



# **NEW ZEALAND FIRE SERVICE**

## **CERTIFICATION FOR AUTOMATIC FIRE ALARM SERVICE PROVIDERS**

**VERSION 1.4**

**21<sup>st</sup> June 2006**

**Document History**

Version	Date	Comment
1.0	25 <sup>th</sup> May 2005	Final
1.1	12 <sup>th</sup> Oct 2005	Update
1.2	25 <sup>th</sup> Nov 2005	Update
1.3	22 <sup>nd</sup> Dec 2005	Changed reference to AS2201.1-2004
1.4	21 <sup>st</sup> June 2006	Appendix 2,

**Copy Right**

The copyright of this document is the property of New Zealand Fire Service.

New Zealand Fire Service  
 80 The Terrace  
 PO Box 2133  
 Wellington  
 New Zealand  
 Phone: 04 – 496 3600

**Table of Contents**

Document History ..... 2

Copy Right..... 2

Table of Contents ..... 2

1 Introduction ..... 3

    1.1 Purpose ..... 3

    1.2 General ..... 3

    1.3 Service Providers Management System ..... 3

    1.4 The Certification Process ..... 4

2 Quality System ..... 7

    2.1 Management of the System ..... 7

    2.2 Control of Documents and Records..... 8

    2.3 Contract Agreement..... 9

    2.4 Facilities, Equipment ..... 9

    2.5 Business Continuity / Business Recovery ..... 9

    2.6 Training and Work Instructions..... 10

    2.7 Continual Improvement ..... 10

Appendix 1: Non-ICT Documentation available for Inspection ..... 11

Appendix 2: Terms of Reference for the Assessment of the Computer and  
 Telecommunications Facilities of a candidate Service Provider..... 13

Appendix 3: Standards and Requirements ..... 14

## **1 Introduction**

### **1.1 Purpose**

The purpose of this Document is to outline the New Zealand Fire Service's requirements for Automatic Fire Alarm Providers (**Service Providers**) becoming and remaining certified to provide services in respect of Automatic Fire Alarm Systems.

### **1.2 General**

This certification has been developed by the New Zealand Fire Service (NZFS) to provide Service Providers with a model for their management system. It is based upon a variety of standards such as ISO9001:2000 and the Telarc Q-Base Code. It also references other documents, specifically the Australian Standard AS 2201.2-2004. It recognises the need for a management system to have formalised structures and systems in place meeting the needs of the NZFS and Service Providers.

Service Providers must be certified in order to provide monitoring services for Automatic Fire Alarms. Certification demonstrates that Service Providers:

- Have a formal commitment to the NZFS through a structured management system;
- Consistently manage processes;
- Possess a structured quality management system to continually improve their processes and service to the general public and the NZFS; and
- Operate within a Grade C2 premises as detailed in Australian Standard AS 2201.2-2004.

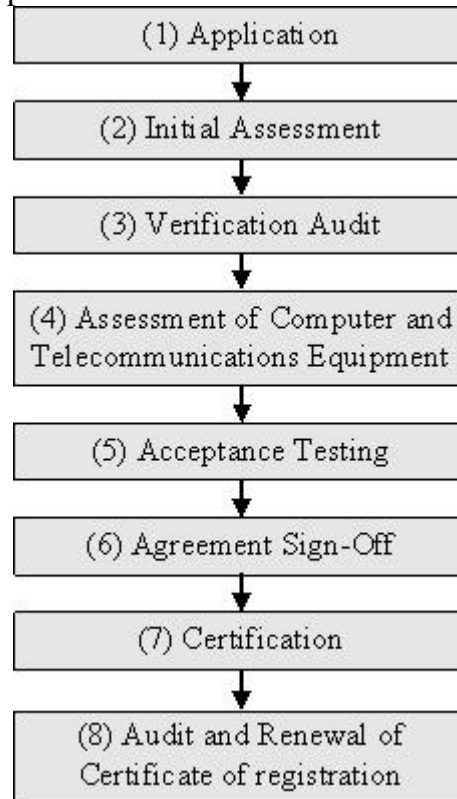
### **1.3 Service Providers Management System**

