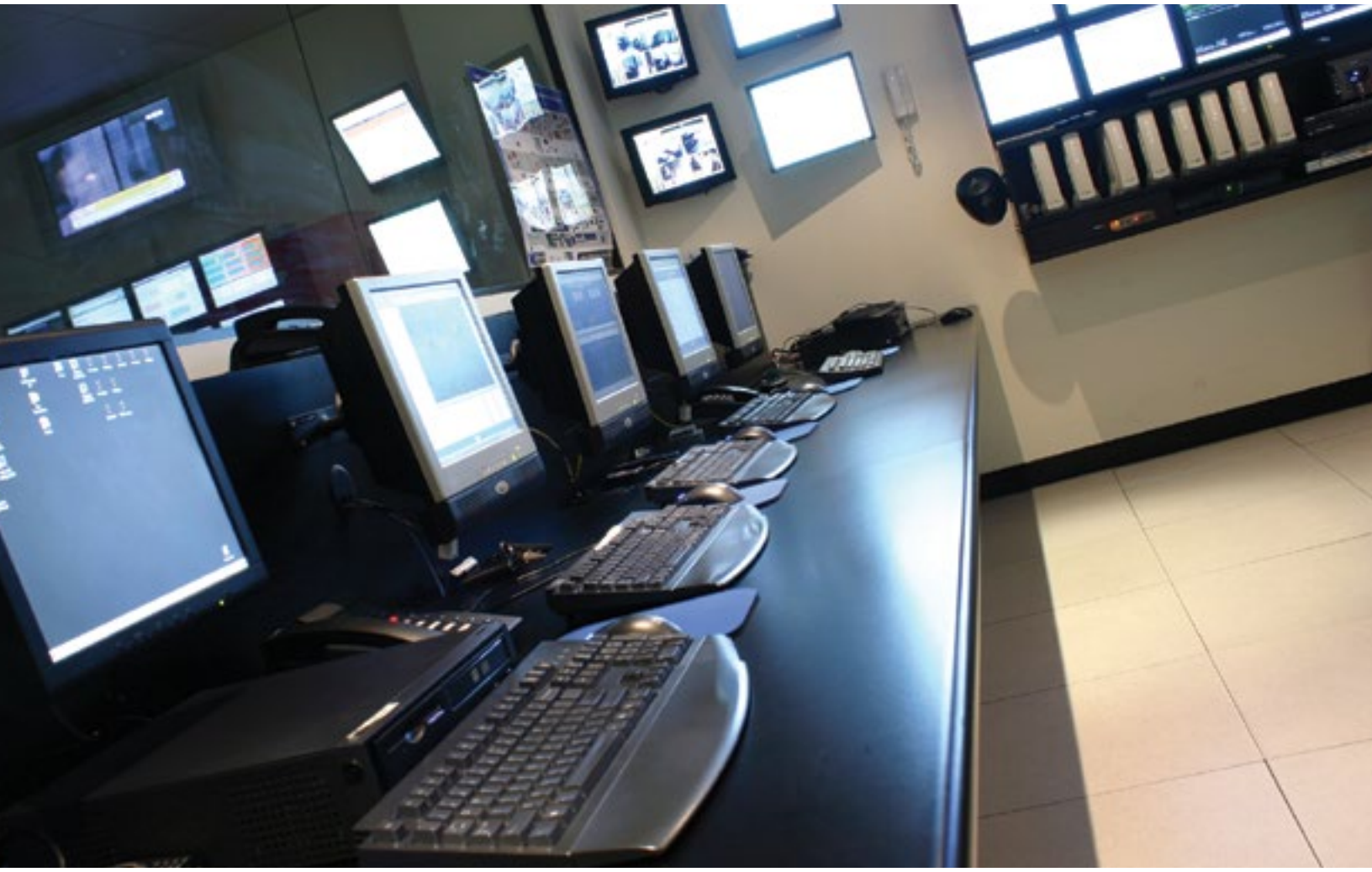
CANASA
Canadian Security Association
Association canadienne de la sécurité



Monitoring Station Reference Guide

Developed by the Canadian Security Association's
National Monitoring Station Committee and
Best Practices Working Group
Last updated September 2018

Foreword

The purpose of this document is to share best practices and reference tools, on a variety of monitoring station related topics, with security professionals industry-wide.

CANASA's Monitoring Station Committee and Best Practices Working Group, supports many methods and techniques that, through research and experience, have consistently resulted in superior outcomes. As the voice of the security industry, CANASA, has pooled these benchmarks to share with others in the industry, as a membership benefit.

This Monitoring Station Reference Guide is published by the Canadian Security Association (CANASA) and was developed and adopted by a consensus of industry volunteers in accordance with CANASA's policies and procedures. CANASA assumes no responsibility for the use, reliance, application or misapplication of this document. Industry members referring to or otherwise using this document acknowledge and confirm that they waive any right they might otherwise have had to assert claims against CANASA.

This document supports and refers to many standards and recommendations already developed by TMA (formerly CSAA) International, ULC, NFPA, PPVAR and SIA. These organizations are working towards standardization and best practices in collaboration with governments and other authorities. CANASA appreciates their cooperation in allowing it to include excerpts and references to its standards, throughout this guide.

CANASA's Monitoring Station Committee will review and update this document on an annual basis. CANASA reserves the right to revise this document at any time.

Authors: Kevin Leonard, Huronia Alarms; Allison Tuke, Paladin; Brittany Hack, Anna de Jager, Wendy Zaporosky and Robert Leduc, Lanvac; Robert Cherun, Muhammed Amarshi and Hugh Wong, Stealth Monitoring | UCIT Online Security; Kevin Allison and Patricia Richardson, Fire Monitoring of Canada; Kim Caron, Armstrong's National Alarm Monitoring; Dawn Burling, Sandy Smith and Jennifer Kukelko, AAA Alarms; Cameron Roberts, Harp Security; John Pniauskas and Mark Phillippi, Securtek; Bev Champagne, SRC; Lewis Jacobson, API; Jessie Gaisson, APS Security, Chris Currie, Damar Security Systems, Division of Lambton Communications Limited; Greg McPherson, CAPSYS; Patti Jones, Telsco Security Systems Inc.; Brent Pokrant, Protelec Limited.

Advisors: Ron Walters, SIAC; Joseph Ferenbok, University of Toronto; Elliott Goldstein, Solicitor.

Table of Contents

Canadian Security Association
50 Acadia Avenue, Unit 201
Markham, Ontario L3R 0B3
Tel: (905) 513-0622
Toll free: 1 (800) 538-9919
Email: info@canasa.org
www.canasa.org

Section 1: Introduction

Currently, while some facets of the security and monitoring industry fall under codes, standards or regional regulations, there are many areas of the industry without standardization of services. While this variation can provide a competitive differentiation, it can also result in confusion for the consumer as they attempt to determine which service best fits their needs.

The best practices and recommendations outlined in this guide are not intended to supersede any pre-existing codes or standards, nor is adherence required in order to maintain CANASA membership.

Through specialized advanced education courses like the Canadian Accredited Security Contractor (CASC) program, and the Alarm Technician Course (ATC), CANASA is working to enhance professional standards as they relate to the industry. Affiliate associations, TMA (formerly CSAA) and SIA, also provide education courses. The Monitoring Station Reference Guide has been developed with the same goal in mind; to enhance the performance of security related companies by unifying the processes and procedures they follow, and improving the reputation of the industry as a whole.

