July 2017
Version 1.8

Certification for Automatic Fire Alarm Service Providers

Table of Contents

Document history

Version	Date	Comments
1.0	25 May 2005	Final
1.1	12 October 2005	Update
1.2	25 November 2005	Update
1.3	22 December 2008	Changed reference to AS2201.1-2004
1.4	21 June 2006	Appendix 2
1.5	28 February 2007	Major revision to incorporate Code of Practice
1.6	6 April 2007	Updates and addition of flowchart
1.7	March 2014	Reformatted, updated and added process maps
1.8	July 2017	References to NZFS removed and replaced with Fire and Emergency New Zealand (FENZ)

Copyright

80 The Terrace
PO Box 2133
Wellington
New Zealand
Phone: (04) 496 3600

Document owner and contact:

Stuart Waring
Information, Communications and Technology Services | Fire and Emergency New Zealand
National Headquarters, Level 12, 80 The Terrace, Wellington | PO Box 2133, Wellington, New Zealand 6140

1. Introduction

1.1. Purpose

The purpose of this Document is to outline Fire and Emergency New Zealand (FENZ) requirements for Automatic Fire Alarm Service 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 FENZ to provide Service Providers with a model for their management system. It is based upon a variety of standards such as ISO9001:2008 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 FENZ and Service Providers.

Service Providers must be certified in order to provide monitoring services for automatic fire alarms (AFAs). Certification demonstrates that Service Providers:

- have a formal commitment to FENZ 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 FENZ
- operate within a Grade C2 premises as detailed in Australian Standard AS 2201.2-2004.

1.3. Objectives

FENZ wants to:

- obtain intelligence from fire alarms
- receive messages related to fire alarm events via the service provider interface of the signal transport system message handling system (STSMHS). These messages: must conform to the ‘Automatic Fire Alarm Service Provider Computer Interface Specification’
- encourage fire alarm owners to connect their fire alarms directly to FENZ
- limit FENZ response to fire calls only.

The Automatic Fire Alarm System must:

- provide a direct connection (forwarded in electronic form, without human intervention) between the fire alarm and the STSMHS
- transmit Fire Alarm signals from buildings to FENZ Communications Centres
- provide for all connected Fire Alarms to be monitored and service agents notified of defects
- promote reduced incidence of false alarms from connected systems
- provide opportunities for FENZ to gain more information from intelligent fire alarm systems than just ‘fire’, ‘defect’, ‘isolate’, and ‘normal’ messages (where the fire alarms have the capacity to provide that additional information).

1.4. Brief description of message flow

A Fire Alarm sends messages indicating events. These messages will be received either by the Service Provider, FENZ or both. Messages can also be forwarded to other parties (like service agents). The signal path between the Fire Alarm and the STSMHS, and also between the STSMHS and the FENZ Despatching System, is an electronic path that does not require human intervention.

Messages to FENZ will go via the Service Provider Interface of the STSMHS. These messages must conform to the ‘Automatic Fire Alarm Service Provider Computer Interface Specification’; the interface must conform to the ‘STSMHS - AFASP Application Programming Interface (API) Design Specification’, which is available on request from the FENZ. For more information, see the Fire Alarm Connections page on FENZ website:

http://www.fire.org.nz/business-fire-safety/fire-alarm-connections/pages/advantages-of-a-fire-service-connection.aspx

FENZ will not specify the details of the transmission path of the messages between the Fire Alarm and the Service Provider Interface of the STSMHS, but the network(s) used must be among those determined to be acceptable by FENZ. The STSMHS will forward messages indicating non-normal events, which are not fire events, to the FENZ database. Examples of these events include defect or isolate messages. The FENZ database will also include information about false alarms, data entered by FENZ staff and outside parties.

The STSMHS will forward messages indicating fire-events to the relevant FENZ Communications Centre and the FENZ database. The Communications Centre staff will initiate a response to the messages indicating fire-events. If a fire alarm sends a message indicating a fire event, data related to the fire alarm (past non-normal events, false alarms, other Fire Alarm related data) will also be forwarded via the STSMHS to the Communications Centres.

FENZ may also query the Service Provider for Fire Alarm related data, as specified in the Automatic Fire Alarm Service Provider Computer Interface Specification.

2. AFASP 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 FENZ 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
- enable the FENZ to gain more information from fire alarms.

3. Certification process

FENZ may appoint an agent to perform various tasks in the certification process. Fees are payable to FENZ 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. See the following step descriptions and process maps detailing the certification process.

