

tel. 1300 655 009

www.centralmonitoring.com.au



Alarm Monitoring HANDBOOK



c|m|s

central
monitoring
services

P O BOX 733
Ryde NSW 1680

Monitoring Centre

Phone. 1300 655 009

(02) 9809 9222

Fax. (02) 9809 9233

Email. controlroom@centralmonitoring.com.au

Administration/Accounts

Phone. (02) 9809 9244

Fax. (02) 9809 9255

Email. alarms@centralmonitoring.com.au

Customer Service

Phone. (02) 9809 9244

Fax. (02) 9809 9255

Email. customerservice@centralmonitoring.com.au

Data Entry

Phone. (02) 9809 9266

Fax. (02) 9809 9233

Email. controlroom@centralmonitoring.com.au



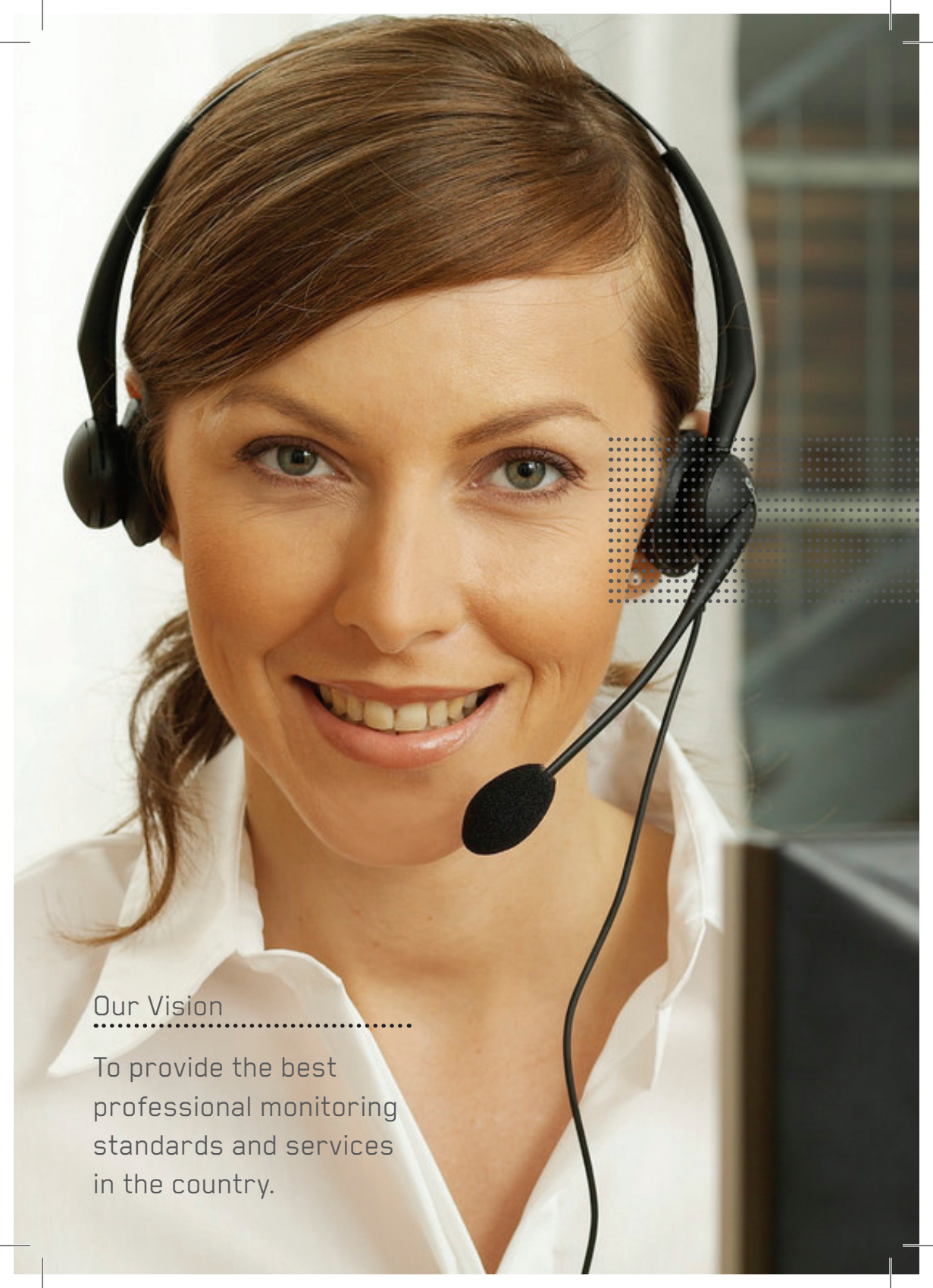
Copyright Central Monitoring Services Pty Ltd 1989 – 2002