Section 2: Glossary of Terms

Introduction	This glossary provides definitions for some commonly used terms, to provide clarity and assist monitoring station personnel when they are communicating with others, specifically in the Canadian security market. Homeowners may also find this glossary helpful when learning to navigate new security systems.
24-Hour Zone	A zone that is permanently active twenty-four (24) hours a day and is not reliant on whether the system is armed or disarmed. A 24-Hour Zone can be programmed as a silent or audible event.
3rd Party Signal Receiving Centre (Wholesale)	A facility that provides monitoring services on behalf of another security installer, alarm dealer or installation company.
Access Control	An entry control system that may include access control equipment such as keys, access cards, locks, card reader, biometric identification devices, recorders, printers, and control equipment to identify, log and supervise access in and out of a facility.
AC Power	A type of electricity that is extremely versatile because the voltage can be changed through a transformer to suit a variety of electrical needs.
Alarm	An audible or visual warning that an event has occurred.
Alarm Administrator	A Person or Persons designated by the governing authority to administer and control the provisions of this bylaw and to review False Alarm reduction efforts
Alarm Communication Path	The method in which an alarm system communicates with a Signal Receiving Centre. Examples include: Plain Old Telephone Service (POTS), Cellular, Internet Protocol (IP), Digital Voice Access Control (DVAC).
Alarm Company	A business that sells, installs, services and monitors alarm systems.
Alarm Dealer	A business that sells, installs and services alarm systems which may be monitored.
Alarm Registration (or Permits)	Is a record of an alarm system which has been registered with the Alarm Administrator pursuant to any terms or provisions within the bylaws.
Alarm System	A combination of electronic equipment used to identify and report a detected condition.
Analytics	The discovery and communication of meaningful patterns in data. Especially valuable in areas rich with recorded information, analytics relies on the simultaneous applications of statistics, computer programming and operations research to quantity performance.

Section 2: Glossary of Terms

ANSI/SIA Control Panel Standard CP-01	The American National Standard Institute (ANSI) approved Security Industry Association – SIA CP-01 Control Panel Standard, as may be updated from time to time, that details recommended design features for security system control panels and their associated arming and disarming devices to reduce the incidence of false alarms. Control panels built and tested to this standard by Underwriters Laboratory (UL), or other nationally recognized testing organizations, will be marked to state: "Design evaluated in accordance with SIA CP-01 Control Panel Standard Features for False Alarm Reduction".
Arm/Arming	The function of turning on non-24-Hour Zones on an alarm system, which indicates that the site is in a closed state.
Arson	The crime of intentionally and maliciously setting a fire.
Automated Secure Alarm Protocol (ASAP)	A computer-aided dispatch system that processes information from alarm monitoring stations needing emergency dispatch and reduces the two- to three-minute delay currently in place.
Audible Alarm	A warning that an event has occurred that includes an audible notification at the premise.
Audio Verification	Means the transfer of sounds from the protected premises to the monitoring company, as a result of activation of one or more devices, as an additional way of verifying the validity of the alarm signal. *Refer to Section 11: Regulation Regarding Audio Recording.*
Authority Having Jurisdiction (AHJ)	A public service agency such as Police, Fire and/or Emergency Medical Services (First Responders) or Authorities Having Jurisdiction (AHJ). AHJ's can include Officials, Agencies, Departments, and Organizations that have the official authority and duty to enforce compliance with a standard or code, and to approve the use of systems, strategies, practices, procedures, protocols, plans, methods, machines, facilities, and installations.
Auxiliary Keys	Programmable buttons located on the keypad commonly labeled "panic", "fire" and "medical".
Away Mode	An arming function available in the programming of an alarm system that allows for complete arming of an alarm system, indicating no one is present at the location.
Back-Up Battery	A temporary back-up power source that ensures the alarm system will continue to work after losing AC Power for a finite period of time.
Back-up Signal Receiving Centre	A support facility that can take over monitoring operations in the event that the primary facility is disabled.
Burglary Alarm (BA Alarm)	An event activated by the breach of one or more intrusion detection devices on an alarm system.

Section 2: Glossary of Terms

Burglary (B&E)	The unlawful entry of any building or structure, with or without force, with the intent to commit a crime.
Bypass	The ability to temporarily disable a zone from the alarm system.
Carbon Monoxide (CO)	A colourless, odourless and tasteless gas that is slightly denser than air. It is toxic to humans when encountered in high concentrations. *Refer to Section 13: Carbon Monoxide Supervising Station Response Standard.*
Carbon Dioxide (CO2)	A naturally occurring gas that is colourless, odourless and vital to plant life.
Cellular Network	A cellular network or mobile network is a communication network where the last link is wireless. The network is distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station.
Cellular Technology	Refers to the underlying technology standards that are used to create a cellular network. These technology standards are broken down into Generations: 2G (GSM (TDMA-based), CDMA), 3G (CDMA2000, EDGE, UMTS, HSPA, HSPA+) and 4G (LTE, WiMAX).
Commercial Fire Alarm Signal	Where the applicable building code or fire code require a fire alarm system to be monitored, disposition of these signals shall be as per ULC s561 or as described in the applicable building, fire codes or AHJ.
Communication Format	A digital communication language developed and utilized by panel manufacturers to facilitate a clear understanding of the coding used in the transmission of the condition of an alarm panel to a Signal Receiving Centre. *See ANSI/SIA Control Panel Standard Definition.*
Control Panel	The central computer of an alarm system. Every device on the alarm system reports back to the control panel, which can be programmed to communicate with a Signal Receiving Centre.
DC Power	Short for direct current power, this type of electrical current travels through a circuit in only one direction. It is produced by fuel cells, batteries, and generators equipped with commutators.
Dead Man Switch	A device that requires movement or manual activation by an individual. The purpose of the device is to monitor ongoing activities in the room and to send an alert when a lack of activity occurs. *See Inactivity Alarm*.
Device/Detector	Electronic equipment that forms part of an alarm system to provide notification of an event to the control panel.

Section 2: Glossary of Terms

Digital Subscriber Line (DSL)	A family of technologies that provides digital data transmission over the wires of a local telephone network for Internet Access purposes. DSL service can be delivered simultaneously with wired telephone service on the same telephone line. This is possible because DSL uses higher frequency bands for data. On the customer premises, a DSL filter on each non-DSL outlet blocks any high-frequency interference to enable simultaneous use of the voice and DSL services. A DSL-filter must also be used on the alarm control panel in order for it to communicate with the Signal Receiving Centre.
Disarm/Disarming	The function of turning off non-24-Hour Zones on an alarm system, which indicates that the site is in an open state.
Dispatch	The act of communicating data to a responding party for the purpose of attending an alarm activation at a specific premise.
Door Contact	Often consists of a reed switch and a magnet designed to report an alarm event when the magnet and reed switch are separated.
Dry System	Fire suppression system that uses automatic sprinkler heads attached to a piping system pressurized with air. These systems use a dry pipe valve and air pressure to hold back the water supply. When the air pressure within the piping is released, water pressure will open the valve and fill the system. Water will only be discharged through the sprinkler heads that have opened. Dry systems are typically installed in unheated buildings or where there is the possibility of sprinkler pipes freezing.
Dual Path Communication	The ability to transmit signals to a Signal Receiving Centre on multiple communication paths.
Duress Code	A designated user code used to alert the Signal Receiving Centre that someone is under duress without alerting the intruder that emergency help has been requested. Alert can be received either verbally or electronically by the station.
Digital Voice Access Channel (DVAC)	A telecommunications medium in which an alarm system communicates to the Signal Receiving Centre by a leased dedicated telephone line. The line is supervised to provide maximum protection and an alarm will occur if the line is cut.
Early Open/Early Close	A disarming or arming signal received outside of a predefined schedule. May be generated via a schedule in the control panel or via automation software at the Signal Receiving Centre.
Electronic Alarm Retransmission	The process of electronically relaying alarm data from a Signal Receiving Centre to an appropriate PSAP.
Emergency Medical Services (EMS)	A public authority that provides the treatment and transport of people during emergency health situations.
End User	The person or organization to which service is provided.