3.1. Application

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

The application must:

- include an audited set of company accounts or documentary evidence to demonstrate the financial and organizational capability and capacity to support the application; the Service Provider must be an incorporated company in New Zealand
- 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 FENZ service levels for the monitoring of AFAs.

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

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

3.2. Initial assessment

Fees for this stage are assessed on an hourly rate.

Documentation that must 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. This documentation is sent to FENZ or its agent(s) for review, including confirmation of compliance with applicable Codes of Practice and government regulations.

Following the review of the documentation, FENZ or its agent(s) may visit the Service Provider's premises and discuss the business processes with key staff. An assessment is undertaken of how the Service Provider's staff will apply the processes described in these documents.

FENZ then produces a report indicating whether the initial assessment has been passed or recommending remedial action if the initial assessment fails.

3.3. Verification audit

This step is required only if the initial assessment is not successful and results in remedial action. The Service Provider contacts FENZ 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 an hourly rate.

3.4. Assessment of computer & telecommunications equipment

FENZ assess the Service Provider’s computer and telecommunications equipment, according to the terms of reference in Appendix 2.

Prior to this assessment, or reassessment, FENZ informs the Service Provider of the fee for this assessment.

FENZ produces a report that indicates whether the assessment of computer and telecommunications equipment has passed or recommends changes if the assessment fails. The Service Provider may address these issues and ask FENZ to repeat the assessment.

3.5. Acceptance testing

The Service Provider must describe the acceptance test with Unisys.

FENZ conduct an onsite assessment to ensure that the system is working effectively. The onsite assessment includes an acceptance test with the Test STSMHS, as specified by FENZ. The acceptance test results are documented in an acceptance test report.

If the Service Provider does not pass the acceptance test, then any non-compliance identified during this process is discussed with the Service Provider and is detailed in the acceptance test report. The Service Provider must address these non-conformances and request that the acceptance test be repeated.

If the Service Provider does not pass the acceptance test the first time, a fee, as advised by FENZ, is payable before each additional acceptance test.

3.6. Agreement sign-off

Following completion of steps in 3.1 to 3.5 the Service Provider and FENZ enter into a contract for the provision of Automatic Fire Alarm Services.

3.7. Certification

Following signing of the contract between the AFASP and FENZ, FENZ issues the Service Provider a Certificate of Registration.

Each Certificate of Registration remains valid for one year and may be renewed in accordance with the audit and renewal procedure in 3.8. Each certificate may also be revoked in accordance with this procedure.

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

3.8. Audit & renewal of Certificate of Registration

At least two months prior to the expiry of a Certificate of Registration a Service Provider must contact FENZ 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.