N.S.W Master Licence Number 401 988 582

TABLE OF CONTENTS

Our Company	3	Low Battery Events	10
Alarm Monitoring Paths	4	Isolation Events	10
Standard Alarm Monitoring	4	Alarms on Entry	10
Dial-up (Dialler)	4	Fire Alarms	11
GSM Monitoring	5	Multiple Alarms	11
Supervised Alarm Monitoring	5	Deprogramming of Your Alarm	11
Fratech MultiPath IP Monitoring	5		
MultiPath Ethernet IP STU or MultiPath GPRS STU	6	FURTHER INFORMATION FOR CLIENTS	
Emizon Networks Monitoring	6	AT COMMERCIAL PREMISES	12
Classes of Service	6	Hold Up and Duress Alarms	12
Telstra Secure Monitoring	7	Supervised Monitoring of Arming and Disarming Times	12
Client Responsibilities	7	Multiple Accounts	13
Client Data Privacy	7	Multiple Area Opening/Closing for Commercial Supervised Clients	13
After Hours Call Outs - Keyholders	7	Dialler	13
Passwords - Voice Codes	8	Monitoring of Commercial Supervised Clients on Public Holidays	13
Response Instructions	8		
Patrol Response	9		
Police Attendance	9		
Medical Alarms	9		
Panic Alarms	10		
Power Failure Events	10		





Our Vision

To provide the best professional monitoring standards and services in the country.

OUR COMPANY

Welcome to Central Monitoring Services. We specialise in the monitoring of alarm systems for residential, commercial and industrial sites.

Having your premises continuously monitored by our 24 hour Monitoring Centre ensures that someone will be notified in the event that your alarm system activates.

Alarm monitoring customers expect reliable service and should receive just that. That's why hundreds of alarm installers, leading corporations and thousands of alarm owners rely on Central Monitoring Services to handle each and every call effectively.

Underpinning the investment in the latest technology and built for purpose premises, CMS has 20 years of experience. Sticking to our principles. And our original vision: to provide the best professional monitoring standards and services in the country.

With outstanding staff, advanced training and active commitment,

CMS pushes quality standards higher and higher within our company – and within our industry.

We anticipate customer needs with innovative products, and continuously refine and develop our training, supervision and systems.

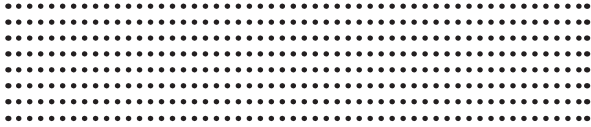
We work with customers, keeping them informed about developments, policies, and trends affecting their needs.

The end result is an industry award winning monitoring centre operated by people with the knowledge, relationships, honesty, commitment, determination, dedication and enthusiasm to succeed.

Our, customers trust CMS to give 100 per cent.

If you need alarm monitoring you can trust and want the service you deserve, the answers are only a call away.

ALARM MONITORING PATHS



We encourage you to test your alarm system manually on a regular basis.

