Station security - procedures

TRANSPOWER **APPROVED** SPECIFICATION

Implementation date: March 2012

PREFACE

This document specifies the services required and procedures to be followed to ensure the on-going security of Transpower assets and the proper control of entry to Transpower stations and sites.

The changes in this *Issue 13, February 2012* are noted at Appendix H – Table of Changes.

Keywords

security
stations

CONTACT

This document is the responsibility of Grid Asset Management - Field, Transpower New Zealand Limited, Wellington. If you have any queries please contact the Grid Asset Manager.
If you would like to make suggestions to improve this document, please use the "Controlled Document Feedback Form" located at the rear of this document or online via the Controlled Documentation homepage of the Transpower website at www.transpower.co.nz

CONFIDENTIALITY

All information disclosed in this document that is not general public knowledge must be treated as strictly confidential and may not be used or disclosed except for the purpose of developing documentation for the benefit of Transpower.

LIMITATION OF LIABILITY AND DISCLAIMER OF WARRANTY

Transpower New Zealand Limited makes no representation or warranties with respect to the accuracy or completeness of the information contained in the document. Unless it is not lawfully permitted to do so, Transpower specifically disclaims any implied warranties of merchantability or fitness for any particular purpose and shall in no event be liable for, any loss of profit or any other commercial damage, including, but not limited to, special, incidental, consequential or other damages.

MINIMUM REQUIREMENTS

The requirements set out in Transpower's standards are minimum requirements that must be complied with by contractors, including designers and other consultants. The contractor is expected to implement any practices which may not be stated but which can reasonably be regarded as good practices relevant to the purpose of this standard. Transpower expects contractors to improve upon these minimum requirements where possible and to integrate these improvements into their procedures and quality assurance plans.

CONTENTS

1. PURPOSE

To specify the responsibilities of personnel entering Transpower stations and communication sites, and to stipulate the entry protocols, safety management and security requirements for those stations and sites.

2. REQUIRED OUTCOMES

The conditions of the station security Service Specifications have been complied with when the relevant requirements have been implemented and this has resulted in the on-going:

(a) Safety of employees and the public;
(b) The security of the power system, and
(c) The secure custody of station assets.

3. REFERENCES

TP.AG 10.02	*Transpower Glossary*
TP.AG 47.09	*Safety, Health and Environmental - Public Safety Management System*
TP.OG 45.03	*Defined operating and maintenance terms and abbreviations*
TP.SS 01.01	*Reporting by contractors*
TP.SS 06.21	*Minimum competencies for substation maintenance and testing*
TP.SS 06.25	*Training, competency and certification requirements for work on Transpower assets*
TP.SS 07.01	*Operational and asset related interfaces*
TP.SS 07.11	*The log*
TP.SS 07.20	*Access for work*
TP.SS 07.21	*Access permit and test permit procedures*
TP.SS 07.25	*Locking of HV switchgear and lockout requirements*
SM-EI	*Safety Manual- Electricity Industry*
CP.CE.PP.003	*Transpower's Drug & Alcohol Policy*

4. PRINCIPAL REQUIREMENTS

Principal requirements include the following:

(a) The Systems within this Service Specification must be used in its entirety.
(b) Only persons holding a valid Competency Certificate or who are under the holder's supervision shall enter a restricted area.
(c) Access control and security alarm systems installed at Transpower stations and sites must be continuously monitored.
(d) Road gates are to be locked when sites are unmanned. When personnel are on site Road gates are to be closed but not locked for emergency access/egress purposes.
(e) Restricted areas such as switchyards, other HV enclosures and buildings shall be kept locked unless the entrance gate or door is continuously kept under close supervision.
(f) Children under 15 years and pets are prohibited from entry into restricted areas at Transpower stations.
(g) All persons entering a restricted area must record their details on the entry log, or be under the RAE Competency Certificate holder's supervision. See **Appendix A**.
(h) Smoking is prohibited on all work-sites, inside all buildings, in all areas designated as restricted areas and areas set aside for the purpose of eating. Work parties must designate their own smoking areas, outside of those prohibited areas listed above, with appropriate signage and supply of a waste receptacle that shall be emptied and contents removed at the end of each day.

(i) Portable metal ladders and other conductive ladders including step ladders are prohibited inside restricted areas.

(j) Anyone entering a Transpower station or site, for any purpose, may be subject to random drug and alcohol testing, in accordance with Transpower's Drug and Alcohol Policy.

5. DEFINITIONS

5.1 General

5.1.1 Unless stated below, words and phrases in this standard have the meaning defined in **TP.OG 45.03** *Defined operating and maintenance terms and abbreviations* and **TP.AG 10.02** *Transpower Glossary* or that of common English usage.

Access device: Cardax keytags and keys for accessing Transpower controlled and/or restricted areas.

Controlled area: A fenced area around station buildings for which entry is only possible via a key or a remote controlled gate, or other means of entry control.

Environment Safety: The controls, exercised by the RAE Competency Certificate holder, necessary to prevent harm to themselves and all others under their direction, due to the hazards existing in Transpower controlled and restricted areas. These will include electrical, physical and location associated hazards.

Occupier: An authorised person or employee on official business.

Public area: The part of a station or communications site that is open for public access.

RAE Competency Certificate Holder: An individual holding a valid Restricted Areas Entry competency certificate as issued by their employer to the requirements of **TP SS 06.25**.

Restricted area: A building, enclosure or area which is subject to an asset owner's entry control system provided to prevent unauthorised entry, where such entry could result in serious harm and/or present a risk to power system security.

Supervision: The provision of appropriate levels of control and direction by a competent employee. It should be applied to the level necessary to ensure that persons do not cause harm to themselves or others.

Note: *The management of the actions of all persons for safety is the key component of those responsible for supervision. It applies to:*

- *supervision of work by the Site Supervisor,*
- *substation environment safety supervision of persons entering a substation with an RAE holder,*
- *substation environment safety supervision of persons working under a primary or other works management system,*
- *supervision of non-certificated persons in a work party by a competent person.*

6. RESPONSIBILITIES

6.1 Site Access & Security Management Provider (Facilities Management Contractor)

6.1.1 The site access & security management provider, as part of the national Facilities Management Contract, is responsible for:

(a) Contracting and managing the Security-monitoring and guard response contractors.

(b) Contracting and managing the access control and security systems support contractor.

(c) Managing all site access and access device requests for stations and other facilities within the national access control and Grid Performance master-keying systems.
(d) Providing all new and replacement locks and lock-cylinders keyed to the Grid Performance national master-keying system.
(e) Assisting personnel having difficulty in routinely accessing a station.
(f) Providing overall coordination of access control systems and master-keyed locks.
(g) Continually reviewing site access and security assets and procedures to enhance station security and delivery of security services.

6.2 Security-monitoring Contractor

6.2.1 The security-monitoring contractor is responsible for:

(a) Monitoring the station access control and security alarm system for system health and defect alarms, station security breaches.
(b) Advising Regional Operator of all access control and security alarm system "security breach" alarm operations and providing details of the area of the substation building where the security has been breached.
(c) Initiating a security guard response to confirmed security breach alarms.
(d) Advising Regional Operator of all station fire and smoke alarms appearing on the access control and security alarm system as a back up to the regional operator's National SCADA alarms.
(e) Advising Regional Operator of all defects on substation-based access control and security alarm system equipment.

6.3 Regional Operators

6.3.1 The Regional Operators are responsible for:

(a) Call-out of station maintenance contractor to accompany security guard for security breach alarms.
(b) Call-out of station maintenance contractor to undertake repair of station-based access control and security alarm equipment.
(c) Monitoring station fire alarms through National SCADA and responding by calling the fire brigade and stations maintenance contractor following a fire alarm operation.
(d) Arranging for the safe entry of fire service, security guard, police or ambulance personnel who are not RAE Competency Certificate holders into restricted areas. A person with a valid RAE Competency Certificate must accompany these personnel.
(e) Informing the police and as appropriate, the Transpower Grid Performance Stations Manager of bomb threats concerning Transpower substations.
(f) Reporting of all incidents involving bomb threats and alarms for security breach or fire.

6.4 Stations Maintenance Contractors

6.4.1 The stations maintenance contractors are responsible for:

(a) Response to station security breach alarms, as requested by a Regional Operator.
(b) Response to repair station-based access control and security alarm equipment, as requested by a Regional Operator or Access Control Systems Support Provider.
(a) Response to provide safe entry of fire service, security guard, police or ambulance personnel who are not RAE Competency Certificate holders into restricted areas, as requested by a Regional Operator.

6.5 RAE Competency Certificate holders

6.5.1 RAE Competency Certificate holders are responsible for:

(a) Holding a valid RAE Competency Certificate. See **TP.SS 06.25.**
(b) Ensuring site security is not breached while undertaking activities at a station or site.
(c) Using the correct entry logging procedures.

(d) If last person on site, confirming all site-specific ODS access keys have been returned to the relay room key-cabinet or electronic KeySafe prior to leaving the site, and immediately advising the site access & security management provider where there is any discrepancy.

