

Electricity Commission

Clearing manager

Draft

Non-functional specification

Version 2.2

July 2006

This document reflects the draft Electricity Governance Rules 2003 (Rules) as at December 2005. Subsequent rule changes and transitional requirements have yet to be included.

Contents

CONTENTS	2
REVISION HISTORY	4
NON-FUNCTIONAL SPECIFICATION	5
CLEARING MANAGER.....	5
1. APPLICATION ARCHITECTURE	5
1.1 INDUSTRY STANDARD	5
1.2 INDEPENDENT ENVIRONMENTS	5
1.3 CURRENT COMPONENTS.....	5
1.4 SCALEABILITY	ERROR! BOOKMARK NOT DEFINED.
1.5 UPGRADES	5
1.6 DATA-INTEGRITY MAINTENANCE	6
1.7 CONCURRENT USERS	6
1.8 SOFTWARE-LICENSING ARRANGEMENTS	6
2. INTEROPERABILITY.....	6
2.1 INTERFACES	6
2.2 OTHER TRANSFER MECHANISMS	6
3. SYSTEM AVAILABILITY	6
4. SERVICE LEVELS.....	7
4.1 TARGET LEVELS	7
4.2 MAINTENANCE	7
4.3 MONTHLY SERVICE-LEVEL REPORTING	7
5. RECOVERABILITY AND BUSINESS CONTINUITY	7
5.1 BACKUP.....	7
5.2 UP-TO-DATE PLAN	8
5.3 RECOVERY TIME.....	8
5.4 DISASTER RECOVERY	8
6. SECURITY AND CONFIDENTIALITY	8
6.1 USER ACCOUNTS	8
6.2 USER PRIVILEGES	8
6.3 SECURITY POLICY	8
6.4 LOGS.....	8
6.5 CONFIDENTIALITY.....	8
7. CAPACITY	9
7.1 CAPACITY PLANNING STRATEGY	9
7.2 MANAGEMENT UTILITIES	9
7.3 EXCESS VOLUMES.....	9
8. DATA-INTEGRITY AND ARCHIVE POLICY	9
8.1 DATA OWNERSHIP	9
8.2 HISTORY.....	9

9.	AUDIT TRAIL/TRACEABILITY	10
10.	HELP DESK	10
10.1	END-USER ASSISTANCE	10
10.2	FAULT MANAGEMENT	10
10.3	INCIDENT REGISTER.....	10
11.	CHANGE MANAGEMENT	10
12.	DEVELOPMENT METHODOLOGY	11
12.1	INDUSTRY STANDARD	11
12.2	FLEXIBILITY.....	11
13.	IMPLEMENTATION AND TRANSITION	11
13.1	IMPLEMENTATION PLAN.....	11
13.2	MIGRATION PLAN.....	11
13.3	HISTORICAL INFORMATION	11
14.	USER LIAISON	11
14.1	CLOSE CONTACT	11
14.2	DATA AUTOMATION.....	12
14.3	NOTIFICATION CHANNELS	12
14.4	ESCALATION PROCESS	12
14.5	DAILY LIAISON.....	12
14.6	USER-SATISFACTION SURVEY	12
15.	TRAINING	12
16.	DOCUMENTATION	12
17.	SYSTEM AUDITS	13
17.1	SPOT AUDITS	13
17.2	AUDIT RECOMMENDATIONS	13
17.3	ANNUAL AND CHANGE AUDITS	13

Revision history

Version	Release Date	Description
Draft 1	April 2005	Initial version for discussion by Senior Adviser Wholesale.
Draft 2.2	July 2006	Updated with after comments received from other project groups reviewing their own non functional specifications.

Non-functional specification

Clearing manager

1. Application architecture

1.1 Industry standard

The system must be built on an industry standard, robust architecture that is reliable and scalable in the following areas:

- a) hardware infrastructure;
- b) operating system;
- c) network topology;
- d) application software;
- e) database;
- f) security;
- g) systems deployment and management; and
- h) external security, firewalls, virus protection etc.