Section 2: Glossary of Terms

Enhanced Call Verification	The attempt by monitoring facility personnel to verify that no emergency appears to exist, at the monitored premises, by means of two (2) or more verification calls to the monitored premises and/or to an individual on the contact list. *Refer to Section 5: Enhanced Call Verification*.
Entry/Exit Delay	A programmable period designed to offer time to enter/exit an alarmed site after disarming/arming an alarm system to avoid setting off the alarm.
Entry/Exit Zone	An alarm zone with a programmable entry/exit delay period that protects the area(s) most frequently used to enter or exit an alarmed site.
Environmental Monitoring	A range of alarm devices that are designed to monitor environmental changes on a 24-hour basis.
Event Based Video Monitoring	A service provided by a monitoring station whereby an operator remotely views a video alarm in order to identify any unauthorized activity at the site that may require a responder.
Event Reports	The ability to extract data generated by the control panel and compile the data on a manual or automated basis.
Fail to Test (FTT)	Notification from the automation software that indicates that the system has not transmitted within a predetermined period of time. *Refer to Section 7: Failure to Test*.
Fail to Open/Fail to Close	A disarming or arming signal HAS NOT BEEN received within a predefined schedule. May be generated via a schedule in the control panel or via automation software at the Signal Receiving Centre.
False Alarm	Signal(s) generated from an alarm system and sent to an SRC (Signal Receiving Centre) where it was found that an emergency event did not exist. *Sometimes refered to as Nuisance Alarm*.
False Dispatch	The dispatch of predetermined person(s) and/or authority to a false alarm.
Faulted Zone	A device within the security system that is in a trouble state and can cause the system not to arm or respond correctly.
Fire Alarm	An event activated by the breach of one or more fire detection devices on an alarm system.
Fire Alarm System/Cabinet (FAS/FAC)	The controlling component of a fire alarm system. The panel receives information from environmental sensors designed to detect changes associated with fire, monitors their integrity and provides for notification and communication of emergency situations. Usually found in commercial or multi-tenant premises.
Fire Alarm Control Panel/ Transmitter (FACP/FAT)	The central computer of a fire alarm system. Every device on the fire alarm system reports back to the control panel, which can be programmed to communicate with a Signal Receiving Centre.

Section 2: Glossary of Terms

Fire Detector	A device which detects a fire condition and automatically initiates an electrical signal to actuate an **alert signal** or **alarm signal** and includes **heat detectors** and **smoke detectors**.
Fire Verification	When there is an applicable Standard (UL, ULC, NFPA) in place, the standard supersedes any recommended best practices contained herein. In cases where a Standard does not apply, it is recommended that a verification call is made to the premise or responsible party in order to attempt to verify if an actual fire condition exists. The purpose of the fire verification call is to minimize the chance of a false fire dispatch, however performing the verification call can introduce a delay of dispatch when an actual fire condition does exist. *Refer to Section 12: Residential Smoke and Heat Alarm Monitoring.*
Follower Zone	A type of zone for an alarm system that is usually assigned to an entry area that one must pass upon entry (after faulting the entry/exit zone) to reach the keypad. It provides an instant alarm if the entry/exit zone is not violated first, and protects an area in the event an intruder has hidden on the premises before the system is armed, or gains access to the premises through an unprotected area. It causes a delayed alarm if the entry zone is faulted first and the user code is not entered in time; and causes an instant alarm in all other situations.
Force Arm	To arm the alarm system in spite of the presence of faulted zones.
Gate Valve	Commonly used to control water supply flow to sprinkler systems. Also known as Outside Screw & Yoke (OS&Y) gate valve. Can be used for controlling the main water supply for sprinkler system or to control water flow to branch lines. Closing the Gate Valve on a sprinkler system can effectively render the system inoperable and should be monitored for position. Monitoring the gate valve for closure would trigger a Supervisory Type Condition.
Glass Break Detector (GBD)	An alarm system device that detects the frequency of breaking glass.
Global Positioning System (GPS) Tracking	A GPS system utilizes signals from a variety of GPS satellites to provide accurate location information reported in latitude and longitude. GPS Tracking is used to determine the location of a moving object in real time. A GPS device can therefore be used in an alarm system that protects a movable asset or person. *Refer to Section 14: Global Positioning Systems (GPS)*.
Global System for Mobile Communication (GSM)	See "Cellular Technology"
Guard Service	An alternate dispatch agency that responds to reported conditions.
Hardwired Alarm System	A combination of electronic equipment connected by low-voltage wiring to a control panel, used to identify and report a detected condition.
Heat Detector	A fire detector designed to operate at a predetermined temperature or rate of temperature rise.

Section 2: Glossary of Terms

Heating, Ventilation, Air Conditioning (HVAC) Alarm	An environmental event that reports various system conditions. Environmental events can include Temperature, Chemical, Biological, Gas, Pressure or Low Current in order to indicate the presence of or level of (high/low) these conditions.
Hold Up	A robbery carried out with the threat of direct physical harm.
Hold Up Alarm	An alarm device that will not set off an audible alarm and is designed for a person in distress to discreetly request help.
Hosted Access Control	The designate hosts the database, server applications and hardware infrastructure, and provides the initial set-up of the account and components, which enables a user to remotely administer the services from either a secure web client or workstation.
Household Fire Alarm Signal	Household is defined in NFPA 72 as the family living unit in single-family detached dwellings, single family attached dwellings, multifamily buildings and mobile homes. The primary purpose of fire alarm systems in households is to provide an audible signal to occupants in order to expedite evacuation of the household. These systems may be connected to the households monitoring system and responded to as per the Signal Receiving Centres standard operating procedures. *Refer to Section 12: Residential Smoke and Heat Alarm Monitoring*.
Hybrid Access Control	The designate provides customizable service offerings that combine both Hosted and Managed access control.
Inactivity Alarm	An alert created by an alarm system when a device enters an idle state. This may include a lack of movement or a missed action within a predefined time frame. *See Dead Man Switch*.
Infrared Illumination	An Infrared light source that can be used to augment the available ambient light, increasing in-the-dark visibility without actually using a visible light source. Most often used in video surveillance systems.
Interactive Service	A portal that can allow direct control/access to the alarm system functionality and also enable a series of end-user notifications and alerts.
Installer Code	An unrestricted code used to enter an alarm system's programming menu during installation or service.
Interior Protection	A series of devices often used as an added layer of security beyond perimeter protection.
Internet Communication	A type of alarm transmission path that uses an Internet Protocol (IP) connection to send signals over the Internet from the control panel to a Signal Receiving Centre's IP receivers. See Internet Protocol.
Internet Protocol (IP)	A data-oriented protocol used for communicating data across a packet switched inter-network. *Refer to Section 6: Internet Monitoring*.