(e) Supervising all persons entering with them for environment safety.

7. ENTRY TO STATIONS

7.1 Access devices

7.1.1 Access control system keytags and/or security keys are required to access Transpower controlled and restricted areas. The access control system keytags are personalised to the RAE Competency Certificate holder by a four digit Personal Identification Number (PIN). The PIN shall be kept confidential by the RAE Competency Certificate holder and shall not be disclosed to others. Additionally, the practice of engraving a PIN on a keytag or in any other way displaying the PIN with a keytag is not acceptable or permitted.

7.1.2 Personal keytag and keys are provided with an "If Found Send to" stainless steel tag. This tag shall remain with the key-set to improve the likelihood of it being returned if lost.

7.1.3 The process for requesting site access, access control system keytags and security keys, and seeking assistance for site access problems, is detailed in **Appendix C**.

7.1.4 Instructions for using the access control system keytags and setting/unsetting the station security alarm system is detailed in **Appendix D**.

7.1.5 Site-specific keys for switchyard gates and other buildings on the station are located in the KeySafe. These must under no circumstances be taken off site from the substation. Site-specific keys not accounted for result in Transpower having to replace all site-specific keys and locks for the respective site. As this replacement is a costly exercise, Transpower may require recovery of these costs from the company responsible for the loss.

7.2 Control of entry

7.2.1 The RAE Competency Certificate holder controls entry to restricted areas by ensuring that:

(a) Their entry is logged;

(b) All other persons entering under their Competency Certificate are supervised.

Notes: *All persons entering a controlled or restricted area who do not hold valid RAE Competency Certification shall be given, prior to entry, a comprehensive safety briefing by the RAE Competency Certificate holder controlling entry. This briefing shall include:*

- *Physical and electrical hazards at the substation,*
- *Personal Protective Equipment requirements,*
- *Minimum approach distances,*
- *Work restrictions with relation to boundaries and activities,*
- *Identification of persons responsible for work supervision and for environment supervision,*
- *Whilst in controlled or restricted areas, these persons shall be closely supervised for environment safety by the RAE Competency Certificate holder controlling entry or another RAE Competency Certificate holder nominated by the RAE Competency Certificate holder controlling entry. The ratio of RAE Competency Certificate holders to non RAE Competency Certificate holders shall be no more than 1:6, and*
- *Those persons entering controlled and restricted areas who hold a valid RAE Competency Certificate shall be supervised for environment safety by the RAE Competency Certificate holder controlling entry, or another RAE Competency Certificate holder nominated by the RAE Competency Certificate holder controlling entry.*

7.2.2 The occupier controls entry to non-restricted areas.

7.2.3 Transpower reserves the right to withdraw approval for any person to enter Transpower controlled and restricted areas.

7.3 Control of public in controlled and restricted areas

7.3.1 Public entry to controlled and restricted areas is not permitted unless:

(a) Prior arrangements are made with the Transpower Grid Performance, Stations Manager, and

(b) Visitors are met and accompanied by a valid RAE Competency Certificate holder.

Notes: *All visitors entering controlled or restricted areas shall be given, prior to entry, a comprehensive safety briefing by the RAE Competency Certificate holder controlling entry. This briefing shall include:*

- *Physical and electrical hazards at the substation,*
- *Minimum approach distances, and*
- *Restrictions with relation to boundaries and activities.*

Whilst in controlled or restricted areas, these persons shall be closely supervised for environment safety by the RAE Competency Certificate holder controlling entry. The ratio of RAE Competency Certificate holders to non RAE Competency Certificate holders shall be no more than 1:6.

7.4 Entry/exit procedure for Transpower stations

7.4.1 On entering a restricted area, enter on the Entry Log sheet:

(a) Surname and initials;

(b) Designation;

(c) Competency Certificate number;

(d) Name of company;

(e) Date;

(f) Time using the 24 hour clock format, i.e. 13:00 hours for 1.00 pm;

(g) Total number in party, including RAE Competency Certificate holder;

(h) A brief and concise description of the purpose of the visit;

(i) Whether a vehicle is to be taken into a switchyard;

(j) The ID number of any ODS access key used (where the KeySafe is not electronic), and

(k) Whether a permit is required.

In the absence of an Entry Log sheet, the above information must be entered in the station log book.

Every time the RAE Competency Certificate holder exits the restricted area to leave the site the exit and re-entry times must be logged. See **Appendix A**.

7.4.2 If the switchyard is to be entered, and the RAE Competency Certificate holder is required to monitor station alarms, then the station local alarms Audible Sounder must be activated. The Audible Sounder can be activated from push buttons in the RTU cabinet, generally immediately under the RTU. Telephone calls to the station switchyard telephone will activate the telephones internal bell to indicate the incoming call.

7.4.3 On stations that have a Power Fence installed to the switchyard, the Power Fence will be deactivated automatically upon Unsetting the Control Building intruder alarm system. Where work is to be undertaken on or in close proximity to the Power Fence it shall be manually isolated using the Power Fence isolation system, as described in **Appendix E.**

7.4.4 If entry is required into a switchyard or other Restricted Area building outside the switchyard then use an ODS access key obtained from the KeySafe. Record the key ID number in the Entry Log sheet (refer **clause 7.4.1(j)**). Instructions for using an electronic KeySafe are described in **Appendix F.**

7.4.5 If a vehicle is required to be taken into a switchyard then the RAE Competency Certificate holder shall ensure that the requirements of SM-EI rule 2.905, Mobile Plant and Vehicles in the Vicinity of Live Conductors are complied with. Record vehicle access in the Entry Log sheet (refer **clause 7.4.1(i)**).

7.4.6 On completion of activities and before leaving the site, ensure all ODS access keys are returned to the KeySafe. Immediately advise the **site access and security management provider** where there is any discrepancy.

7.4.7 Record time of leaving on the Entry Log sheet. See **Appendix A**.

7.4.8 If the site is being vacated, check the entry log for other personnel that could be still on site before setting access control and alarms. Check all switchyard gates and control room doors are locked closed, all windows are closed and lights are left as required by **subsection 9.3** of this Service Specification and if installed and previously deactivated, by the Isolation Switch (refer **Appendix E**), the Power Fence is to be re-armed. Set the access control and security alarm, ensure door is latched and locked securely and exit the station. **Note:** the access control and security system will not Set if any monitored door or gate remains open, or the Power Fence, if installed, has been isolated.

7.5 Entry to Transpower stations located on third-party sites

7.5.1 All Transpower RAE Competency Certificate holders accessing a Transpower station on a third-party controlled site shall comply with the entry requirements of the third-party site owner prior to entry into the Transpower station.

8. ENTRY TO STATIONS WITH ACCESS CONTROL SYSTEM FAULT

8.1 General

8.1.1 Where the failure of the access control and security system or a access keytag prevents normal entry to a station, the following procedures shall be adopted.

8.2 Routine entry where a fault exists within the Access Control system equipment

8.2.1 Personnel requiring routine entry into a station but are prevented from doing so due to an access and security system fault or a faulty keytag shall contact the **Site Access & Security Management Provider** to authorise and arrange the Security-alarm Monitoring Contractor to remotely Unset the intruder alarm system and unlock the electronically-controlled main entry door if achievable.

8.2.2 Where the station intruder alarm system cannot be remotely Unset then personnel will not be permitted to access the station, except where entry is required to undertake repair of faulty access control and security equipment (see **subsection 8.3**), or where entry is required for critical operation of power system equipment (see **subsection 8.4**).

8.2.3 The **Site Access & Security Management Provider** shall contact the respective stations maintenance contractor to undertake repair of the faulty access control and security system.

8.2.4 Request for replacement of a faulty keytag shall be made to the Site Access & Security Management Provider as outlined in **Appendix C**.

8.3 Entry to repair faulty access control & security equipment

8.3.1 Personnel requiring entry into a station to undertake repair of the access and security system equipment but are prevented from doing so due to the fault shall contact the **Site Access & Security Management Provider** to authorise and arrange **the Security-alarm Monitoring Contractor** to remotely Unset the intruder alarm system and unlock the electronically-controlled main entry door if achievable. (Stations' maintenance contractors have also been provided with an over-ride key in order to gain alternate access.)

8.3.2 Where the station intruder alarm system cannot be remotely Unset then the Stations Maintenance Contractor's representative shall liaise with the **Site Access & Security Management Provider** to confirm alternate entry actions. The **Site Access & Security**

Management Provider shall advise the **Security-alarm Monitoring Contractor** of these proposed actions.

8.4 Entry for critical operation of power system equipment

8.4.1 Personnel requiring entry into a station to undertake critical operation of power system equipment but are prevented from doing so due to an access control and security system fault or faulty keytag shall contact the **Site Access & Security Management Provider** or the respective **Regional Operator.** They are to authorise and arrange the Security-alarm Monitoring Contractor to remotely Unset the intruder alarm system and unlock the electronically-controlled main entry door if needed

8.4.2 Where the station intruder alarm system cannot be remotely Unset and/or the electronically-controlled main entry door cannot be remotely unlocked and there is no alternate key-only option available then personnel shall liaise with the **Site Access & Security Management Provider** or the respective **Regional Operator** to confirm alternate emergency entry actions. The **Site Access & Security Management Provider** or **Regional Operator** shall advise the Security-alarm Monitoring Contractor of these proposed actions.