1.2 Independent environments

There must be separate and independent environments for production, user acceptance testing and development.

1.3 Current components

The architecture should not contain any components that are no longer supported.

1.4 Scalability

The architecture should be easily scalable to accommodate a 10 per cent growth in users and transactions per annum, without significantly affecting performance and reliability.

1.5 Upgrades

There must be agreed procedures in place for the implementation of upgrades to hardware and software. All upgrades must be carefully planned, scheduled, notified to all relevant parties well in advance and implemented efficiently at times that cause minimum disruption to users. The timetable for the implementation of all upgrades should be approved by the Commission.

The vendor must implement all available, proven operating system, database and system software upgrades, in a timely manner.

1.6 Data-integrity maintenance

The vendor will be responsible for the maintenance of the data environment and must ensure that functionality is available within the application to reverse the effects of any material errors made by users in loading of the data via file transfer. The vendor must provide assistance to users in executing any such recovery.

The vendor must undertake the recovery (where possible) of any database integrity and corruption issues and correct any errors that occur as a result of the system incorrectly processing any information.

1.7 Concurrent users

The system must be designed to cope with at least 70 concurrent online users and the transaction volumes detailed in the appendix. A breakdown of the costs associated with concurrent usage numbers above 70 should be provided.

1.8 Software-licensing arrangements

The vendor should provide details and prices for a range of software licensing options that include, as a minimum:

- a) escrow arrangements;
- b) annual software license;
- c) perpetual software license; and
- d) purchase-of-source code.

2. Interoperability

2.1 Interfaces

Three types of interface should be provided.

- a) A web browser user-interface for viewing information online.
- b) As a minimum, a facility to transfer flat-files (CSV) via FTP, to handle multiple and/or batch updates and for downloading reports.
- c) System-to-system interfaces, which may be via direct database links or via flat files.

2.2 Other transfer mechanisms

The provision of interfaces using other mechanisms or formats that may have advantages over the above three interfaces should be considered and recommended if and where appropriate.

3. System availability

The system must be available, as a minimum, to end-users during business hours.

4. Service levels

4.1 Target levels

Measure	Target
Wash-up notifications distributed to parties by 5th business day of each month	92%
Invoices released by 6pm on 9th business day	92%
Constrained on/off amounts released to System Operator by 9am on 8th business day	92%
Amounts payable to payees sent through to the bank by 5:30pm on settlement day	92%
Number of invoice calculation errors	0%
Number of security level calculation errors	0%

The target level of 92 per cent relates to the equivalent of no more than one instance of missing the deadline within a twelve-month period. The zero percent standards indicate that the board expects there to be no calculation errors, in either invoices or the establishment of security levels.

4.2 Maintenance

The vendor must undertake all preventative, corrective maintenance and the implementation of enhancements outside business hours where possible.

For urgent corrective maintenance (to fix software faults that are threatening the service levels set out in this document), the vendor may, having notified the Commission, undertake maintenance at any time. Any such unavailability will count against service level targets.

4.3 Monthly service-level reporting

The vendor must provide the Commission a monthly report detailing whether service levels were met during the month and if not, reasons for any failure.

5. Recoverability and business continuity

5.1 Backup

Backup copies of data must be taken at least daily and stored in a secure location. The retention and recycle policy of backup media and the storage location must be agreed with the Commission. Likewise, copies of the latest version of the software should also be kept off-site. At least weekly, a backup copy of the data and software must be delivered and stored at an offsite

location at least 100 kms from the premises used to provide the regular service.

5.2 Up-to-date plan

The vendor must develop and keep up-to-date a disaster recovery plan as agreed with the Commission.

5.3 Recovery time

The disaster recovery plan must be designed to recover in the event the vendor's site (that contains the system) is destroyed by fire, earthquake or otherwise. Recovery is required of the system within 36 hours following a major disaster.