The Service Provider's system to monitor Fire Alarms must:

- Be technically robust and be able to transmit fire alarm signals from fire alarms to the NZFS Communication Centres rapidly, reliably and unambiguously (refer to Appendix 2 for standards and requirements);
- Provide for new fire alarms to connect in a straightforward manner, no matter where they are in the country;
- Provide for all connected fire alarms to be monitored and service agents notified of non-normal events;
- Promote reduced incidence of false alarms from connected fire alarms; and
- Enables the NZFS to gain more information from fire alarms.

## 1.4 The Certification Process

Certification is an eight-step process:



The NZFS may appoint an agent to undertake various tasks in the certification process. Fees are payable to the NZFS as indicated below. Fees may be required to be paid in advance of the relevant stage and, if so, are non-refundable. The schedule of fees is available on request.

### **(1) Application**

The Service Provider submits an application and a non-refundable application fee to the NZFS.

The application must include:

- An audited set of accounts;
- Provide evidence that their building services, construction, operation, equipment and staff meet the requirements of AS 2201.2-2004 for grade C2 as a minimum;
- Provide a business continuity or business recovery plan;
- Detail concerning:
  - The size of the Service Provider's entity;
  - The Service Provider's organisational structure;
  - The relevant experience of key staff;
  - That the Service Provider can meet the relevant NZFS service levels for the monitoring of Automatic Fire Alarms.

NZFS will assess the application on a qualitative basis and may undertake credit references as it sees fit.

Upon the NZFS being satisfied that the Service Provider's application is in order the Service Provider may continue with the next step.

## **(2) Initial Assessment**

Fees for this stage are assessed on an hourly rate.

This is a two-step process. First, the NZFS may visit the Service Provider's premises and discuss with the Service Provider documentation requirements e.g. Business Manual, Quality Manual etc.

'Non-Information and Communication Technologies' documentation that should be made available for inspection in support of a company's Application for Certification as an Automatic Fire Alarm Service Provider is listed in Appendix 1.

Secondly, following completion of the identified documentation the Service Provider will provide copies for review, including compliance with applicable Codes of Practice and government regulations etc. An assessment will be undertaken as to how the Service Provider's staff will apply the processes described in these documents.

The NZFS will then produce a report indicating whether the Initial Assessment has been passed or recommending remedial action should the Initial Assessment be failed.

## **(3) Verification Audit**

This step would be required only if the Initial Assessment resulted in the requirement of remedial action. The Service Provider will contact the NZFS to arrange a verification audit after undertaking the remedial actions. This step may be repeated in whole or in part as required.

There is a fee for the Verification Audit(s) based on a hourly rate.

## **(4) Assessment of Computer and Telecommunications Equipment**

An assessment will be undertaken of the Service Provider's computer and telecommunications equipment, according to the terms of reference in Appendix 2.

Prior to this assessment, or reassessment, the NZFS will inform the Service Provider of the fee for this assessment.

The NZFS will then produce a report indicating whether the Assessment of Computer and Telecommunications equipment has been passed or recommending changes should the assessment be failed. The Service Provider may then address these issues and ask the NZFS to repeat the assessment.

**(5) Acceptance Testing**

The NZFS may conduct an onsite assessment to ensure that the system is working effectively. The onsite assessment will include an Acceptance Test with the Test STSMHS, as specified by the NZFS. The Acceptance Test results will be documented in an Acceptance Test Report.

Should the Service Provider not pass the Acceptance Test, then any non-compliance identified during this process is discussed with the Service Provider and will be detailed in the Acceptance Test Report. The Service Provider must address these non-conformances and request that the Acceptance Test be repeated.

Should the Service Provider not pass the Acceptance Test the first time, then a fee as advised by NZFS, will be payable before each additional Acceptance Test.