8.4.3 Upon exiting the station on-site personnel shall contact the Security Alarm Monitoring Company to have them attempt a remote Setting of the intruder alarm system.

8.4.4 The Regional Operator shall advise the respective stations maintenance contractor to undertake repair of the access control system as appropriate.

9. STATION SWITCHYARD AND SWITCHROOM SECURITY

9.1 Gates and doors

9.1.1 All switchyard and Switchroom gates and doors must be kept locked at all times except when the entry location is continuously kept under close supervision.

9.1.2 Unauthorised entry through an unlocked gate or door must be stopped. Any unauthorised entry is to be reported immediately to the appropriate Transpower Stations Manager and the details entered in the station Log Book. A Security Breach Report (ICAR-TP518) shall also be generated.

9.2 Security breach and fire alarms

9.2.1 Security breach alarms must be operative when the station is unattended.

9.2.2 Fire alarms must remain operative at all times.

9.2.3 The security-monitoring contractor/Regional Operator must respond immediately to security breach and fire alarms. See **section 10** and **subsection 11.2**.

9.3 Lighting

9.3.1 When stations are unattended switchyard lighting at night is to be left off unless otherwise required by the appropriate Transpower Grid Performance, Stations Manager.

9.4 Control of entry to and from a construction area

9.4.1 Where it is necessary to remove or relocate an existing switchyard fence, the appropriate Transpower Grid Performance, Stations Manager must first be informed at the planning stage.

9.4.2 The Project Contractor is responsible for controlling entry to a construction work site. Construction personnel must comply with this Service Specification when entering a restricted area.

10. FIRE BRIGADE ENTRY

10.1 General

10.1.1 Fire Service personnel are prohibited by their management to enter a restricted area to attend fires unless they are accompanied by the holder of a valid Competency Certificate.

10.1.2 The RAE Competency Certificate holder accompanying the fire brigade must obtain a permit where required to ensure any fire brigade activities in the vicinity of high voltage equipment can be carried out safely.

11. DEALING WITH INTRUDERS

11.1 Security contractor and/or Police arrangements

11.1.1 Arrangements approved by the appropriate Transpower Grid Performance, Stations Manager exist for contacting a security contractor or other organisation when an intruder is suspected at a Transpower station.

Note: *Contractors' employees are not to challenge suspicious intruders. Safety of personnel is the first priority.*

11.1.2 Any security guard checking for intruders in restricted areas must be the holder of a valid RAE Competency Certificate or be accompanied by a RAE Competency Certificate holder familiar with the station.

11.1.3 The police must be notified if there is evidence of an intruder.

11.2 Action when security breach alarm is activated

11.2.1 When a security breach alarm is activated at a station **and after consulting** with the respective Regional Operator, the security-monitoring contractor shall initiate the required security guard response.

11.2.2 Where required the Regional Operator must arrange for a RAE Competency Certificate holder to meet and accompany the security guard or police during the search.

11.2.3 Where the Regional Operator determines that a security guard is not required due to the circumstances and type of security breach alarm(s) then the Regional Operator shall advise the RAE Competency Certificate holder that a guard response has **not** been initiated.

11.2.4 Where it has been decided by the Regional Operator that a security breach alarm will not be attended by a guard response as in **clause 11.2.3**, but the attending RAE Competency Certificate holder requests that a guard also attend, the Regional Operator shall request the security-monitoring contractor initiate the required security guard response as in **clause 11.2.1**.

11.2.5 The Regional Operator is to record in the log all security breach alarm activations, and calls to the security contractor and the police. The outcome of all checks and other actions taken are to be recorded.

11.2.6 The appropriate Transpower Grid Performance, Stations Manager is to be informed on the next working day of all confirmed intrusions or breaches of security. A report is to be compiled and despatched as specified in **TP.SS 01.01** for all incidents involving intruders or security breach alarms, including false alarms, at Transpower stations.

11.2.7 The Regional Operator is to report any communications site security alarms or breaches of security according to the arrangements made by the appropriate Transpower Grid Performance, Stations Manager, for Transpower sites.

12. BOMB THREATS

12.1 Warnings

12.1.1 Most bomb threats or warnings are made by telephone. A copy of the bomb threat telephone check list and questionnaire (**Appendix B**) is to be kept beside the telephone at Regional Operating Centres. Be calm and courteous and do not interrupt the caller. To assist the police, continue the discussion as long as possible, asking the bomb threat caller as many of the questions as possible and noting the details in the questionnaire.

12.1.2 Regional Operator action:

(a) Complete the questionnaire (**Appendix B**) during or as soon as possible after the call.

(b) If the threat concerns an unattended station, determine if anyone is on site and advise the person in charge. The person in charge will make specific decisions about evacuation. Detailed evacuation plans are the responsibility of the station's equipment maintenance contractor.

(c) Inform the police (111). Give as much information from the questioning of the caller as possible.

(d) Inform the Security Co-ordinator and the appropriate Transpower Grid Performance, Stations Manager.

(e) Inform the Security Co-ordinator and the appropriate Transpower Grid Performance, Stations Manager if a search does not locate a suspicious object.

12.2 Suspicious objects

12.2.1 If a suspicious object is found, do not move it, clear the area and inform the police.

REMOVAL AND DISPOSAL OF A SUSPICIOUS OBJECT IS TOTALLY THE RESPONSIBILITY OF THE POLICE.

12.2.2 Entry for the removal of a suspected bomb is subject to the normal entry control requirements. If a permit is required, the boundaries of the equipment covered under the permit must be outside the potential blast zone as defined by the police.

12.3 Reporting

12.3.1 On completion of any search and/or bomb disposal, the person in charge of the search must:

(a) Inform the Regional Operator;

(b) Inform the appropriate Transpower Grid Performance, Regional Service Manager;

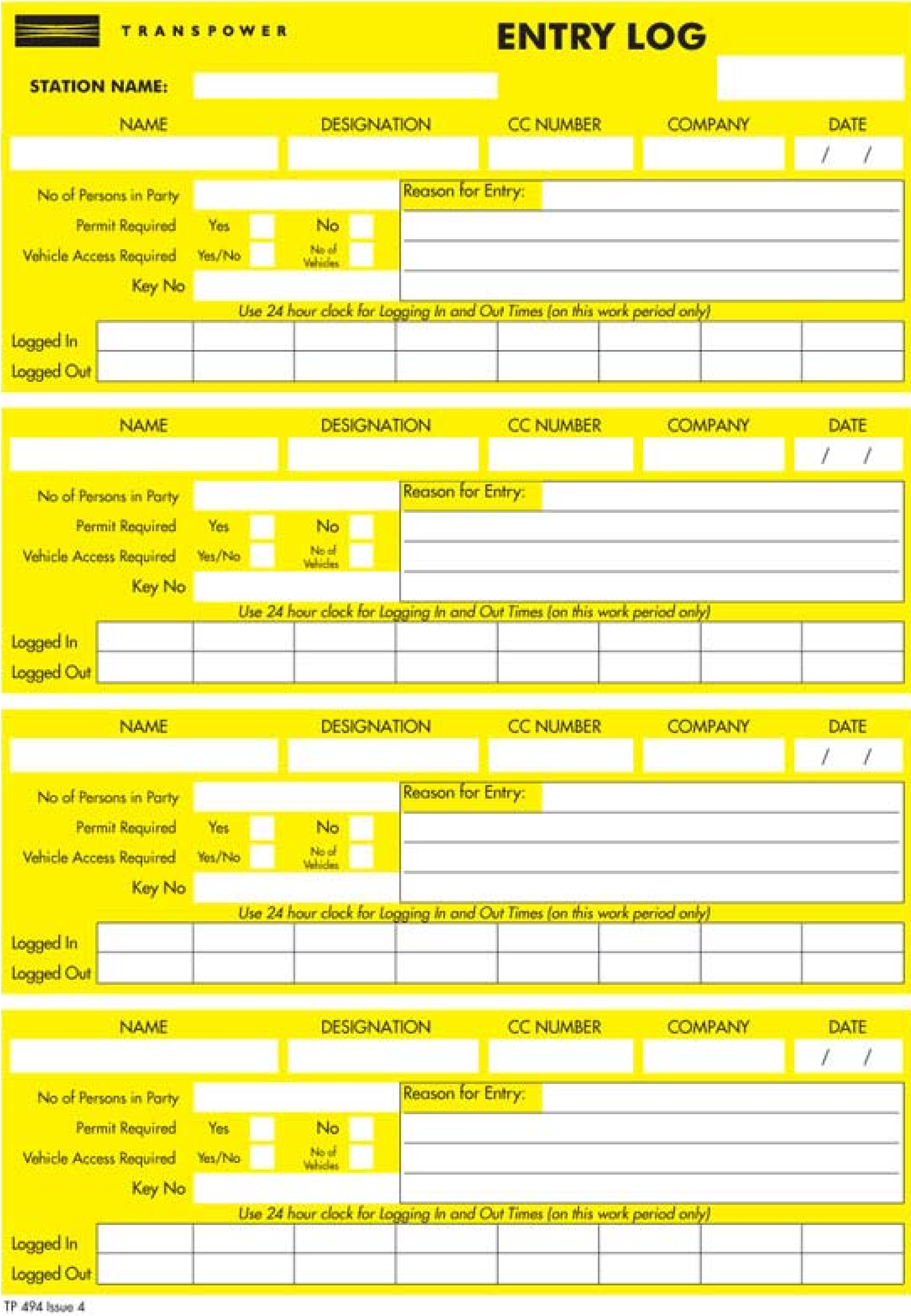
(c) Log details of the event.