5.4 Disaster recovery

The vendor must test the disaster recovery procedure prior to the commencement of operation and every six months thereafter. The test must include:

- a) restoration of the system to the remote location;
- b) restoration and roll-forward to a known time; and
- c) verification of system availability to an external user.

6. Security and confidentiality

6.1 User accounts

The system shall have a framework for the management of user accounts.

6.2 User privileges

User privileges shall be able to control access at both function and specific data level.

6.3 Security policy

The system shall have a security policy in place and have mechanisms that enforce the password standard, account lockout for unsuccessful logon attempts, session timeouts. Session timeouts should be configurable per user.

6.4 Logs

The system should maintain logs of user interactions with the system and action all alerts of repeated unsuccessful logons to prevent hacking.

6.5 Confidentiality

The system must maintain the confidentiality of each participant's information by allowing requests only by parties that have been granted authority by

participants to access the system on their behalf by the exchange of digital certificates and/or password authentication.

7. Capacity

7.1 Capacity planning strategy

There should be a well-defined and documented capacity planning strategy in place.

7.2 Management utilities

There should be system management utilities implemented that will measure the capacity of the system, to show trends and, therefore, assist with predicting future capacity requirements.

7.3 Excess volumes

The vendor must promptly advise the Commission if increases in transactional volume beyond the levels agreed in the service provider contract threaten the achievement of service levels. The Commission and the vendor must promptly review the capacity of the system and increase its capacity, if necessary, to maintain the service levels.

If the service levels cannot be met with current levels of capacity, and transaction and/or database volumes are less than those agreed with the vendor, the vendor will be responsible for taking such remedial action as is necessary to meet service levels.

Where transaction and/or database volumes exceed those agreed with the vendor, or rule changes have increased complexity to the extent that service levels cannot be met, then the vendor and the Commission will initiate the agreed change control procedures.

8. Data-integrity and archive policy

8.1 Data ownership

All data collected, calculated and published as required in the functional specification is the property of the Commission. The vendor must store the data securely and be able to provide it to the Commission on request within a reasonable timeframe.

8.2 History

The system should retain history for immediate access for seven years, after which the information should be archived (DVD or other such medium) and available for retrieval on request.

9. Audit trail/traceability

The system must have an audit trail of all data input, confirmations delivered, notifications delivered and the delivery of information to other parties. Audit information should include time, party, method and any other pertinent information to allow for full tracking from source to destination.

10. Help desk

10.1 End-user assistance

The vendor is required to provide a contact that is available business hours to assist with user queries. The vendor must pro-actively assist users to resolve their issues.

10.2 Fault management

The vendor must provide a fault management service during business hours to rectify operational incidents and system faults. Operational incidents are those where the user reports that the system is unobtainable. A system fault means a defect, error or malfunction in the system that renders all or any part of it inoperable or unusable. The vendor must commence work to rectify operational incidents and system faults within two hours of their detection or reporting.

The vendor must pro-actively manage all aspects of the service.

If an incident affects more than one user, the vendor should notify all participants.

10.3 Incident register

The vendor must maintain a register of all help-desk requests, system faults and other operational incidents reported by each user during the previous twelve-month period. The register should contain the user, time and details of the incident as well as the time and details of their resolution. The vendor will notify users when incidents are resolved or the time when they are expected to be resolved. The vendor should develop an incident management process for users to view all incidents and to report any faults. A summary of all incidents and their resolution times should be included in the monthly report on service levels.

11. Change management

The vendor must follow the change management procedure as set out in Appendix I of this document. The change management procedure must be integrated into the vendor's internal change management processes with respect to the efficient management and reporting of progress.

12. Development methodology

12.1 Industry standard

The vendor should employ industry standard software engineering practices including robust quality assurance processes. Any methodology should cover the whole system development life-cycle (SDLC) in the development and maintenance of software.

12.2 Flexibility

The software should be designed for flexibility to accommodate changes to functions as a result of user requests and rule changes.