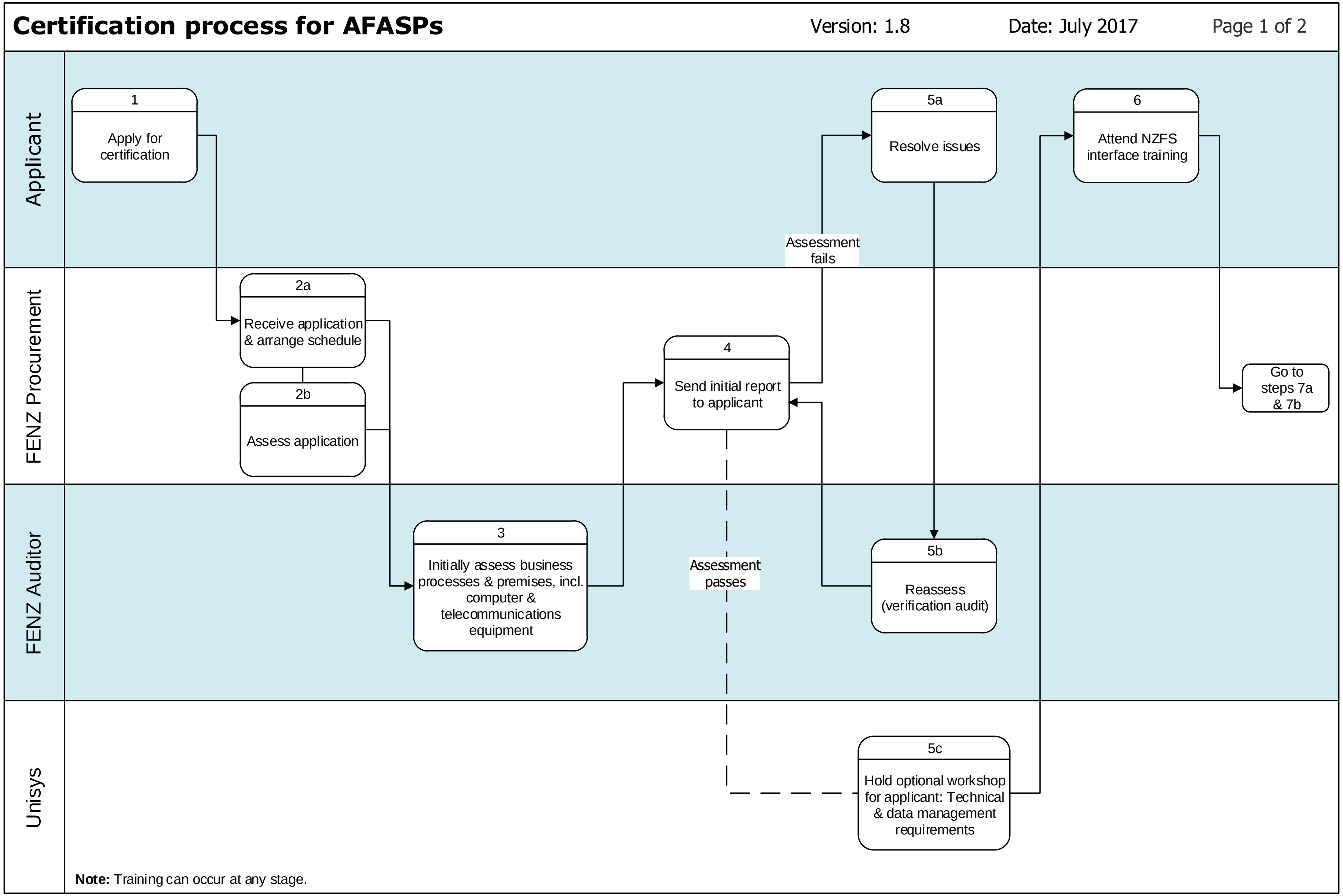
Fees apply to these audits.

FENZ or its agent(s) perform this audit, which may include a site visit, and produce an audit report. A copy of the report is provided to the Service Provider.

If FENZ is satisfied with the audit results the Certificate of Registration will be renewed for a further year.