Section 2: Glossary of Terms

Internet Protocol Address (IP Address)	A unique address that identifies a computer or device on an IP network. XXX.XXX.XXX.XXX is the format for an IP address with each X representing a number between 0 and 255. IP networks use the IP address to forward messages between different devices on the network. *Refer to Section 6: Internet Monitoring*.
Intrusion	See definition 'Burglary'.
Keyfob	A wireless device that can be programmed to perform a series of functions, most commonly arming, disarming and/or alerting of emergency conditions.
Key Holder	A designated contact for an alarm site that has authority and access to the premise. Also known as responsible party, call list, or contact person.
Keypad	The user interface for operating the alarm system.
Liquid Crystal Display (LCD)	The technology used to display alphanumeric characters on an alarm system keypad.
Life Safety System	Any type of alarm system that is meant to protect one's life instead of property. Fire alarms, panic buttons, or medical alert systems are all examples of life safety systems.
Light Emitting Diode (LED)	A semiconductor diode that emits light when an electric current is applied. It is most commonly used in the security industry to illuminate icons on a keypad, conditions on a control panel (or enunciator panel), and amplify lighting in a dark room so that security cameras are able to capture better quality images.
Line Card	The digital component of a receiver that is connected to a telephone line, cellular or Internet path and receives alarm signals and data from a protected premise.
Local Alarm System	An alarm system that does not send an alarm signal to a Signal Receiving Centre, but relies instead on one or more visual or audible devices onsite to alert occupants or neighbors to a detected condition.
Local Area Network (LAN)	A group of computers and associated devices that share a common communications line.
Lone Worker	An employee who performs an activity in isolation without close or direct supervision. *Refer to Section 15: Lone Worker Guidelines*.
Low Sprinkler Pressure	Indicates a 10psi drop in pressure within the sprinkler system. Typical wet sprinkler system should be maintained at 120psi (Wet System) or 40psi (Dry System) and should also be monitored for high pressure as well to prevent damage to the sprinkler system and long delay of a water flow alarm. Can also indicate low water pressure for public water supplies. This is considered to be a Supervisory Type Condition.
Man Trap	A restricted access point into a Signal Receiving Centre that usually requires interlocking doors, access controls and video surveillance.

Section 2: Glossary of Terms

Managed Access Control	A service where a host manages the database, server applications and hardware infrastructure. The end-user makes requests to the host, most commonly a Signal Receiving Centre, for all changes and operation.
Master Code	A code in an alarm control panel that has elevated privileges over a regular user code. Master codes can be used to add, delete or modify other user codes on an alarm system and is required to perform certain system functions.
Medical Alarm	An event activated by the breach of one or more Personal Emergency Response System (PERS) devices. *See Personal Emergency Response System*.
Monitored Alarm System	An alarm system that sends a signal to a Signal Receiving Centre.
Motion Activated Cameras	A security camera that is set to activate based on the detection of motion.
Motion Detector	An electronic device that uses passive infrared or microwave technology to detect motion in a protected property.
National Fire Protection Association (NFPA)	An international non-profit organization advocating codes and standard consensus, training, education and research for fire prevention.
Network Bandwidth Capacity	The maximum data transfer rate of a network or Internet connection. It measures how much data can be sent over a specific connection in a given amount of time.
Panel Programming	The act of setting up, defining or changing the settings in an alarm panel, whether onsite or remotely, that has a direct effect on how the panel works and communicates.
Panic Button	A 24-hour electronic device that causes a silent or audible alarm event when activated.
Partition	The ability to program unique segments of an alarm system to act independently of one another.
Passive Infrared	An electronic sensor that measures infrared (IR) light radiating from objects in its field of view. Most often used in PIR-based motion detectors.
Passive Infra-Red (PIR) Motion Detector	An electronic device that measures infrared (IR) light radiating from objects in its field of view to sense motion and activate an alarm condition.
Perimeter Protection	A series of electronic devices designed to protect the entry points of a secured property.
Personal Emergency Response System (PERS)	A combination of electronic equipment whose purpose it is to identify and report a detected medical condition.
Pet Immunity	Technology used in a motion detector to exclude animals of a certain size and weight in order to reduce false alarms.

Section 2: Glossary of Terms

Plain Old Telephone Service (POTS)	The standard telephone service that most homes use that is not based on high-speed digital communication lines.
Power Supply	An electronic device that supplies energy to an electrical load. The primary function in an alarm system application is to provide additional electrical power to powered devices such as motion sensors, smoke alarms and glass break sensors.
Proximity Card	A badge, tag, or card that if authorized, grants a user access to a restricted area when placed close to a proximity reader.
Proximity Reader	An access control device that sends information to an access control panel that controls an electronic lock. When a proximity card is placed near a proximity reader, and that card has authority to allow access, access is granted.
Public Safety Answering Point (PSAP)	A physical location where 9-1-1 emergency telephone calls are received and then routed to the proper emergency service.
Radio Frequency (RF) Wireless Signal	A form of wireless communication between alarm devices and control panels.
Rate-of-Rise (ROR)	A fire alarm device that is connected to an alarm system and programmed to detect a rapid change in temperature.
Receiver	The digital equipment housed in a Signal Receiving Centre that receives, decodes and communicates to an automation system or operator alarm signals and data from a protected premise.
Regulatory Agencies	• American National Standards Institute (ANSI) www.ansi.org • Building Industry Consulting Service International, Inc. (BICSI) www.bicsi.org • Canadian Accredited Security Contractor (CASC) http://www.canasa.org/CANASA/EN/Membership/Canadian_Accredited_Security_Contractor_Program/CANASA/CASC_Pages/Program_overview.aspx • Canadian Fire Alarm Associations (CFAA) www.cfaa.ca • Canadian Fire Code (CFO) www.nrc-cnrc.gc.ca • Canadian Security Association (CANASA) www.canasa.org • Canadian Standards Association (CSA) www.csagroup.org • Electronic Security Association (ESA) www.esaweb.org • International Code Council www.iccsafe.org • National Fire Protection Association (NFPA) www.nfpa.org • Partnership for Priority Video Alarm Response (PPVAR) www.ppvar.org • Security Industry Association (SIA) www.securityindustry.org • The Monitoring Association (formerly CSAA) www.csaaintl.org • Underwriters Laboratories of Canada Ltd. (ULC) https://canada.ul.com/
Repeater	An electronic device that receives a signal and retransmits it at a higher level or power to cover longer distances.
Restore	The return of an alarm point or sensor to a former, original or normal state.

Section 2: Glossary of Terms

Robbery	The unlawful removal or attempted removal of property that is in the immediate possession of another by force or threat of force.
Satellite Station	An unmanned receiving centre that houses equipment used to gather signals which are forwarded to the primary Signal Receiving Centre for processing and response.
Security Camera	A video camera that is used for electronic motion picture acquisition in various forms of video surveillance.
Security System	An electronic system that is designed to alert a designated contact(s) that a situation exists.
Signal Disposition Centre	A monitoring station without receiving equipment but with staff to process and disposition signals.
Signal Receiving Centre	A facility that receives alarm signals for processing and response. Also known as Monitoring Station, Central Station, and Signal Disposition Centre.
Silent Alarm	An alarm condition that offers no audible alert at the secured site but indicates an interruption in a circuit on the control panel at the monitoring station.
Siren	A sounding device built into an alarm system that can emit a noise when the alarm system is triggered.
Smoke Alarm	A combined **smoke detector** and audible alarm device that is designed to sound an alarm within a room or dwelling in which it is located when there is smoke within the room or dwelling. A smoke alarm with an extra relay built in is often connected to a typical security system.
Smoke Detector	A **fire detector** designed to operate when the concentration of airborne combustion products exceeds a predetermined level.
Stay Mode	An arming function of an alarm system that permits the bypassing of selected interior devices. This enables the end-user to occupy the interior of an armed location without setting off the alarm.
Sump Pump Detector	An electronic device that detects the height of water or potential flooding within the sump pit.
Strobe	A visual warning device located at a protected premise.
Supervisory Signal	An alarm signal designed to alert the designated contact(s) that a condition exists.
Telephone Line Monitoring (TLM)	Supervision of the alarm system's phone line connection by measuring voltage on the line.
Temperature Alarm	An audible or visual warning that indicates a change of ambient temperature at a protected premise from a pre-set temperature. Indicating either HIGH or LOW temperature changes.

