

Attachment B to the Designated Multinetwork Determination (Decision [2026] NZCC XX)

Terms for Local and Mobile Number Portability in New Zealand

“LMNP TERMS”

TABLE OF CONTENTS

EXPLANATORY STATEMENT	4
THE KEY ATTRIBUTES OF THE IPMS	5
SERVICE PROVIDER/CARRIER ENVIRONMENT OPTIONS	6
EFFECT OF THE LMNP TERMS.....	7
PURPOSE	7
STATUS OF THE LMNP TERMS	7
ANTICIPATED BENEFITS TO INDUSTRY	7
SCOPE AND OBJECTIVES	7
SCOPE	7
OBJECTIVES.....	8
CONVENTIONS IN THE LMNP TERMS.....	9
INTERPRETATIONS.....	9
DEFINITIONS	10
BUSINESS RULES	15
GENERAL BUSINESS RULES	15
NUMBER MANAGEMENT	19
EQUIVALENT SERVICE.....	20
NEW ENTRANTS	20
ACCESS TO THE IPMS BY AN ENTITY NOT PARTY TO THE LMNP TERMS.....	21
SERVICE PROVIDER RESPONSIBILITIES.....	21
GENERAL SERVICE PROVIDER RESPONSIBILITIES	21
GSP RESPONSIBILITIES.....	23
LSP RESPONSIBILITIES.....	26
FAULT MANAGEMENT.....	27
TRANSFER OF PORTED NUMBER TO ANOTHER PERSON	27
RIGHT TO USE THE PORTED NUMBER REGISTER	27
CARRIER RESPONSIBILITIES.....	27
CARRIER RULES.....	27
MAINTAINING RECORDS OF PORTED NUMBERS	28
RFS DATE NOTICE PERIOD	28
PLANNED AND UNPLANNED OUTAGES.....	28
ADMINISTRATIVE ISSUES.....	32
CLARIFICATION AND RECONSIDERATION OF THE LMNP TERMS	32
DISPUTE RESOLUTION	32
EXITING THE IPMS	37
FAILURE TO MEET SERVICE LEVELS	38
EXEMPTIONS	42
SUBPART 2 OF PART 4A.....	43
PUBLICATION OF PORTING STATISTICS.....	43
PORTING PROCESSES	43
PORT REQUEST PROCESS	45
PORT ACTIVATION PROCESS	49
APPROVED PORT CHANGE	54
PORTED NUMBER RELINQUISHMENT PROCESS.....	58
PORT EXPIRY PROCESS	60
PORT WITHDRAWAL PROCESS	62
NUMBER QUARANTINE	63
IPMS CAPABILITIES.....	64
BASIC METHODOLOGIES	64

TECHNOLOGY SPECIFICATIONS	64
USERS AND SECURITY	67
ERROR HANDLING	68
REPORTING AND DATA EXTRACTS	68
ENQUIRY SCREENS.....	69
ARCHIVING	69
MIGRATION	69
DATA INTEGRITY/SYNCHRONISATION.....	69
APPENDIX: TABLES.....	70
TABLE 1: PORT REQUEST FIELDS	70
TABLE 2: SERVICE LEVELS	71
TABLE 3: RFS DATE MINIMUM AND MAXIMUM NOTICE PERIODS.....	73
TABLE 4: PORT REQUEST TESTS.....	74
TABLE 5: CHECKS PERFORMED BY THE LOSING SERVICE PROVIDER AT STEP PR5.....	75

Explanatory Statement

The Number Porting arrangements for Local Numbers and Mobile Numbers in New Zealand are provided for in the Commerce Commission's (the Commission) Determination pursuant to Decision [2026] NZCC XX, including:

- Terms for Local and Mobile Number Portability in New Zealand (LMNP Terms); and
- Network Terms for Local and Mobile Number Portability in New Zealand (Network Terms).

LMNP is governed by two sets of terms and conditions, the LMNP Terms and the Network Terms. Therefore, a party will have to comply with both the LMNP Terms and the Network Terms to deliver LMNP in compliance with the Commission's Determination.

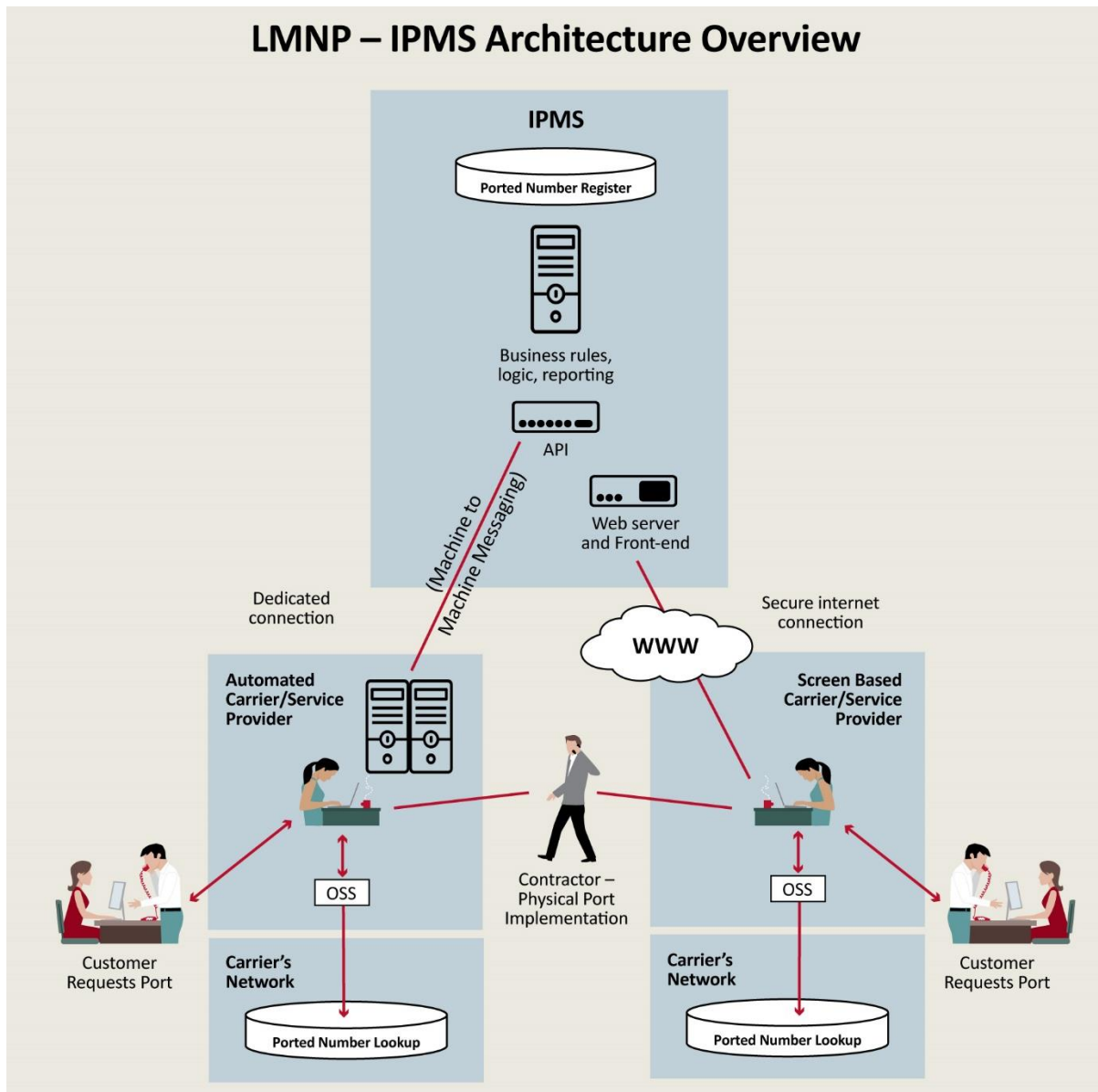
The LMNP Terms detail the processes that enable end-users to Port their Numbers and set out the rights and obligations of parties to these terms in a number portability environment. These processes are based around an Industry Portability Management System (IPMS) which facilitates number portability between Service Providers and Carriers but relies on Carriers to configure and update their Networks and support systems to ensure calls to and from Ported Numbers are correctly routed.

In a number portability environment, changes are required to the traditional way in which calls are routed from originating Carriers to terminating Carriers. For voice services, this applies to local, national, fixed-to-mobile, mobile-to-fixed, mobile-to-mobile, incoming and outgoing international and other calls involving Local or Mobile Numbers.

These LMNP Terms detail the processes that will enable Customers to Port their Local and Mobile Numbers. They set out the rights and obligations of participating Carriers in a Local and Mobile Number Portability (LMNP) environment.

The processes for portability in New Zealand will continue to be based around a centralised IPMS.

The role of the IPMS is to provide reliable message transport, process tracking, coordination, and management. It is a tool which facilitates LMNP but relies on the Networks being able to support portability. The IPMS does not handle call routing but is the sole authority on all Ported Numbers. This is used by Carriers to update their own Networks to ensure calls to Ported Numbers are correctly routed.



All the participants in LMNP need to communicate their requests and responses via the IPMS.

The Key Attributes of the IPMS

- A Ported Number database containing the Ported Number Register;
- A Number Portability Management System, containing the business rules, logic and systems for managing Port Requests;
- An applications programming interface (API) for a consistent transactional interface with Carriers and Service Providers to the IPMS;
- A web server providing HTTP service interface for browser-based sessions using the same rules and capabilities that the API uses; and
- Management applications, reporting, logging, and security reports.

Access may be either via a dedicated leased line or secure internet connection.

Service Provider/Carrier Environment Options

Access to the IPMS will be flexible and will allow parties to select the approach that best suits them:

- Screen based: parties may choose to access IPMS via simple Screen GUIs;
- Automated: transactions could be responded to automatically via a machine-to-machine interface. Transactions will be presented to a user within internal systems if the response cannot be dealt with automatically; or
- Hybrid: parties could use a combination of both screen based and automated processes, selecting the most appropriate option. IPMS has the ability to send certain alerts and updates to parties that lack full automation.

Further details are contained in the body of these LMNP Terms.

For more information, please contact the administrator on: info@tcf.org.nz.

Effect of the LMNP Terms

Purpose

1. The purpose of these LMNP Terms is to provide for the business requirements for Local and Mobile Number Portability (LMNP).

Status of the LMNP Terms

2. These LMNP Terms are determined under the Telecommunications Act 2001 (Act), for the implementation of the processes that will allow the ongoing management of LMNP. The LMNP Terms apply to all parties to the Determination who are access seekers or access providers in relation to either of the designated multinet network services local telephone number portability service or cellular telephone number portability service, and any person who becomes an access provider subsequent to the Determination being made.

Anticipated Benefits to Industry

3. The purpose of these LMNP Terms is to provide benefits to the industry and end-users of telecommunications services in New Zealand, including by:
 - 3.1 Standardising industry practices in relation to LMNP, and providing certainty in their operation as well as cost effectiveness and efficiency;
 - 3.2 Minimising industry costs of compliance to implement and maintain the IPMS;
 - 3.3 Ensuring that all Carriers can meet their call routing responsibilities so that calls to Customers with Ported Numbers are routed successfully;
 - 3.4 Ensuring service to the Customer is maintained by specifying Service Levels; and
 - 3.5 Ensuring the efficient and effective inter-Service Provider and inter-Carrier operational arrangements using the IPMS.

Scope and Objectives

Scope

4. The LMNP Terms set out operational procedures and processes, between Service Providers and Carriers, for the implementation and ongoing management of Porting Processes.
5. It is expected that there will be a continuing relationship between a given Service Provider and its Carriers. This relationship shall enable the parties to meet the requirements of the LMNP Terms. These LMNP Terms do not define all the details of this relationship. Service Providers and the Carriers, on whose Network they are providing services, may agree procedures for those transactions that take place between them, consistent with the procedures detailed in the LMNP Terms. Procedures provided in the LMNP Terms must be supported.

6. The LMNP Terms are binding on all parties to the Determination, in accordance with the Act, including any person who becomes an access provider subsequent to the Determination being made.
7. All Service Providers and Carriers must provide LMNP in accordance with these LMNP Terms and any relevant legislation or determinations of regulatory bodies except to the extent that an exemption has been granted to a Carrier under the Network Terms. If such an exemption has been granted under the Network Terms, the relevant Carrier will be exempted from particular provisions in these LMNP Terms in relation to the specific period and purposes, Customers or classes of Customers, or conditions for which the relaxation has been granted under the Network Terms.
8. In the event of any inconsistency between these LMNP Terms and any legislation or determinations of regulatory bodies, then such legislation or determinations will prevail, to the extent of the inconsistency. For the avoidance of doubt, nothing in this Determination ousts the jurisdiction of the Commission to enforce the Determination in accordance with Subpart 2 of Part 4A of the Act.
9. The Service Levels in these LMNP Terms will be the default minimum industry standard and can be improved by bilateral arrangements provided that those bilateral arrangements do not impact on the ability of other participants to interwork with parties to those arrangements in accordance with the minimum Service Levels. The timeframes and notice periods set out in these LMNP Terms, including in the Appendix, Tables 2 and 3, are minimum standards and do not prevent parties from performing more quickly or adopting more demanding operational arrangements, provided the requirements of these LMNP Terms continue to be met.
10. The functionality of the IPMS will allow for the following scenarios:

	Change in Carrier	No Change in Carrier
Change in Service Provider	Yes	Yes
No Change in Service Provider	Yes	X

11. These LMNP Terms apply specifically to enable LMNP. Clarification or reconsideration of these LMNP Terms by the Commission may be sought in accordance with the Act.
12. Nothing in these LMNP Terms shall prevent any party, or the Commission, from enforcing these LMNP Terms in accordance with Subpart 2 of Part 4A of the Act.

Objectives

13. The objectives of the LMNP Terms are to:

- 13.1 Set out procedures between Service Providers to enable a Customer to retain their Number when transferring from one Service Provider to another, notwithstanding that the relevant Number range containing the Number will continue to be held by the Donor Carrier;
- 13.2 Allow a Customer to relocate premises coincident with, or after the Porting of their Local Number, provided the premises remain in the same Donor Carrier Local Calling Area;
- 13.3 Set out competitively neutral and non-discriminatory processes for the implementation and operation of LMNP;
- 13.4 Set out competitively neutral processes by which Service Providers may exchange relevant information with each other to support the Porting Processes;
- 13.5 Set out procedures that will ensure a minimum break in or loss of service during a Port;
- 13.6 Set out criteria against which the compliance of Service Providers and Carriers with the LMNP Terms may be measured; and
- 13.7 Provide a robust process that can support LMNP in a timely fashion.

Conventions in the LMNP Terms

Interpretations

- 14. In the LMNP Terms:
 - 14.1 Sections, clauses, paragraphs, and other headings are for ease of reference only and will be ignored in constructing the LMNP Terms;
 - 14.2 Unless the context otherwise requires, references to sections, clauses, paragraphs, and appendices are references to sections and clauses of, and appendices to the LMNP Terms;
 - 14.3 Any reference in the LMNP Terms to a statute, statutory instrument, regulation or order will be construed as a reference to such statute, statutory instrument, regulation or order as amended or re-enacted from time to time;
 - 14.4 Any reference to a “party” is to a party to the Determination (unless specifically provided to the contrary) and will be deemed to include its successors and permitted assigns and includes any person who becomes an access provider subsequent to the Determination being made;
 - 14.5 A reference to a “person” includes an individual, firm, company, corporation, unincorporated body of persons, state or government or agency thereof, and any other body or entity (in each case whether or not having separate legal personality);

- 14.6 Any reference in the LMNP Terms to any gender includes all genders and a reference to the singular includes the plural and vice versa;
- 14.7 If a period of time is specified and dates from a given day or the day of an act or event, it is to be calculated exclusive of that day; and
- 14.8 A reference to a day is to be interpreted as the period of time commencing at midnight and ending 24 hours later.

Definitions

15. In the LMNP Terms, unless the context requires otherwise:

Term	Definition
Account Number	Means the unique reference number used by a Service Provider for a given Customer, which should appear on invoices.
Act	Means the Telecommunications Act 2001.
Approved Port	Means a Port that has been approved in accordance with the Port Request Process.
Approved Port Change or APC	Means the process set out in paragraph 262.
Audit IPMS Client	Means a Service Provider or Carrier whose compliance with a Service Level set out in these LMNP Terms is being audited by the Enforcement Agency under the Audit by the Enforcement Agency section of the Network Terms.
Bilateral Agreement	Means an agreement between a party who is obliged to comply with the LMNP Terms and another party (who might or might not also be a party to the LMNP Terms), relating in full or in part to Porting.
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 Local Services or Mobile Services provided to that Customer.
Business Day	Means “working day” as defined in section 5 of the Act but includes Saturdays and the days set out in paragraph (b) of the definition of “working day” in section 5 of the Act.
Carrier	Means an entity that operates a public switched telephone network (or a functionally equivalent system) that originates, transits or terminates calls. The same person may be both a Carrier and a Service Provider. If a party to the LMNP Terms has more than one Network, it can be classified as more than one Carrier.
Change Requester	Means the person who requests an Approved Port Change and, for the avoidance of doubt, may be the Gaining Carrier, Gaining Service Provider or Losing Carrier.
Commission	Means the Commerce Commission.
Complex Dispute	Has the meaning set out in paragraph 112.2.