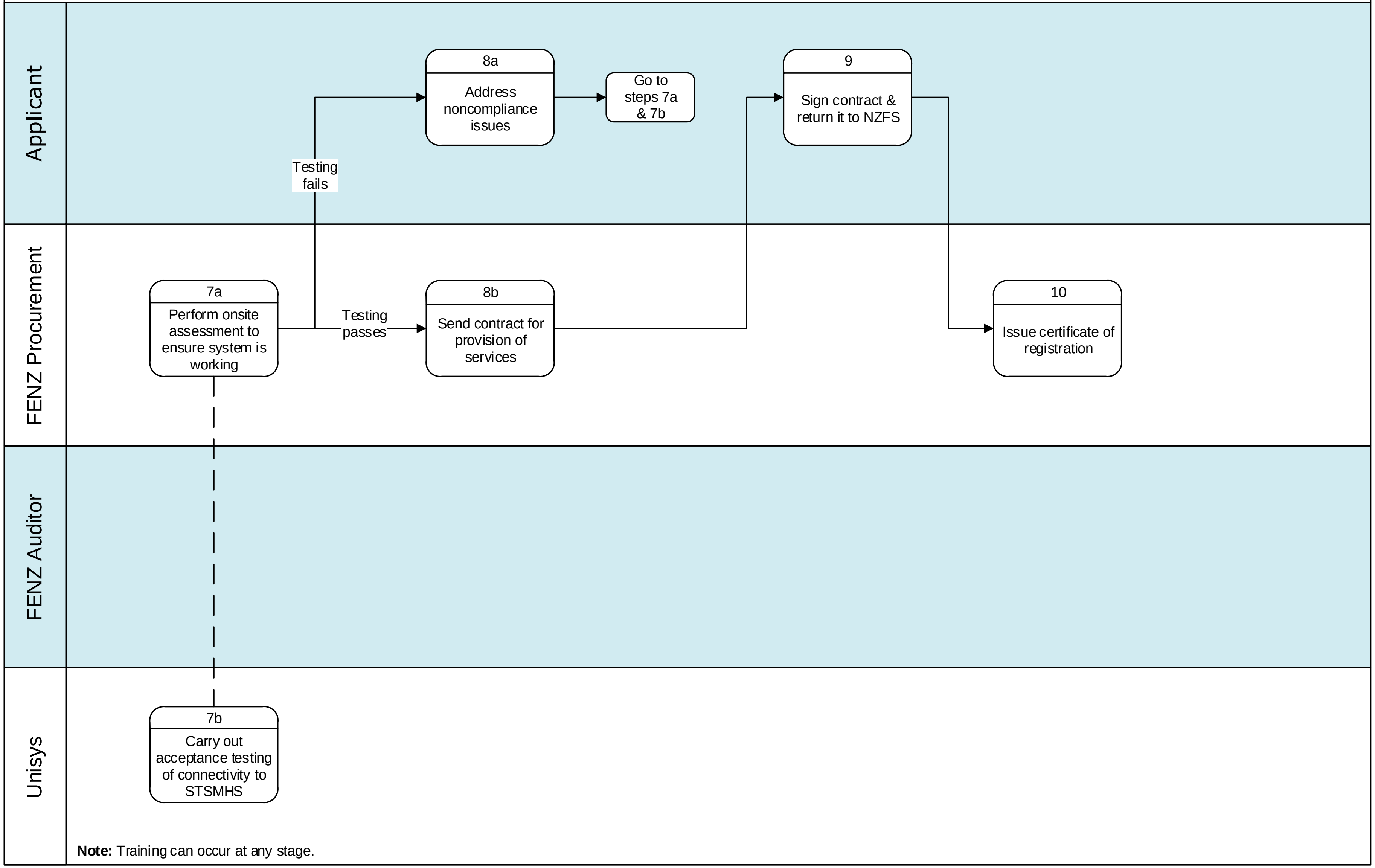
If FENZ is not satisfied with the audit results the Service Provider’s Certificate of Registration will not be renewed. In order to continue to be able to provide services as an Automatic Fire Alarm Service Provider the Service Provider must address the issues of non-compliance detailed in the audit report and request a follow-up audit. Depending on the nature of the areas of non-compliance, a time limit to remedy deficiencies may be set by FENZ. This step may be repeated if necessary. If FENZ is satisfied with the audit results the Certificate of Registration will be renewed.

FENZ may perform more frequent audits as a result of audit findings. There is a fee associated with these additional audits.


Certification process for AFASPs
Version: 1.8
Date: July 2017
Page 1 of 2
Applicant
FENZ Procurement
FENZ Auditor
Unisys
1
Apply for certification
2a
Receive application & arrange schedule
2b
Assess application
3
Initially assess business processes & premises, incl. computer & telecommunications equipment
4
Send initial report to applicant
Assessment fails
Assessment passes
5a
Resolve issues
5b
Reassess (verification audit)
5c
Hold optional workshop for applicant: Technical & data management requirements
6
Attend NZFS interface training
Go to steps 7a & 7b
Note: Training can occur at any stage.

Certification process for AFASPs

Version: 1.8 Date: July 2017 Page 2 of 2


Applicant
FENZ Procurement
FENZ Auditor
Unisys
7a
Perform onsite assessment to ensure system is working
Testing fails
8a
Address noncompliance issues
Go to steps 7a & 7b
Testing passes
8b
Send contract for provision of services
9
Sign contract & return it to NZFS
10
Issue certificate of registration
7b
Carry out acceptance testing of connectivity to STSMHS

Note: Training can occur at any stage.

4. Management of the system

4.1. Requirements

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 follow 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 includes the requirements of this document.

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

- Health and 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 made available upon request by FENZ for inspection.

5. Control of documents & records

5.1. Requirements

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 do not have to rely on memory for information.

Records must be sufficient to demonstrate that all essential processes have been carried out, and that all essential inspections or tests have been undertaken in compliance with 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. The following table lists several types of records and their retention periods:

Record type	Retention period
Customer & contract records	7 years
Computer system logs	18 months
Staff records	5–7 years*
Premise inspections & NZSA Certificate	12 months after expiry of certificate
Customer contact & complaint records	Approx. 2 years
Incident reports & actions records**	Minimum of 18 months

* Dependent on the organisation's policies.