Section 2: Glossary of Terms

Test Interval	The length of time set between timer test signals. *Refer to Section 7: Failure to Test*.
Theft	The unlawful removal or attempted removal of property (other than a motor vehicle) from the possession of another, by stealth, without force and without deceit, with intent to permanently deprive the owner of the property.
Timer Test	A signal sent from the system at a specific test interval to safeguard that it is communicating properly. *Refer to Section 7: Failure to Test*.
Transformer	A device used to plug an alarm system into a standard AC wall outlet or is wired into the electrical system to provide AC power.
Trouble Signal	An alarm signal designed to alert the designated contact(s) that a condition exists.
ULC Listed Protective Signalling	A fire certificate service offered by ULC approved Alarm Companies and Signal Receiving Centres that is designed to uphold the installation, commissioning and monitoring of an alarm system as outlined in ULC Standard CAN/ULC-S561. *Refer to Section 16: Security Employee Education and Training Resources.*
ULC Listed Burglar	An alarm system certificate service offered by ULC approved Alarm Companies and Signal Receiving Centres that is designed to uphold the installation, commissioning and monitoring of an alarm system as outlined in ULC Standards CAN/ULC-S301. *Refer to Section 16: Security Employee Education and Training Resources.*
ULC Listed Burglar - Financial	A certificate service offered by ULC approved Alarm Companies and Signal Receiving Centres that is designed to uphold the installation, commissioning and monitoring of an alarm system as outlined in CAN/ULC-S302. *Refer to Section 16: Security Employee Education and Training Resources.*
User Code	A numeric code used to arm and disarm a security system.
Unscheduled Opening (USO)	A condition generated by automation software when an Opening occurs outside of a predefined time schedule.
Verified Alarms	An alarm in which a monitoring station operator confirms the presence of humans (at a specific site), and has information that shows a probable crime in progress.
Video Alarm	An alarm received from a camera (video input). This can be derived from either hardware plugged into the camera (e.g. a motion detector) or camera/software analytics (e.g. video motion or audio detection). *Refer to Section 8: Video Monitoring Definition; Section 9: Video Monitoring (Live/Continuous); Section 10: Data Usage and Storage in Video and Audio Applications.*
Video Monitoring	The ability to continuously view live video at designated times from an off-site facility. *Refer to Section 8: Video Monitoring Definition; Section 9: Video Monitoring (Live/Continuous); Section 10: Data Usage and Storage in Video and Audio Applications.*

Section 2: Glossary of Terms

Video Verification	The pairing of real-time video data or jpg images and an independent alarm signal to provide enhanced information in determining a response protocol. *Refer to Section 8: Video Monitoring Definition; Section 10: Data Usage and Storage in Video and Audio Applications.*
Virtual Guard Tour	A service provided whereby an operator remotely views live video data at a protected premise on a scheduled interval. The operator performs a check of each camera in order to identify any unauthorized activity at the site that may require a responder. *Refer to Section 8: Video Monitoring Definition.*
Visual Alarm	A warning that an event has occurred that includes a visual notification at the premise.
Water Detector	An electronic device that detects the presence of water or potential flooding.
Water Flow	An indication that water is actively flowing through the sprinkler system. This can be triggered by either a Pressure Style Water Flow Switch or by a Vane Type Water Flow Switch. A water flow trigger would be considered an Alarm Type Condition.
Wet System	Fire suppression system that uses automatic sprinkler heads attached to piping containing water and connected to a water supply so that water will be discharged immediately from an open sprinkler.
Window Contact	A connection that consists of a reed switch and a magnet designed to trigger an alarm event when the magnet and reed switch are separated.
Wireless Alarm System	A combination of electronic battery powered transmitters connected to a control unit using radio frequency, used to identify and report a detected condition.
Zones	The capability of an alarm system to separate and report events by alarm point. (Example: Zone 1 – Front Door Contact; Zone 2 – Front Entry Motion Detector)
Zone Description	Information that identifies the type of alarm device connected to a security system, as well as the location assigned to that device.
Zone Expanders	A module that can be added to an alarm system in order to provide additional capacity beyond what the control panel has as default.

References/Resources:

Glossary of Terms (CSAA.GOT1) January 1996 as reviewed 1998, prepared and submitted by CSAA Standards Committee – Copyrighted CSAA 1996.

http://www.kantech.com/Products/hattrix.aspx
http://www.geoarm.com/security-system-glossary.html

NFPA 72

2015 Ontario Fire Code

Section 3: Alarm Response Guidelines

Intrusion Alarms

(Carbon Monoxide is detailed in section 13 of this document)

The guidelines below are what we have found through experience to provide the best balance of ensuring the end user's security and safety while minimizing reliance and potential fees for authorities responding to alarm activations.
In all cases any local bylaws, regulations or policies will supersede these recommended responses.

In addition any ULC Certified systems (or any systems with a different standard in place) need to be responded to as per the appropriate standard guidelines. Customer or end user preferences and special requests may also override the protocols outlined below.

At any point in the verification process if a user is reached who can confirm that no emergency exists, and provides any confirmation or password verification required, the process may end without completing the next stages.

Upon receipt of an intrusion type alarm the base or minimum procedure should be as follows:

- Call protected premise main contact number
- Dispatch Authorities
- Call the keyholder list

Additional notes for Best Practice suggestions/recommendations- the items below should be taken into consideration when determining best practices for alarm response. All or a combination of the recommendations below will impact Authority dispatches for False Alarms.

- ECV (Enhanced call verification) is recommended and in many jurisdictions is mandatory. Section 5 in this document further defines ECV but to summarize briefly, this is two verification calls to determine if a dispatch of authorities is required.
- If an authorized contact is not able to provide a correct password this is treated as no contact and notification should continue.
- Any alarm with an open/alarm cancel code/abort code that is received by the station should be considered a non-emergency and no authority dispatch should take place.
- If an answering machine is reached during the notification process, a clear and brief message should be left.
- If at any point after dispatch a user/keyholder/contact confirms no emergency exists, the dispatched authority should be notified.
- If an alarm is received in connection with a scheduled opening or closing, additional attempts should be made to verify the alarm is an emergency before dispatch.

Unscheduled Openings

Unscheduled or unexpected openings or closings should not be treated as an emergency requiring dispatch unless there is a request for dispatch from a user/keyholder.

Hold Up and Panic Type Alarms

Commercial Hold Up Alarm – upon receipt, dispatch authorities immediately.
- After dispatch, wait up to 30 minutes, then proceed to contact primary number for protected premise and keyholders as necessary.

Residential Panic Alarm
- Call protected premise main contact number
- Dispatch authorities
- Call the keyholder list

Keypad Panic
- Call protected premise main contact number
- Call the keyholder list
- Dispatch authorities

In App Panic
- Call protected premise main contact number
- Call the 1st keyholder
- Only the primary login will have access to the In App Panic feature (not everyone on the account)
- Dispatch authorities
- Stations should check with local AHJ's as some may require enhanced call verification, or video/onsite confirmation before attending to In App Panic.

Fire Alarms

Household Fire Alarm
- Call protected premise main contact number to attempt to verify if this is a false alarm, if no confirmation of a false alarm, then Dispatch authorities within 45 seconds of receiving the signal as per our recommendations. *Refer to Section 12: Residential Smoke and Heat Alarm Monitoring, for further information*.

Residential Smoke and Heat Alarm Monitoring
- Dispatch authorities
- Call the keyholder list
- If a non-emergency is confirmed, advise authority.