Term	Definition
Complex Port	Means a Port which involves a group of Local Numbers or a group of Mobile Numbers for a Customer, which the GSP and LSP agree are to be treated as a Complex Port.
Contractor	Means a third-party that performs on-site work on behalf of a Carrier.
Co-operative Period	Means the period of time beginning when an LSP queries a Port Request or Approved Port Change with a GSP, or vice versa, and ending on the earlier of resumption of the Porting Process or the expiry of the RFS Date of the Port Request or Approved Port Change (as the case may be), during which the parties will liaise directly to identify and endeavour in good faith to resolve any problems. The parties shall co-operate to facilitate Porting for the Customer.
Costs Allocation Issue	Means any disagreement or dispute between the parties which relates to the quantification of industry common system costs or per-line set-up costs for the purpose of allocation in accordance with the Commission's Determination in Decision [2026] NZCC XX.
Customer	Means a person who has a bona fide Billing Relationship with a Service Provider in respect of a Local Service or Mobile Service.
Customer Authorisation	Means a valid authorisation by the Customer or the Customer's duly appointed agent to Port the Number assigned to that Customer.
Customer Request	Means a request from a Customer to a GSP to Port a Number.
Departing Party	Has the meaning set out in paragraph 135.
Determination	Means the Commission's Determination pursuant to Decision [2026] NZCC XX.
Donor Carrier or DC	Means the Carrier that has been allocated the Number by the NAD, or that is recognised by the NAD as having been allocated the Number.
Enforcement Agency	Means the person nominated by the TCF and approved by the Commission or, if the TCF fails to nominate a person, a person appointed by the Commission, whose role is to monitor and enforce compliance with the Service Levels. The nominated person may perform the audits referred to in the LMNP Terms itself, or appoint an independent expert to conduct the audit on its behalf. Until such time as a person is appointed in accordance with the above, the Enforcement Agency shall be the last appointed Enforcement Agency under [2016] NZCC 32.
Event	Means an instance of one of the agreed set of processes that can arise from a specific Customer action, for which a specific Process exists.

Term	Definition
Fraud and Security Protection Requirements	Means the requirements set out in paragraphs 23 and 24.
Gaining Carrier or GC	Means the Carrier that will become the Host Carrier, after the completion of a Port.
Gaining Service Provider or GSP	Means the Service Provider to which the Number is moving, or has already moved, in a Port.
Host Carrier	Means the Carrier on whose Network the Ported Number is connected.
Industry Portability Management System or IPMS	Means the software, hardware and other shared facilities used to give effect to the LMNP Terms.
Initiator	Has the meaning set out in paragraph 117.
IPMS Based Reseller	Means a Service Provider that is not a party to this Determination but has been granted access to IPMS and is directly involved in the porting of Local Numbers and Mobile Numbers.
IPMS User Guide	Means the user guide for the IPMS prepared by the vendor responsible for developing the IPMS, as amended from time to time by the vendor responsible for IPMS application maintenance and support.
LMNP Terms	Means these Terms for Local and Mobile Number Portability in New Zealand, including all Appendices hereto, as determined by the Commission.
Local and Mobile Number Portability or LMNP	Means Local Number Portability and Mobile Number Portability.
Local Calling Area	Means that geographic area defined by the Donor Carrier within which Customers of the Donor Carrier have access to a Local Service.
Local Number	Means an 8-digit number, in the form: area code + NXXXXXX where area code equals 3,4,6,7 or 9 and "N" equals digits 2 to 9 (excluding 50AB).
Local Number Portability or LNP	Means the local telephone number portability service, as defined in the Act.
Local Service	Means the service associated with a Local Number.
Losing Carrier or LC	Means the Carrier that is the Host Carrier prior to the completion of the Port.
Losing Service Provider or LSP	Means the Service Provider that is losing the Number in a given Port Event.
Mediation Period	Has the meaning set out in paragraph 123.
Message	Means an identifiable step in the Porting Process. It is a defined communication between Service Providers or between Carriers. Examples of Messages include completion advice in relation to a Port Activation, or a rejection of a Port Request.

Term	Definition
Mobile Number	Means a number in the form 02N + XXXXXX[XX] where “N” equals 0,1, 2,5,7,8 or 9 and other cellular numbers allocated by the NAD, or recognised by the NAD as having been allocated.
Mobile Number Portability or MNP	Means the cellular telephone number portability service, as defined in the Act.
Mobile Service	Means the service associated with a Mobile Number.
Multiple Number Port	Means a Port of more than one Number, of the same type, for the same Customer and the same RFS Date, under the same SOM.
Negotiation Period	Has the meaning set out in paragraph 120.
Network	Means a system comprising telecommunication links to permit telecommunication.
Network Terms	Means the Network Terms for Local and Mobile Number Portability in New Zealand determined by the Commission.
Number	Means a Local Number, a Mobile Number or both, as the case requires.
Number Block	Means a contiguous set of individual Numbers that are managed as a single entity. Number Blocks will typically exist for multi-line Customer configurations such as PBX, DDI, and centrex implementations. Where the LMNP Terms refer to a Number Block, it could be referring to a contiguous block of centrex or DDI numbers.
Numbering Administration Deed or NAD	Means the organisation established under the Numbering Administration Deed dated 20 December 1998, or any such successor organisation or agreement that may be formed.
Off-IPMS Reseller	Means a Service Provider that is not a party to the Determination, does not have access to IPMS and cannot port Local Numbers directly.
Operational and Support Manual for LMNP	Means a multilateral agreement between Carriers that covers operational issues that are not dealt with by the LMNP Terms or Network Terms.
Originating Carrier	Means the Carrier on whose Network a call originates.
Other Carrier	Means a Carrier that is a party to the LMNP Terms, but is not involved in a given Port Event as a Gaining Carrier, Losing Carrier, or Donor Carrier.
Planned Outage	Has the meaning set out in paragraph 102.
Port Activation or PA	Means the process set out in paragraph 219.
Port Expiry Process or PE	Means the process set out in paragraph 307.
Port or Porting	Means a process which achieves LMNP.
Port Request or PR	Means a request for a Port pursuant to paragraph 178 and including the data required as per the Appendix, Table 1.
Port Withdrawal or PW	Means the process set out in paragraph 323.

Term	Definition
Ported Number	Means a Number that is currently hosted by any Carrier other than the Donor Carrier.
Ported Number Register or Register	Means a file maintained by the IPMS, which contains a list of the Numbers that have been Ported. Access to this Register is required for all participating Carriers.
Ported Number Relinquishment Process	Means the process set out in paragraph 287.
Porting Process	Means the processes described from paragraph 170.
Privacy Act	Means the Privacy Act 2020.
Privacy Code	Means the Telecommunications Information Privacy Code 2020.
Public Holiday	Means a nationwide public holiday.
Ready for Service Date or RFS Date	Means the intended date and the time window for the Port Activation.
Relevant Party	Has the meaning set out in paragraph 119.
Service Levels	Means the Fraud and Security Protection Requirements and the Service Levels set out in the Appendix, Table 2.
Service Order Management Number or SOM Number	Means a unique reference to a given single Port or Multiple Number Port.
Service Provider or SP	Means any person providing a Local Service or Mobile Service to a Customer and who has the Billing Relationship with the Customer for that service. The same person may be both a Carrier and a Service Provider.
Simple Port	Means a Port involving one or more Local Numbers or Mobile Numbers for a Customer which the gaining and losing parties agree is to be treated as a simple Port.
Standard Hours of Operation	Means 8.00am to 6.00pm on Business Days.
TCF	Means the New Zealand Telecommunications Forum Incorporated.
Technical Dispute	Has the meaning set out in paragraph 112.1.
Unplanned Outage	Means an outage in the Carrier's System that may affect LMNP that is not a Planned Outage.
Working Days	As defined in section 5 of the Act.
Working Hours	Means elapsed hours during the Standard Hours of Operation.
Working Minutes	Means the elapsed minutes during the Standard Hours of Operation.

Business Rules

General Business Rules

Prior Notice

16. The GSP is not required to give any prior notice of a Port outside of the processes described in the LMNP Terms. This does not prevent consultation between the parties for coordinating Ports.

Non-discrimination

17. In implementing and operating the LMNP Terms, all parties must act in a competitively neutral and non-discriminatory manner and must facilitate Porting by acting in compliance with principles and processes that are consistent with section 18 of the Act.

Compliance with Service Levels

18. Each party subject to the LMNP Terms must comply with the Service Levels. If a party fails to meet the Service Levels, the provisions set out from the Failure to meet Service Levels section to the Publication of Porting Statistics section will apply. Despite these sections, a party to the Determination, or the Commission, may enforce the Determination in accordance with Subpart 2 of Part 4A of the Act.

Privacy and Use of Information

19. Information relating to Porting Processes will be kept confidential at all times by the parties to the LMNP Terms except as set out in the Privacy and Use of Information section.
20. Information provided in Porting Processes can only be used for Porting, the routing of calls or in association with the delivery of telecommunications services, for Customer and network fault management, for fraud and security protection as set out in paragraphs 23 and 24, and complaint handling. Information provided in Porting Processes must not be used for any other purposes (including winback and marketing purposes).
21. A Service Provider or Carrier, which receives any type of information relating to the Porting of a Number may only use such information in accordance with the Privacy Act 2020, the Telecommunications Information Privacy Code 2020, and the LMNP Terms.
22. If there is any inconsistency between the LMNP Terms, the Privacy Act 2020, and the Telecommunications Information Privacy Code 2020, the Privacy Act and the Telecommunications Information Privacy Code prevail.

Fraud and Security protection

23. In implementing and operating the LMNP Terms, all parties to the LMNP Terms must ensure that they have appropriate policies and processes to mitigate security risks

and prevent fraud during Porting, and that such policies and processes are consistent with the Operational and Support Manual for LMNP.

- 23.1 The Commission acknowledges that fraud, scams and unauthorised porting activity continue to evolve and may require industry participants to implement new or enhanced preventative measures.
- 23.2 Nothing in these LMNP Terms shall prevent Service Providers, Carriers, or the industry collectively from developing, implementing and maintaining reasonable measures, processes, controls and system functionality designed to prevent, detect, investigate, respond to or mitigate such activity, where such measures are undertaken for the protection of Customers or the integrity of the LMNP service.
- 23.3 Such measures may be implemented by Service Providers, Carriers, through the IPMS, or through industry operational procedures agreed from time to time, and may include amendments to the Operational and Support Manual for LMNP and enhancements to IPMS functionality where reasonably required to address emerging fraud and scam risks.
- 23.4 Where a Service Provider or Carrier has reasonable grounds to believe that a Port Request for a number is, or is likely to be, associated with fraud, a scam or unauthorised Porting activity, an industry measure implemented under this clause may provide for the Porting of that Number to be temporarily suspended or otherwise prevented for the minimum period reasonably necessary to verify the Port Request, protect the affected Customer or investigate the suspected activity.
- 23.5 A Service Provider or Carrier relying on paragraph 23.4 must commence verification promptly and review the suspension at intervals appropriate to the circumstances. The suspension must end as soon as the grounds for it no longer exist. Any suspension continuing beyond two Business Days must be escalated to an appropriately authorised person for review and approval, and must be reviewed at least once each Business Day thereafter.
- 23.6 The Service Provider or Carrier must keep a contemporaneous record of the grounds for the measure, the information relied on, the time it began and ended, each review and decision to continue it, any steps taken to verify the Port Request or protect the Customer, when the Customer was notified, and the outcome. The record must be retained for 12 months and provided to the Commission or Enforcement Agency on request.
- 23.7 The affected Customer must be notified as soon as reasonably practicable that the Port has been temporarily suspended and given information about the steps available to verify or progress the Port, unless and for so long as notice would be likely to prejudice fraud prevention, the protection of the Customer, or an investigation. Where notice is deferred, the reasons must be recorded and notice must be given once that risk no longer applies."

- 23.8 Each Service Provider and Carrier must provide the Commission, within one month after 30 June and 31 December each year, with aggregated information on the number of temporary suspensions under paragraph 23.4, their duration and outcomes, including the number continuing beyond two Business Days, together with any further information the Commission reasonably requests. The reporting must not include Customer-identifying information unless requested by the Commission under applicable law.
- 23.9 Any measures implemented under this clause must be reasonable, proportionate, non-discriminatory, and consistent with applicable law and the Determination. A temporary suspension or prevention of Porting undertaken in accordance with paragraph 23.4 will not, of itself, constitute a failure to comply with any Porting Process or Service Level under these LMNP Terms.
24. Two-factor authentication (2FA) is the default customer authentication method for Mobile Ports. A Gaining Service Provider must not proceed without 2FA unless an exception permitted under the Operational and Support Manual applies, or the Gaining Service Provider has a reasonable and documented basis for determining that 2FA was not required.

Subject to New Zealand Law

25. Parties to the LMNP Terms must comply with the laws of New Zealand (including any statute, subordinated legislation or decision of any court or regulatory body). In the event of any conflict or inconsistency, the laws of New Zealand prevail.

Good Faith

26. All parties will act co-operatively and in good faith to facilitate Porting Processes.

Bilateral and other agreements

27. Parties to the LMNP Terms may agree terms and conditions, in their Bilateral Agreements, for the provision of all appropriate and relevant services and service information that is required to facilitate and support the Porting Processes in an efficient and expeditious manner.
28. Parties to the LMNP Terms must ensure that any (subsequent) Bilateral Agreements are consistent with the LMNP Terms. Bilateral Agreements shall not reduce the minimum level of service prescribed in the LMNP Terms, but they can improve upon them.
29. Carriers may enter into Bilateral Agreements for higher Service Levels for standards and practices than those set out in the LMNP Terms, in which case the Bilateral Agreement will prevail over the LMNP Terms with respect to the relevant Service Level for standards and practices, to the extent of the inconsistency. In all other circumstances, if there is a conflict between the LMNP Terms and a Bilateral Agreement, the LMNP Terms shall prevail over the Bilateral Agreement to the extent of the inconsistency.

30. For the avoidance of doubt, Carriers may set out more detailed standards and practices in their Bilateral Agreements than are outlined in the LMNP Terms, provided that the more detailed standards and practices are consistent with, or provide for higher Service Levels than the standards and practices set out in the LMNP Terms.
31. All Carriers that are bound by the LMNP Terms must comply with the provisions of the Operational and Support Manual for LMNP, dealing with the operational issues not included in the LMNP Terms, which is to be agreed by the Carriers. In addition to the matters set out in paragraph 22 of the Network Terms, the Operational and Support Manual for LMNP must include:
 - 31.1 appropriate fraud prevention and security procedures;
 - 31.2 provided that if the Operational and Support Manual for LMNP contains anything inconsistent with these LMNP Terms or the Network Terms, then, to the extent of the inconsistency, the LMNP Terms or Network Terms, as the case may be, shall prevail.

Local Calling Area Requirements

32. The premises of a Customer with a Ported Local Number must be within the Donor Carrier's relevant Local Calling Area. A Customer with a Ported Local Number wishing to move premises can retain that Local Number provided that the new premises are within the same Donor Carrier's Local Calling Area. For the avoidance of doubt, the Gaining Carrier is under no obligation to transfer the Customer's Ported Local Number to the Customer's new premises.
33. The GSP is responsible for determining if a Ported Number can be allocated to new premises. The Donor Carrier will provide this information on request in a timely manner.

Message Timing

34. Messages sent outside Standard Hours of Operation are deemed to have been sent at 8.00am on the next Business Day.

After Hours Porting

35. Customers wishing to Port Numbers may require those Numbers to be Ported at a time convenient to the requirements of the Customers, including any time outside Standard Hours of Operation. The LMNP Terms do not impose an obligation on a Service Provider or Carrier to process, or continue to process to completion, a Port outside the Standard Hours of Operation. Arrangements for processing and completing Ports outside the Standard Hours of Operation may be the subject of Bilateral Agreement.

Multiple Porting of Numbers

36. A Customer must be able to Port their Number more than once to different Carriers. That is, an initial Port from the Donor Carrier to a new Host Carrier may be followed

at later dates by subsequent Ports from that Host Carrier to other Host Carriers, including the original Donor Carrier.

Change of Directory Number

37. Porting shall not require Customers to change their directory number, nor have to know, nor use any Number other than their directory number.

IoT and Data-only Mobile Services

38. For the avoidance of doubt, these LMNP Terms apply only to numbers used to provide the cellular telephone number portability service described in Schedule 1 of the Act. Accordingly, they do not apply to a mobile number used solely for an IoT or data-only service where voice services are not supported and are not reasonably expected to be supported, where that service falls outside the scope of the cellular telephone number portability service described in Schedule 1 of the Act.
39. Nothing in paragraph 38 prevents the voluntary transfer of such a number where the Customer can identify the relevant number, the number complies with the numbering plan, and the relevant Carrier supports the transfer. Any such transfer is outside the mandatory Porting obligations in these LMNP Terms only because the service is outside the Schedule 1 service description, not because paragraph 38 creates an exception to that service.

Number Management

40. No ownership rights, title, or interest in any Number or numbering scheme will be conferred upon a Carrier, Service Provider, or Customer by the LMNP Terms or by any Porting Process pursuant to the LMNP Terms.
41. Each Number shall only have a single Service Provider and Host Carrier associated with it at any given point in time.
42. Each Number shall only have a single Donor Carrier associated with it. The Donor Carrier does not change as a result of any of the Porting Processes pursuant to the LMNP Terms.
43. Service Providers and Carriers are required to ensure the continuing integrity of Number Blocks associated with a Porting Process, and:
 - 43.1 Number Blocks may from time to time contain unused or inactive Numbers, these Numbers are considered to be part of the Port, and hence all Numbers within a Number Block may be Ported;
 - 43.2 Unused or inactive Numbers within a Number Block may not be allocated or used for any purpose for any Customer other than the Customer who has the other Numbers within that Number Block;
 - 43.3 Unless the Billing Relationship has ceased, to keep the Number Block intact Numbers within a Ported Number Block that are relinquished do not need to

be relinquished under the prescribed Ported Number Relinquishment Process; and

- 43.4 Where a Port Request includes Number Blocks, the Port Request may include relinquishment information for Numbers that are specifically not required to be Ported.