13. Implementation and transition

13.1 Implementation plan

The vendor must provide an implementation plan that includes:

- key SDLC steps, deliverables and milestones;
- the identification of the project critical-path, any external dependencies and areas of uncertainty;
- regular reporting to the industry project team that will be set up to help the vendor;
- a robust testing strategy that includes sufficient program testing, system testing, acceptance testing by the industry and a market trial; and
- commencement dates and duration when resources will be required, especially from the industry.

13.2 Migration plan

The vendor must develop a migration implementation plan, agreed between the vendor and the Commission.

13.3 Historical information

The vendor will be required to load all the historical information contained in the current system into any new system. At the end of the contract term, the vendor must deliver all the data in the system to the Commission, on request, within an agreed time-scale in an agreed format.

14. User liaison

14.1 Close contact

The vendor is required to maintain close contact with users, be pro-active, and provide additional services and support to ensure that the system remains responsive, up-to-date and consistent with the needs of the industry.

Each participant company appoints a nominated manager to be responsible for all of that participant's communications with the vendor. The Commission also has a representative for liaison purposes.

14.2 Data automation

Most participant companies have developed their own automated systems that interface to the current system whereby files for them are automatically retrieved and processed and this automation must continue to function correctly with minimum interruption. However, this does not mean the development of new technology for use in this area cannot be considered and introduced over time.

14.3 Notification channels

The vendor must develop formal notification channels to notify users, the representative of the Commission of outages and likely timeframes for restoration of service.

14.4 Escalation process

The vendor must provide an escalation process for users in the event of either a major failure of the system extending beyond service level thresholds or in the event of continued user service issues.

14.5 Daily liaison

During periods when the system is not available, the vendor must also liaise with the representative of the Commission and users not less than daily, including advising of expected times for the resumption of service.

14.6 User-satisfaction survey

The vendor is required to develop, distribute and consolidate a survey of all participants that analyses the satisfaction levels of their service provision. The survey is to be conducted annually and the results reported to the Commission.

15. Training

The vendor must be able to provide training in the use of the software to new users.

16. Documentation

The vendor must maintain and provide as a minimum:

- a) an up-to-date functional specification against which the software can be audited as per the requirement in the Regulations clauses 51 to 53. The functional specification and any subsequent changes are the property of the Commission;
- b) a user manual and online help facilities to enable new users to configure their systems correctly and access the system. The documentation should

- provide sufficient detail for new users to locate and use all the relevant functions;
- c) disaster-recovery procedures manual that describes the procedure, possible impacts on users and their operation and instructions on what users will need to do for business continuity;
 - d) in addition, the vendor must ensure they have sufficient technical documentation for business continuity in case of the loss of key personnel.

17. System audits

17.1 Spot audits

The Commission may carry out audits of the records and procedures of the software within normal working hours on reasonable notice. The vendor of the software must give the auditor access to all relevant facilities, personnel, records and manuals, and provide to the auditor any additional information that the auditor reasonably considers is necessary to enable an assessment of whether or not the software continues to meet the criteria for approval.