The following types of alarm monitoring are currently available. Please ensure that the installed alarm system meets the requirements and standards of your insurers. Monitoring is available in both Standard and Supervised formats.

STANDARD ALARM MONITORING Dial-Up (Dialler)

Dialler alarm systems use conventional telephone lines to transmit alarm signals from your premises to our monitoring centre. Every time the alarm is triggered or reports a test event, a local phone call is made and charged to your phone bill.

If the phone line connection is interrupted at any point between your premises and our monitoring centre, or if the alarm system becomes faulty or damaged, no alarm signals will be received. It could take hours or days before this becomes apparent, hence it is important to have the alarm system programmed to report regular test events. In addition, we encourage you to test your alarm system manually on a regular basis by calling us and then triggering your alarm.

Dialler alarm monitoring is an inexpensive monitoring path for the small to medium size alarm system with minimal reporting and the most common type of alarm monitoring conducted in Australia. However, it may not be sufficient for your security

needs for the higher risk premises or if reporting of events from your alarm creates a large amount of signals which produce an excessive phone bill.

We recommend you consult your alarm technician and insurance provider before you decide on a monitoring path and for existing monitored clients a check with the monitoring centre will verify all signals sent by your system.

If dialler alarm monitoring is not the correct option or insufficient for your security needs, the following alternative monitoring paths are available. All of them can work on their own or in conjunction with a dialler for enhanced safety and protection. Changing technology may also have an effect on your existing dialler alarm or may not be compatible for the new digital networks and IP technology.

GSM Monitoring

A GSM module can be attached to most dialler alarm systems. It contains a SIM card as used in mobile phones and transmits alarm signals using mobile phone carriers such as Telstra, Optus and Vodafone. GSM modules are compatible with all alarm systems and can be used as a back-up or primary alarm monitoring path. Most GSM systems work in a similar format to the Dialler and compatibility with telephone network should be checked prior to proceeding with this type of alarm monitoring. Call costs should also be checked as each call is charged and normally at the standard rate.

Some systems also use the SMS (short message service) path to transmit signals completely wireless directly to our monitoring centre.

This is not recommended by CMS for critical security, safety or high risk monitoring as it uses store and forward technology which does not guarantee delivery of service in a timed parameter.

SUPERVISED ALARM MONITORING

Fratech Multipath IP Monitoring

Central Monitoring Services has introduced a new High Security monitoring service which utilises a combination of Internet, GPRS and PSTN to transmit signals to special servers at CMS. This was the first of the new services of this type developed by one of the Security Industry's leading equipment suppliers Inner Range. The Fratech MultiPath Transmission Service was first installed at CMS 2007 with hundreds of Class 3 services in 2010.

The following are the paths available for this product to communicate with CMS.

Path 1:

IP ADSL connection using Public IP or Proprietary Ethernet service and 128 bit AES encryption.

Path 1 or 2:

GPRS reporting via a Telstra National VPN as the primary or backup path where Ethernet or IP is not available.

Path 2 or 3:

PSTN reporting via the normal Telephone Service, where the GPRS VPN is unavailable.

Path 3:

GSM reporting via a dedicated SIM on the Telstra Network as the third path where GPRS is the Primary path.

There are two Multipath IP STU types which intelligently select the most available Path to transmit alarm information in accordance with Australian Standards AS/NZS2201:5, 2008 to achieve Class 3, 4 or 5 signaling.

MultiPath Ethernet IP STU or MultiPath GPRS STU.

The standard selected polling rate of one hundred and twenty (120) seconds is available with either STU as agreed with the client using a combination of the transmission paths. This is a Class 3 service suitable for higher security risks, or for fixed price monitoring, or for compatibility with new networks.

The MultiPath Ethernet IP STU will always attempt to transmit all signals via the Ethernet connection as Path 1, but provides via Path 2 - GPRS - same performance specification, then Path 3 - unlimited PSTN communication. Use of the Ethernet Service via the Client ADSL or other Ethernet or Intranet Service ensures the service is offered at the most competitive price as all traffic is transmitted on an existing service with no additional cost of service. The GPRS is only used to provide an alternative Path using a different technology at the same high security specification. A truly redundant and reliable service provided by an equally reliable Monitoring Service at CMS.