Equivalent Service

44. To the extent that the IPMS contains Service Levels performance data, and data on the status and timings of Porting Processes, these may be relevant to investigations into Equivalent Service (as that term is defined in the Network Terms).

New Entrants

45. Each new party to the Determination must use its best endeavours to Port Local Numbers as soon as possible after the date that the Commission confirms that it qualifies as a new party to the Determination, having been satisfied that the new party and at least one existing party have successfully interconnected (the “Qualifying Date”). Each new party to the Determination must ensure that Customers are able to Port Local Numbers no later than three months after the Qualifying Date, (the “Implementation Period”).
46. Where a new party to the Determination is unable to Port Local Numbers on or before the expiry of the Implementation Period, it must apply to the Commission for an extension of time.
47. Each new party to the Determination must use its best endeavours to Port Mobile Numbers as soon as possible after the date that the Commission confirms that it qualifies as a new party to the Determination, having been satisfied that the new party and at least one existing party have successfully interconnected (the “Qualifying Date”). Each new party to the Determination must ensure that Customers are able to Port Mobile Numbers no later than three months after the Qualifying Date, (the “Implementation Period”).
48. Where a new party to the Determination is unable to Port Mobile Numbers on or before the expiry of the Implementation Period, it must apply to the Commission for an extension of time.
49. Once a new party has been issued a Number range by the NAD and operates a PSTN they are a party to the Determination and are liable for costs under this Determination.
50. Unless it is aware of anything to the contrary the Commission will accept that a party has met the above criteria when it receives written notification from the NAD that the party has been allocated a Number range and confirmation that notification has also been sent to the new party.
51. Each new party to the Determination must use its best endeavours to Port Local and/or Mobile Numbers as soon as possible after the date the new party and at least

one existing party have successfully interconnected (the “Qualifying Date”). Each new party to the Determination must ensure that Customers are able to Port Local and/or Mobile Numbers no later than three months after the Qualifying Date.

52. All parties to the Determination will act co-operatively and in good faith to facilitate new parties to the Determination gaining access to Local Number Portability and Mobile Number Portability.

Access to the IPMS by an Entity Not Party to the LMNP Terms

53. Government agencies (including without limitation emergency services such as the Police and Fire Service) and third parties will be entitled to access the IPMS for information purposes only in the conduct of their lawful operations. The terms on which these parties will be granted access will be specified by the TCF and set out in an IPMS access agreement between the TCF and the party seeking access.
54. Parties to these LMNP Terms recognise that Service Providers who are not in IPMS can create difficulties in the porting process as neither they, nor their Carrier, can be readily identified by IPMS. This can hinder the ability to lodge a Port Request. Parties to these LMNP Terms must use reasonable endeavours to ensure that any Off-IPMS Reseller which resells services from its network, either:
 - 54.1 Becomes an IPMS Based Reseller in its own right; or
 - 54.2 Has a Service Provider ID created for it in IPMS (which may be administered by the party) to facilitate the porting of numbers.
55. For the avoidance of doubt, the reasonable endeavours standard in paragraph 54 applies only to the steps taken to involve the Off-IPMS Reseller in the porting process under paragraphs 54.1 and 54.2. It does not qualify, limit, or excuse the party’s obligation to comply with any Porting Process or Service Level under these LMNP Terms.

Service Provider Responsibilities

General Service Provider Responsibilities

56. Once the Port Activation Process commences, the GSP will be considered the primary Service Provider. It is the GSP’s responsibility to ensure the smooth transition of the Port for the Customer.

Right to Port

57. Service Providers shall only initiate a Port Request for a Number where the person requesting the Port has made a representation that they are the Customer for that Number, and that they have the authority to request the Port. Prior to submitting a Port Request for each Number, the GSP must obtain a valid Customer Authorisation from the Customer seeking to Port the Number.

Right to refuse to Port

58. GSPs have the right to accept or reject a Customer's request to Port to that GSP a Number that is assigned to the Customer.

Categorisation of Ports

59. The GSP must initially nominate a category to be used to Port a Number. These categories are:
- 59.1 Simple Local;
 - 59.2 Simple Mobile;
 - 59.3 Complex Local; or
 - 59.4 Complex Mobile.
60. If the LSP disagrees with the category of the Port nominated, it must be resolved between the GSP and the LSP during the Co-operative Period. If the GSP and LSP cannot resolve such disagreement before the expiry of the Co-operative Period, that Port shall be treated as a Complex Port.

RFS Date

61. The RFS Date notice period must comply with the minimum and maximum notice periods set out in the Appendix, Table 3. The RFS Date is determined by the GSP.

SOM Number to be used to Track Events

62. All Numbers associated with a GSP's Port Request for the Customer must be identified by a unique SOM Number covering all the Numbers being Ported from an LSP. Once a SOM Number is issued, all Messages for Porting Processes must include that SOM Number.

Port Request Content

63. A valid Port Request must include the information indicated as required information in the Appendix, Table 1.

Port Request Rejection

64. Where the details required to be supplied by the LSP are incomplete or incorrect or there is material doubt as to their completeness or correctness, and the issue cannot be resolved in accordance with the PR7. GSP Checks LSP Response section, the GSP is required to reject the Port Request.

Porting Delays

65. A Service Provider must advise all affected Service Providers as soon as practicable after becoming aware of any Porting delays, whether system or validation, that prevent processing of Porting Events in compliance with the Service Levels. Such advice does not relieve the Service Provider from its responsibility to meet the Service Levels or the consequences of any failure to do so.

66. Other delays such as Network failures or major outages shall be managed in accordance with the relevant provision contained in Bilateral Agreements between the parties.

Service Provider Responsibilities

67. The Service Provider is responsible for maintaining:
- 67.1 Appropriate records to satisfy the routing, billing, and audit requirements of the LMNP Terms; and
 - 67.2 An interface with the processes required for the Porting Process through which they can request Ports, respond to Port Requests, and carry out all other Porting Processes prescribed in the Porting Processes section.

GSP Responsibilities

Customer's Right to Information

68. The GSP must advise the Customer that:
- 68.1 Any changes to the Port Request may impact the Porting RFS Date;
 - 68.2 Once the Port Activation Process has begun it shall be completed; and
 - 68.3 A subsequent Port Request will be required to change part or all of the original Port Request.

Port Requests

69. The GSP bears sole responsibility for ensuring:
- 69.1 that all Port Requests are valid and correct; and
 - 69.2 that, prior to inputting a Port Request into the Porting Process for each Number, a valid and complete Customer Authorisation has been obtained from the Customer requesting Porting of the Number.

Customer Authorisation

70. A Customer Authorisation must contain, at a minimum, the following:
- 70.1 the Customer's details including name or business name and contact number and (where applicable) the name and contact number of the Customer's duly authorised representative;
 - 70.2 acknowledgement that the Customer is authorised to request Porting in respect of the Number(s) referred to in the Customer Authorisation;
 - 70.3 name of the Gaining Carrier or GSP;
 - 70.4 name of the Losing Carrier or LSP;

- 70.5 the Numbers to be Ported and any associated Account Numbers;
 - 70.6 the date of the Customer Authorisation; and
 - 70.7 the Customer's express acknowledgement that he or she has been informed by the GSP of, and accepts, the information set out in paragraph 72 and the Customer's express authorisation for the relevant Numbers to be Ported to the GSP.
71. A Customer Authorisation shall cease to be valid at the end of thirty (30) days following the day on which it is given.

Informed Consent

72. In the process of obtaining a Customer Authorisation, the Gaining Carrier or GSP must inform the Customer:
- 72.1 that the Customer is Porting a Number from their current Service Provider to the GSP;
 - 72.2 that by Porting the Number, the service(s) associated with that Number will be disconnected by the Losing Carrier or LSP and may result in finalisation of the Customer's account for the service(s);
 - 72.3 that the Customer may continue to have outstanding obligations to the LSP and it is the Customer's responsibility to check the terms and conditions of their current contract with the LSP in relation to the Numbers sought to be Ported;
 - 72.4 that although the Customer has the right to Port their Number(s), there may be costs and obligations associated with the Port, which may include early termination fees and Porting fees;
 - 72.5 of any costs and obligations to the GSP associated with the Port;
 - 72.6 that after Porting the Number, particular services that were associated with that Number might not be supported by the Gaining Carrier or GSP; and
 - 72.7 that they may need to give notice to the LSP of termination of the Customer's contract with the LSP.

Customer Authorisation Validity Period

73. The GSP must make a Port Request not more than sixty (60) days after receipt of the relevant Customer Authorisation, unless the Customer and GSP expressly agreed otherwise.
74. In the instance of a Customer connection being delayed for reasons beyond the control of the GSP leading to new services not being available until after the prescribed sixty (60) days, the Customer Authorisation will be deemed valid to

complete the transfer unless the Customer has expressed their wishes to cancel the transfer in the meantime.

Retention of Customer Authorisation

75. The GSP must:
 - 75.1 retain all Customer Authorisations; or
 - 75.2 where a Customer Authorisation is completed on-line or via non-documentary methods, sufficient evidence of the on-line Customer Authorisation or other non-documentary evidence to establish that the GSP complied with paragraph 70;
 - 75.3 be able to produce for inspection evidence of a valid Customer Authorisation on request:
76. To the Commission within 5 Business Days for a period of 12 months from the completion of the Port.
77. To the LSP within 4 Working Hours for a period of 5 Business Days from the completion of the Port, for the purpose of investigating a possible unauthorised Port.
78. To the LSP within 5 working days for a period of 12 months from the completion of the Port, for the purpose of resolving a Customer complaint other than that which falls under the conditions of paragraph 77.

Unauthorised Ports

79. A Port shall be deemed to be unauthorised if the Customer Authorisation or the evidence referred to in paragraph 75.2 relating to the Number and Port in question:
 - 79.1 cannot be produced by the GSP on request within the specified time;
 - 79.2 is not complete and valid;
 - 79.3 is illegible or indecipherable; or
 - 79.4 records that the Customer Authorisation was given more than sixty (60) days before the Port Request was made, unless the Customer and GSP expressly agreed otherwise.

Reversal of Unauthorised Ports

80. If a Port is unauthorised and the Customer wishes to return the Number assigned to him or her to the LSP, then the LSP will contact and work with the GSP to confirm the Port was not subject to a valid Customer Authorisation, in order to restore the Number promptly to the LSP:
 - 80.1 If the Port is completed, the LSP shall make a new Port Request and the parties involved shall Port the Number as a matter of urgency and within a

shorter period than is required by the Service Levels that normally apply to a Port; or

80.2 If the Port has not commenced, the GSP shall withdraw the Port; or

80.3 If the Port Activation has commenced but has not been completed, the GSP shall fail the Port.

Relinquishment

81. Subject to paragraph 43, the Service Provider must commence Ported Number Relinquishment for a Ported Number within 5 Business Days after the Billing Relationship with the relevant Customer for that Ported Number terminates.

LSP Responsibilities

Porting Facilitation

82. The LSP:

82.1 Must not initiate any activity associated with the Numbers in the Port, including Customer or Service Provider initiated changes, that impact adversely on the Porting Process once the GSP has approved the Port;

82.2 Must use all reasonable endeavours to minimise the length of the Co-operative Period and to facilitate the Porting of the Number. Regardless of the Co-operative Period, the Service Levels shall continue to apply; and

82.3 Subject to paragraph 43, is not obliged to advise the GSP of additional Numbers beyond those included in the Port Request.

83. To reverse an unauthorised Port the Service Providers will work together as detailed in paragraph 80. For the avoidance of doubt, failure of the original GSP to provide evidence of the Customer Authorisation within the timeframes set out in paragraphs 76-78 is sufficient evidence to deem the Port unauthorised and initiate a Port reversal.

Bad Debts are not a reason for Port Rejection

84. The fact that a Customer has a bad debt or unpaid invoice with the LSP is not in itself sufficient grounds to reject the Porting of that Customer's Number in accordance with the LMNP Terms.

Third-party resellers

85. The fact that a Customer is being billed through an Off-IPMS Reseller who has failed to respond to a porting step within the timeframes provided under the relevant Service Level is not sufficient grounds to reject or delay a porting step. A party's obligations to adhere to the Service Levels are not invalidated by the involvement of a third-party Reseller.

86. The absence of response from the Off-IPMS Reseller within the required timeframe will be considered to be confirmation that the supplied details are correct, and the LSP has the right to respond in IPMS as such.

Fault Management

87. Prior to commencement of the Port Activation Process, the LSP and Losing Carrier are jointly responsible for management of all faults associated with a Number and will liaise with other parties, as required.
88. On and from commencement of the Port Activation Process, the GSP will be responsible for the management of all faults associated with a Ported Number and will liaise with the LSP, Losing Carrier, Donor Carrier and other parties, as required.

Transfer of Ported Number to Another Person

89. The legitimate transfer of a Ported Number to another person when requested by the Customer is allowable if it meets the Service Provider's normal criteria used in the case of non-Ported Numbers. The transferee has the same rights as the transferor to subsequently Port the Number if they wish. In case of a Customer wishing to simultaneously transfer and Port a particular Number, the transfer should be completed prior to the Port and these LMNP Terms shall apply only in relation to the Port.

Right to use the Ported Number Register

90. All Service Providers participating in Porting have the right to access the Register in accordance with paragraph 375, and to access information contained in the Register regarding the Ported Numbers for which they are the Service Provider.

Carrier Responsibilities

91. It will be the responsibility of each Carrier to ensure that they meet the required Service Levels. Each Carrier is free to determine how it handles calls, either within its own Network or with the assistance of another Carrier. Where the LMNP Terms refer to the responsibility of a Carrier, the responsibility under the LMNP Terms remains with the Carrier, regardless of whether the Carrier may have contracted with a third-party for performance of the activity in question.

Carrier Rules

92. Each Carrier will maintain an interface with the IPMS for the transmission of messages for the Porting Process.
93. Carriers will receive Porting Messages via their interface to the IPMS. The Porting Process will only be accessed by Carriers in this manner.
94. Carriers providing Local Service and Mobile Service will require awareness of the other aspect of portability if they want to route calls directly to the current Host Carrier.

95. Subject to paragraph 96, each Carrier will make the necessary changes, additions, or deletions to its Network to give effect to the instructions issued by the Porting Process.
96. The LMNP Terms do not cover the requirements for the routing of calls to or from Ported Numbers, nor the details of the call/signalling inter-operability between the Networks of the Carriers.
97. The Network aspects of LMNP are set out in the Network Terms.
98. Carriers must act in good faith to facilitate Porting.

Maintaining Records of Ported Numbers

Accuracy of Ported Number Register

99. The IPMS will be the sole source of information for the status of any or all Ported Numbers. Carriers should check their routing tables with the IPMS only and ensure they maintain consistency with it. Tools for helping this are detailed from paragraph 367.

Right to use the Ported Number Register

100. All Carriers participating in Porting have the right to access the Register. The information contained in the Register is to be used for the sole purpose of ensuring that participating Carriers' Network records are consistent with the IPMS.

RFS Date Notice Period

101. A Port Request must specify an RFS Date which complies with the minimum and maximum notice periods set out in the Appendix, Table 3. The notice period is the elapsed time between when the Port Request is sent and the RFS Date.

Planned and Unplanned Outages

Planned Outages

102. Every effort must be made to ensure that Planned Outages that may affect LMNP do occur between 8.00 pm and 6.00 am Monday to Sunday, between 4.00 pm and 6.00 am Sunday to Monday and between 4.00 pm on Public Holidays to 6.00 am the following day.
103. In the event that a Carrier or Service Provider identifies that there will be an outage in their system(s) that may affect LMNP, that Carrier or Service Provider must advise all involved parties via email at least 5 Business Days before the outage occurs. If there is any change to the Planned Outage date or time the change must be advised to all parties via phone call and email as soon as possible.
104. Carriers or Service Providers must provide details of all Planned Outages (including any change to those Planned Outages) to the TCF and the TCF must ensure those details are provided on the IPMS homepage and updated when there is any change.

Unplanned Outages

105. In the event that a Carrier or Service Provider identifies that it is experiencing an Unplanned Outage, it must as soon as practicable notify all parties involved in LMNP via email.
106. The following information must be included in the notification:
 - 106.1 Nature of problem;
 - 106.2 Location of problem;
 - 106.3 Impact of problem;
 - 106.4 Estimated time of resolution;
 - 106.5 Next update time.
107. The Carrier or Service Provider that had the system outage must give notice of the conclusion of the outage to all parties via phone call and email or fax (as a backup) as soon as practicable. To the extent that parties may have ceased processing Porting transactions during an Unplanned Outage, they must recommence processing those transactions as soon as practicable after the system fault has been rectified.
108. Each Carrier and Service Provider must provide the TCF with contact details for appropriate personnel in relation to Planned Outages and Unplanned Outages and the TCF shall maintain a contact list for each of the parties on the Number Portability Users shared drive.

Escalation Procedures

109. Procedure
 - 109.1 If a fault is specific to LMNP traffic and does not affect other traffic types and if Bilateral Agreements do not provide specific arrangements for escalation procedures in the context of Network issues relating to LMNP, then parties shall use the following procedure:
 - 109.1.1 In an LMNP environment, the Service Provider that owns the relationship with the Customer who originates the fault call is also responsible for coordination and escalation of the fault resolution process.
 - 109.1.2 The escalation procedure is to be used as a means of bringing unresolved issues to the attention of Carriers at all levels responsible for, or having authority to, expedite corrective action. To that end all LMNP participants must ensure that they nominate relevant contact points for the escalation of Porting issues.
 - 109.1.3 In the case that any Porting activity is not resolved within the specified time frame or is resolved unsatisfactorily, any LMNP

participant may escalate this matter to the next escalation point nominated by the other party. Unless otherwise specified, that escalation point will have the relevant amount of time to investigate, resolve and respond as specified for that point of escalation.