** Records of serious incidents must be retained in the event of claims or litigation.

5.2. 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 (the current version and one previous version must be retained)
- reference manuals
- procedure manuals
- job descriptions
- regulations.

The term 'document' includes any method of recording or displaying information. Documents may be in the form of paper, computer files, wall charts, posters, videos, photographs, Codes of Practice and so on. 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 must 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.

6. Contract agreement

6.1. Requirements

The Service Provider must ensure that FENZ performance standards (as per Appendix 3) and performance standard-related reporting requirements are adhered to.

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

6.2. Guidance

The agreement between FENZ and the Service Provider and the 'Code of Practice for the Automatic Alarm System' details expectations of the Service Provider, e.g. objectives and reporting requirements. The Service Provider must ensure that these expectations and the methodologies to manage these expectations are detailed within their documented procedures.

7. Facilities & equipment

7.1. Requirements

With respect to building services, construction, operation, equipment and staff, FENZ adopts the standards of the Australian Standard AS 2201.2-2004 ‘Intruder alarm systems - 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.

7.2. Guidance

The Service Provider must identify the critical equipment and services that they buy. The service levels related to these items must be correct if they are not to detract from the quality or safety aspects of the Service Provider’s own goods or services.

8. Business continuity/business recovery

8.1. Requirements

The Service Provider must provide a business continuity plan.

8.2. Guidance

The business continuity/business recovery document should include the:

- critical resources
- related risks
- risk assessment (including business impact analysis)
- risk management
- 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.

9. Training & work instructions

9.1. Requirements

The Service Provider must ensure that staff are 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.

The Service Provider practices must comply with reference standard(s)/code(s), and regulations where applicable.

Records of training must be kept and staff competence must be reviewed six-monthly to determine whether retraining is required.

9.2. Guidance

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.

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.

Competency of staff may vary over time depending upon the complexity and nature of the tasks regularly undertaken.

Staff must have ready access to work instructions.

10. Continual improvement

10.1. Requirements

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.

The Service Provider must have a register of incidents of substandard service, complaints or other quality or system failures and their remedies available to FENZ upon request.

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.

10.2. Guidance

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.

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.

Appendix 1: Documentation available for inspection

The documentation that must be made available for inspection in support of a company's application for certification as an Automatic Fire Alarm Service Provider is listed below:

1. Business or quality manual

A business or quality manual describes fully and in detail the management and staff hierarchy of the company, staff positions and related job descriptions, and processes and procedures to be followed by all staff in both normal and exceptional conditions when fulfilling their particular duties. Such job descriptions identify what qualifications and experiences are required to fulfil the role competently.

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

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

Staff need access to those parts of the manual(s) that are relevant to their job performance.

A business or quality manual(s) should include the processes used to investigate failures to maintain contracted levels of service and to implement remedial action, at all levels relevant to the contracted service.

2. Business Continuity Plan (BCP)

A Business Continuity Plan (BCP) must be provided for inspection. A business continuity / business recovery document includes the critical resources, 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
- any activity, unrelated to malfunctioning equipment, that results in a denial of service contracted to be provided by the staff and equipment at the normal premises, e.g. staff disruptions, loss of access to premises, etc.
- Failover procedures, processes and capability
- Fall back procedures, processes and capability.

A BCP shows how and how soon the contracted service would be provided in the event of any of the above contingencies. Evidence is required to demonstrate the ability of the service provider to meet the requirements of this plan in practice.

3. Staff training and review records

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

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

4. Document control

A Document Control System (DCS) available to all relevant staff needs to be in place. This must include version control and an archiving facility so that all staff receive and have access to all recent versions of documentation.

5. Systems Coordinator

Adherence to all the procedures and disciplines referred to in the previous paragraphs is the responsibility of a Systems Coordinator. A senior executive with these responsibilities in their role/job description must be appointed to this position and documentation describing this appointment and its responsibilities must be made available.

6. Health and safety policies

Documentation must 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.

7. Environmental policy

If the Service Provider stores or needs to handle any hazardous material on any of its premises of relevance to the contracted service, environmental policies must be presented for inspection that demonstrate that the 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) works 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 fulfills FENZ performance standards and requirements, as described in Appendix 3.
3) 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 ensure continuity in the event the corporate network is compromised. Assessment to include possible remedy of single point of failure.
4) 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.
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 unauthorised access to:
    a) the STSMHS
    b) the Service Provider's equipment
    c) fire alarms.
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 control of network loading.
7) 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.
8) If applicable, describe any potential problems arising from IP addressing.
9) 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.
10) 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.
11) Assess whether monitoring and reporting facilities are in place to monitor and report on the performance parameters.
12) Include all comments and descriptions in a report and provide 1 paper copy and 1 electronic copy (PDF file) to both FENZ and the Service Provider.