**(6) Agreement Sign-Off**

Following completion of steps 1 to 5 the Service Provider and NZFS will enter into a contract for the provision of Automatic Fire Alarm Services.

**(7) Certification**

Following step 6 the NZFS will issue to the Service Provider a Certificate of Registration.

Each Certificate of Registration will remain valid for one year and may be renewed in accordance with step 8. Each certificate may also be revoked in accordance with step 8.

There is no fee for the issue of a Certificate of Registration.

**(8) Audit and Renewal of Certificate of Registration**

At least two months prior to the expiry of a Certificate of Registration a Service Provider must contact the NZFS to arrange an audit to assess compliance with this document. This audit will not be as detailed as the initial audit; it will be a sampling exercise to ensure that the Service Provider continues to meet the certification requirements.

There is a fee for the audits undertaken.

The NZFS will produce an audit report and provide a copy to the Service Provider.

Should the NZFS be satisfied with the audit results the Certificate of Registration will be renewed for a further year.

Should the NZFS not be satisfied with the audit results the Service Provider's Certificate of Registration will not be renewed. In order to continue to be able to provide services as a Service Provider the Service Provider must address the issues of non-compliance detailed in the audit report and request a follow up audit. This step may be repeated as often as necessary. Should the NZFS be satisfied with the audit results the Certificate of Registration will be renewed.

The NZFS may undertake more frequent audits as a result of audit findings. There will be a fee associated with these additional audits.

## **2 Quality System**

### **2.1 Management of the System**

---

**Requirement**

The Service Provider must appoint one of its staff (the Systems Coordinator) to have overall responsibility for compliance with the requirements of this document in the day-to-day work of the organisation. This must be a senior person with sufficient authority in the organisation to ensure that all other staff follows the management system at all times.

The responsibility and authority of this Systems Coordinator must be defined in a written job description or similar document approved by the Chief Executive or equivalent of the company. The Service Provider must establish either a business or quality manual that include the requirements of this document.

The Service Provider must document, authorise and advise staff of the following policies:

- Health & Safety Policy
- Quality Policy
- Environmental Policy

The Service Provider must conduct management reviews at six monthly intervals to monitor the management system and ensure its effectiveness.

The Service Provider must conduct monthly internal audits to reinforce agreed best practices and to continually improve the system.

Records of the management reviews and internal audits are to be maintained and upon request by NZFS made available for inspection.

---

## 2.2 Control of Documents and Records

---

**Requirement** The Service Provider must have a system for uniquely identifying and controlling all its documents to ensure that only the current editions are in use and that no unauthorised changes are made.

The document control system must also ensure that copies of documents are given to everyone who needs them so that they are not tempted to rely on memory for information.

Records must be sufficient to demonstrate that all essential processes have been carried out, that all essential inspections or tests have been undertaken in compliance to the management system and the requirements of this document.

Records must be retained for an appropriate period. This period will depend upon the nature of the record e.g. inspection records.

---

**Guidance** Documents are those that are essential for ensuring the quality of the service and the proper operation of the Service Providers management system. Documents include drawings, material specifications, work instructions, risk assessments, equipment and specifications, operation manuals, reference manuals, procedure manuals, job descriptions, regulations, etc.

The term “document” includes any method of recording or displaying information. Documents may be in the form of paper, computer disks, wall charts, posters, videos, photographs, Codes of Practice etc. Whatever the format, documents should be authorised and kept up to date if used as a permanent reference.

The key records necessary to demonstrate the performance of the management system should be listed. To ensure the system is easily checked, the records should show who is responsible for them, where they are kept and for how long.

---

### 2.3 Contract Agreement

---

**Requirement** The Service Provider must ensure that the NZFS's performance standards (as per Appendix 3) and performance standard related reporting requirements are adhered to.

The Service Provider must at least meet the performance standards as set out in the 'Code of Practice for the Automatic Fire Alarm System' and in the agreement between NZFS and the Service Provider.