109.1.4 The escalation procedure is to be initiated when an issue that requires resolution has been reported to an LMNP participant for remedial or corrective action, and after a given period, either:

- (a) no response has been provided in relation to the issue raised; or
- (b) the issue raised has not been resolved; or
- (c) an unsatisfactory reason is given for the delay in remedial/corrective action to resolve the issue raised.

109.1.5 Prior to initiating the escalation procedure, the affected LMNP participant should conduct preliminary enquiries within their own organisation to resolve any issues raised. At this point, the Relevant Party should identify if the issue is the result of a known problem. Where it is identified that the problem is associated with an existing unresolved problem (and all other conditions have been met) then the affected LMNP participant can raise an escalation.

109.1.6 Once the above steps have been undertaken, the Relevant Party should initiate the escalation procedure as follows:

- (a) Advise the nominated escalation contact point.
- (b) If the issue cannot be resolved at the first level, advise that Carrier's or Service Provider's second level escalation of the affected parties for resolution.

110. Contact details for faults escalation procedure

110.1 At each level, the relevant escalation contact points must:

110.1.1 supply adequate facilities for contact and commit to maintenance of that contact and when necessary, provide an alternate point of contact; and

110.1.2 acknowledge receipt of information provided by the other escalation contact point as soon as possible.

110.2 Each Carrier and Service Provider must provide the TCF with contact details for appropriate personnel in relation to faults escalation. The TCF shall maintain a list of escalation contacts for each of the parties on the Number Portability Users shared drive.

110.3 The levels of escalation and standard timeframes to escalate to the next level are:

Escalation level	Description	Standard timeframe for contacting next escalation level
Business As Usual	Represents the handover point for initial fault investigation and repair.	
Level One	Escalation level where Service Level agreements are assessed as being “in danger of” being compromised or are not met.	2 hours
Level Two	Escalation level where Service Level agreements are impacted and Level One escalation has not effected a satisfactory resolution. Also, may be invoked where multiple Customers’ services are affected by the same problem.	4 hours
Level Three	Level Two escalation has not effected a satisfactory resolution. Serious process or infrastructure integrity failure.	8 hours

Administrative Issues

Clarification and Reconsideration of the LMNP Terms

111. The LMNP Terms are subject to Subpart 5 of Part 2, and Subpart 2 of Part 4A of the Act.

Dispute Resolution

Dispute

112. For the purposes of these dispute resolution procedures, a “dispute” is any Costs Allocation Issue or any matter relating to the LMNP Terms about which any of the parties to the LMNP Terms disagree or are unable to agree where a matter requires their agreement and which:
- 112.1 Is substantially a dispute of fact of a technical nature (Technical Dispute), including a Service Level default, but is not a Complex Dispute as defined in paragraph 112.2; or
 - 112.2 Is a dispute (Complex Dispute) that:
 - 112.2.1 May, in the opinion of a party to the dispute and the LMNP Terms have significant commercial implications for that party; or
 - 112.2.2 Includes a substantial issue of fact of a non-technical nature or a substantial issue of law; or
 - 112.2.3 is a Costs Allocation Issue.
113. If a dispute is not a Technical Dispute, then it is to be resolved as if it is a Complex Dispute. A Complex Dispute may include, without limitation, a dispute as to whether Local Number Portability or Mobile Number Portability is required to be provided in relation to a particular Local Service or Mobile Service.

Telecommunications Act 2001

114. No party to the LMNP Terms is prevented by these dispute resolution procedures from exercising any rights under the Act, including but not limited to:
- 114.1 Applications for determinations, price reviews, clarifications, reconsiderations to the Commission under Part 2 of the Act;
 - 114.2 Appeals against Commission determinations under Subpart 5 of Part 2 and proceedings for enforcement of Commission determinations to the High Court under Subpart 2 of Part 4A of the Act; and
 - 114.3 Investigations by the Commission under subpart 6 of Part 2 and Schedule 3 of the Act.

115. If there is a dispute about the extent of a party's rights under the Act, then that dispute may be resolved in accordance with the procedures in the Act and these dispute resolution procedures will not apply to such a dispute.
116. If a dispute has not been resolved by the end of the Negotiation Period as defined below (and, if applicable, the Mediation Period as defined below), a party to the dispute may choose to resolve the dispute by pursuing any applicable rights under the Act or, in the alternative, by submitting a Technical Dispute for expert determination under paragraph 124 or by submitting a Complex Dispute for arbitration under paragraph 129.
117. Once a party (the "Initiator"):
 - 117.1 has commenced a process under the Act; or
 - 117.2 has submitted a dispute for expert determination or arbitration,then, subject to paragraph 130 below, the Initiator cannot commence an alternative process, unless the process that has been commenced is held by the decision maker of that process not to apply to the resolution of the dispute in question.
118. If the Initiator submits a dispute for expert determination or arbitration, that will not preclude the other parties to the dispute, or the Commission, from pursuing any rights under the Act.

Good faith negotiation

119. Any party to the LMNP Terms may at any time give notice describing a dispute to any other party (or parties) to the LMNP Terms who are involved in the dispute (**Relevant Party**). The party who gave notice of the dispute and the Relevant Parties are together referred to as the "parties to the dispute".
120. If a party gives notice of a dispute, then during a period of 10 Business Days from the date notice of the dispute was given (**Negotiation Period**), the authorised representatives of the parties to the dispute must attempt in good faith to negotiate a resolution of the dispute.
121. If the authorised representatives are unable to resolve the dispute within the 10 Business Day Negotiation Period, the parties to the dispute may agree to each refer the dispute to their respective Chief Executive (or equivalent officer, or their nominee), in the case of a Complex Dispute, or operational manager, in the case of a Technical Dispute, who must attempt in good faith to resolve the dispute within a further 10 Business Days. If the parties agree to this further Negotiation Period, then for the purposes of paragraph 122, the Telecommunications Act 2001 section and the Mediation section the "Negotiation Period" includes this further 10 Business Day period.
122. If by the end of the Negotiation Period the parties to the dispute are unable to agree whether the dispute is a Technical Dispute or a Complex Dispute then, for the purposes of these dispute resolution procedures, the dispute shall be regarded as a

Complex Dispute, and subject to the Telecommunications Act 2001 section of these LMNP Terms resolved under these dispute resolution procedures as such.

Mediation

123. At any time during the Negotiation Period, the parties to a dispute may agree to refer the dispute to mediation. The mediator will be appointed by agreement between the parties to the dispute but failing agreement within 5 Business Days of the parties agreeing to refer the dispute to mediation, will be selected by the Chairperson of Resolution Institute (or their nominee). Unless otherwise agreed in writing, the then current model mediation agreement issued by Resolution Institute must be used and the mediation must be completed within 20 Business Days of the mediator's appointment (**Mediation Period**). The costs of the mediator will be paid by the parties to the dispute equally.

Determination of Technical Disputes by an independent expert

124. If a Technical Dispute has not been resolved by the end of the Negotiation Period (and, if applicable, the Mediation Period), a party to the dispute may give written notice to the relevant parties requiring the dispute to be determined by an independent expert.
125. The independent expert will be appointed by agreement between the parties to the dispute, but failing agreement within 5 Business Days from the date the notice was given under this clause, will, at the request of the Initiator, be nominated by the Chairperson of the Board of the TCF and approved by the Commission.
126. To be eligible for appointment, the expert must be independent and impartial, must be experienced in telecommunications and will preferably be experienced in dispute resolution procedures. He or she must not have performed any duties, whether as an employee, consultant, or Contractor, for any of the parties to the dispute or any related party during a 12-month period prior to the date the notice of the dispute was given.
127. The expert will act as an independent expert and not as an arbitrator. The dispute will be resolved as soon as possible in accordance with the procedure determined by the expert, but in accordance with the principles of natural justice. Where the independent expert has primarily technical qualifications, he or she may seek independent legal advice regarding the appropriate procedures for resolution of the dispute.
128. The parties to the dispute agree to be bound by the decision of the independent expert, in the absence of manifest error. The costs of the independent expert (including the costs of any independent legal advice sought by the expert in accordance with these dispute resolution procedures) will be shared equally by the parties to the dispute. Reference to the independent expert will not be a submission to arbitration for the purposes of the Arbitration Act 1996 and that Act will not apply to or govern resolution of the dispute.

Arbitration of complex disputes

129. If a Complex Dispute has not been resolved by the end of the Negotiation Period (and, if applicable, the Mediation Period), a party to the dispute may then give notice referring any part of the dispute to arbitration. The notice will, subject to the Telecommunications Act 2001 section, be a submission by the parties to the dispute of the dispute to arbitration and each party to the dispute agrees to confirm this submission if requested by any other party to the dispute. Unless otherwise agreed in writing:

129.1 The arbitration will be subject to the Arbitration Act 1996 and its Schedules;

129.2 The parties to the dispute will endeavour to appoint a single arbitrator within 10 Business Days of notice being given;

129.3 The arbitrator must have experience and expertise in telecommunications and competition issues;

129.4 If the parties to the dispute fail to agree on a single arbitrator within the 10 Business Day period, then the President of the New Zealand Law Society (or their nominee) shall appoint the arbitrator at the request of any of the parties to the dispute;

129.5 The arbitrator must adopt a procedure which, in the arbitrator's opinion, is expeditious. If feasible in the circumstances the arbitrator will endeavour to complete the arbitration within 2 months of the arbitrator's appointment (or such lesser period as is appropriate);

129.6 The arbitrator may determine the dispute without a hearing unless any party gives notice requiring one, in which case the arbitrator must treat that as a material consideration in assessing costs;

129.7 The arbitrator must not adopt inquisitorial processes;

129.8 The arbitration must take place in Wellington or Auckland (at the arbitrator's discretion);

129.9 The arbitrator must determine the dispute under New Zealand law;

129.10 Any party may appeal to the High Court on any question of law arising from an award; and

129.11 The arbitrator may commission assistance or any reports from any expert or other person which, in their opinion, would assist him or her in making the award. The cost of this assistance or report is:

129.11.1 To be a cost of the arbitration; and

129.11.2 Unless the arbitrator orders otherwise, to be shared equally between the parties to the dispute.

129.12 The arbitrator must:

- 129.12.1 provide copies of any assistance or report to the parties to the dispute;
- 129.12.2 allow each party to make submissions in response to that assistance or report;
- 129.12.3 allow each party to produce evidence on any issue raised in that assistance or report; and
- 129.12.4 allow each party to make submissions in response to any evidence produced by any party.

Court proceedings

130. Notwithstanding the above dispute resolution procedures, a party to the LMNP Terms may at any time commence court proceedings relating to any dispute if that party seeks urgent interlocutory or interim relief. Otherwise, and except where a party to the dispute chooses to pursue any rights it may have under the Act as contemplated by the Telecommunications Act 2001 section in the LMNP Terms, the dispute resolution procedures in the LMNP Terms are mandatory and parties to the LMNP Terms contemplate that they will not resort to court proceedings. If court proceedings other than proceedings contemplated by the Telecommunications Act 2001 section in the LMNP Terms are commenced, a Relevant Party shall be entitled to seek a stay of court proceedings in favour of an appropriate dispute resolution procedure under the LMNP Terms. All the provisions in the Dispute Resolution section shall apply, irrespective of whether any party to the Determination of which they form part, or the Commission, has filed the Determination in the High Court as provided for in section 156P of the Act.

Continuance of obligations

131. Except where the dispute renders it impossible to do so, the parties to the dispute must continue performing their respective obligations under the LMNP Terms whilst the dispute is being resolved or is subject to expert determination, arbitration or court proceedings, or a party is pursuing its rights under the Act. Each party to the LMNP Terms must use all reasonable endeavours to ensure that where a dispute is reasonably foreseeable, it is dealt with at a sufficiently early stage to ensure that there is a minimum effect on the ability of any party to perform its obligations under the LMNP Terms.

Use or disclosure of information

132. No party to a dispute may use, other than to attempt to resolve the dispute, any information disclosed by any other party to the dispute in the course of negotiation, expert determination, mediation or arbitration under the dispute resolution procedures. Any such information remains the property of the party supplying it and remains confidential to that party. Disclosure in the course of negotiation, expert

determination, mediation or arbitration under the above procedures shall not constitute a waiver of confidentiality.

133. Neither party may disclose any such information to anyone other than an adviser or independent witness who has entered into a deed undertaking:
 - 133.1 not to disclose any of the information, or any analysis of the information, other than to the parties to the dispute, an independent expert, a mediator, an arbitrator or court, except as compelled by law; and
 - 133.2 to return all material on which such information is recorded on completion of the adviser's or independent witness' services.

Bilateral Agreements

134. The dispute resolution procedures set out in the Dispute Resolution section apply to the extent they are not inconsistent with the dispute resolution procedures in a Bilateral Agreement that incorporates the LMNP Terms in full or in part for a dispute under the Bilateral Agreement relating to the subject matter of the LMNP Terms.

Exiting the IPMS

135. In the event that a Service Provider or Carrier ceases to be a Service Provider, Carrier, or both ("Departing Party"), or their use of the IPMS is terminated for any reason, the Departing Party shall activate arrangements to make the necessary changes to the IPMS to:
 - 135.1 Maintain the integrity of the IPMS;
 - 135.2 Continue to facilitate LMNP in accordance with the LMNP Terms; and
 - 135.3 Ensure that calls to Ported Numbers managed by the IPMS can continue to be correctly routed.
136. The Departing Party shall agree the proposed changes with the TCF to meet the requirements set out in paragraphs 135.1, 135.2, and 135.3.
 - 136.1 Where a Service Provider who is a Departing Party ceases operations, becomes uncontactable, or is otherwise unable to meet its obligations under paragraph 135, the TCF may take such reasonable measures as are necessary to ensure that:
 - 136.1.1 Affected end-users are able to Port their Numbers to another participating Service Provider without undue delay;
 - 136.1.2 Calls to affected Ported Numbers continue to be correctly routed; and
 - 136.1.3 the integrity of the IPMS is maintained.

Failure to meet Service Levels

137. If an Audit IPMS Client does not meet the Service Levels, the Enforcement Agency must issue that Audit IPMS Client with a written:
 - 137.1 Caution Notice of Breach;
 - 137.2 Warning Notice of Breach; or
 - 137.3 Public Censure Notice.
138. The Enforcement Agency must consider the seriousness of the non-compliance of the Audit IPMS Client, and the Audit IPMS Client's past conduct with respect to compliance with the Service Levels when determining the appropriate enforcement action under paragraph 137. The Enforcement Agency is not required to issue a notice where it is satisfied that the failure to meet a Service Level was minor or immaterial. A failure that has affected, or is likely to have affected, a Customer (including by delaying or preventing a port) is not minor or immaterial.
139. The Enforcement Agency must first have issued a Caution Notice of Breach and then a Warning Notice of Breach to the Audit IPMS Client in relation to the particular breach in question before making a determination to issue a Public Censure Notice relating to the Audit IPMS Client.
140. For the purposes of paragraph 138, the Enforcement Agency must have regard to patterns of non-compliance by the Audit IPMS Client, including previous Notices of Breach issued to the Audit IPMS Client, when determining whether a Caution Notice of Breach, Warning Notice of Breach, or Public Censure Notice is appropriate.
141. The Enforcement Agency will provide a copy of any Caution Notice of Breach, Warning Notice of Breach or Public Censure Notice issued to all parties to the LMNP Terms and, at the same time, to the Commission. Parties to the LMNP Terms who receive a copy of a Caution Notice of Breach or Warning Notice of Breach shall keep such notice confidential.
142. The Enforcement Agency must maintain a record of:
 - 142.1 confirmation of receipt of the Caution Notice of Breach;
 - 142.2 the Audit IPMS Client's explanation of the breach;
 - 142.3 corrective actions, remediation proposed or internal reviews;
 - 142.4 any timetable for implementation of corrective actions;
 - 142.5 the outcome of those corrective actions; and
 - 142.6 each occasion on which the Enforcement Agency decided not to issue a notice because it was satisfied that the failure to meet a Service Level was minor or immaterial, including the nature and cause of the failure, the

reasons for that assessment, any corrective action taken, and whether a similar failure has occurred previously.

143. The Enforcement Agency must provide this record under paragraph 142 to the Commission on a quarterly basis, and at any other time upon request.

Caution Notice of Breach

144. The written Caution Notice of Breach to the Audit IPMS Client will include a request that one or more of the following actions be undertaken by the Audit IPMS Client:
 - 144.1 rectification of the breach;
 - 144.2 specific corrective actions; and
 - 144.3 an internal review of the Audit IPMS Client's state of compliance with the Service Levels.
145. The Caution Notice of Breach will specify a timetable within which the action is required to be completed, with duration dependent upon the nature and complexity of the action. The Enforcement Agency will also seek confirmation from the Audit IPMS Client of receipt of the Caution Notice of Breach.
146. Where the Audit IPMS Client has identified the cause of a breach and implemented corrective action prior to the issue of a subsequent Caution Notice of Breach, the Enforcement Agency may modify the requirements of paragraphs 144 and 145.
147. In circumstances under paragraph 146, the Caution Notice of Breach must record instead:
 - 147.1 the cause of the breach;
 - 147.2 the corrective action taken;
 - 147.3 the date corrective action was implemented; and
 - 147.4 the expected date by which the corrective action is anticipated to be reflected in the compliance reports.
148. The Enforcement Agency must monitor the Audit IPMS Client's compliance with the expected resolution date recorded in the Caution Notice of Breach.
149. The fact that corrective action has been implemented does not prevent the Enforcement Agency from issuing a Warning Notice of Breach where the anticipated period of non-compliance is prolonged. In such circumstances, the Enforcement Agency must consider whether a Warning Notice of Breach is appropriate.
150. Where non-compliance continues after the expected resolution date recorded under paragraph 147, the Enforcement Agency must consider whether a Warning Notice of Breach is appropriate.