12.3.2 No information is to be given to the news media regarding any bomb threat. All enquiries must be referred to the appropriate Transpower Grid Performance, Stations Manager.

12.3.3 A report to the appropriate Transpower Grid Performance, Stations Manager is required for all bomb threats and alerts caused by suspicious objects at Transpower stations and Regional Operating Centres.

A ENTRY LOG SAMPLE (TP 494 ISSUE 4)

The Entry Log forms must be ordered from Chaucer Press.



TRANSPOWER

ENTRY LOG

STATION NAME:

NAME | DESIGNATION | CC NUMBER | COMPANY | DATE / /

No of Persons in Party
Permit Required Yes No
Vehicle Access Required Yes/No No of Vehicles
Key No
Reason for Entry:
Use 24 hour clock for Logging In and Out Times (on this work period only)
Logged In
Logged Out

NAME | DESIGNATION | CC NUMBER | COMPANY | DATE / /

No of Persons in Party
Permit Required Yes No
Vehicle Access Required Yes/No No of Vehicles
Key No
Reason for Entry:
Use 24 hour clock for Logging In and Out Times (on this work period only)
Logged In
Logged Out

NAME | DESIGNATION | CC NUMBER | COMPANY | DATE / /

No of Persons in Party
Permit Required Yes No
Vehicle Access Required Yes/No No of Vehicles
Key No
Reason for Entry:
Use 24 hour clock for Logging In and Out Times (on this work period only)
Logged In
Logged Out

NAME | DESIGNATION | CC NUMBER | COMPANY | DATE / /

No of Persons in Party
Permit Required Yes No
Vehicle Access Required Yes/No No of Vehicles
Key No
Reason for Entry:
Use 24 hour clock for Logging In and Out Times (on this work period only)
Logged In
Logged Out

TP 494 Issue 4

B BOMB THREAT QUESTIONNAIRE

BOMB THREAT CHECK LIST QUESTIONS TO ASK:

- When is the Bomb going to explode?
- Where is the Bomb?
- What does the Bomb look like?
- What kind of Bomb is it?
- What will make the Bomb explode?
- What is the Explosive Type and Quantity?
- Why did you place the Bomb?
- What is your name?
- Where are you?
- What is your address?

EXACT WORDING OF THREAT:

ACTION

Report call immediately to:_____

Phone Number:_____

Trace 111:_____

Police Advised:_____

Date/Time:_____

Members name:_____

COPY THIS QUESTIONNIARE AND KEEP IT BY THE PHONE

CALLER'S VOICE

Accent:_____

Any impediment (specify):_____

Voice (loud, soft, etc):_____

Speech (fast, slow, etc):_____

Diction (clear, muffled):_____

Manner (calm, emotional, etc):_____

Did you recognise the voice?_____

If so, who do you think it was?_____

Was the caller familiar with the area?_____

THREAT LANGUAGE

Well spoken:_____

Incoherent:_____

Irrational:_____

Taped:_____

Message read by caller:_____

Abusive:_____

Other:_____

BACKGROUND NOISES

Street noises:_____

House noises:_____

Aircraft:_____

Voices:_____ Standard Call:_____

Music: _____ 111/Cellular:_____

Machinery:_____ STD:_____

Vehicle (Cellular):_____

Other:_____

OTHER

Sex of caller:_____ Estimated age:_____

CALL TAKEN

Date: ___ / ___ / ___ Time:_____

Duration of call:_____ Number called:_____

RECIPIENT

Name (print):_____

Telephone number:_____

Signature: _____

C SITE ACCESS & KEY REQUESTS AND SITE ACCESS ASSISTANCE

C1 Purpose

This Appendix provides further explanation and implementation details of Transpower's policies for control of and requesting access to restricted and controlled area sites.

Information is also provided to assist personnel with access problems and provide them contact details for liaising with the companies providing security management functions.

C2 Definitions

Access device: Proximity keytags ("bullets"), and keys used to gain entry to Transpower Controlled and Restricted Areas.

Authorised representative: A company representative who is permitted to make site access and access device requests.

Competency [certification]: Training and certification to minimum competency levels to the requirements of Transpower Service Specification **TP.SS 06.21** *Minimum competencies for substation maintenance and testing,* and **TP.SS 06.25** *Training, competency and certification requirements for work on Transpower assets.*

Customers / service providers: Transpower Customers, Contractors and Consultants, Lines and Generators companies, who require access to Transpower's restricted, and controlled-areas sites and facilities.

Opus on-line services: Web-based service providing Opus Clients access to Opus-developed on-line systems and services.

Transpower Controlled and Restricted Areas: Transpower sites and facilities that require access equipment to gain entry, as defined in **TP.SS 07.40 clause 5.1.1.**

Transpower Period Maintenance Contractors: Main Contractors carrying out Stations, Lines, Transformer refurbishment, or Facilities Management Period Maintenance contract work.

Transpower Site Access & Key Management Web Site: An Opus On-line Service developed and provided for Transpower New Zealand to assist in managing site access and key requests.

C3 References

- **TP.SS 06.21** *Minimum competencies for substation maintenance and testing*
- **TP.SS 06.25** *Training, competency and certification requirements for work on Transpower assets*

The Transpower documents are available from the Contractors/Consultants section of the Transpower web site, from the Help page of the Security Management Provider's Site Access & Key Management Web Site, or by emailing a request to Transpower.Access@opus.co.nz

C4 Scope of Site Access and Security Management Services

C4.1 Summary of Site Access and Security Management Contract Services

The services provided by the Site Access & Security Management Provider, as part of the Facilities Management Contract, are outlined in **TP.SS 07.40 subsection 6.1.**

C4.2 The facilities presently covered by these services include:

- Substations and Cable Stations, including switchyards, cranehouses, etc.;
- Storage facilities, e.g. Pole Yards;
- Addington Warehouse;
- Regional Operating Centres, and Emergency Operating Centre South;
- National Coordination Centre North – Hamilton;
- Transpower Regional Offices - Auckland, Palmerston North and Christchurch;
- Communications site facilities;

- Omaka, Bunnythorpe and Western Road Training Facilities;
- Selected other facilities requiring 'special' keys within the Transpower Grid Performance National master-keying system, e.g. Emergency Accommodation, Miramar Cable Store, etc.

C4.3 The facilities not covered by this service are:

- Transpower House Wellington;
- Otahuhu and Bunnythorpe Warehouses;
- Access onto third-party facilities, e.g. Power stations, Lines Company owned substations;
- Rental housing.

C4.4 Monitoring of Access Control and Security Systems

All monitoring of the networked Access Control and Security Systems is centralised with a single monitoring company.

The Security-monitoring Contractor is responsible for:

- Monitoring all access and alarm systems for alarm activation or faults;
- Liaising with on-site staff to manage alarms;
- Liaising with Regional Operating Centres to resolve alarm activations;
- Dispatching security guards to security breach alarms.

Contact details for the Security-monitoring Contractor are in **clause C7.3**.

C4.5 Managing requests for Site Access and Site-access devices

Transpower's policy for control of site access and managing requests for site access and access equipment, are outlined in **subsection C5**.
Procedures for making requests for site access and access devices are outlined in **clauses C5.16** and **C5.17**.

C4.6 Site access problems

The Site Access & Security Management Provider will assist personnel with site access difficulties.

Guidelines and contact details for assisting personnel with site access difficulties are outlined in **subsection C7.**

C4.7 Technical support to Security System Maintenance Contractors

The Access Control & Security Systems Support Contractor will, upon request, assist security system maintenance contractors with resolving on-site security system faults.

Contact details for the Access Control & Security Systems Support Contractor are in **clause C7.4**.

C5 Site access management policies

C5.1 Overview

This section outlines Transpower's policies for control of access and for requesting access and access devices for restricted-access sites.

Any issues in respect to these policies, and in particular to any changes from previous policy, shall in the first instance be directed to Transpower's the Site Access & Security Management Provider – refer **clause C7.7.**

It is noted that Transpower RAE Competency Certificate holders accessing a Transpower station on a third-party owned & controlled site shall comply with the entry requirements of the third-party site owner prior to entry into the Transpower station.