The Service Provider must monitor and report on the performance standards as set out in the 'Code of Practice for the Automatic Fire Alarm System'.

---

**Guidance** Detailed in both the Agreement between NZFS and the Service Provider and the 'Code of Practice for the Automatic Alarm System' are detailed expectations, e.g., objectives and reporting requirements. The Service Provider needs to ensure that such expectations and the methodologies to manage these expectations are detailed within the documented procedures.

---

### 2.4 Facilities, Equipment

---

**Requirements** With respect to building services, construction, operation, equipment and staff, New Zealand Fire Service adopts the standards according to the Australian Standard AS 2201.2-2004 'Intruder Alarm Systems, Part2: Monitoring Centres'. It is expected that all building services and construction will meet the requirements of Grade C, and all operation, equipment and staff will meet the requirements of Grade 2.

The Service Provider must produce evidence that their facilities and equipment meet these requirements as a minimum.

---

**Guidance** The Service Provider should identify the critical equipment and services that it buys. The service levels related to these items must be correct if they are not to detract from the quality or safety aspects of its own goods or services.

---

### 2.5 Business Continuity / Business Recovery

---

**Requirements** The Service Provider must provide a business continuity plan.

---

**Guidance** The business continuity / business recovery document should include the critical resources, the related risks, risk assessment (including business impact analysis), risk management and risk monitoring. Evidence of systems to assist business continuity should be detailed in the plan e.g. automatic fire suppression systems at the Service Provider's premises.

---

## 2.6 Training and Work Instructions

<b>Requirements</b>	<p>The Service Provider must ensure that staff is fully trained for the work that they do. Staff must be provided with written work instructions/procedures setting out how the Service Provider requires critical jobs or tasks to be carried out.</p> <p>The Service Provider practices must comply with reference standard(s)/Code(s), and regulations where applicable.</p> <p>Records of training must be kept and staff competence must be reviewed six-monthly to determine whether retraining is required.</p>
<b>Guidance</b>	<p>A properly designed training programme will ensure that each person's training needs have been evaluated, and that qualified people have carried out the appropriate training.</p> <p>Training should be carried out by experienced staff, with the proviso that they have been trained and competency-rated as effective, i.e. "trained trainers". Training should also refer back to approved work instructions, where applicable, so that variations and inconsistencies are eliminated in the process.</p> <p>Competency of staff may vary over time depending upon the complexity and nature of the tasks regularly undertaken.</p> <p>Staff must have ready access to work instructions.</p>

## 2.7 Continual Improvement

<b>Requirement</b>	<p>The Service Provider must have a procedure for investigating any incidence of substandard service, complaints and other quality or system failures, to determine the root cause of the problems.</p> <p>The Service Provider must have a register of incidents of substandard service, complaints or other quality or system failures and their remedies, available to NZFS upon request.</p> <p>Corrective action must then be taken to ensure that a similar problem will not occur again. The effectiveness of the corrective action must be evaluated to ensure that it has rectified the root cause of the problem.</p>
<b>Guidance</b>	<p>The Service Provider should develop a formal Continual Improvement Programme that analyses each problem as it occurs and attempts to find a permanent solution to prevent the same problem from happening again. This involves looking beyond the symptoms of the problem to find out why it happened in the first place.</p> <p>A register could be used to monitor the simple issues that are easily resolved while a more formal approach should be taken for customer complaints and more complex issues. Cost and/or cause codes should be given to each incident so that trends can be monitored and the management system continually improved.</p>

## **Appendix 1: Non-ICT Documentation available for Inspection**

'Non-Information and Communication Technologies' documentation that should be made available for inspection in support of a company's Application for Certification as an Automatic Fire Alarm Service Provider.

### **a) Business or Quality Manual**

Business or Quality Manual(s) would describe fully and in detail the management and staff hierarchy, staff positions and related job descriptions, and processes or procedures to be followed by all staff in both normal and exceptional conditions when fulfilling their particular duties. Such descriptions should identify what qualifications and experiences are required to fulfill them competently.