Warning Notice of Breach

151. The written Warning Notice of Breach to the Audit IPMS Client is a more severe version of the Caution Notice of Breach, and must be considered by the Enforcement Agency where:
 - 151.1 the Audit IPMS Client has failed to undertake voluntarily the actions requested by the Caution Notice of Breach, within the timetable specified therein;
 - 151.2 the Audit IPMS Client receives repeated Caution Notices of Breach arising from the same underlying cause;
 - 151.3 non-compliance continues after the expected resolution date recorded in a Caution Notice of Breach;
 - 151.4 the anticipated period of non-compliance is prolonged, despite corrective action having been implemented by the Audit IPMS Client; or
 - 151.5 the Enforcement Agency determines that the customer impact of the breach is significant.
152. The Warning Notice of Breach to the Audit IPMS Client will include an order that one or more of the following actions be undertaken by the Audit IPMS Client:
 - 152.1 rectification of the breach;
 - 152.2 specific corrective actions;
 - 152.3 arrange for an independent audit of its compliance procedures in relation to the Service Levels. The auditor must be approved by and report to the Enforcement Agency on compliance with the Service Levels. The Audit IPMS Client will be required to implement recommendations of the audit; and
 - 152.4 that the Audit IPMS Client conduct relevant education of its relevant staff to address knowledge inadequacies that may have led to the breach.
153. The Warning Notice of Breach will nominate a timetable within which the action is required to be completed, and the steps needed to be taken by the Audit IPMS Client to address the action required by the Warning Notice of Breach, with duration dependent upon the nature and complexity of the action. The Enforcement Agency will also seek confirmation from the Audit IPMS Client of receipt of the notice.

Public Censure Notice

154. In the event of a refusal or failure on the part of the Audit IPMS Client to undertake to the Enforcement Agency's satisfaction any actions required by a Warning Notice of Breach within the timetable specified therein, or where non-compliance continues after the expected resolution date recorded in a Warning Notice of Breach, the Audit

IPMS Client will promptly be formally advised by the Enforcement Agency that a Public Censure Notice is to be prepared for widespread publication.

155. The fact that corrective action has been implemented does not prevent the Enforcement Agency from progressing to a Public Censure Notice where the anticipated period of non-compliance remains prolonged.
156. The Audit IPMS Client will be sent an advance copy of the intended Public Censure Notice, which will:
 - 156.1 identify the Audit IPMS Client by name;
 - 156.2 give details of the breach;
 - 156.3 list all requests/orders previously made of the Audit IPMS Client;
 - 156.4 report on whether an independent audit has been ordered and, if so, state the results of the audit;
 - 156.5 state that at the date of publication, the requests of the Caution Notice(s) of Breach and the orders of the Warning Notice(s) of Breach have not been complied with;
 - 156.6 specify the status of any corrective action required of the Audit IPMS Client, including whether that action remains outstanding or has been completed.
157. The Audit IPMS Client will also be advised that publication of the Public Censure Notice will not occur until 10 working days have elapsed from the date the advance copy of the Public Censure Notice is sent. The purpose of this period is to allow the Audit IPMS Client to comment on the accuracy of the Public Censure Notice and provide any relevant updates regarding compliance.
158. If the Enforcement Agency is fully satisfied that the Audit IPMS Client has fully complied as ordered prior to the date the Public Censure Notice is due to be published, the Enforcement Agency may elect not to publish the Public Censure Notice, having regard to the seriousness of the non-compliance, the duration of the non-compliance, the Audit IPMS Client's past conduct, and any customer impact arising from the breach.
159. If the Public Censure Notice is proceeded with, it must be published, as soon as reasonably practicable:
 - 159.1 in the New Zealand Gazette;
 - 159.2 in the TCF's newsletter;
 - 159.3 on the TCF's website for at least six months (or until there is no Determination in place);

- 159.4 on the censured party's website for at least six months (or until the Determination expires) in the form of a summary of the notice that has been approved by the Enforcement Agency with a link to the notice published under paragraph 159.3 above. The summary and link to the notice must be clearly visible and placed on the most frequently visited page of the censured party's website that is associated with switching to the censured party.
- 160. If the Public Censure Notice is proceeded with, it may be published in any relevant industry newsletter or magazine, in the national newspapers, in Consumer bulletins or on the Commission's website.
- 161. If the audit report states that the Audit IPMS Client has complied with the Service Levels then:
 - 161.1 if the audit was undertaken due to a request from another Service Provider and/or Carrier, then the Audit Costs will be payable to the Enforcement Agency by that other Service Provider or Carrier and, upon receipt of payment of that sum, the Enforcement Agency will reimburse the Audit IPMS Client its costs; or
 - 161.2 if the audit was undertaken otherwise than due to a request of a Service Provider or Carrier, the Audit IPMS Client shall bear its own costs and the costs of the Enforcement Agency shall be reimbursed to it by the party that initiated the audit; or
- 162. If the audit report states that the Audit IPMS Client has not complied with the Service Levels, then the Audit Costs will be payable by the Audit IPMS Client.
- 163. For the purposes of paragraphs 161 and 162, "Audit Costs" means the aggregate of:
 - 163.1 Enforcement Agency reasonable direct costs in respect of the audit (including auditing and legal fees); and
 - 163.2 such costs of the Audit IPMS Client in respect of time involved in assisting the audit as are submitted by the Audit IPMS Client to the Enforcement Agency which the Enforcement Agency determines are fair and reasonable.

Exemptions

- 164. The Audit IPMS Client may advise the Enforcement Agency of an exemption granted in accordance with the Process for Exemption from Compliance with Obligations contained in the Network Terms section of the Network Terms, exempting the Audit IPMS Client from meeting specified obligations under the LMNP Terms in respect of the Service Levels. If the Enforcement Agency is satisfied that the exemption under the Network Terms will prevent the Audit IPMS Client from carrying out any sanction imposed on it by the Enforcement Agency under the LMNP Terms within the timeframe provided for by the Enforcement Agency, the Enforcement Agency will have the discretion to suspend the sanction for so long as, and to the extent that, the

Audit IPMS Client is exempt from compliance with the Service Levels. The Enforcement Agency will notify all interested parties of any such decision.

Subpart 2 of Part 4A

165. For the avoidance of doubt, the procedures set out in the Dispute Resolution section, Exiting the IPMS section, Failure to meet Service Levels section, and Exemptions section are additional to, and not exclusive of, any other rights a party, or the Commission, may have under the Act, at law or in equity and nothing in those sections will prevent any party, or the Commission, from exercising its right to enforce compliance with the Service Levels, or the Determination generally, in accordance with Subpart 2 of Part 4A of the Act.

Publication of Porting Statistics

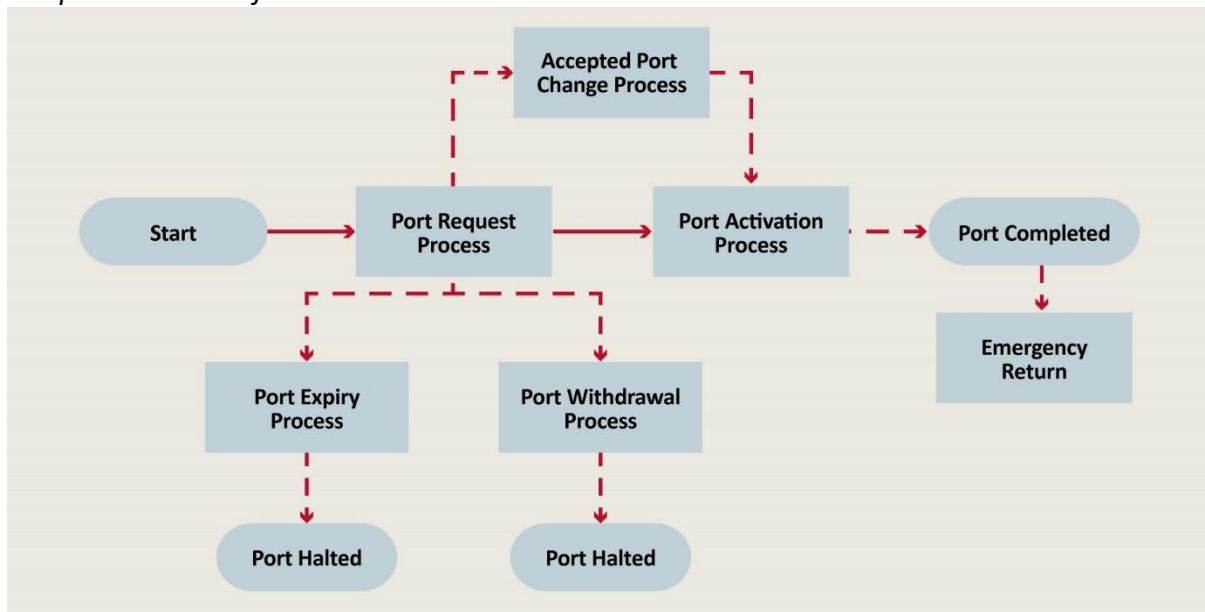
166. The TCF must publish, within one month of the end of each financial quarter, the following information for both mobile and local number Ports for the previous 12 months:
- 166.1 number of gross Ports by month (including Ports of previously Ported Numbers);
 - 166.2 cumulative count of gross Ports since 2007;
 - 166.3 cumulative count of gross Ports as a percentage of active numbers; and
 - 166.4 percentage of Ports completed within the service level timeframes for the key customer-impacting measures, by GSP and LSP, port type, and network updates.
167. For the purposes of paragraphs 166.1 to 166.4, each Port of a Number from one provider to another must be counted as a separate Port transaction. A Number Ported from Provider A to Provider B counts as one Port, and if that Number is subsequently Ported from Provider B back to Provider A, that subsequent Port counts as an additional Port.
168. The active number figure is based on the most current active number data collected by the TCF for the purpose of cost allocation if more up-to-date figures are not available.
169. The basis on which the Porting statistics are calculated must be clearly stated where they are published.

Porting Processes

170. The focus of the LMNP Terms is on the Porting Processes that are required in an LMNP environment.
171. Service Providers and Carriers may be separate parts of the same organisation. There may be more than one Gaining Carrier or Losing Carrier in a Port. There can be only one GSP and LSP in a Port.

172. Functions are normally classified in these processes as being either a Service Provider or Carrier function. It is not a requirement that these functions are performed by resource clearly identified as being part of the Service Provider or Carrier. In some circumstances there will not be a business need to pass information from the Service Provider to the Carrier function. In some circumstances the Gaining Service Provider can also be the Losing Service Provider or the Gaining Carrier can also be the Losing Carrier.
173. The following outline flowchart illustrates how the separate Porting Processes work for a typical Port:

Pre-port Processes flowchart



174. There are six major Porting Processes defined in this section:

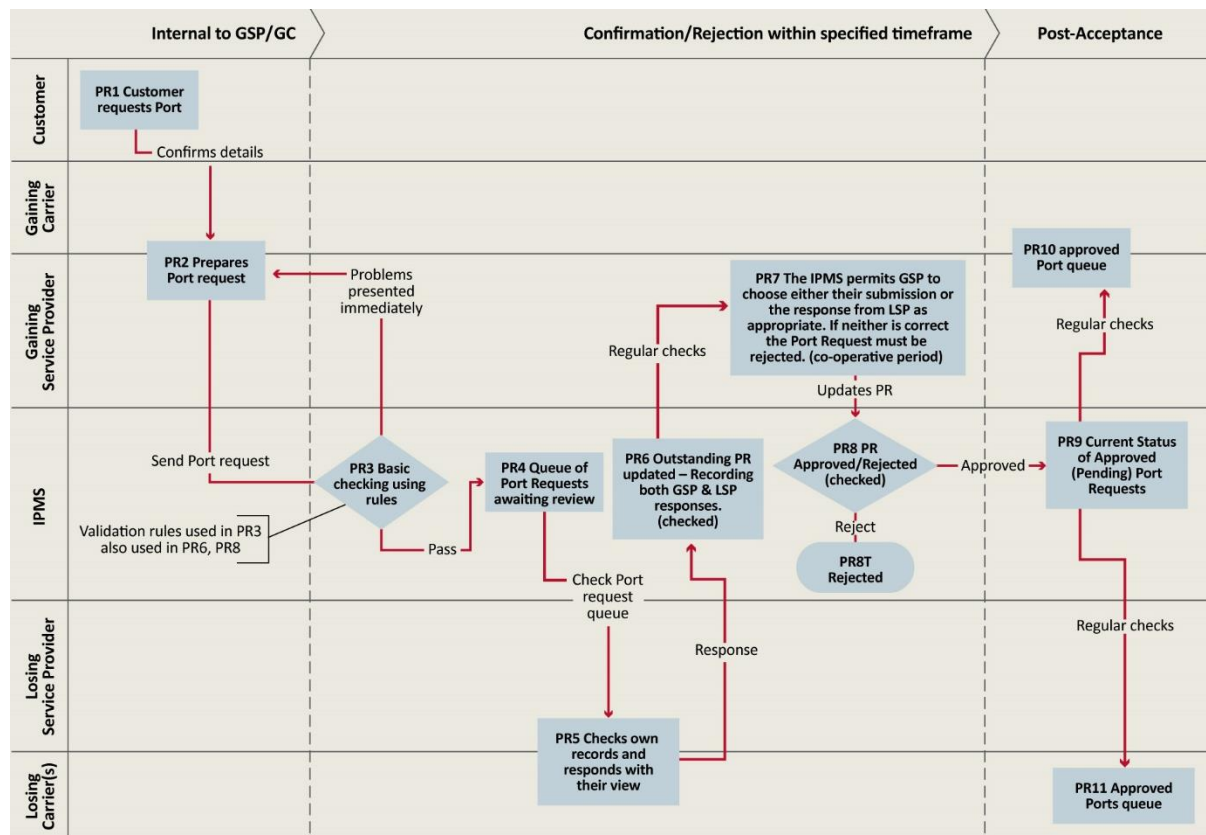
Process	Function
Port Request	Enables the Customer's request to Port Numbers to be validated, approved, and subsequently managed by the IPMS.
Port Activation	Activates Ports registered in the IPMS in compliance with the LMNP Terms. Initiated and managed by the GSP.
Approved Port Change	Enables specific Port details to be amended in IPMS. Typical of these are RFS Dates and Numbers to be Ported.
Ported Number Relinquishment	Allows IPMS to make the necessary Carrier notifications to enable a Customer to relinquish a Ported Number. The Number is returned to the Donor Carrier.
Port Expiry	This Process warns the GSP to reschedule or withdraw a Port Request that has not been activated on the RFS Date.
Port Withdrawal	Enables a Port that is currently active in the IPMS to be withdrawn. Typically, the Customer would initiate this.

Port Request Process

175. The Port Request Process is the first step in Porting. It achieves two main objectives – to ensure all Ports are valid, and to enable all parties to be ready for the Port Activation.

176. A GSP must initiate a Port Request in order to Port a Number.

Port Request Process Flowchart



Port Request Process Timing Table

Flowchart	Port Request Process	Response Times		
		Simple Local Port	Complex Local and Mobile Port	Simple Mobile Port
PR3 to PR8	RFS Notice	RFS Date minimum two Business Days' notice, maximum 30 days	RFS Date minimum five Business Days' notice, maximum 30 days	RFS Date minimum one hour notice, maximum 30 days
PR4 to PR6	LSP responds to Port Request	Within four Working Hours	Within two Business Days	Within 30 Working Minutes
PR6 to PR8	Port Request Complete	Within four Working Hours	Within two Business Days	Within 30 Working Minutes

PR1. Customer Requests Port

177. The Customer makes a request to Port the Number assigned to that Customer to the GSP.

PR2. GSP Prepares the Port Request

178. The GSP must follow an appropriate Customer Authorisation process to ensure that the GSP obtains all relevant information required to ensure a valid Customer Authorisation.
179. The purpose of the Customer Authorisation process is to:
- 179.1 Validate that the person requesting the Port is the Customer or the Customer's duly authorised agent;
 - 179.2 Collect the information required by the GSP; and
 - 179.3 Collect the information required for the Port Request.
180. The GSP is expected to verify the details with their nominated Gaining Carrier(s). It is assumed that the Gaining Carrier(s) will discuss any issues with the GSP and resolve any issues before proceeding. A site audit is likely to be part of the investigation in Local Ports.
181. Problems and issues identified by the Gaining Carrier(s) and the site audit should be resolved as an internal matter between the GSP, Gaining Carrier(s), and the Customer. The Port Request Process is not to proceed until the details are correct.
182. The Port Request is submitted to the IPMS. This will include the data required as per the Appendix, Table 1.

183. If the Port Request has been rejected due to the LSP being incorrect (for example, where a Number is currently reassigned), the GSP can override the IPMS rejection so that the transaction can be processed by the LSP.

PR3. IPMS Performs Basic Checking Using Rules

184. The IPMS shall perform all the basic tests listed in the Appendix, Table 4.
185. The IPMS will respond based on whether the Port Request passes or fails any of the basic tests listed in the Appendix, Table 4.
186. IPMS performs basic tests on Port Request, as follows:
- 186.1 The IPMS will immediately respond to the CSR at the GSP if the Port Request fails the basic tests;
 - 186.2 The IPMS will include all reasons for failure (if there are more than one);
 - 186.3 The GSP is expected to correct all errors before submitting the Port Request again; and
 - 186.4 A counter for the number of rejections of a given Port Request may be used.
187. If the GSP manually overrides the LSP validation, as set out in the PR2. GSP Prepares the Port Request section, the IPMS will not check the LSP and will continue the process.

PR4. IPMS Queues the Port Request for Review by the Losing Service Provider

188. The IPMS will record the time that the Port Request was added to the queue.
189. The status of the Port Request in the IPMS changes to “awaiting review”.
190. The Port Request is presented by the IPMS to the LSP for the LSP’s response.