Commercial Fire Alarm
- Dispatch authorities as per applicable standard
- Call protected premise main contact number
- Call the keyholder list
- If a non-emergency is confirmed, advise authority.

Medical Alarms

Medical Alarm – no answer
- Call protected premise/persons main contact number
- Call at least one additional alternate number (cell phone or keyholder number)
- Dispatch authorities
- Call the keyholder list

Medical Alarm – answered
- Call protected premise/persons main contact number
- If person on site verifies emergency, Dispatch then contact keyholder list
- If person on site verifies no emergency, contact keyholder list.

Notes:
The additional precaution of contacting a keyholder upon receipt of any alarm is first, to notify if a dispatch has taken place, and secondly in the case of a person on site verifying no emergency, we recommend keyholders or persons responsible be contacted in the event the protected person requires further assistance (even if this request is not communicated to the Central Station upon first contact)

References: Portions of these Alarm Response Guidelines are based on the CSAA Alarm Confirmation, Verification and Notification Procedures ANSI/CSAA CS-V-01-2016. For more detail on this standard, please visit their website: http://csaaintl.org/

Communication

Notification is not necessarily by voice, escalation may be required for communication by text or email. There is a recommendation by CANASA for companies to have an internal policy in place for verification of signal traffic communicated for text or email through the central station.

Environmental / Supervisory j20 – Monitoring Station Application Only

A supervisory type signal from a module or device that is not considered an Alarm including, but not limited to: wired circuit fault, wireless connectivity, low battery, communication faults, loss of power, general system faults and environmental changes, the monitoring station shall:

- Begin efforts to notify the protected premises or Persons of Authority on the Call List within 30 minutes to ensure they are aware of the event and/or an emergency condition does not exist.
- Attempts to contact the Persons of Authority shall continue at 4-hour increments until direct communications is acquired or notification indicating a restoration of the supervisory signal is received.
- Verbal or Electronic messaging shall be considered as contact with the Persons of Authority and notification complete.
- Upon contacting the Persons of Authority, notification of the situation to determine the source of the trouble the appropriate corrective action should be discussed.
- The monitoring station bears no responsibility beyond notification and it shall be the responsibility of the Persons of Authority to determine if a service technician is required and if so, dispatched.

Please Note
Multiple supervisory signals within a short period of time could indicate system tampering, system attack, catastrophic failure or unauthorized testing. This best practice is not intended to be applied to alarm conditions where those procedures take precedence.

A Supervisory signal can be defined as critical and non-critical and is defined by the station or Persons of Authority and would carry unique response times.

References/Resources:
CAN/ULC-S301 Standards for Signal Receiving Centre's Configurations and Operations

Section 4: Alarm Service Contracts

Introduction

A benefit of CANASA Membership is access to alarm service contract templates for all Canadian provinces -- for both commercial and residential use. Members can download contracts in Microsoft Word format and can easily adapt them to include personalized, company information. CANASA will review these contracts on an annual basis to ensure accuracy and adherence to provincial laws, and update them when necessary.

While many companies incur expensive fees for legal review and creation of alarm service contracts, CANASA offers them to Members free-of-charge.

References/Resources:
Visit www.canasa.org. Login and select the "Members Only" button on the left sidebar, then select the heading "Contracts".

Section 5: Enhanced Call Verification (ECV)

Introduction

CANASA recently revised its policy on ECV to clarify its strong support of the requirement that mandates two (2) calls be placed to contacts to verify an alarm incident prior to requesting emergency response. The policy is as follows:

Policy Number: 006
Released: September 1990
Revised: April 2014

Verification of Intrusion Alarm Signals – Enhanced Call Verification (ECV)

Policy Statement

That CANASA endorses Enhanced Call Verification (ECV), verification of the alarm by telephoning at least two (2) contact points, prior to notification of police, as its policy regarding verification of intrusion alarms.

Background Material

The intent of Enhanced Call Verification (ECV) or alarm verification by telephone is to reduce false alarm traffic. It is based upon the premise that most false alarm dispatches are due to customer error and can be prevented by the customer. ECV requires that the monitoring agency attempt to establish telephone contact with the premise and at least one authorized person in order to verify an alarm, before police are notified.

When local authorities mandate ECV, significant reductions in false alarm traffic, as measured by police, can be achieved. ECV can also highlight the need for customers to maintain and operate their alarm systems in a responsible manner. Monitoring stations can also realize benefits in reduced call volume.

Definition

Enhanced Call Verification is the attempt by monitoring facility personnel to verify that no emergency appears to exist, at the monitored premises, by means of two (2) or more verification calls to the monitored premises and/or to an individual on the contact list.

References/Resources:
CANASA policy #006

Section 6: Internet Monitoring

Introduction

A type of alarm communication path that uses an IP (internet protocol) connection to send signals over the internet from the control panel (usually via Ethernet or Wi-Fi) to a Signal Receiving Centre's IP receivers.

The internet has become the pathway for much of the communication done in our social and business lives. It can also be a pathway for alarm systems to communicate with Signal Receiving Centres and subscribers as well. Many stations now have the ability to accept alarm signals via the internet. The communicator at the premise usually connects to the premise local area network or LAN the same as any other computer at the premise. Much of our communication networks travel via the internet either through voice over IP (VoIP), cellular (many cellular alarm communicators clearing houses send the signals to the Signal Receiving Centre via IP). Sometimes port forwarding may be required to get through any existing firewalls etc. on the premise router etc.

The advantages of internet monitoring

- Advanced speed: Internet protocol (IP) transmissions can be very fast
- Supervised: Some communicators can be supervised to indicate the system at the premise is not communicating or offline. They can also be ULC listed with the proper equipment and configuration
- Versatility: With the alarm panel connected to the internet many possibilities become available for home automation, emails to clients etc.

The disadvantages of internet monitoring

- Accountability: There may be many different internet service providers (ISP) between the subscribers premise and the Signal Receiving Centre so connectivity problems can be hard to diagnose. The modem and router are often controlled by the ISP or the premise owner and they may change the equipment without letting stations know. Also, most routers, modems and switches do not have any battery backup so may fail during a power failure. ULC does require 24 hours of standby. A backup form of communication via cellular or pots is usually recommended. Most internet communicators can also transmit to a backup location which could be an alternate station or connection. The station may have a secondary internet connection as well.
- Reliability: Just like POTS lines were never designed for alarm panel communication or supervision, internet connections are designed for internet traffic. Losing an internet connection in the middle of the night for maintenance is not an issue for most internet surfers but is an issue for 24 hour supervision of an alarm system.
- Compatibility: As always, most providers of this equipment will have proprietary equipment needed at both the premise and station
- Most signals from systems monitored via the internet will be responded to in a similar fashion to existing POTS service. The one main difference is a loss of communication with the premise. Best practice would be to follow any specific instructions and/or ULC's requirement as listed in their latest standards (see next page).

Recommended Best Practices for Loss of Internet Communication

IP communication paths can sometimes be supervised to detect a loss of communication with the subscribers transmitting unit. When the station detects a communication trouble you obviously need to first follow any prescribed procedures for the account e.g. dispatch, etc. It is important to identify the problem is widespread, localized or with the monitoring stations own internet connection. If the outage is at the Signal Receiving Centre's site an attempt should be made to correct the communication trouble. Rebooting the modem or router often corrects these issues. Good records of all ISP providers and corrective measures should be kept to expedite service repairs.

If after a few minutes this can't be corrected, then the subscriber needs to be contacted. If the problem is at the subscribers end, they should be instructed to contact their own provider or ISP to correct the problem if necessary.