The MultiPath GPRS STU will always attempt to transmit all signals via the GPRS Telstra VPN network as Path 1. It is used when no Ethernet Service is available.

Emizon Networks Monitoring

The second new service provided by CMS to fill the changing needs of the communications world we now live in. Emizon is a product developed in the UK to meet the demanding European Standards as a product to replace the UK version of Securitel.

It is similar in structure to the MultiPath Product described above. Once again it uses an inexpensive Ethernet service as the Primary Path, backed by a GPRS radio service to provide the availability required for a truly high security product.

Classes of Service:

Emizon have their product certified to the Australian Standard AS/NZS 2201.5:2008 for Class 3, 4 and 5 and each service connected to CMS receives this confirmation of Class service and guarantee.

Emizon is available in the following configurations:

Class 2

Supervised every 24 hours
Domestic Dialler Equivalent
Low Risk- Low Cost- New Technology
Ethernet and/or GPRS Paths

Class 2+

Supervised every 1 hour
Commercial Dialler Equivalent
Medium Risk-Low Cost-New Technology
Ethernet and/or GPRS Paths

Class 3

Supervised every 120 secs
Commercial High Risk
Medium/High Risk-Know Cost C3R3
Ethernet and/or GPRS Paths

Class 4

Polled every 60 secs
Bank/Govt High Risk
High Risk-New Technology C4R3
Ethernet and GPRS Paths

Class 5

Polled every 20 secs
Government High Security
Extra High Security New Tech C5R

This product can be connected to every new and existing alarm system available. It may look complicated but CMS have engineered a solution to ensure selection suits the risk, the technology available and at a known cost.

Futureproof your security with Emizon and CMS. CMS first commissioned this service in 2008 with many hundreds of connections in 2010 utilising all classes.

Telstra Secure Monitoring

The newest service provided by CMS suits the changing needs of the communications world we now live in. Even with two products in and working for over two years it was evident with the closure of the Telstra Securitel Network there are many loyal Telstra Clients who have lived with the stable Securitel product for many years.

CMS have installed this service in 2010 and have already hundreds of connections to this Next G Network.

With the experience of the older GPRS Networks Telstra have every confidence that this "Next G" service will provide the difference and prove the most reliable of all radio Networks.

Connect to any Alarm Panel with the convenience of no wires or involvement with an IT Department or the Client's Internet Service this is a Stand-Alone service.

Telstra provide coverage maps of the Next G so you can be assured that service is available.

Central Monitoring Services Pty Ltd have added Telstra Secure Product to our service range to complete what we believe is the most comprehensive and technically sound new product offering available in the Australian Security market today.

CLIENT RESPONSIBILITIES

It is your responsibility to provide adequate details about the alarm system, keyholders and alarm response requirement. Changes in details must be forwarded as soon as possible to ensure effective monitoring.

If you are unavailable for an extended period of time, we encourage you to advise us on 1300 655 009.

It is your responsibility to ensure that your alarm system is regularly checked and maintained to Australian Standard AS/NZS AS2201.1:2007.

For insurance purposes and for your benefit, it is important that all dial-up panels regularly report an open/close or a periodic test condition accordance to AS/NZS 2201.5:2008. Central Monitoring Services recommend that the alarm system must transmit a periodic test report at least once every three days for residential alarms, however we recommend a daily test for commercial premises.

CLIENT DATA PRIVACY

We will only provide client account information to the alarm installation company and keyholders listed on your account if a valid password can be quoted. No confidential information can be provided to an unidentified person. All information on your account is used for alarm monitoring purposes only.