PR5. LSP checks the Port Request Queue

191. The LSP checks that the Port Request has been correctly completed.
192. The LSP is presented with the Port Request as per the detail in the Appendix, Table 5.
193. Discussion between the LSP and the GSP regarding the Port Request is allowed during the Co-operative Period. In the interests of preventing unnecessary rejection or confusion, the LSP has the right to contact the GSP to check if there is any doubt or concern over the details of the Port Request before they submit their response.
194. Subject to paragraph 195 the LSP enters their understanding of the details if they differ from the information presented by the IPMS. This can include addition or removal of Numbers for a Multiple Number Port.
195. If the Account Number presented by the IPMS is not correct or not substantially correct (having regard to the other information presented by the IPMS for the Port

Request), the LSP will indicate that it cannot match the Account Number presented by the IPMS to an active account for the relevant Number(s) and therefore cannot proceed with checking the Port Request.

196. The LSP submits their response to the IPMS.

PR6. IPMS Updates the Queue of Reviewed Port Requests Awaiting GSP Check

197. The queue of reviewed Port Requests is available for checking.

198. The response time of the LSP is recorded when it is updated in the IPMS.

199. The IPMS uses the same basic tests in PR3, to ensure the LSP responses appear to be valid.

PR7. GSP Checks LSP Response

200. The GSP reviews the Port Request after the Losing Service Provider's response.

201. The GSP can make use of the Co-operative Period to contact the LSP if there is any doubt.

202. Should the LSP have marked the Account Number as incorrect, the GSP shall have the option of making the necessary correction and resubmitting the Port Request. This option may be exercised no more than twice for the same Port Request.

203. The GSP may need to contact the Customer or the Contractor that performed the audit whilst investigating any differences.

204. The IPMS will permit the GSP to choose either the data they submitted or the response from the LSP as appropriate. No other alternative will be possible. If the correct answer is neither that submitted by the GSP nor the LSP the Port Request must be rejected.

205. The GSP must act in good faith and only accept Port Requests that are correct.

206. The GSP must reject a Port Request at this point if the required details are incomplete or incorrect or there is material doubt as to their completeness or correctness.

207. The result of the GSP review is recorded in the IPMS and the status is set to "approved" or "rejected".

208. If the Port Request is rejected, it must be presented as a new Port Request if it is to be resubmitted later.

PR8. IPMS Stores the Port Request and Updates Status

209. The IPMS re-performs the basic tests on the final result of the Port Request to ensure it is correct. If the GSP has manually overridden the LSP validation, the LSP is not checked. The IPMS will update the Ported Number Register with the correct LSP.

- 210. The Port Request is flagged as being either approved or rejected.
- 211. The Port Request status will be visible on the Port Request queue for both the LSP and GSP.

PR8T. IPMS Logs Port Request Rejection

- 212. The IPMS logs the rejected Port Requests.
- 213. The formal process for a rejected Port Request finishes at this point.

PR9. The Port Request is Added to the Approved Queue

- 214. The Approved Port Requests are presented in this queue to both the Gaining Carrier(s) and Losing Carrier(s).
- 215. The Approved Port Change process handles any changes required beyond this point.
- 216. The Port Request Process is complete at this point.

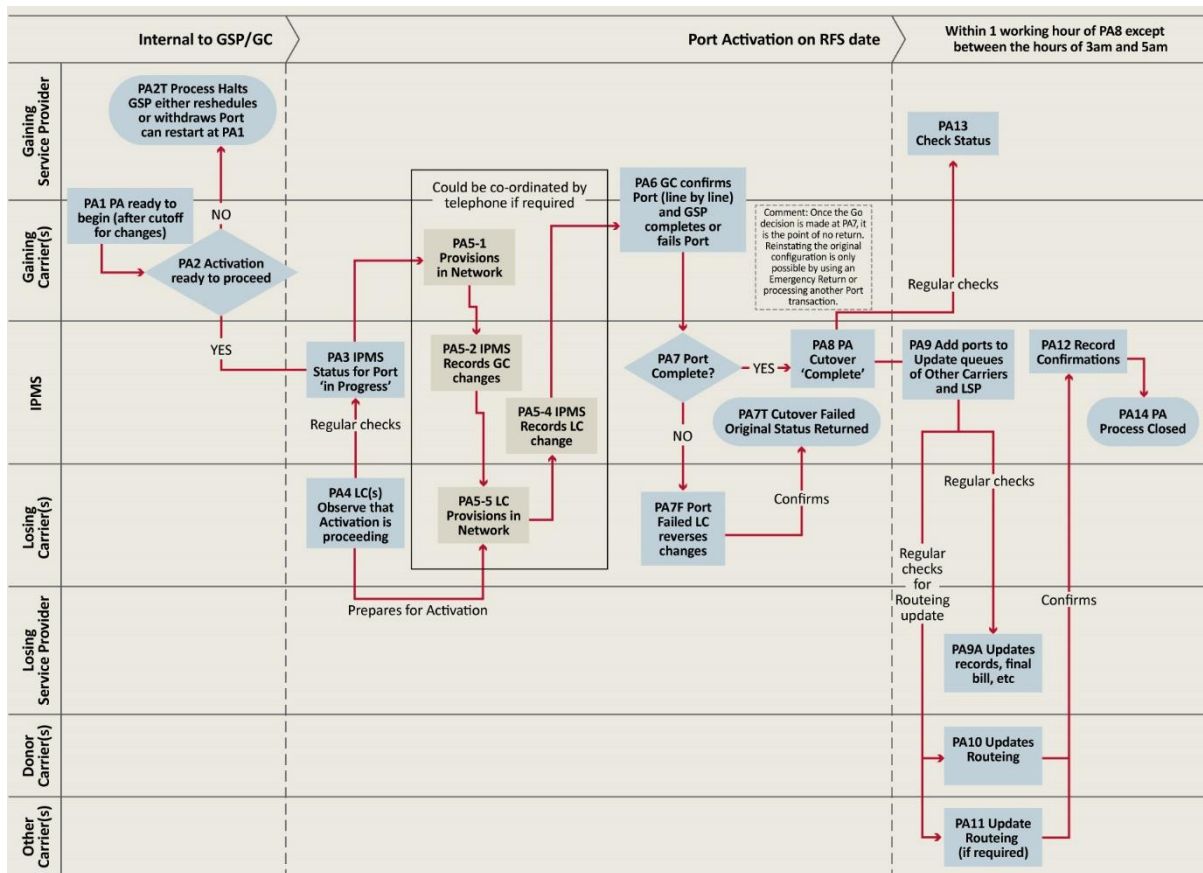
PR10-11. Approved Ports Can be Reviewed by all Interested Parties

- 217. Interested parties are able to review all outstanding Approved Port Requests. The interested parties are the Gaining Carrier(s), GSP, Losing Carrier(s), LSP.
- 218. The Gaining Carrier(s) and Losing Carrier(s) are required to use this queue to ensure they are prepared for all impending Ports.

Port Activation Process

- 219. The Port Activation Process is used to implement a Port that has been already approved.
- 220. The order of Network updates will vary depending upon the process. The LSP and GSP will be the primary coordinators of the Porting Process. In some cases, the Donor Carrier will be a third-party and will need to be notified. Other Carriers will be notified when it is appropriate for them to re-route calls.

Port Activation Process Flowchart



Port Activation Process Timing Table

Flowchart	Port Activation Process	Response Times		
		Simple Local Port	Complex Local/Mobile Port	Simple Mobile Port
PA3 to PA7	Port Complete	Within 5 Working Hours of PA3 (Being 4 Working Hours for GSP actions and 1 Working Hour for LC action)	Within 8 Working Hours of PA3 (Being 4 Working Hours for GSP actions and 4 Working Hours for LC action)	Within 40 Working Minutes of PA3 (Being 30 Working Minutes for GSP actions and 10 Working Minutes for LC action)

Flowchart	Port Activation Process	Response Times		
		Simple Local Port	Complex Local/Mobile Port	Simple Mobile Port
PA12	Confirm Network Update	Within 1 Working Hour of PA8 except during a planned outage to the extent that planned outage occurs during the hours set out at paragraph 102	Within 1 Working Hour of PA8 except during a planned outage to the extent that planned outage occurs during the hours set out at paragraph 102	Within 1 Working Hour of PA8 except during a planned outage to the extent that planned outage occurs during the hours set out at paragraph 102

Note: Where the above Table refers to the GSP, it is acknowledged that the GSP actions include the GC actions.

Changes to the RFS Date

221. All parties have the right to change the RFS Date after approval of the Port Request and before Port Activation, within the prescribed window. This is addressed in the Approved Port Change section.

PA1. GSP Ready to Begin

222. The GSP communicates with the Gaining Carrier(s) to establish whether or not they are ready to proceed. This should be timed to enable completion on the RFS Date.

PA2. GSP Decides whether they are Ready for Port Activation

223. The GSP will make an entry in the IPMS to either reschedule the Port or proceed.
224. This will be done within the RFS Date window.

PA2T. GSP Halts Port Activation

225. The GSP will either use the Port Withdrawal Process or the Approved Port Change process at this point.

PA3. The IPMS Changes the Port Status to "In Progress"

226. This information will update the queue for both the Gaining Carrier and Losing Carrier.

PA4. Losing Carriers Observe that Port Activation is proceeding

227. The Losing Carrier(s) needs to regularly review the Port Activation queue to ensure that they are ready for all Ports to proceed.
228. The Losing Carrier(s) prepare for the Port Activation.

PA5. Closely Co-ordinated Port Activation

- 229. Port Activation is a time-sensitive process that requires close coordination between the Gaining Carrier(s), the Contractor, and the Losing Carrier(s).
- 230. There are three key aspects to the Port Activation:
 - 230.1 PA5-1. The Technician/Contractor cuts over the Customer to connections of the Gaining Carrier(s) whilst the Gaining Carrier(s) provision the routing changes in their Network(s);
 - 230.2 PA5-2. The Gaining Carrier(s) update the IPMS and confirm that the change has been made and that they should activate the changes in their Network;
 - 230.3 PA5-3. The Losing Carrier(s) are notified by the IPMS and make the changes in their Network; and
 - 230.4 PA5-4. The Losing Carrier(s) update the IPMS by confirming that their provisioning is complete.
 - 230.5 The Gaining Carrier(s) are entitled to contact the Losing Carrier(s) by telephone and ensure that they are aware of the change and can await verbal confirmation that the change has taken place.
- 231. Once these steps are complete, the Gaining Carrier(s) performs a test and either:
 - 231.1 Confirms each Number is “Tested and Complete”; or
 - 231.2 Confirms one or more Numbers have failed and need to be “Reversed” and instructs the Losing Carrier and the on-site technician to return the configuration to that pre-Port state.
- 232. A Port can be cancelled at any point where it is agreed by the Gaining Carrier and the Losing Carrier that there is less work to reverse existing changes than complete the process and then Port back to the LSP. The decision as to which approach should be taken should be agreed between the parties (with input from GSP as appropriate).
- 233. The process then continues at step PA6.

PA6. Confirmation that the Port is Complete

- 234. If the Port is completed in PA5, the GSP marks the Port Activation as “complete” in the IPMS.
- 235. If the Port is not completed in PA5, the GSP marks the Port Activation as “failed” and the Port Request re-enters the queue for re-scheduling and Port Activation.
- 236. The Gaining Carrier can select a partial Port Activation if some lines were not Ported in a multiple line Port. The Gaining Carrier must co-ordinate this with the Losing Carrier to ensure consistent routing for all affected Numbers.

PA7. The IPMS records the Port as Complete or Failed

- 237. If none of the Numbers are successfully Ported, the Port fails and the process terminates at step PA7T.
- 238. The IPMS notifies the Losing Carrier of work they need to reverse if the Port fails, in step PA7F.

PA7F. The Losing Carrier Reverses the Failed Port

- 239. The Losing Carrier reverses the Port, returning all Ported Numbers to their pre-Port state.
- 240. Once the work is complete, the Losing Carrier confirms the action in the IPMS.
- 241. The process is then complete at step PA7T.
- 242. The GSP must then either reschedule using the Approved Port Change process or withdraw using the Port Withdrawal Process.

PA7T. The Original Status is Restored

- 243. In respect of a failed Port, the Numbers to be Ported are restored in the IPMS to their original pre-Port state.

PA8. The Port Cutover is Complete

- 244. If the Port is completed, the Port Activation is marked as completed.
- 245. The GSP can observe that the Port Activation is complete.

PA9. IPMS Adds Ports to Update Queues of Other Carriers and of LSP

- 246. At this point, notice of the Port Activation is available to all other interested parties.

PA9A. The LSP Updates Their Records

- 247. The LSP has a number of tasks to perform.
- 248. The LSP's involvement in the process is complete.

PA10. The Donor Carrier Routing Update

- 249. This may be an addition, a removal or a change, depending on whether the Donor Carrier is a Losing Carrier, Gaining Carrier, or Other Carrier.
- 250. The IPMS will not notify the Donor Carrier if they are also a Losing Carrier or Gaining Carrier in the Port Activation.
- 251. The Donor Carrier will update their Network Routing and confirm with the IPMS.

PA11. Other Carriers update their records

- 252. If required for their routing, Other Carriers will update their routing tables from their IPMS Update queue on a regular basis.

253. If they do update their routing, they need to inform the IPMS when it is completed.

PA12. The IPMS receives notification of Routing Updates

254. The IPMS records the network update confirmations of all Other Carriers (being neither a Gaining Carrier nor Losing Carrier).
255. The Gaining Carrier(s) have the right to view the progress of a Port Activation and observe which Carriers have completed the updates.
256. When all required updates are confirmed, the Port Activation Process is completed.

PA13. GSP Notified of Port Activation Result

257. The GSP will be able to observe the result of the Port Activation and take appropriate action.
258. Steps taken to resolve any issue are outside the scope of this process.
259. Restarting this process to activate the same Port relies on the GSP and the LSP agreeing a new RFS Date once the problems have been resolved.
260. The Port could be withdrawn as a result of a failed Port Activation.

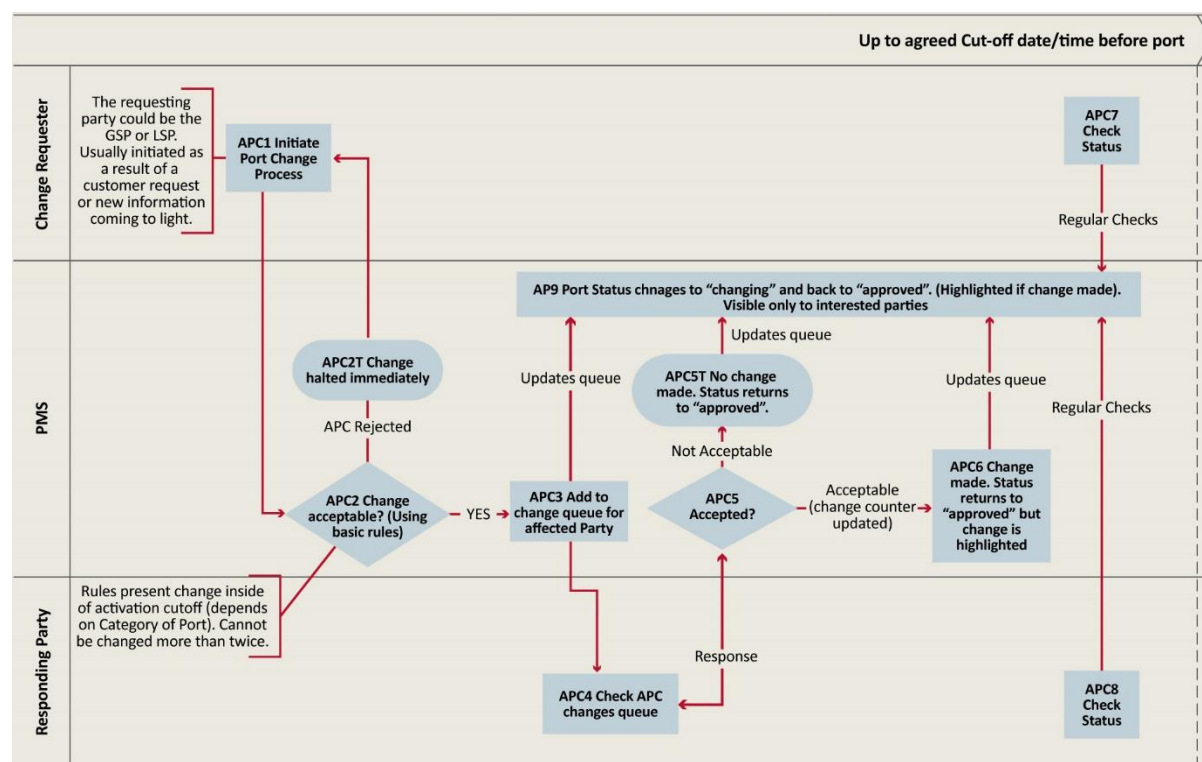
PA14. The IPMS Closes the Port Activation

261. Once all updates are confirmed the Port Activation is closed. No further changes are possible without a new Port Request.

Approved Port Change

262. The Approved Port Change (APC) Process allows the GSP or LSP to request a change to the details of an Approved Port. It may be used to change an Approved Port before the RFS Date, after the RFS Date has been missed, or after a Port failed to be completed.