Appendix 3: FENZ performance standards, requirements & transmission networks

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 in 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.
   - 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 FENZ.
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 FENZ 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.

Telecommunications transmission networks

1) The telecommunications transmission networks listed below (in alphabetical order) have been assessed as acceptable for the transmission of fire alarm messages:
   - MCS Networks' network
   - RadioNet Monitoring Ltd network
   - TeamTalk's Trunk Mobile Radio
   - Telecom's ATS2
   - Telecom's DSL
   - Vodafone FARM
   - Vodafone's GPRS.
   - Wired broadband
   - Wireless broadband

More than one telecommunications path may be required between a given fire alarm and the Service Provider's communication facility to achieve the required performance standards.

FENZ may add to or delete from this list from time to time.

2) Connection to FENZ equipment

Two independent telecommunications paths must be provided between the Service Provider’s communication facility and FENZ interconnection device.

Appendix 4: Glossary of terms

Term	Definition
Access device	The access device connects a fire alarm with a telecommunications network.
AFA	Automatic fire alarm
AFASP	Automatic Fire Alarm Service Provider. Provides telecommunications and/or management services in respect of the Automatic Fire Alarm System.
Annual availability	The annual proportion of time during which a unit or a system is able to perform its required function within the scheduled service hours (service hours are: 24 hours per day, 7 days per week).
API	Application programming interface
Certificate of Registration	Certificate confirming the registration of the applicant as an AFASP. Issued following the signing of the contract between the AFASP and FENZ
Code of Practice	Code of Practice for the Automatic Fire Alarm System.
Communications Centre	FENZ personnel who are responsible for dispatching fire appliances to fire alarm alarm-events and 111 calls. FENZ operates three Communications Centres, located in Auckland, Wellington and Christchurch.
Computer Interface Specification	The protocol specification, including the extended alarm protocol specification (XAP) and associated application programming interface specification, for the computer interface between FENZ Interconnection Device and the Contractor Interconnection Device, as available on FENZ public internet page, as amended from time to time
Contractor	AFASP
Contractor Interconnection Device	Device under control of the Contractor that exchanges messages with FENZ Interconnection Device in accordance with the Computer Interface Specification.
Customer	Owner or occupier of protected premises who has entered into an agreement with the Contractor.
Direct connection	Telecommunications connection where messages are sent electronically without human intervention.
False alarm	False alarm (as defined under FENZ False Alarms Policy (POLFA 7.5) as amended from time to time.

Term	Definition
FENZ	Fire and Emergency New Zealand - or its appointed agent.
Fire alarm (FA)	An apparatus that performs specified fire-related functions in response to the operation of a sprinkler, detector, manual call point or other input, as defined in the relevant NZ Standard, as amended from time to time, that is connected to the AFAS by the Contractor
Force Majeure	Any cause reasonably beyond a party's control as mentioned in Appendix 3.
IP	Internet protocol.
FENZ Interconnection Device	The STSMHS servers that route messages received from the Contractor and Fire Alarms to FENZ
FENZ Interconnection Device Contractor	The entity that supports and manages the STSMHS under a contract and service level agreement with FENZ.
NZS	New Zealand Standard
Protected premises	a building or part of a building that is: a) fitted with one or more fire alarms; and b) physically separate from other buildings at a given location (provided that, in determining whether or not a building is physically separate, common walls, walk ways and service tunnels must be ignored).
Rural fire alarm	Fire alarm located in a district, and where FENZ is not the Fire Authority.
Service Agent	The agent responsible for the testing and maintenance of particular fire alarms (in particular the company or person responsible for attending to fire alarms in the event of an activation). The Service Agents are contractors to the fire alarm owners.
Services	Fire Alarm monitoring and transmission services provided by the Contractor in accordance with their Agreement with FENZ.
STSMHS	Collection of servers, equipment and transmission links between the Contractor Interconnection Device and the Communications Centres alarm interface servers (which transports messages from FENZ Interconnection Device to the Communications Centres

Term	Definition
	alarm terminals), as contracted to and managed by FENZ Interconnection Device Contractor
Urban fire alarm	Fire Alarm located in a fire district