A document showing the names of current employees in all established positions as described in the above Manual(s) should be provided. Where there are unfilled positions, details should be provided of the current status of recruitment procedures to fill them.

The roles, duties, tasks descriptions, instructions and responsibilities of the described positions need to be checked to ensure that all functions described in the document known a "Code of Practice of the Automatic Alarm System" are fully covered.

Staff needs to have access to those parts of the manual(s) of relevance to their job performance.

The manual(s) should show what processes are used to investigate failures to maintain contracted levels of service and to implement remedial action, at all levels relevant to the contracted service.

### **b) Business Continuity Plan (BCP)**

A Business Continuity Plan (BCP) should be provided for inspection. The Business Continuity / Business Recovery document should include the critical resources, the related risks, risk assessment (including business impact analysis), risk management and risk monitoring. Evidence of systems to assist business continuity should be detailed in the plan e.g. automatic fire suppression systems at the Service Provider's premises.

The BCP should clearly state the procedures that would be followed in the event of

- malfunction of individual items of equipment;
- malfunction of the configuration as a whole in the normal working environment; and
- any activity unrelated to malfunctioning equipment, which resulted in a denial of service, contracted to be provided by the staff and equipment at the normal premises.

The BCP should show how and how soon the contracted service would be provided in the event of any of the above contingencies. Evidence should be provided to demonstrate the ability of the service provider to meet the requirements of this plan in practice.

**c) Staff Training and Review Records**

The certification procedure requires that records be kept that demonstrate that staff have received training to the level necessary to enable them to fulfill their responsibilities.

Records of staff performance reviews must show that these take place at 6 monthly intervals and show decisions regarding remedial training requirements.

**d) Document Control**

All documentation referred to above should themselves be subject to a Document Control System (DCS) that is itself documented. The documentation of the DCS should show how all issued documents are subject to change, version and circulation control such that all staff receive all relevant versions on time and that prior versions are archived.

**e) Systems Coordinator**

Adherence to all the procedures and disciplines referred to in the previous paragraphs is required to be the responsibility of a Systems Coordinator. Documentation is to be provided which shows the appointment of a senior executive to this position with these responsibilities. This documentation should include a job description making describing the functions outlined above.

**f) Health and Safety Policies**

Documentation should be provided which demonstrates that the Service Provider is complying with all legal duties and responsibilities as defined in the Health and Safety in Employment Act 1992, Amendment Act 2002 and Regulations 1995 and OSH Guidelines for First Aid provision.

**g) Environmental Policy**

Should the service provider store or require the handling of any hazardous material on any of its premises of relevance to the contracted service, environmental policies shall be presented for inspection that demonstrate that appropriate standards of use, handling and disposal are adhered to.

## **Appendix 2: Terms of Reference for the Assessment of the Computer and Telecommunications Facilities of a candidate Service Provider**

- 1) Assess whether the telecommunications path(s) would work end-to-end between the network-interface of a Fire Alarm and the Service Provider interface of the Signal Transport System Message Handling System (STSMHS) described in the candidate Service Provider's proposal.
- 2) Assess whether the telecommunications path(s) between the network-interface of a Fire Alarm and the SP-interface of the STSMHS described in the candidate Service Provider's proposal would fulfill the New Zealand Fire Service's performance standards and requirements, as described in Appendix 3.
- 3) Assess whether the telecommunications path(s) between the network-interfaces of a Fire Alarm and the SP-interface of the STSMHS described in the candidate Service Provider's proposal would enable all Fire Alarms currently connected to the existing Signal Transport System to be connected to the new Automatic Fire Alarm System.

Note: The item above would become obsolete once the migration of all fire alarm panels to the new automatic fire alarm system was completed.