Approved Port Change Process Flowchart



Approved Port Change Process Timing Table

Flowchart	APC Process	Response Times		
		Simple Local Port	Complex Local/Mobile Port	Simple Mobile Port
APC3 to APC5	Responding Party checks change queue and responds	Two Working Hours	Four Working Hours	Two Working Hours
		Frequency		
APC7 and APC8	Gaining Carrier(s) and Losing Carrier(s) should review this queue regularly	Every Working Hour	Every Two Working Hours	Every Working Hour

APC1. Change Requester Initiates APC Process

263. The Change Requester may be the GSP or the LSP. The Gaining Carrier or Losing Carrier must liaise with the relevant Service Provider in relation to any change identified as they may not be the only Gaining Carrier or Losing Carrier.
264. An Approved Port Change may be requested as the result of:
- 264.1 a request by a Customer;
 - 264.2 by the GSP or LSP following the discovery of pertinent information that is required for the Port Activation to be carried out successfully;

264.3 by the GSP, after reaching point PA2T; or

264.4 by the GSP or LSP after reaching point PA7T in a Port Activation.

265. APC changes will be limited to moving the RFS Date and changes to the Numbers involved in a given Approved Port.

266. Parties must use the APC process in good faith and not to enable Ports to be scheduled at times outside the proposed RFS Date range.

APC2. IPMS Checks that the Change is Acceptable

267. An Approved Port Change is not possible once a Port is expired or withdrawn.

268. The Approved Port Change may not be used more than the number of times defined in the Operational and Support Manual for LMNP on a Port.

269. The IPMS will check that the changes to Numbers pass the tests used in the Port Request Process. It will reject a change on a Port whilst a change is already in progress.

APC2T. IPMS Aborts the Change

270. If the APC fails the tests, the Change Requester is immediately informed.

APC3. IPMS Queues the APC Request

271. If the APC passes the tests, the IPMS adds the request to the change queue of the responding party.

APC4. Responding Party Checks their APC Request Queue

272. Each party to the LMNP Terms is required to regularly check this queue.

273. The responding party should respond to requests in good faith, bearing in mind that the requesting party should only be asking for change when there is a genuine need.

274. The respondent has the ability to accept a change that does not comply with normal RFS Date notice periods, but only if they can reschedule resource to allow them to comply.

275. The responding party may use a Co-operative Period to communicate with the requesting party at this stage.

APC5. IPMS Receives Response

276. The IPMS will change the status of the APC request to either “accepted” or “rejected”.

APC5T. IPMS Updates the APC Queue with a Rejection

277. The IPMS will flag the APC request as being rejected.

278. The change will be visible in the queue to the requesting party.

APC6. IPMS Updates the APC Queue with an Acceptance

279. The IPMS will change the status of the APC request to “accepted”.

280. It will then update the details in the Approved Port Requests queue, as appropriate with new RFS Date or change to the Numbers.

281. The change will be highlighted to ensure that the responding party is notified to update their works order.

APC7. The Change Requester Checks the IPMS APC Queue for Acceptance

282. The Change Requester must then reschedule any work required for the Port Activation to take place.

APC8. The Responding Party Checks the IPMS APC Queue for Changes

283. The responding party should already be aware of any APCs that it accepted.

284. All parties must monitor this queue for changes.

285. All parties must update their records as per the details in the Approved Port Requests queue as required.

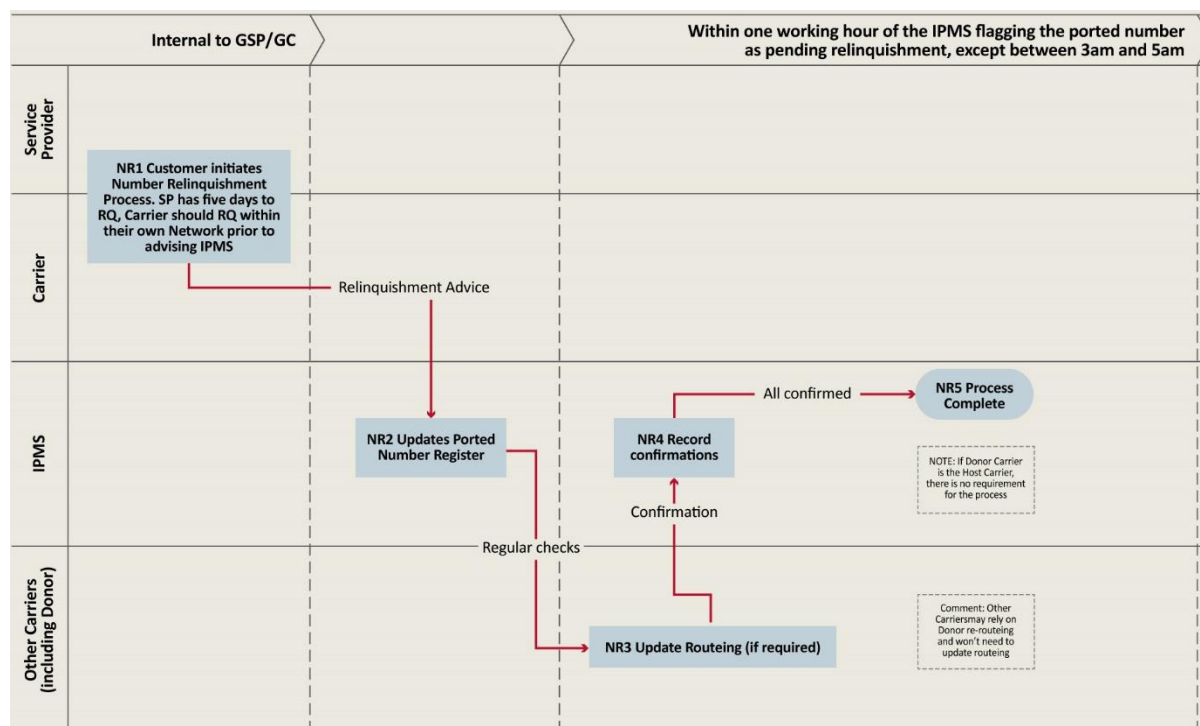
APC9. The IPMS Continually Updates the Approved Port Queue

286. Any interested Carrier or Service Provider can review this queue at any time and observe those approved Ports that are subject to change and those that have changed.

Ported Number Relinquishment Process

287. The Ported Number Relinquishment (NR) Process is used when a Customer relinquishes a Ported Number. The Ported Number Relinquishment Process is not required if the Host Carrier is the Donor Carrier (as the Number is not considered to be Ported, even if it has been Ported out and back again).

Ported Number Relinquishment Process Flowchart



Ported Number Relinquishment Process Timing Table

Flowchart	Ported Number Relinquishment Process	All Relinquishments
NR2	Notification to IPMS that the Ported Number has been relinquished.	Within five Business Days of Customer initiating Ported Number Relinquishment Process.
NR2 to NR4	Donor Carrier and Other Carriers (if required) update routing.	Within one Working Hour of the IPMS flagging the Ported Number as pending relinquishment, except during a planned outage to the extent that planned outage occurs during the hours set out in paragraph 102.

288. The Service Levels for notification to IPMS that the Ported Number has been relinquished cannot be measured in IPMS.

NR1. The Customer Notifies their Service Provider of the Relinquishment

- 289. For a Ported Number, the Service Provider shall follow their standard procedure as for relinquishment of a non-Ported Number. For a Ported Number, the Service Provider must initiate the Ported Number Relinquishment Process within five Business Days of the Customer relinquishing the Number.
- 290. The Service Provider should not relinquish a Number that is part of a Number Block.
- 291. If all the Numbers in a given Number Block are being relinquished at the same time, or the last Numbers that are in use in a given Number Block are relinquished, then the Ported Number Relinquishment Process applies.
- 292. The Carrier checks that the Numbers are not part of a Number Block that needs to be kept intact, as per paragraphs 290 and 291.
- 293. The Carrier provisions the relinquishment in their Network.
- 294. The Carrier then sends a relinquishment advice to the IPMS.

NR2. The IPMS updates the Ported Number Register

- 295. The IPMS flags the Ported Number as pending relinquishment.
- 296. At this point, the Ported Number cannot be Ported and any Port Request will be rejected as it is pending relinquishment. During the 30-day quarantine period (see Number Quarantine section), the Service Provider who initiated the Ported Number Relinquishment Process may wish to cancel the relinquishment if it was made in error or the Customer has changed their mind.
- 297. After 30 calendar days from the date of the relinquishment advice, the IPMS will flag the Ported Number as relinquished and will allow step NR3 to commence.

NR3. Other Carriers Update Routing

- 298. The Donor Carrier must update their Network Routing to reflect this change.
- 299. If it is their policy to do so, the Other Carriers should remove the relinquished Number from their routing tables. Carriers that rely on donor network re-routing do not need to follow steps NR3 and NR4.
- 300. The Donor Carrier is able to allocate the relinquished Numbers to another Customer once this process is complete.
- 301. When complete, they send confirmation of updated routing information to the IPMS.

NR4. IPMS Records the Confirmations

- 302. The IPMS updates the Ported Number Register as it receives notification of updates.
- 303. A live version of this information is available in the enquiry screen for all Carriers.

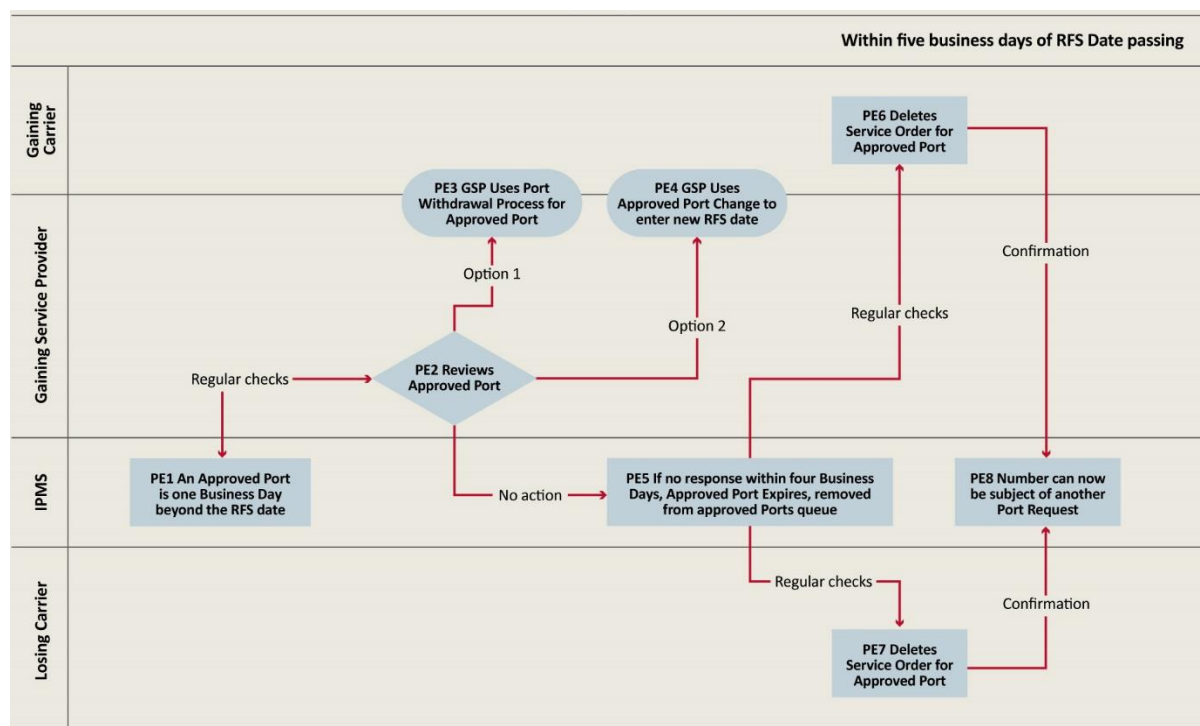
NR5. Number Relinquishment Process Complete

304. The Number is no longer considered to be a Ported Number.
305. The Donor Carrier is now able to allocate the Number, subject to the Number Quarantine section.
306. If the Donor Carrier is the Host Carrier, there is no requirement for this Ported Number Relinquishment Process.

Port Expiry Process

307. The Port Expiry (PE) Process occurs when an accepted Port Request has not been activated within the RFS Date. The IPMS will run the Port Expiry Process at midnight on each Business Day.

Port Expiry Process Flowchart



Port Expiry Process Timing Table

Flowchart	Port Expiry Process	Response Times
Entire Port Expiry Process		Within five Business Days of RFS Date.
PE5 to PE8	Gaining Carrier and Losing Carrier confirming expiry.	Within four Working Hours.

308. These Service Levels are not measured in IPMS.

PE1. The IPMS Identifies Expired Port

- 309. The IPMS identifies an Approved Port that has lapsed one Business Day beyond the due RFS Date.
- 310. The IPMS notifies the GSP that an Approved Port is about to expire and requires action.

PE2. GSP Checks the Expiry Notification

- 311. The GSP has four Business Days to consult with the Customer to confirm the Customer preference if not already known.
- 312. The GSP has three courses of action open to it. It may use the Port Withdrawal to withdraw the Approved Port, it may use the Approved Port Change to reschedule the Port, or it may choose to do nothing.

PE3. The GSP Withdraws the Approved Port

- 313. The GSP can use the Port Withdrawal Process to withdraw the Approved Port if the Port is not going to be rescheduled.

PE4. The GSP Reschedules the Approved Port

- 314. The GSP can use the Approved Port Change process to reschedule the Port.

PE5. The IPMS Records the Approved Port as Expired

- 315. If there is no response from the GSP within four Business Days, the IPMS will mark the Approved Port as expired.
- 316. The Approved Port is marked as “expired” in the approved Ports queue for both the Gaining Carrier and Losing Carrier.

PE6. Gaining Carrier Notifies the IPMS of Update

- 317. The Gaining Carrier observes the change in the approved Ports queue.
- 318. The Gaining Carrier confirms that they have deleted the works order for the Approved Port from their internal update queue.

PE7. Losing Carrier Notifies the IPMS of Update

- 319. The Losing Carrier observes the change in the approved Ports queue.
- 320. The Losing Carrier confirms that they have deleted the service order for the Approved Port from their internal update queue.

PE8. Port Expiry Process Complete

- 321. The IPMS marks the Port Expiry Process as complete.
- 322. The GSP is able to resubmit a new Port Request if required.

- 327. The GSP must inform the Customer of any charges that may be incurred due to Port Withdrawal.
- 328. The Gaining Carrier looks up the SOM Number, verifies that the details are correct, and deletes their internal works order.
- 329. Removing the internal works order ensures that the Port will not be implemented.
- 330. The GSP then notifies the IPMS that the Port is withdrawn.

PW3. IPMS notifies the Losing Carrier of Withdrawal

- 331. The IPMS changes the Approved Port to “withdrawn” and removes it from the approved Ports queue for the Losing Carrier.
- 332. IPMS checks that Port Withdrawal is possible. It will not allow withdrawal of a Port that is in the process of being activated.

PW4. Losing Carrier Deletes Internal Works Order

- 333. The Losing Carrier deletes the works order within their system.
- 334. They confirm the deletion on the IPMS.

PW5. IPMS Records the Port Withdrawal is Complete

- 335. A new Port Request can now be processed for that Number.
- 336. Should the GSP wish to pursue the Port, it can approach the Customer and resubmit a Port Request.

Number Quarantine

- 337. The IPMS will hold relinquished Numbers in quarantine for 30 calendar days prior to notifying Other Carriers of the relinquishment. After this period the Donor Carrier may further quarantine the Number in accordance with their existing practices.
- 338. During the quarantine period the Service Provider who initiated the Ported Number Relinquishment Process may wish to cancel the relinquishment if it was made in error or the Customer has changed their mind.
- 339. In addition, there are circumstances where the relinquishment needs to be expedited so as to reduce or remove the 30 calendar day requirement. A reduction or removal of the 30 calendar day requirement may be made by mutual agreement between the Donor Carrier and the Service Provider who wishes to initiate the Ported Number Relinquishment Process.
- 340. If a Customer requests a recently relinquished Ported Number, the Service Provider is entitled to warn the Customer of the recent relinquishment of the Number and the implications of using such a Number before they allocate the Number.

IPMS Capabilities

Basic Methodologies

- 341. The same messaging transport and package method will be used for all Local and Mobile Porting messages but there will be some differences:
 - 341.1 Some elements of given messages will differ between message types;
 - 341.2 Some elements of given messages will differ between classes of messages;
 - 341.3 Rules for turnaround will vary;
 - 341.4 Rules for validation will vary; and
 - 341.5 The IPMS will need to take these differences into account.