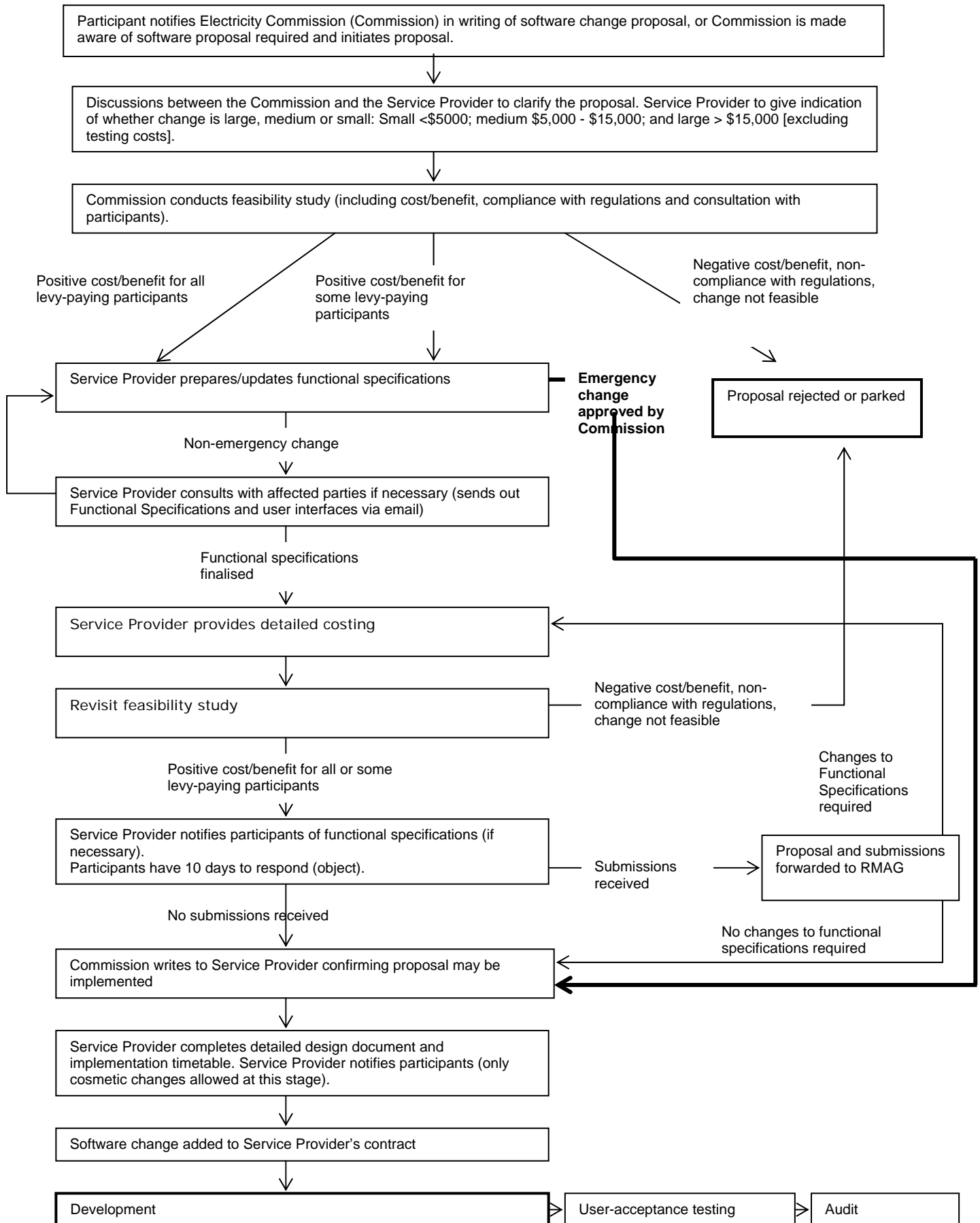
17.2 Audit recommendations

The vendor of the software must implement, under the change control procedure, any changes necessary to give effect to any reasonable recommendations made by an auditor, with the objective of constantly improving services.

17.3 Annual and change audits

The vendor must comply with the audit requirements as set out in Electricity Governance Regulations 2003 (Regulations) clauses 51, 52 and 53 with respect to conducting audits of the software, annually, on first-time use and for software changes. The Regulations can be found at www.electricitycommission.govt.nz/rulesandregs/rules.

Appendix I—change-control process



Appendix II—volumes (Provided courtesy of M-co)

Transaction volumes

Reconciliation data

Purchaser (buyer) meter readings. Typical file size: 823 KB, 3183 rows

Generator (seller) meter readings. Typical file size: 6,564 KB, 26869 rows

No of GXP's the five largest retailers purchase at

CTCT—177 GXPs

GENE—164 GXPs

MERI—182 GXPs

MRPL—143 GX's

TRUS—166 GXPs

Ancillary services

Input files from system operator —seven files containing approximately 13,000 rows

Invoices

There are typically about 45 tax invoices and pro-forma invoices produced, followed by another about 23 buyer-created tax invoices after settlement. There are also, on average, 20 washup notifications generated for each washup month.