AFTER HOURS CALL OUTS - KEYHOLDERS

Please list at least 3 persons (keyholders) who have access to your premises and the alarm system. These keyholders should be able to attend in case the alarm activates or a problem is found. Please advise each keyholder that we monitor the alarm day

and night, hence their attendance could be required at any time. Listing contacts who are unable to attend to alarm activations will slow our response time as other keyholders must be contacted.

PASSWORDS - VOICE CODES

We strongly recommend the use of a password (also called voicecode) for anybody having ongoing access to your premises. You may choose one common word or code or you can allocate one for each authorised person.

Using a password or voice code will help us identify intruders at your premises. If a password is listed on your account, then it must be quoted no other means of identification can be accepted.

If a password cannot be quoted, we will confirm identification by following your selected response instructions.

A duress password can also be nominated to verify duress situations.

RESPONSE INSTRUCTIONS

We will call your premises first on receipt of most alarms (some exceptions apply) to establish whether the alarm was accidentally activated. In case we are unable to resolve the situation by contacting your premises, we will follow a pre-selected response instruction. Please choose one of the following (you can change your instruction anytime):

.....

If an authorised person accidentally sets off your alarm system please call our Monitoring Centre immediatley: 1300 655 009.

Option 1 KEYHOLDERS TO ALL EVENTS

1. Phone keyholders until first available has been notified.
2. Do not notify a patrol car.

Option 2 IF N/A KEYHOLDERS SEND PATROL

1. Phone keyholders until first available has been notified.
2. Notify a patrol car on request or if no keyholder is available.

Option 3 PATROL TO ALL EVENTS (EXTERNAL)

1. Notify a patrol car IMMEDIATELY to EXTERNALLY check the premises. (The patrol does not hold keys to your premises.)
2. Notify a keyholder ONLY if a problem or genuine incident has been detected or on events requiring internal inspection, (i.e.: power failure, low battery, isolations).

Option 4 PATROL TO ALL EVENTS (INTERNAL)

1. Notify a patrol car IMMEDIATELY to INTERNALLY check the premises. (The patrol must hold keys to your premises.)
2. Notify a keyholder ONLY if a problem or genuine incident has been detected.

Option 5 PATROL & KEYHOLDERS TO ALL EVENTS

1. Notify a patrol car IMMEDIATELY to check the premises. (The patrol may or may not hold keys to the premises.)
2. Notify a keyholder IMMEDIATELY AFTER a patrol car has been notified.

PATROL RESPONSE

A patrol response vehicle will be dispatched if nominated in your standard pre-selected response instruction. A security officer will attend to your premises to ensure your premises are safe and secure. Response times can vary and the current Australian standard AS 4421 calls for response times under 35 minutes for certain events.

Patrol responses are usually charged in addition to monitoring fees. We recommend you check with your alarm installation company.

A patrol response vehicle may not be able to catch intruders at your premises as it could only take seconds for them to break and enter your premises. A patrol response will however deter intruders from taking their time in removing valuables from your own premises.

If your premises appear secure, a patrol officer will leave a small docket at your site informing you of the response. If your premises are found broken and entered, the officer will attempt to secure your premises and in most cases remain on site until police and you or one of your keyholders can attend.

Please note that a patrol car, if pre-selected, will be dispatched to ALL events at commercial premises if no other keyholders are available. This includes non-burglary alarms such as power failures, isolations, trouble alarms, low batteries as well as alarm systems left unarmed. We believe it is in your interest that we ensure that your premises and valuables are secure. Sometimes, a power failure or isolation signal could be the last event your alarm system was capable of transmitting before it was damaged by intruders.

POLICE ATTENDANCE

Police will not be contacted in the first instance for alarms, except for hold up or duress alarms from commercial premises where a double press device is fitted and a fixed location can be provided. Pre-authorisation is required if police "Direct Access Number" is to be called. Police will give priority to verified alarms where keyholder attendance is assured. Police will not report back to our monitoring centre on what was found, and we are not able to query police on action taken. Police attendance varies between each state and territory of Australia. In summary, police should not be called unless a verified crime is in progress or for multiple alarms for a high risk premises. It is very important to consider these options prior to alarms being received.