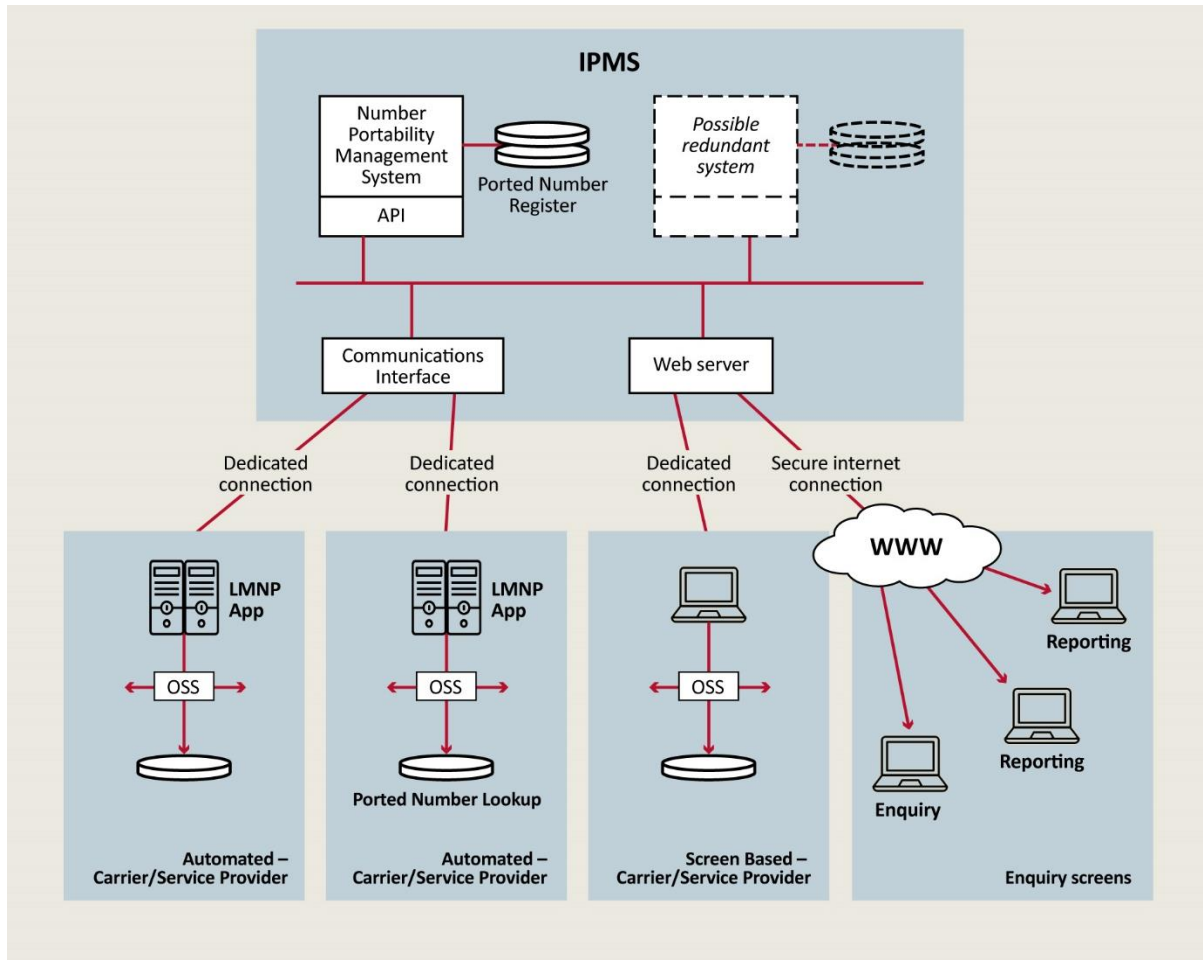
Technology Specifications

- 342. This section sets out the required functions of the IPMS.

Architecture

- 343. The IPMS is a centralised system, the role of which is to provide reliable message transport, process tracking, coordination, and management. It is a tool, which will facilitate LMNP but relies on the Networks being able to support portability. The IPMS will not handle call routing but will be the sole authority on all Ported Numbers. This will be used by Carriers to update their own Networks.

Architecture overview of the IPMS:



344. The architecture is based around a logically centralised IPMS node. Physically this may be mirrored to achieve the required Service Levels.
345. The IPMS provides transaction processing logic to manage the Porting Process. Management of the Porting Process involves the IPMS maintaining a database of Ported Numbers (the Ported Number Register). All Carriers synchronise their Ported Number lookup tables with the IPMS. Typical information in the IPMS will include:
 - 345.1 Number and current Service Provider;
 - 345.2 Status of Numbers and when service is to be implemented;
 - 345.3 Tasks that are still to be completed and by what Service Providers.
346. All Service Providers shall access the IPMS via an IPMS API. All the participants in LMNP shall achieve rapid and reliable communication of their requests and responses from the IPMS.

347. Basic API functionality requires:
- 347.1 The ability to accept requests to perform a function, for example processing a Port Request;
 - 347.2 The ability to notify a Service Provider automatically to do something, for example the notification of a Port Activation; and
 - 347.3 Allowing a Service Provider system to monitor transaction queues for messages, and then respond to them with the appropriate result.
348. In the case of automated access, there is a direct interface with the API. A web server is to be available to allow Service Providers and Carriers to perform Port-related functions manually, as well as generate queries and reports. The web server must also use the API to interface with the IPMS.
349. The API will be a “black box system”, meaning Service Providers and Carriers would only know the interface and messaging specifications. They will not require awareness of how the API communicates to the IPMS.

System Interface

350. The IPMS interface will be standardised to ensure ease of communication. It is likely to be based around some form of XML messaging. The IPMS will be able to communicate with parties via a web browser front-end or a machine-to-machine interface.
351. All the logic and business rules will be in a common layer in the IPMS. This will ensure that the same rules are used for all communication with the parties.
352. The IPMS User Guide may include detailed screen layouts and specifications for all aspects of web browser screen design.

Connection Methods

353. The type of connection between each party and the IPMS must meet basic standards for speed, security, and reliability.
354. Each party will access the IPMS by dedicated private communications connection or secure internet connection. If parties wish to use a VPN, this will need to be acceptable to all parties, to ensure system security and integrity.
355. Connections to the IPMS must be protected by software encryption/authentication protocols such as SSL and HTTPS.

Queues

356. The IPMS will use a set of transaction queues to facilitate the management of outstanding Port Events. The contents of these queues and associated screens shall be described in the IPMS User Guide.

357. Their usage will vary between those parties using a web client and those using a machine-to-machine connection.

System Response Times

358. Most processes will require some immediate feedback in terms of basic checking or presentation of information to the user. Such on-line interactive use will be supported by short response times. Under normal system load, an interactive processing request is intended to be responded to in less than one second.
359. The response time will depend on the connection method used by an individual party, as well as the performance of the IPMS. Performance will be measured as the elapsed time for the IPMS to queue a response to the router at the central site. Any further network latency introduced due to the capacity of the network connection or Client LAN will be the responsibility of the organisation.

Reliability

360. The reliability targets for the IPMS are:
- 360.1 It should be available for transmitting messages 99% of the time on a 24 hour by 7 day a week basis, except for scheduled maintenance periods;
 - 360.2 It should not be unavailable for more than four contiguous Working Hours; and
 - 360.3 There will be no provision for a formal or structured fallback procedure for when the IPMS is down. It is expected that all Porting activity will halt during an outage. In such a situation, calls to Ported Numbers are not impacted.

Users and Security

361. A record must be created in the database for each user who has access to the IPMS. All transactions and responses made will be tracked and logged by user. User access controls will ensure that users are confined to the parts of the IPMS demanded by their role.
362. Processes will be available to enable user records to be maintained, along with security access and user preference options.
363. Parties to the LMNP Terms that use a machine-to-machine connection may use only a limited number of users, as few as one. They are expected to track their own user activity within their system and may be required to do so if investigation of a given event is required.
364. Security access and user preference/default values will be held in user profile records. Groups of users within each party to the LMNP Terms who have common access requirements will share a common user profile. That will simplify the process of maintaining access for a large number of users. A user administrator responsible for user access and preferences will be able to change the preferences for a group of

users by changing a single user profile record. Users will not have access to change their own user profile.

365. It will be possible to create, change and activate/deactivate user and user profile records. Those records may also be deleted, but only after all other references to the record have been removed from the database by archiving/ageing processes (to ensure data integrity).

Error Handling

366. The IPMS must endeavour to ensure that the processes are reliable and accurate. The following tools will be used to minimise and handle errors:

366.1 Logging of faults/abnormal events;

366.2 The ability to roll back and/or recover within the IPMS; and

366.3 Track process confirmations and acknowledgements.

Reporting and Data Extracts

367. A number of reports will be required to enable and manage the Porting Processes. The reports detailed here may be supplemented during the implementation of the IPMS.
368. The following reports will be produced by the IPMS on a regular basis, outside of Standard Hours of Operation. All reports will be available either in a form for viewing or in a standard format (such as comma separated value (CSV) format text files) for importing into other applications. Automated processes will generate the regular reports.
369. Reports with a limited number of pages may be viewed directly from the web browser interface. Longer reports may be required to be downloaded, before viewing, to minimise the impact on system performance.
370. Access to reports and data extracts will be controlled by parameters in the user profile.
371. The intention of the data extracts is to enable parties to the LMNP Terms to produce their own reports, in whatever format they prefer, involving any transactions to which they are a party.
372. Each IPMS user will have access to a data extract or report giving the details of any transaction performed by users belonging to their organisation.
373. Reports shall be generated for each of the following categories:
- 373.1 Ported Number Register activity logging, status and audit;
- 373.2 Service Level and activity monitoring of Service Providers and Carriers; and

373.3 Extracts for Directories and Emergency Services.

374. Further details of these reports shall be included in the IPMS User Guide.

Enquiry Screens

375. Enquiry functions must be provided in the IPMS to ensure that various participants have the necessary visibility of Port Requests, Ports and other Port-related events to allow them to respond to other parties' Ports and manage their own.

Archiving

376. Messages, logs, and histories must not be deleted and must be archived in a form that is readily accessible.

Migration

377. The IPMS shall have the capacity to migrate current Porting data onto the IPMS.

378. New parties will be able to follow a migration process to move onto the IPMS and take part in LMNP.

Data Integrity/Synchronisation

379. Where there is inconsistency between Carriers' data and the IPMS Ported Number Register, the IPMS will be considered to be the correct data. Carriers shall develop processes for using the reports specified in the LMNP Terms to verify their own routing tables and procedures for correcting them.

Appendix: Tables

Table 1: Port Request Fields

The following Table sets out a list of the required items to include in a Port Request, with their relevance to different types of Ports:

Field	Source	Local		Mobile	
		Simple	Complex	Pre-Pay	Post-Pay
SOM	Auto	Required	Required	Required	Required
Type of message	GSP	Required	Required	Required	Required
Category of message	GSP	Required	Required	Required	Required
Date of request	Auto	Required	Required	Required	Required
Time of request	Auto	Required	Required	Required	Required
Account Number	Customer	Required	Required	N/A	Required
Handset Reference	Customer	N/A	N/A	Required	N/A
Phone number	Customer	Required	Required	Required	Required
GSP	Auto	Required	Required	Required	Required
Losing Service Provider	Customer	Required	Required	Required	Required
Gaining Carrier	GSP	Required	Required	Required	Required
RFS Date	Customer	Required	Required	Required	Required
Customer name	Customer	Required	Required	Required	Required
Customer service address	Customer	Optional	Optional	N/A	N/A
Customer contact number	Customer	Optional	Optional	N/A	N/A
Losing Carrier	Auto	Required	Required	Required	Required

“Type of message” refers to whether it is a Port, APC, Port Withdrawal, Port Expiry, or Ported Number Relinquishment.

“Category of message” refers to whether it is a simple local, simple mobile, complex local, or complex mobile.

“Gaining Carrier” is completed by the GSP.

“Losing Carrier” is completed by the IPMS.

“Handset Reference” is required for Pre-Pay.

“Pre-Pay” or “Post-Pay” is at the time of the Port Request, not what the Customer intends to be with the new Service Provider.

Some fields will be inserted into the request by the IPMS – specifically the SOM Number, date of request, and time of request.

380. Other Transaction Fields:

380.1 These have yet to be defined in detail, but it is expected that most other messages will consist of date, time, SOM Number, and message type.

Table 2: Service Levels

The Table below sets out the Service Level for given steps in the Porting Processes.

Party	Process	Action	Local		Mobile	
			Simple	Complex	Simple Pre-Pay or Post-Pay	Complex Post-Pay
LSP	Port Request	Responds to Port Request (PR4 to PR6)	Within four Working Hours	Within two Business Days	Within 30 Working Minutes	Within two Business Days
GSP	Port Request	Reviews LSP response and Approves/Rejects (PR6 to PR8)	Within four Working Hours	Within two Business Days	Within 30 Working Minutes	Within two Business Days
GSP	Port Activation	Port as GSP/GC (PA3 to PA5-2 and PA5-4 to PA7)	Within four Working Hours	Within four Working Hours	Within one Working Hour	Within four Working Hours
Losing Carrier	Port Activation	Port as Losing Carrier (PA5-3 to PA5-4)	Within one Working Hour	Within four Working Hours	Within ten Working Minutes	Within four Working Hours
Other Carrier and Donor Carrier	Port Activation	Port as 3rd party and Donor Carrier (if required PA8 to PA12)	Within one Working Hour except during a planned outage to the extent that planned outage occurs during the hours set out at paragraph 102	Within one Working Hour except during a planned outage to the extent that planned outage occurs during the hours set out at paragraph 102	Within one Working Hour except during a planned outage to the extent that planned outage occurs during the hours set out at paragraph 102	Within one Working Hour except during a planned outage to the extent that planned outage occurs during the hours set out at paragraph 102

Responding Party (GSP or LSP)	Approved Port Change	APC Response to request (APC3 to APC5)	Within two Working Hours	Within four Working Hours	Within two Working Hours	Within four Working Hours
Gaining Carrier and Losing Carrier	Approved Port Change	APC update service orders from APC changes (APC7 and APC8)	Every Working Hour	Every two Working Hours	Every Working Hour	Every two Working Hours
Host Carrier	Ported Number Relinquishment	Relinquishment of Ported Number (NR2)	Within five Business Days	Within five Business Days	Within five Business Days	Within five Business Days
Other Carrier and Donor Carrier	Ported Number Relinquishment	Relinquishment as 3rd party and Donor Carrier (if required NR2 to NR4)	Within one Working Hour except during a planned outage to the extent that planned outage occurs during the hours set out at paragraph 102	Within one Working Hour except during a planned outage to the extent that planned outage occurs during the hours set out at paragraph 102	Within one Working Hour except during a planned outage to the extent that planned outage occurs during the hours set out at paragraph 102	Within one Working Hour except during a planned outage to the extent that planned outage occurs during the hours set out at paragraph 102
Gaining Carrier and Losing Carrier	Port Expiry	Confirmation of service order deletion for Port Expiry (PE5 to PE8)	Within four Working Hours	Within four Working Hours	Within four Working Hours	Within four Working Hours
GSP	Port Withdrawal	Port Withdrawal (entire process)	Within four Working Hours	Within four Working Hours	Within four Working Hours	Within four Working Hours
Losing Carrier	Port Withdrawal	Confirming Port Withdrawal (PW3 to PW5)	Within two Working Hours	Within two Working Hours	Within two Working Hours	Within two Working Hours

381. Where the SOM count per Service Provider or Carrier is:

381.1 more than 40 for Mobile Numbers or Local Numbers in a calendar month.
(Parties are expected to meet these Service Levels 95% of the time);

381.2 40 or less for Mobile Numbers or Local Numbers in a calendar month. Parties are expected to have no more than 2 failures. The Enforcement Agency has discretion to investigate cases where a party regularly fails to meet a Service Level on 2 occasions per calendar month and, in the Enforcement Agency's view it appears to be a systemic issue.

382. The measurement of the achievement of the Service Levels for Local and Mobile SOMs in each case includes the combined results for Simple and Complex Ports.

Table 3: RFS Date Minimum and Maximum Notice Periods

	Minimum	Maximum
Local Number Ports:		
Simple Ports	Two Business Days	30 calendar days
Complex Ports	Five Business Days	30 calendar days
Mobile Number Ports:		
Simple Ports	One hour	30 calendar days
Complex Ports	Five Business Days	30 calendar days

Table 4: Port Request Tests*Initial IPMS Port Request Tests:*

383. Actions performed on Port Request in initial IPMS check at PR3 and repeated in PR6 and PR8.

Field	Test
SOM	Not checked but must be present.
Type of Message	Must be valid type, rules are enforced based on type.
Category of Message	Checks that the Port Request is correctly categorised as Local or Mobile, Simple or Complex.
Date of request	Not checked but must be present (automatically inserted in web client).
Time of request	Not checked but must be present (automatically inserted in web client).
Account Number	If not Pre-Pay, checks for the presence of an account number that meets the account number length test.
Handset reference	If Pre-Pay, checks for the presence of a handset reference number that meets the handset reference number length test.
Phone number	Checks the presence of valid Numbers, based on the Message category and prefix and number length rules. Checks Number is not the subject of an outstanding Port Request or Approved Port.
GSP	Could be checked but should be inserted automatically.
Losing Service Provider	Can check number in Ported Number Database, if not present can check if the Numbers are in the Number range of the Losing Service Provider.
Gaining Carrier	Check for completion with valid Gaining Carrier.
RFS Date	Check that it is in the proper window for the category of Message.
Customer name	No check.
Customer service address	No check.
Customer contact number	No check.
Losing Carrier	The IPMS can insert this based on Carrier Number ranges, or from the Ported Number Register.

Table 5: Checks Performed by the Losing Service Provider at Step PR5

384. This Table sets out the mandatory checks to be performed by the LSP at step PR5 and it gives examples of other information that may be provided to the LSP and checks may be performed by the LSP. This may be supplemented, but not derogated from, by agreement among Carriers and Service Providers.

Field	Description
SOM Number	No check.
Type of Message	No check.
Category of Message	Mandatory - LSP must confirm that they agree, shall only disagree if they consider the Port to be Complex when the GSP has nominated Simple.
Date of request	No check.
Time of request	No check.
Account Number	Mandatory - for non-Pre-Pay, checks that the account number is valid and checks the Numbers are allocated to this account.
Handset Reference	Mandatory - for Pre-Pay, checks that the Handset reference is valid and checks the Number is allocated to this reference.
Phone Number	Mandatory - see Account Number/Handset Reference above.
Gaining Service Provider	Mandatory - allows the LSP to contact the GSP if required during the Co-operative Period.
Losing Service Provider	Mandatory - the LSP checks that this is their Number above.
Gaining Carrier	Not presented to the LSP.
RFS Date	Presented to the LSP for reference but not subject to checking, already validated by IPMS.
Customer name	If completed by GSP – it will be presented to the LSP. It can be used to help ensure the details are correct.
Customer service address	If completed by GSP – it will be presented to the LSP. It can be used to help ensure the details are correct.
Customer contact number	If completed by GSP – it will be presented to the LSP. It can be used to help ensure the details are correct.
Losing Carrier	Presented to the LSP, no check required.