For all access privileges to sites and facilities detailed below, personnel must meet the appropriate requirements of **TP.SS 06.21** *Minimum competencies for substation maintenance and testing.*

C5.2 Access to Stations for Employees of Period-maintenance Contractors

Employees of Period-maintenance Contractors shall be permitted unrestricted access to all HVAC Substations throughout New Zealand, if requested by the Contractor. Access to any non-HVAC Substation facilities is subject to specific request. Where a Period-Maintenance Contractor elects to not allow its employees unrestricted access to all HVAC Substations throughout New Zealand then access to HVAC Substations outside that Contractor's contracted maintenance group area is subject to specific request as and when access is required.

C5.3 Access to HVAC Substations for Employees of Subcontractors of Period-Maintenance Contractors

Employees of Subcontractors of Transpower Period-maintenance Contractors shall be permitted access to only those sites within the region contracted by the Period-Maintenance Contractor. Access to any sites and facilities outside this region is subject to specific request as and when access is required.

C5.4 Access to Stations for Project Contractors and their Subcontractors

Employees of Contractors (not being Period-maintenance Contractors) and their Subcontractors undertaking Project works shall be permitted temporary access to only those sites required to undertake the works, for the period of those works.

C5.5 Access to HVDC Stations for Period-maintenance Contractors and their Subcontractors

Employees and Subcontractors of Period maintenance Contractors for HVDC Stations shall be permitted access to only those HVDC sites within the region contracted by the Period-maintenance Contractor. Access to any other HVDC sites outside this region is subject to specific request as and when access is required.

C5.6 Access to Stations for Transpower-engaged Preferred Consultants and for Transpower Training Providers

Transpower-engaged Preferred Consultants and Training Providers shall be permitted unrestricted access to all HVAC Substations throughout New Zealand, if requested. Access to any non-HVAC Substation facilities is subject to specific request. Where a Transpower-engaged Preferred Consultant or Training Provider elects to not allow its employees unrestricted access to all HVAC Substations throughout New Zealand then access to sites is subject to specific request as and when access is required.

C5.7 Access to Stations for Transpower Employees

Transpower employees deemed competent to enter station restricted areas shall be permitted access to all HV Stations throughout New Zealand, if requested.

All requests from Transpower employees shall be directed to the respective nominated Transpower Grid Performance representative for processing. The nominated representatives will make all requests directly to the Site Access & Security Management Provider using the On-line services or forms, as outlined in this Appendix.

C5.8 Access to Regional Operating Centres and Emergency Operating Centres

Access to Operating areas at Regional Operating and Emergency Operating Centres for all personnel is restricted and subject to specific request.

C5.9 Access for Connected Parties

Employees, Consultants, and Contractors (and their Subcontractors), of a Connected Party company (as defined by **TP.SS 07.01** *Operational and asset related interfaces*), i.e. Lines companies, Generation companies, and Transpower Direct Supply customers, shall be

permitted access to only those sites defined in their *Site Entry Agreement*. Access to any sites and facilities not defined in their *Site Entry Agreement* is subject to specific request.

Access requests for personnel from within all the above defined companies shall be made to the Connected Party's representative responsible for managing access to Transpower sites and facilities. The Connected Party's representatives shall make all requests directly to the Site Access & Security Management Provider using the On-line services or forms as outlined in this Appendix.

C5.10 Requesting approval to make direct requests for site access

Should any company that is currently not permitted to make direct requests for site access to Transpower's Site Access & Security Management Provider wish to be able to make such direct requests, they must firstly seek approval from a Transpower Grid Performance Representative. Should approval be given, the Transpower Representative shall provide relevant details to the Site Access & Security Management Provider.

C5.11 Site access devices for short duration use

Access devices provided for short duration access shall be returned to the Site Access & Security Management Provider at the end of the limited-access period.

C5.12 Return of personal access devices

Upon an employee leaving a company or their duties do not require them to access Transpower facilities, their access device(s) shall be returned to the Site Access & Security Management Provider.

Under urgent circumstances access devices are 'transferable'. Please contact the Site Access & Security Management Provider to discuss available options.

Where Transpower or the Transpower Site Access & Security Management Provider become aware of personal access devices not being returned within a reasonable period, the company to which the equipment was issued will be billed the reasonable cost of replacement of the equipment and the overheads associated with the billing process.

C5.13 Lost or damaged access equipment

Replacement of lost or damaged access equipment shall be the responsibility of the recipient employer.

The Site Access & Security Management Provider will charge the cost of returning lost access devices if found and for the cost of replacement access devices to the recipient employer. Charges for these services are available upon request to the Site Access & Security Management Provider.

C5.14 Site-specific and other special keys and locks

The Site Access & Security Management Provider will, upon request, provide site-specific and other special keys and locks that are keyed within the Grid Performance national master-keying system. Contact the Site Access & Security Management Provider to discuss your request for 'special' keys and locks.

C5.15 Making On-line Site Access Requests

Those permitted to make requests directly to the Site Access & Security Management Provider shall use the On-line Web service as outlined in the separate document entitled "Transpower New Zealand Security Management Site Access & Key Management On-line Services" provided by Transpower's Site Access & Security Management Provider.

Note: *The On-line Site Access Request Service is being introduced progressively company-by-company. Until on-line access to the Transpower Site Access & Key Management Web Site is made available then all requests shall be made to the Site Access & Security Management Provider using the 'manual' method as described below.*

C5.16 Making 'Manual' Site Access Requests

Where the on-line service has yet to be made available, those permitted to make requests directly to the Site Access & Security Management Provider shall direct these to:

E-mail: Transpower. Access@opus.co.nz, or
Facsimile: (03) 474 8995, or
Phone: 0800 TPACCESS (0800 87 2223)

Requests may be submitted using any previously developed forms or spreadsheets. To assist, a MS-Word-form has also been developed and is available upon request to the above E-mail address, or can be downloaded from the Controlled Documentation > General Forms section of the Contractors & Consultants page of the Transpower Web Site.

C6 Description of Electronic Access & Security Systems and Keying

C6.1 Cardax Smartprox System Access Control card readers

Most Transpower restricted-access sites have PEC Cardax Smartprox access card reader systems.

The systems control both entry/exit through gates and doors, and provide intruder alarm setting and unsetting.

Entry Readers are proximity operated with a keypad. To access, a valid proximity keytag (or "bullet") and four-digit PIN is required. (Some Entry Readers, such as those at site entry gates, do not require the use of a PIN.)

All operations and activities associated with the access and security system are logged by the access control and security server and alarms monitored by the Security-monitoring Contractor.

Instructions for operating the Cardax systems are detailed in **Appendix D**.

C6.2 Station Access Keys

Most gates and doors require an SA (Station Access) key to gain access. A number of other key types are used to gain access to non-station facilities. For advice on personal access key requirements contact the Site Access & Security Management Provider.

C6.3 Changes to Access Control & Security System Hardware and Software, and Locking

All proposed additions and removals associated with access control and security alarm system hardware and software and associated with restricted-keyed locks must be approved by Transpower and notified prior to undertaking the work. Contractors shall advise the Site Access & Security Management Provider to discuss procedures for undertaking such work.

C7 Site Access and Security Management Assistance

C7.1 Assistance for On-site Personnel

Refer to **Appendix D** for instructions on use of substation access control and security system. The following is additional information to assist in determining possible issues preventing normal access into stations.

C7.2 Unable to gain access

If operational access through a access control and security system controlled gate or door is rejected, carry out the following checks before seeking further assistance from the Site Access & Security Management Provider:

Checking Valid Access

Contact your [contracted] company's nominated/authorised representative and have them check the Opus *"Transpower Site Access & Key Management Web Site"* to ensure access has been requested, approved and established for the facility, and your keytag has not expired.

If the keytag is not valid for the site or your access has expired, the company's nominated representative will need to make a formal request to access the facility.

If you are not permitted to view the Web Site, or if access details have been checked on the Web Site and found correct, contact the Site Access & Security Management Provider on **0800 TPACCESS (0800 87 2223)** to have them confirm access privileges.

Correct Reader Keypad Operations

If access privileges have been validated then check that the on-site access keypad operations have been followed correctly (refer **Appendix D**), in particular noting:

- That the correct sequence of keypad keys is used – Present keytag, enter 'PIN' when prompted, press [IN];
- The correct 'PIN' is entered (If you cannot remember your PIN contact the Site Access & Security Management Provider – see **clause C7.7** for 24/7 contact details);
- Keypad key presses are timely and firm.

New or First-time Use of Keytag at the Facility

Some sites only receive an updated copy of the Cardax access privileges database each night. However, should the nightly update not occur through a system fault then the site will not have been updated with your keytag data.

In this situation the Access Reader will reject the keytag presentation, indicating a "Card Unknown" or "Invalid Card" message. The system will attempt to communicate with the central Cardax Server to validate access. Re-try by presenting the keytag again within 1 minute of the system communicating.

Still No Success? – Probable Faults

If all the previous checks and attempts have been followed and access has still not been gained there are three likely scenarios:

1. The site's security system does not have your latest access data and has not been able to download it from the central access control and security system Server.
2. There is a security system fault at the site. This may be evident by display anomalies or lack of response on the Entry Reader.
3. There is a fault with your Keytag.