If there is an alternate path for communications or if the issue is widespread amongst many subscribers, then you may want to wait an hour before contacting the client.

Current ULC standards on alarm monitoring for active communications is a guideline for dealing with internet communication faults. Please refer to the applicable standards for more detailed information.

Managed Facilities-Based Voice Network Providers (MFVN)

A physical facilities-based network capable of transmitting real time signals with formats unchanged that is managed, operated, and maintained by the service provider to ensure service quality and reliability from the subscriber location to public switched telephone network (PSTN) interconnection points or other MFVN peer networks.

Public Switched Telephone Network (PSTN)

An assembly of communications equipment and telephone service providers that utilize managed facilities-based voice networks (MFVN) to provide the general public with the ability to establish communications channels via discrete dialing codes.

References/Resources:
ULC s561, ULC s302

Section 7: Failure to Test

Introduction

An alarm panel has an internal health monitoring system. On a regular basis the alarm panel will check its main electrical power source, backup power supply and communication path(s). When this health check is completed, the alarm system can be programmed to report its status to a Signal Receiving Centre.

A normal status is reported as an Automatic System Test or Timer Test.

Each organization has their own process regarding communication of an Automatic System Test or Timer Test. Generally, supervision polling can range anywhere from 24 hours to 30 days. Higher security and ULC sites may even require smaller intervals for their supervision polling.

Fail to Test, Late to Test or No Test Code (NTC) – Signal Receiving Centre

Most Signal Receiving Centres use automation software that is programmed to provide health monitoring for each site in their database.

When an expected event such as an Automatic Test Signal or Timer Test is not received, the automation software will present an operator with a failed event. A Fail to Test signal is such an event.

Once an operator is presented with a Fail to Test event, it is recommended that they contact the authorized individual (e.g. dealer, customer, service department) to notify of the communication failure status.

Section 8: Video Monitoring Definition

Policy Statement

The definitions for video monitoring and verification require clarification in order to incorporate changes in technology and to industry practices. CANASA endorses the following three definitions and recommends that CANASA members ensure that they use these terms consistently in their interactions with customers and within their marketing materials.

Video Monitoring

Video Monitoring is the ability to continuously view live video at designated times from an offsite facility.

Video Alarm Verification

Video Alarm Verification is the pairing of real-time video data and an independent alarm signal so as to provide enhanced information in determining a response protocol.

Virtual Tour

A Virtual Tour is a service provided by a monitoring station whereby an operator remotely views live video data on a scheduled interval. The operator performs a check of each camera in order to identify any unauthorized activity at the site that may require a responder.

Section 9: Video Monitoring (Live/Continuous)

Introduction

Live video monitoring enables Signal Receiving Centres to view live video on a PC, tablet, or mobile device from just about anywhere in the world provided there is Internet access. This dynamic access is incredibly efficient, but is vulnerable if security protocols are not implemented and followed. All stakeholders (integrator, Signal Receiving Centre, telecom provider, end-user) need to be involved to ensure an appropriately secure and effective solution.

Private sector privacy laws require that an organization's need to conduct video surveillance must be balanced with the individual's right to privacy. Information about an organization's personal information management practices, including video surveillance, should be readily accessible.

Installation and Operation of Cameras

With the design, build and installation of systems for customers, it is important to document and develop policy on the use and management of video surveillance information both internally and externally at your company. This information should be provided to customers (end-users) as they learn about the operation of their system along with benefits and risks.

The video surveillance system should be set up and operated to collect the minimum amount of information to be effective. This helps reduce the intrusion on individuals' privacy. Specifically:

- Cameras that are turned on for limited periods in the day are preferable to "always on" surveillance.
- Cameras should be positioned to reduce capturing images of individuals who are not being targeted. For example, a store security camera should not be recording passers-by outside the store.
- Cameras should typically not be installed in areas where a person expects a high level of personal privacy, such as bathrooms, locker rooms, changing/dressing rooms, bedrooms and windows. Steps should be taken to ensure that cameras cannot be adjusted or manipulated by the operator to capture images in such areas.
- Camera operators need to fully understand their obligation to protect the privacy of individuals.
- Sound should not be recorded unless there is a specific need to do so.
- If a camera is monitored, the recording function should be turned on only when unlawful activity is suspected or observed.

Signage Requirements

Most privacy laws require the organization conducting video surveillance to post a clear notice about the use of cameras on its premises before individuals enter the premises. This gives people the option of not entering the premises if they object to the surveillance. Signs should include: the PURPOSE for the surveillance; the name of the operator of the system; and contact information should individuals have questions or want access to images related to them.

External Communication

1. Establish the business reason (PURPOSE) for conducting video surveillance and use video surveillance only for that reason.
2. Inform the public that video surveillance is taking place.
3. Be ready to answer questions from the public. Individuals have the right to know who is watching them and why, what information is being captured, and what is being done with recorded images.
4. Give individuals access to information about themselves when requested. This includes video images.

References/Resources:

Office of the Privacy Commissioner of Canada: Guidance on Covert Video Surveillance in the Private Sector
https://www.priv.gc.ca/en/privacy-topics/surveillance-and-monitoring/gd_cvs_20090527/

Office of the Privacy Commissioner of Canada: Guidelines for Overt Video Surveillance in the Private Sector
https://www.priv.gc.ca/information/guide/2008/gl_vs_080306_e.asp

Office of the Privacy Commissioner of Canada: Findings under the Personal Information Protection and Electronic Documents Act (PIPEDA)
https://www.priv.gc.ca/cf-dc/2011/2011_003_0325_e.asp

Information and Privacy Commissioner of Ontario: Guidelines for the Use of Video Surveillance
https://www.ipc.on.ca/wp-content/uploads/Resources/2015_Guidelines_Surveillance.pdf

Partnership for Priority Video Alarm Response - Video Verified Alarms Best Practices
http://www.ppvar.org

Section 10: Data Usage and Storage in Video and Audio Applications

Introduction

The details in this section are taken from the Office of the Privacy Commissioner of Canada website – Guidelines for Overt Video Surveillance in the Private Sector and would be the minimum standard organizations would need to comply with. In general, any retention of personal information falls under the Personal Information Protection and Electronic Documents Act, (PIPEDA), or any Provincial privacy acts, so we recommend that each organization is familiar with the PIPEDA Act, as well as any provincial legislation regulations that might apply.

Information collected through video surveillance should only be used for the purpose that surveillance is being undertaken, or for purposes that are permitted by law or if required by law enforcement. For example, if cameras are installed in an apartment building parking garage for safety purposes, the information cannot be used to track the movements of tenants. However, if a car is broken into, the information can be disclosed to law enforcement.

Organizations should also ensure that the video surveillance complies with all applicable laws, in addition to privacy legislation. For example, an organization using a video camera that captures sound needs to consider the Criminal Code provisions dealing with the collection of private communications.

Recorded images must be stored in a secure location, and access should be granted only to a limited number of authorized individuals. Individuals have the right to access images relating to them. When disclosing recordings to individuals who appear in them, the organization must ensure that identifying information about any other individuals on the recording is not revealed. This can be done through technologies that mask identity. Any disclosure of video surveillance recordings outside the organization should be justified and documented.

Recordings should only be kept as long as necessary to fulfill the purpose of the video surveillance. Recordings no longer required should be destroyed. Organizations must ensure that the destruction is secure.

