It is further proposed that this testing should be completed at least 12 monthly or when there is configuration activity affecting the routing of this traffic or for other reasons as agreed between the parties.

- 1. The VSP should complete a paper audit to confirm the routing
- 2. Make a test call to confirm the normal routing (and speech quality and calling number presentation).
- 3. Activate the plan to push the 111 Emergency calls to an alternate route.
- 4. Make a test call to confirm the routing (and speech quality and calling number presentation).
- 5. Repeat steps 3 and 4 to confirm all the functionality of all routes.

In addition to the above testing, the paper audit should be confirmed with the ICAP Provider to ensure that the plan is consistent with the contingency plan for a node(s) failure prepared by them.

In cooperation with the ICAP Provider, the contingency should be activated at the ICAP Providers Point-of-Interconnect node to confirm that the actions taken cause the VSP's 111 Emergency Calls to be diverted in accordance with the VSPs plan.

The Test Plan Results and the routing should be signed off by both parties and each should hold a copy of this documentation for audit purposes.

END

Schedule 7: TESA database specification for the provision of customer information

Introduction

This sets out the ESP requirements for customer information.

While the TESA database specification is maintained by the Police. Where there has been a material change to the TESA database specification inclusion of those changes in this Manual will be approved by the TCF Board (as per the Manual change process).

VSPs are required to provide regular file updates to the Police ICT Department in accordance with the attached data specification and interface requirements. In summary a full extract of mobile customer data will need to be loaded initially with regular extracts containing updates and deletions provided on a daily basis. The data maintained in TESA should relate to active customer accounts.





END