For problems 1 and 2, advise the respective Stations Maintenance Contractor or ROC to have them arrange an investigation.

Once all access and system checks have been made and all procedures correctly and repeatedly followed, and access is still not gained, then it is likely there is a fault with your Keytag – see below.

Suspected Faulty Keytag

To determine/confirm whether you have a faulty Keytag:

Does the Keytag currently work at other facilities that it should work at?

- If Yes, then the Keytag is not faulty. Re-check you have requested and been set-up access for the site and the keytag has not expired. See 'Checking Valid Access'. Re-check all on-site access procedures as outlined above.
- If No, then the keytag is probably faulty. This can also be verified if an Entry Reader unit does not beep when the keytag is presented to it. If you believe you have a faulty keytag contact your company representative to request a replacement keytag from Transpower's Site Access & Security Management Provider.

Access Assistance
Contact the Site Access & Security Management Provider to assist with gaining access where there is an access control and security system fault or a faulty/invalid keytag is preventing normal access. (Refer **TP.SS 07.40 section 8** and **Appendix C clause C7.7**.)

C7.3 Required notifications to the Security Monitoring Contractor

In the following situations the Security monitoring company shall be advised:

- Repairs and testing of substation access control and security alarm systems;
- Repairs and testing of fire alarm systems;
- Any others situations where a security or fire alarm may activate during system maintenance or repair operations, either directly on the systems or as a result of work within the buildings which house these systems.

Phone: **TPSN 7502**, or
Where TPSN is not available then Telecom **0800 TPALARMS (0800 87 2527).**

C7.4 Security System Fault

Suspected faults with an access control and security system shall be reported to the respective Regional Operating Centre or directly to the respective Stations Maintenance Contractor. Issues at non-substations' sites shall be directed to the respective Transpower Representative or Facilities Management Contractor.

For Security Maintenance Contractors the Access Control & Security Systems Support Contractor will assist in rectifying security system faults. Contact ECL Security:

(03) 339 8788 (Monday to Friday 8:00 a.m. to 4:30 p.m., except Public Holidays).

C7.5 Security Guard Response – Information for Stations Maintenance Contractors

Confirmed security breach alarm activations will be attended by:

- A Guard – arranged by the Security-monitoring Contractor, and
- A Stations Maintenance Contractor representative – arranged by the respective ROC.

Where it has been decided by the Regional Operator that a security breach alarm will not be attended by a guard response, as defined in **TP.SS 07.40 clause 11.2.3**, but the attending Stations Maintenance Contractor requests that a guard is required, then the Stations Maintenance Contractor shall request that the Regional Operator contacts the security-monitoring contractor to initiate the required security guard response as defined in **TP.SS 07.40 clause 11.2.1**.

Should a Stations Maintenance Contractor's representative require an ETA on a guard-response or further details of an alarm activation, the Stations Maintenance Contractor shall contact the Security-monitoring company on **0800 TPALARMS (0800 87 2527).** The Security-monitoring company will contact the guard-response contractor to obtain the required guard-response information, and then communicate this back to the attending Stations Maintenance Contractor.

Note **The above 0800 number is ONLY for requesting ETA's (or additional alarm information) – and not for requesting or cancelling guard call-outs.**

Refer to **Appendix G** for security guard response capabilities.

C7.6 Regional Operating Centres

The three Transpower Regional Operating Centres provide the following tasks in security management:

- To assist the Security-monitoring Contractor and Stations Maintenance Contractors in resolving on-site security issues, and Security Breach Reporting;

- Dispatching a Stations Maintenance Contractor representative to accompany a Guard;
- Dispatching a Security Maintenance Contractor to attend to a security system fault;
- Authorising the remote un-setting of a station intruder alarm, and if required the unlocking of electronically-locked entry door, for entry to undertake critical operation of power system equipment when personnel are prevented from normal station entry due to an access control system or access keytag fault.

Contact details for Regional Operating Centres (ROCs) are:

North	Auckland	TPSN 2400	Telecom (09) 274 8736
Central	Wellington	TPSN 5555	Telecom (04) 563 5087
South	Christchurch	TPSN 7905	Telecom (03) 349 7043
HVDC	Christchurch	TPSN 7902	Telecom (03) 349 8671

C7.7 Transpower's Site Access & Security Management Provider

For general assistance with site access and security management issues, queries relating to requests for access to restricted sites and access devices, and for assistance with site access problems, contact:

Opus International Consultants Limited, Dunedin

Phone	**0800 TPACCESS (0800 87 2223)** – 24 hours, 7 days
E-mail	Transpower.Access@opus.co.nz
Address	Opus House 197 Rattray Street Private Bag 1913 Dunedin

D ACCESS CONTROL AND SECURITY SYSTEM OPERATING INSTRUCTIONS

D1 Purpose

Transpower's access control and security alarms are integrated Cardax FT systems providing both access and egress control to and from Transpower facilities and security alarms. All operations and activities on the system are logged and monitored at a central location.

While the systems at the various types of facilities are generally the same, there are configurations and system operations specific to some sites. These instructions cover the generic operations for all facilities plus the additional site-specific instructions for Substations with access control on Switchyards, and Substations with alarmed power fences. Additional-specific instructions for Transpower Offices, the Addington Warehouse, and the Regional Operating Centres are not included in this document.

D2 'Cardax FT' access control & security system description

A "Cardax FT" access control and security system is distinguished by the main reader unit displaying status and messages in text.

D2.1 Cardax FT access control & security system Prox Card Readers

The access control and security system's Prox readers are used for gaining access, and for Setting/Un-setting the security alarm system. The system's entry reader is a proximity reader complete with keypad, requiring both a valid keytag and a 4-digit PIN number for gaining access and Setting/Unsetting the security alarm system.

The system's entry reader has an LCD panel that displays four lines of text to indicate the status of the system and to provide feedback to the user.

Common texts and their meanings are as follows:

Secure: – indicates that the door is locked and is ready to receive a keytag;

Enter PIN: – indicates that the reader expects the entry of your 4 digit PIN number;

Please enter: – indicates that the door is electrically unlocked and, once unlocked with a key (if required), is ready to be opened;

Alarms SET: – indicates that the status of the security alarm system is Set. If this text is not visible, the security alarm system is UNSET;

Wrong PIN!: – indicates that the incorrect 4 digit PIN number has been entered;

No Access!: – indicates that your keytag is not valid for this door;

Unknown card!: – indicates that your keytag has not been programmed into the system;

Failed to SET: – indicates that the security alarm system failed to Arm. This could be because a monitored door has been left open;

Standby: – indicates that the reader is performing a function that requires you to wait for a response.

Keypad Function Keys:

F1 Key – Use to arm the alarm zone
F2 Key and F3 Key – Not used

D3 'Cardax FT' access control & security system operating instructions

D3.1 Gaining access and un-setting the Security Alarm System – Buildings

Present your access keytag in front of the system's Prox/keypad main door entry reader. The reader will beep and "PIN Please" text will appear on the LCD display. Enter your personal 4-digit pin number and push the "IN" key. The text "Please Enter" will appear on the display, the main door will electrically unlock and the security alarm system for the

substation will UNSET. The door will remain electrically unlocked for 30 seconds allowing you this period of time to enter through the door once the door has been unlocked with a key (if required).

After 30 seconds, the door will automatically electrically lock.

D3.2 Egress from buildings

All Station doors can be exited without use of electronic devices.

D3.3 Setting the Security Alarm System

After exiting the building as described above, the security alarm system has to be SET if you are the last person to leave the building.

Note: *The setting of security alarm systems at Regional Operating Centres is undertaken, where required, by the Centre's Operators.*

Firstly, ensure that the substation doors and switchyard gates are securely closed and locked. (Also, where Power Fences are installed on switchyard security fences, ensure that if the Power Fence has been manually isolated that this has been restored to normal.)

Perform the following procedure at the system's Prox/keypad entry reader:

To SET the security alarm system, first push the "F1" key on the keypad. The text "Card Please" will appear on the LCD display. Now present your access keytag to the front of the Prox/keypad entry reader. The text "Enter PIN" will now appear on the LCD display. Now enter your personal 4-digit pin number, and then push the "IN" key on the keypad. The text "Alarms Set" will now be displayed on the LCD display, along with "Secure" and the "Date & Time". The security alarm system is now SET.

D3.4 Normal Access/Egress when the Security Alarm System is UNSET

For normal access, follow step **D3.1** above. For normal egress, follow step **D3.2** above.

D3.5 Door Held Open Too Long Alarm

Transpower is required to ensure that its Substations are secure from unauthorised entry at ALL times. Transpower requires that the main controlled building door is kept closed and secured (Fully Closed and unable to be opened without the appropriate key) at ALL times unless otherwise secured by authorised personnel visually monitoring and standing near to the door, and with a clear view of it.