- 4) Identify single points of failure in the candidate Service Provider's corporate telecommunications network that could affect forwarding messages from a Fire Alarm to the STSMHS, and the means in place to manage the risk of failure of these points.
- 5) Assess the extent to which the telecommunications path(s) between the network-interface of a Fire Alarm and the SP-interface of the STSMHS described in the candidate Service Provider's proposal would offer protection against viruses.
- 6) Assess the extent to which the telecommunications path(s) between the network-interface of a Fire Alarm and the SP-interface of the STSMHS described in the candidate Service Provider's proposal would offer protection against unauthorised access to:
  - a) The STSMHS;
  - b) The Service Provider's equipment; and
  - c) Fire Alarms.
- 7) Assess the extent to which the telecommunications path(s) between the network-interface of a fire alarm and the SP-interface of the STSMHS described in the candidate Service Provider's proposal would offer control of network loading.
- 8) Assess whether the telecommunications path(s) between the network-interface of a Fire Alarm and the SP-interface of the STSMHS described in the candidate Service Provider's proposal would be capable of forwarding Fire Alarm event messages to the STSMHS.
- 9) If applicable describe any potential problems arising from IP addressing.
- 10) If any potential problems with the telecommunications path(s) between a Fire Alarm and the SP-interface of the STSMHS described in the candidate Service Provider's proposal are identified, describe these in detail and propose and define the enhancements or changes that would need to be made to correct these deficiencies.
- 11) Assess whether all equipment and software used for service provision (e.g. telecommunications equipment, hardware, application software) are suitably supported

(e.g. maintenance contract) so they could fulfil the performance requirements as per Appendix 3.

- 12) Assess whether monitoring and reporting facilities are in place to monitor and report on the performance parameter as described in Appendix 3.
- 13) Include all comments and descriptions in a report and provide 1 paper copy and 1 electronic copy (PDF file) to both the NZFS and the Service Provider.

### **Appendix 3: Standards and Requirements**

- 1) Failure of any section of the telecommunications path between the Fire Alarm alarm-output and the Service Provider interface of the STSMHS must not cause a message indicating a fire-event.
- 2) The direct connection line between a Fire Alarm and the Service Provider interface of the STSMHS must comply with the following standards at all times:
  - A signal from the Fire Alarm must travel to the STSMHS is no more than 10 seconds for 97% of all messages, and no more than 15 seconds for all messages;
  - The link between the Fire Alarm alarm-output and the Service Provider Interface of the STSMHS must have a minimum Annual Availability of 99.7%;
  - No more than 1 in 1,000,000 messages received by the STSMHS from telecommunications line are allowed to be unintelligible;
  - The single failure maximum outage time for the telecommunications connection between the Access Device and the Service Provider interface of the STSMHS is 6 hours for urban Fire Alarm locations, and 12 hours for rural Fire Alarm locations; and
  - The disruption of the telecommunications connection between the Access Device and the Service Provider interface of the STSMHS must be detected in less than 10 minutes, and a message indicating the status of the telecommunications connection must be forwarded immediately to the NZFS.
- 3) The following exclusions are to be taken into account:
  - Force Majeure events (include circumstances reasonably beyond the control of the affected party, but do not include financial difficulties or delay caused by or in connection with the Service Provider and its employees, agents or contractors);
  - Faults that have been carried over to the next day with agreement of the NZFS will have the corresponding delay subtracted from the outage time;
  - Where access to end-user sites is not available the corresponding delay will be subtracted from the outage time; or
  - Faults that are caused by the end-user.
  - Faults that are caused by Service Agents servicing the Fire Alarms.

**Note:**

The telecommunications transmission networks listed below (in alphabetical order) have been assessed to the Terms of Reference above. New Zealand Fire Service deems any one of them or any combination of them acceptable.

- MCS Networks' network
- RadioNet Monitoring Ltd network
- TeamTalk's Trunk Mobile Radio
- Telecom's ATS2
- Telecom's CDMA
- Telecom's DSL
- Vodafone FARM
- Vodafone's GPRS