MEDICAL ALARMS

Medical emergency alarms can be triggered by a range of applications such as pendants, buttons and keypads. Ambulance services can be notified either on request or if no other keyholders are able to respond.

To ensure effective monitoring, we recommend that a spare key to your premises is kept with a neighbour or in a safe, hidden location. This will allow ambulance officers access to your premises in case you are unable to provide access. We also recommend that you provide us with a very brief medical which we can pass on to the ambulance.

Please note that our monitoring centre staff are not trained or qualified to provide any medical advice. On receipt of a medical alarm, we will attempt to call your premises first. If we are unable to establish that you are in good health, ambulance and/or keyholders will be contacted.

PANIC ALARMS

On receipt of a panic alarm, our operators will call your premises. Should you answer the phone, we will ask if you require police assistance and if you are well. We will also ask you for your password to confirm your identity. If no password can be quoted or nobody can be reached, the pre-authorised response instructions will be followed, patrol and keyholders will be contacted to ensure you are safe. Police will be not be called.

POWER FAILURE EVENTS

If your alarm system loses connection to its main power supply, a power failure signal should be transmitted to our monitoring centre. Most alarm systems will delay transmission of this event for some time to allow for short term power interruptions such as black-outs or turned off fuse switches. Despite main power failure, your alarm system should still function if it is backed up by a battery, hence your premises are still protected if you are absent. We will attempt to notify you if the main power supply to your alarm system remains interrupted for an extended period of time.

LOW BATTERY EVENTS

Your alarm should transmit low battery signals when the back-up battery becomes faulty or loses its charge, possibly due to a previous main power failure. Depending on the state and specification of your back-up battery, it may be able to supply power to your alarm system for days, hours or just minutes.

Low battery signals can sometimes be the last event received by our monitoring

centre before your premises are unprotected due to complete loss of power to the alarm system. On receipt of these events from commercial premises, we will attempt to contact you straight away, day or night.

We recommend you have your battery checked on a regular basis in accordance with Australian Standard AS2201.

ISOLATION EVENTS

Isolation events may be transmitted if one or more zones of your alarm system are no longer active, provided your alarm system is in an armed state. For example, you may choose to have the upstairs area of your residence disarmed at night while the downstairs part is armed and secured.

Residential isolations will be ignored at our monitoring centre, unless the signal received indicates a fault or trouble event. Isolation events from commercial premises will be responded to immediately on all occasions.

ALARMS ON ENTRY

Alarms on entry are intruder alarms immediately followed by a valid disarm (opening or cancel) signal and are usually the result of the alarm not being disarmed in time. For example, you enter your premises but take too long to enter your code in the keypad. Both an intruder alarm event and valid disarm event are transmitted to our monitoring centre.

Alarms on entry are ignored at our monitoring centre as the alarm system has been successfully disarmed with a valid pin number.

FIRE ALARMS

Fire brigades have the authority and power under the relevant acts to gain entry to premises for the purposes of fighting fires. This means when our monitoring centre notifies the Fire Brigade, we are authorising entry to your premises to ensure that any danger to life or property by fire or smoke is eliminated. If you have smoke detectors reporting to our monitoring centre, a Fire Authorisation Form must be completed and returned to our office in case we are unable to contact you on receipt of a fire alarm.

MULTIPLE ALARMS

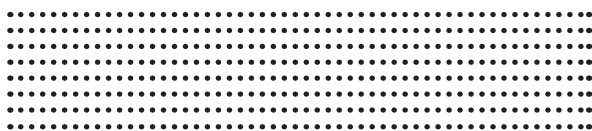
We respond to the first alarm signal received from one detection device connected to your alarm system. We cannot enter into permanent arrangements such as to only take action when two or more alarms are received.