To ensure compliance with this regulatory requirement, the access control and security alarm system installed in Transpower substations monitors the length of time the main access door is left open. Should the door be held open for a period exceeding 2 minutes, a "Door Held Open Too Long Alarm" will be enunciated by the main entry door Prox/keypad entry reader – as a continuous beeping sound until the door is closed again.

"Door Open Too Long" alarms will be reported to the Transpower access control and security system server.

D3.6 Access to Switchyards with Access Control System

You must first enter and unset the Control Building security system (see **clause D3.1**).

The switchyard Prox reader will now be enabled. Present your access keytag in front of the Prox switchyard entry reader. The reader will beep and if your keytag is valid, the gate is electrically unlocked for 30 seconds allowing you this period of time to enter the switchyard.

After passing through the gate it will automatically electrically lock afterwards.

Switchyard personnel gates with access control are also generally able to be accessed with a Station's ODS access key.

D3.7 Egress from Switchyards with Access Control System

Turn the free handle nightlatch to exit the switchyard. After passing through the gate it will automatically lock afterwards.

The system monitors how long the switchyard access gate is open for. Should the gate be held open for a period exceeding 99 seconds a Door held Open Too Long Alarm will occur. This is enunciated to the central station until the gate is closed again.

D3.8 Switchyard Power Fences

Power Fences on Switchyards and secure compounds are automatically controlled by the Access Control System – when the security system is Unset or Set then the Power Fence will also Disarm or Arm accordingly.

Where work is being undertaken on or within close proximity to a Power Fence the respective Power Fence isolation system switch shall be used. Refer **Appendix E** for Power Fence Operating Instructions.

D3.9 National SCADA Alarms

"Security Breach" alarm activations are enunciated at the ROCs via National SCADA.

D3.10 Typical Access Control & Security Alarm System Operational Problems

Occasionally, you may experience problems in operating the access control and security alarm system. The following notes may assist you in rectifying any such problems.

Building Security alarm system does not SET:

This is indicated by the display of the text "Alarms SET Failed!" on the LCD display.

Possible reasons are:

- Incorrect sequence of operations.
- A monitored door is still open in the substation. Check that all doors are securely closed/locked and that no PIR detectors have been damaged or tampered with.
- The alarm setting procedure was not carried out quickly enough. Note that after a valid keytag is presented to the card reader the user has a period of approximately 10 seconds to carry out the remainder of the relevant procedure.
- A switchyard personnel gate is still open.
- A Switchyard Power Fence has not been re-stored from the isolated to operational state.
- A Switchyard Power Fence is in an activated state – check that any paper, birds or vermin are not triggering the system and preventing it arming.

Building access is not granted:

This is indicated by the text "No Access" or "Unknown Card" or "Invalid Card" or "Wrong PIN".

Possible reasons are:

- Your keytag is not valid for this site/access group.
- Your keytag has expired (your keytag validity date is identical to your Competency expiry date. To guarantee access to Transpower's substations, renewal of your Competency must be notified to the Security Management Contractor).
- Your PIN number is invalid or has been incorrectly entered.
- The door access procedure was not carried out quickly enough. Note that after a valid keytag is presented to the card reader, you have a period of 30 seconds to carry out the remainder of the relevant procedure.

Switchyard access is not granted (where Access Control System installed):
This is indicated by three low tone beeps on the Switchyard Prox reader.

Possible reasons are:

- You have not Unset the Control Building alarm system yet;
- Your keytag is not valid for this switchyard;
- Your keytag has expired (see "Building Access is not granted", above).

Should you continue to have problems refer to **Appendix C** for further assistance.

E POWER FENCE OPERATING INSTRUCTIONS

E1 Overview

E1.1 Substations may have a high voltage Power Fence installed to their:

(i) site perimeter security fence, and/or

(ii) Control Building security fence, and/or

(iii) outdoor switchyard security fence.

E2 Integration of Power Fence to Access Control and Security System

E2.1 Power Fences operate via a Cardax Trophy FT Power Fence Controller connected to the Substation Cardax FT access control and security system.

E2.2 For normal operation the arming and disarming of a Power Fence Controller is controlled by the Control Building Cardax access control and security system. For programming and fault resolution technicians can also operate the Power Fence via a Remote Arming Terminal (RAT) located inside the Control Building. The RAT also displays the status of the Power Fence.

E2.3 Where a Power Fence is on a site perimeter security fence or Control Building security fence then the Power Fence system provides an entry and exit delay operation where:

(i) after entering a gate using a proximity access device the Power Fence will not alarm for 1 minute to allow for disarming of the Power Fence at the Control Building main door access control and security system Entry Reader;

(ii) after Setting the Control Building security system using a proximity access device the Power Fence will not arm until 1 minute later to allow exiting through the security gate.

E2.4 Where a Power Fence is on an outdoor switchyard security fence the Power Fence arming and disarming is automatically undertaken by the setting and unsettling of the Control Building access control and security system.

E3 Power Fence Isolation System

E3.1 Where work is to be undertaken in close proximity to a Power Fence a manual isolation system is provided to allow personnel to disable the Power Fence conductors while leaving the Cardax Trophy FT Power Fence Controller operating. *Power Fence Controllers shall not be turned off except for servicing by trained technicians.*

E3.2 The Power Fence isolation system comprises a switch installed in a green lock-out box. The lock-out box will be located in the vicinity of its respective Power Fence Controller, the KeySafe, or just inside the main entry door to the station.

E3.3 To isolate the Power Fence open the lock-out box and turn the switch to the "Isolated" position. A red LED will illuminate. Take one of the padlocks provided with the lock-out box and secure this to lock the lid of the box. Take the key to prevent others accessing the lock-out box. *Power Fence lock-out boxes are provided with two padlocks. The lock-out box lid will accommodate up to four padlocks. Where the two padlocks provided with the lock-out box are already in use then either a Recipient (blue) padlock or a personal padlock may be used.*

E3.4 The person who removes the last locked padlock from the lock-out box lid shall return the isolation switch to the neutral position. ***The Power Fence isolation switch must be in the neutral position in order for the security system to be Set.***

E3.5 Power Fence Isolation Switch/Lock-out Box

E4 Otahuhu Substation Transition Stations' Power Fences

E4.1 The Power Fences on the security fences to the Transitions Stations at Otahuhu Substation are controlled manually via a key-switch located in a KeySafe:

(i) at Otahuhu 220kV Substation Control Building the Transition Stations KeySafe located in the ground floor foyer operates the Huntly, Ohinewai, Otahuhu C, Pakuranga, and Southdown Transition Station Power Fences;

(ii) at Otahuhu North (GIS) Substation Control Room that Station's KeySafe includes a key-switch that operates the Henderson Transition Station Power Fence.

E4.2 When a Transition Station access key is withdrawn from a KeySafe the respective Power Fence is disarmed. That key is then used to open the gate locks. There is only one key for each Transition Station – so the fence cannot be armed while its key is in use.

E4.3 A Transition Stations master access key is held in the Otahuhu 220kV Substation Control Building Transition Stations KeySafe. This key is only able to be withdrawn by selected personnel, and shall only be used where it has been confirmed that a Transition Station key has been lost and that Transition Station Power Fence is urgently required to be armed or disarmed for access prior to the lost key being found or a replacement key being provided.

F KEYSAFE OPERATING INSTRUCTIONS

F1 Overview

F1.1 Keysafes are installed at Substations and the Regional Control Centre South to control outdoor switchyard access keys (ODS access keys), the switchgear key-press door key, and the Issuer key. *Some Substations do not have ODS access keys and therefore the KeySafe will only contain the switchgear key-press door key and the Issuer key.*

F1.2 Where the site has a Cardax access control and security system the KeySafe will be electronically controlled. Where the site does not have a Cardax access control and security system the KeySafe will have no electronics but still provide similar functionality.

F2 Electronic KeySafe Operating Instructions

F2.1 Open the KeySafe door using a personal proximity keytag. *A KeySafe can be opened with proximity keytags that are configured for the access-controlled entry door of the respective facility.*

F2.2 A KeySafe may have four, six or eight ODS access keys. (The number of ODS access keys has been determined by the size of the station and the configuration of its switchyard(s) and other buildings that are accessed with these keys) *Sites that do not have ODS access keys will either have a smaller KeySafe with no provision for ODS access keys, or a standard KeySafes with provision for future ODS access keys.*

F2.3 An ODS access key is taken by turning and withdrawing its respective key-switch key. When this key is withdrawn the corresponding LED on the outside of the KeySafe will illuminate. *An ODS access key can be taken by all those that are able to open the KeySafe door with their personal proximity keytag.* ***Note: ODS access keys withdrawn will be logged to the person who was logged as last opening the KeySafe door. It is therefore recommended that each person close the KeySafe door immediately after withdrawing a key, and they do not allow others to withdraw keys while they have the door open.***

F2.4 A KeySafe will have a switchgear key-press door key and an Issuer key attached together. The switchgear key-press key is captured by a key-switch and is only removable by those personnel that have the appropriate Switching Competency and their proximity keytag has been configured to allow access to these keys. When this keyset is withdrawn the corresponding LED on the outside of the KeySafe will illuminate.