Constrained on/off

Outputs: approximately 11,000 rows published to the information system and sent to the system operator each month

Inputs: approximately 70,000 dispatch instructions a month
approximately 100,000 offers
approximately 300,000 final prices
block and station dispatch group details

Block dispatch settlement differences

Inputs: approximately 300,000 dispatch quantities a month

Additional information

There are about 40 major electricity generation stations connected to the grid.

There are about 28 lines companies that own the local distribution networks throughout New Zealand.

Current participant codes

ADHB	Auckland District Health Board	MRPL	Mighty River Power Limited
AIAL	Auckland International Airport Ltd	NDHB	Northland District Health Board
ALDI	Aluminium Diecasting Ltd	NELS	Nelson Electricity
ALNT	Alinta ENZ Limited	NPOW	Northpower Ltd
ALPE	Alpine Energy	NZAS	New Zealand Aluminium Smelters Ltd
BIRC	Birchfield Minerals Ltd	NZEM	New Zealand Electricity Market
BLUE	Blue Mountain Lumber	NZRN	New Zealand Rail
BOPE	Bay of Plenty Electricity	NZST	BHP New Zealand Steel
BUEL	Buller Electricity Ltd	OBER	Obertech Group Ltd
CDHB	Christchurch District Health Board	ONRG	On energy
CHBP	Central Hawkes Bay Power Ltd	ORON	Orion New Zealand Limited
CHCL	CWF Hamilton & Co Limited	OTPO	Otago Power Ltd
CHHE	Carter Holt Harvey Ltd	PNCC	Palmerston North City Council
CIAL	Christchurch International Airport	PANP	Pan Pacific Forest Industries Ltd
COUP	Counties Power Ltd	POCO	Powerco Ltd
CTCT	Contact Energy	RAYN	Rayonier Ltd
CYPH	ems Limited	RMBE	RMB Energy Group NZ Ltd
DHCL	Drysdale Hydro Company Limited	SCAN	Scanpower Ltd
DUNE	Aurora Energy Ltd	SHPK	Southpark Corporation Ltd
EASH	Electricity Ashburton Ltd	SKOG	Norske Skog Tasman Ltd
EAST	Eastland Network Ltd	SMAL	Smales Farm
ELEC	ElectraLines	SWFT	Swift Energy
ELIN	Electricity Invercargill Ltd	TASM	Network Tasman Ltd
EMCO	M-co	TODD	Todd Energy Limited
FRST	First Electric Limited	TOPE	Top Energy Ltd
GENE	Genesis Power	TPCO	The Power Company Ltd
HAWK	Unison Network Ltd	TPNZ	Transpower New Zealand Limited
HEDL	Horizon Energy Distribution Limited	TRUS	TrustPower Ltd
KAPE	Kapuni Energy Ltd	TSCN	Thomas Cameron
KING	King Country Energy Ltd	TUAR	Tuaropaki Power Company Ltd
KIPT	Kiwi Income Property Trust	UNET	United Networks Ltd
KIWI	Kiwi Power (Cogen Plant)	VECT	Vector Limited
LINE	The Lines Company	WAIK	W E L Energy Group
LLNW	Lakeland Network	WAIP	Waipa Power Ltd
MACQ	Macquarrie Goodman	WATA	Waitaki Power Ltd
MALL	Mall	WBSL	WD Boyes & Sons Ltd
MARL	Marlborough Lines Ltd	WFNZ	Westfield's New Zealand
MEEN	Mercury Energy	WHSP	Whisper Tech Ltd
MERI	Meridian Energy Ltd	WNSL	Lloyd Wensley
MOPO	Mountain Power Ltd	WNST	Winstone Pulp International
MPOW	MainPower NZ Ltd	WPOW	Westpower Ltd