We believe that only one (1) device should be connected to any one reporting channel of your alarm system and we insist that only one alarm is sent from that channel/zone in any armed period. This is a requirement of the Noise Abatement Act. This is referred to as single alarm reporting, which is normally implemented by programming the lockout or conditional lockout function provided in most alarm panels.

DEPROGRAMMING OF YOUR ALARM SYSTEM

Should monitoring be cancelled please ensure that the alarm system is de-programmed by your alarm installation company. Otherwise you will continue to incur phone call charges and our monitoring equipment will receive unnecessary events which may lead to congestions.





FURTHER INFORMATION FOR MONITORED CLIENTS AT COMMERCIAL PREMISES

We will notify you if the alarm remains unarmed after the latest acceptable arming time.

HOLD UP AND DURESS ALARMS

Hold up and duress alarms can be received by commercial alarm systems only devices must be dual press devices and must have a fixed location. Police "Direct Access Number" will not be called unless pre-authorisation is received.

Approximately 30 minutes later, we will attempt to contact you or one of your keyholders to ensure you are safe. Please note that you will be charged by police for consecutive false alarm activations. Please note that we cannot cancel police once notified.

SUPERVISED MONITORING OF ARMING AND DISARMING TIMES OF COMMERCIAL PREMISES

In addition to standard alarm monitoring, you may elect to have the arming and disarming times of your alarm system monitored. Your alarm system needs to report to us every time it is armed and disarmed.

To ensure that the alarm system has been turned on after trading hours, you need to supply us with a time schedule for each day of the week. Please record the earliest acceptable disarming time and latest acceptable arming time of the alarm system. Do not enter a time schedule if your premises will be closed on a particular day of the week. Please note that we will allow a 30 minute tolerance on any given time schedules.

We will notify you if the alarm remains unarmed after the latest acceptable arming time. Should the alarm be turned off before the earliest disarming time and we have not been contacted, we will treat this event as an unauthorised entry. We therefore strongly recommend that anyone who is authorised to turn the alarm off outside the provided time schedule contact us before entering your premises.

MULTIPLE ACCOUNTS FOR COMMERCIAL CLIENTS

Multiple Client Account Numbers are required when any of the following items are present in an alarm system:

1. You choose to have different alarm actions for different zones.
2. Individual arming and disarming supervision is required for more than one area.
3. Different keyholders are to be called for different areas or zones.
4. Access to different areas is to be limited to individual users.

MULTIPLE AREA OPENING/CLOSINGS FOR COMMERCIAL SUPERVISED CLIENTS

Dialler

If a dialler is transmitting area openings/closings (disarming/arming), it should be realised that on a single client account, the first area closing will close the account and we are unable to check for any other opening/closing signals. Thus the risk of areas not being turned on exists and areas may be left without security as no late to close (premises unarmed) events will be generated.

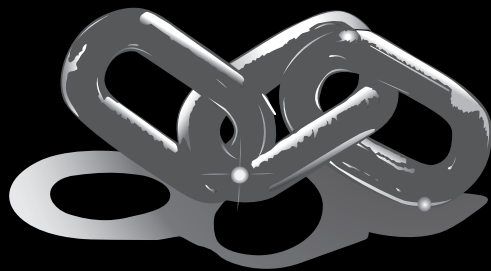
MONITORING OF COMMERCIAL SUPERVISED CLIENTS ON PUBLIC HOLIDAYS

To ensure that your premises are properly monitored on public holidays, Central Monitoring has adopted the following policy:

Unless you advise us otherwise, we will treat all public holidays as normal working days.

For example, if a public holiday falls on a Monday and your premises are usually open on Mondays, then the normal time schedule will apply and the alarm can be disarmed during the time schedule as usual. We will not query any entries to your premises within the usual arming and disarming times.

Should your usual time schedule change due to public holidays, please advise our monitoring centre as soon as possible. Please note that public holiday time schedules are automatically erased after each public holiday and therefore must be re-advised each year.



www.centralmonitoring.com.au