F2.5 Repeat the above instructions for return of KeySafe keys. **Note:** Ensure that keys inserted into the key-switches are turned to the closed/locked position to confirm their return – the corresponding LED will go out when the key is in the correct position. *Note: While some-one has the KeySafe door open it is acceptable to allow others to return the keys they removed.*

F2.6 Where normal access with a proximity keytag is not functioning then the KeySafe door can be opened by pressing the emergency door release (EDR) switch. The switch shall be re-set using the plastic key inside the KeySafe. ***These actions will be electronically logged and tracking its use will include all those logged into the Station at that time.***

F3 Non-electronic KeySafes

F3.1 Non-electronic KeySafes differ from electronic KeySafes in that they:

(i) Have no electric lock, and are therefore accessed with a Station Access key (SA or RS) rather than a proximity-keytag.

(ii) Have no LED's to indicate keys that have been withdrawn. Keys taken shall be recorded in the Station Entry Log – refer **clause 7.4.1**.

(iii) Have no other electronic components for control or monitoring of keys and alarms.

F4 Otahuhu Substation Transition Stations' Power Fence KeySafes

F4.1 Refer **Appendix E**.

F5 Electronic KeySafe Images

ODS Access Keys and Key Out Status LED's

Mag-lock, Prox-entry Reader, EDR, EDR Re-set key, Switchgear Key-press and Issuer Keys

ODS Access Key Key-switches not [yet] used

Captured Switching Key-press Key and Issuer Key

Emergency Door Release and Re-set Key

G SECURITY GUARD RESPONSE CAPABILITIES

G1 Overview

This Appendix details the national security guard response arrangements for stations and other facilities with intruder alarm systems monitored through the National access control and security system alarm monitoring system.

G2 Facilities with monitored intruder alarm systems

G2.1 All stations having Cardax access control and security alarm systems are monitored through a national alarm-monitoring company. Responses to alarms shall be managed in accordance with **TP.SS 07.40 section 11** and **Appendix C clause C7.5.**

G2.2 The following sites, while having monitored access control and security alarm systems, are **not** provided with a guard-response service:

- Arthurs Pass (S3)
- Castle Hill (S3)
- Fighting Bay (DC2)
- Manapouri (S1)
- Ohakune (N5)
- Oteranga Bay (DC2)
- Otira (S3)
- Tangiwai (N5)
- Tiwai (S1)
- Tokomaru Bay (N7)

G3 Facilities with no intruder alarm system

G3.1 The following sites do not have Transpower intruder alarm systems or their intruder alarm system and responses are managed by a third-party asset owner:

- Aratiatia
- Argyle
- Cobb
- Coleridge
- Clyde
- Huntly
- Kensington
- Maretai
- Marsden
- Matahina
- Meremere
- Okere
- Otahuhu Generation switchyards
- Rangipo
- Waipapa

G4 Guard response times

G4.1 Station Maintenance Contractors assisting in responding to security breach alarms are advised that due to the remote location of many stations and/or the guard-response capability in some areas of New Zealand, some guard-response times will be less than that of the accompanying Stations Maintenance Contractor. To obtain an ETA on a guard response contact the security monitoring company – refer **Appendix C, clause C7.5**.

H TABLE OF CHANGES

Issue Number	Section or Clause Number	Change	Date
13	Sections 1 & 3	Very minor changes out of Public Safety Management System	Feb 2012
	Clause 7.4.8	Added requirement to check for others on site and also to reactivate the Power Fence, where fitted, prior to setting alarms.	
	Appendix C5.8 and C5.9	Previous clause C5.8 deleted as there are now no operating contractors with the in-sourcing of ROC's into Transpower. Clause C5.9 now becomes clause C5.8 etc. Replaced 'Back-up Operating Centres' with "Emergency Operating Centres" Deleted phrase "except as defined in clause C5.8"	
12	Appendix E	E3.1 – 'disabling' changed to 'disable' E3.2 – updated 2nd sentence E3.4 changed two occurrences of 'normal' to 'neutral' E3.5 image changed E4.2 and E4.3 – changed two occurrences of 'removed' to 'withdrawn'	May 2011
	Appendix F	F2.3, F2.4, F3.1 – changed six occurrences of 'removing', 'removed', or 'remove' to 'withdrawing', withdrawn', or 'withdraw' respectively F2.3 – First sentence – changed 'attached' to respective' F2.6 – Last sentence – changed 'it' to 'its'	
11	Section 3	Transpower's Drug & Alcohol Policy has been added to the References.	Mar 2011
	Section 4	Item (j) has been added to advise that any person entering a Transpower location may be subject to random drug & alcohol testing.	
	Clauses 7.1.5, 7.4.4, 7.4.6, and Appendix F	Reference to new electronic KeySafes that hold ODS access keys, switchgear key-press key, and Issuer key.	
	Clauses 7.4.3, 7.4.8, D3.9	Change in operation of Power Fences.	
	Clause 8.2.3	Change in procedure for Cardax fault response.	
	Clauses 8.3.1, 8.4.1	Change references to master keys held by Stations Maintenance Contractors.	
	Clause 9.1.2	Requirements for generating at Security Breach Report.	
	Clauses C6.1, C7.2, and Appendix D	Removal of reference to older Cardax NT access control & security systems.	
	Clause C6.1	Removal of reference to using Cardax Exit Readers for	

Issue Number	Section or Clause Number	Change	Date
		existing Substations.	
	Clause C7.3	Change of TPSN for security alarm monitoring company.	
	Clause C7.6	Contact number for HVDC Operating Centre added.	
	Appendix E	New Power Fence Operating Instructions. (Previous Appendix E is now Appendix G.)	
	Appendix F	New KeySafe Operating Instructions. (Previous Appendix F removed.)	
	Note:	*The list of pending changes detailed in previous Appendix F are currently in the process of being implemented – completion of all enhancements and changes is June 2011.*	
10	Section 4	Item (h) has been altered to prohibit smoking on work-sites, in all buildings, restricted areas and areas set aside for eating.	Jul 2010
	Sections 5.1.1, 6.5.1 (e), 7.2.1, 7.3.1,	Changes incorporated remove references to "Direct and continuous supervision" and "General supervision" and replace these with "Supervision" and "Environment Safety" to better define the responsibilities of the RAE Competency Certificate holder for site safety supervision of staff as opposed to specific work task supervision.	
9	Section 4	Item (d) has been added to clarify the expectations around for Roadgates (boundary gate) when staff are on or off site. Item (i) has been added, prohibiting the use of portable metal/conductive ladders in restricted areas.	Nov 2009
	Subsection 7.2.1 & 7.3.1	A ratio of 1:6 has been added to the notes in these clauses for the number of non competent persons being supervised by an RAE competent person.	
	General	Grid Asset Management – Field changed to Grid Performance throughout the document.	
8	Subsection 7.2	Notes: 1 – Updated	Apr 2008
	Appendix C5.17	0800 TPACCESS corrected	
	Appendix G	Added Table of Changes	
7		1. Change of Reference from Service Specification TP.SS 06.23 to TP.SS 06.21, and inclusion of new Service Specification TP.SS 06.25 (Section 3, subsection 6.5, and Appendix C – C2, C3). 2. Change of definition from "access equipment" to "access device" (subsection 5.1). 3. Inclusion of responsibilities of Site Access & Security Management Provider (subsection 6.1), and of Stations Maintenance Contractor (subsection 6.4). 4. Removal of one responsibility from the Security-monitoring Contractor (subsection 6.2). 5. Clarification of site entry/exit procedures (subsections 7.4 and 7.5). 6. Inclusion of station entry procedures when there is an access system or device fault (section 8).	Oct 2007

Issue Number	Section or Clause Number	Change	Date
		7. Clarification of security breach alarm activation actions (subsection 11.2). 8. Change of name for Appendix C. 9. Change of definition from "access equipment" to "access device" (section C2). 10. Clarification of scope of Site Access & Security Management Services (section C4). 11. Complete update of Site access management policies (section C5). 12. Clarification of description of electronic access & security systems and keying (section C6). 13. Update to Site Access & Security Management Assistance information (section C7). 14. Insertion of new Appendix E – Security Guard Response Capabilities. 15. Insertion of new Appendix F – Pending Changes to Station Security Procedures. 16. Renaming of previous Appendix E to Appendix G.	

I CONTROLLED DOCUMENT FEEDBACK FORM

If you would like to submit any feedback or suggestions to Transpower to improve this document, there are two ways you can do this. You can either complete the form below and fax it to: Controlled Documentation Services, Transpower New Zealand Ltd, on 04 495 7100; **or** you can submit a form online – just look for the *Controlled Document Feedback Form* on the Contractors/Consultants section on our website at www.transpower.co.nz .

Content change request	No:
Date:	Initiator's name/title:
Company:	Phone: Fax: Email:
Controlled document number:	TP.
Controlled document title:	
Affected section or clause number(s):	
Present clause:	
Proposed change:	
Reason for change:	
If you are including supporting information or attachments, please list here, e.g. photos:	