Reference and Resource Information and Links:

Guidelines for Overt Video Surveillance in the Private Sector:
https://www.priv.gc.ca/en/privacy-topics/surveillance-and-monitoring/gl_vs_080306/
Personal Information Protection and Electronic Documents Act (PIPEDA)
Alberta's Personal Information Protection Act (PIPA)
British Columbia's Personal Information Protection Act (PIPA)
Quebec's An Act Respecting the Protection of Personal Information in the Private Sector
In Ontario, FIPPA: https://www.ontario.ca/laws/statute/90f31 and MFIPPA: https://www.ontario.ca/laws/statute/90m56?search=Municipal+Freedom+of+Information set out rules for the collection, use and disclosure of personal information by institutions.
Guidelines for the Use of Video Surveillance – Information and Privacy Commissioner for Ontario:
https://www.ipc.on.ca/resource/guidelines-for-the-use-of-video-surveillance/

Section 11: Regulation Regarding Audio Recording

Introduction

Most audio recordings without consent of one or all parties are illegal. Recording audio is very different from video as there are definite federal and provincial laws prohibiting surreptitious recording and monitoring of audio conversations. Authorities take these laws seriously and failure to abide by them could result in severe consequences.

Canada's Legal Code

In Canada, the Criminal Code makes it illegal to wilfully (i.e., intentionally) intercept a private communication.

Section 184(1) reads: "Everyone who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years." There are saving provisions. Section 184(2) provides that subsection (1) does not apply to "a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it."

In Canada, it is not illegal to monitor or record sound, but it is illegal to monitor "private communications". If the originator has a reasonable expectation that his or her oral communication with the recipient will not be intercepted, then that oral communication is a private communication.

It should be noted however, that it is not illegal to intercept a private communication if you have the consent, express or implied, of the person who originated the private communication or of his or her intended recipient.

Express consent is obvious where the person announces that he or she consents to having their voice monitored or recorded.

Implied consent can be tricky. It must be inferred from the circumstances. For example, the person sees and reads the decal, notice or signage and continues to converse with someone else. Or the person is specifically informed that his or her conversations are being recorded or monitored and, notwithstanding, the person continues speaking to another. Commonly, one of the two, or more, persons involved in the oral communication is an employee, agent or subcontractor of the individual, business, institution or organization that is conducting the audio surveillance. That employee/agent/subcontractor can expressly consent, in advance, to the interception of his or her oral communication with the customer, client, guest, intruder or member of the public by signing an employment contract or subcontracting agreement, or a waiver containing the appropriate consent clause(s). The aforementioned situation would apply in the case of alarm monitoring companies that offer "two-way live voice communication" with operators at their central monitoring station. Once an alarm is triggered, the operators establish a live audio link with the monitored premises and then assess the emergency situation. In the case of an actual burglary or home invasion, the operators may even voice-threaten the intruder that the police have been notified.

Canada's Legal Code *(continued)*

Those intending to conduct audio surveillance should also be aware that federal and provincial privacy legislation (e.g. PIPEDA) may apply. Monitoring oral communications and the resulting audio/video recordings fall within the definitions of "personal information" (e.g., "information about an identifiable individual") and "record" (e.g. "sound recording, videotape"), respectively. PIPEDA and its substantially similar provincial counterparts (e.g., the Privacy Acts of British Columbia, Alberta and Quebec) require consent to the collection, use and disclosure of personal information in the course of commercial activities. Without consent, those conducting audio surveillance are at risk of being named in a complaint to the Federal (or Provincial) Privacy Commissioner. In addition, if information obtained through the monitoring or recording of private communications is disclosed to the media or "published" on the Internet, the originator or recipient may sue for invasion of privacy under provincial legislation or the common law.

Customer Audio Recording

Due to the legal code explained above, it is not recommended to provide an audio recording system to a customer, or "add audio" to video recording systems without a legal discussion. There are a number of nuances that need to be taken into account, for example, recording an open-air conversation between two people. In this scenario, there are legal issues that may arise when other people become subjected to open-air recording, and the use of this type of recorded information could open additional legal issues (employee rights, etc.).

Monitoring Station Use of Audio Recording

Unlike the recommendation NOT to provide audio recording at a customer premise (unless under specific circumstances), the use of telephone and radio audio recording for a monitoring station is HIGHLY recommended. It is important to have a record of what was said, and, in the security business, it is possible that it may be called upon as evidence in a court proceeding.

The statement from the previous page; "…if you have the consent, express or implied, of the person who originated the private communication or of his or her intended recipient…", can be applied to a telephone conversation in this way: An employee, (who must be aware that the telephone lines are being recorded) is the "originator" of an outgoing call, and the "recipient" of an incoming call. As such, with all employees aware that the telephone lines in use at the monitoring station are recorded, or subject to being recorded, then the legalities have been addressed.

It is important to note that there will be circumstances that will require a more specific approach. As an example, if a client or supplier is visiting your office, and asks to use your phone to make a call, you should notify him/her that the telephone lines are being recorded. It is recommended that you do so regardless of signage in place. Once the visitor uses the phone it is implied consent.

Conclusion

There may be a definite need to record audio in certain circumstances, but prior to the use of audio recording in any situation, consulting legal advice is the best first step.

For further information it is advised that you contact your local municipality or the provincial government to inquire about audio recording polices in your province.

References/Resources:

Office of the Information and Privacy Commissioner of Alberta
Office of the Privacy Commissioner of Canada
Office of the Information and Privacy Commissioner of British Columbia
Partnership for Priority Video Alarm Response - Audio Verified Alarms Best Practices
http://www.ppvar.org

Section 12: Residential Smoke and Heat Alarm Monitoring

Introduction

Fire doubles in size every minute, after the first 4 minutes, thus early notification of fire alarm signals to the fire department is crucial in mitigating the consequences of a fire. This is particularly true in newer residential units, which contain materials and design aspects (size of the home, open concept rooms, vaulted ceilings, etc.) that actually allow for faster fire propagation than in older residential counterparts (UL, 2012). For prompt fire department response, UL 2012 suggests a "conservative" estimate of alarm notification within 2 minutes from fire ignition.

NFPA guidelines state that from time of receipt of the emergency call, crews should arrive on site within 6 minutes (UL, 2012) for career fire departments and 11 to 16 minutes for volunteer departments (UL, 2012). The average US time for arrival on scene from time of ignition in 2012 was 10 minutes.

That said, residential installations can be more prone to false alarms than their commercial counterparts for reasons not limited to:

- Lack of regulation around installation, in terms of set-up, installer qualifications and installation location;
- Lack of regulation around regular inspection and maintenance;
- Changing variables within the home;
- User knowledge of systems and processes in place.

The following recommended best practices have been developed with these factors in mind, and are provided from the perspective of the monitoring company.

Recommended Best Practice

Fire Signals:

- Upon receipt of an alarm at the monitoring station, an attempt for verification is completed within 45 seconds;
- Should the call immediately go to voice mail or be "busy", it is acceptable for the monitoring station to re-try the verification process one time, so long as it does not fall outside of the 45 second verification time frame listed above;
- Unless provided with notice in writing from the local authority having jurisdiction, should the monitoring station not be able to verify directly with the home owner that the alarm is false, a call shall be placed for notification, without further verification, to the appropriate public service fire communication centre;
- Attempts to notify key holders of the alarm dispatch shall be made to the appropriate key holders within 5 minutes;
- In the event that the premise is contacted and a fire is confirmed:
  - The monitoring station operator shall advise the customer to immediately evacuate the premises and that the monitoring station shall notify the fire department. A call to the appropriate public service fire communication centre advising of a confirmed fire shall be made immediately.

Recommended Best Practice

Supervisory Alarms:

- Upon receipt of a supervisory-type alarm from a smoke or heat detector (all alarms not considered a 'fire alarm' including, but not limited to, low battery, wiring fault, general trouble, etc.) the monitoring station shall, within 5 minutes, begin notifying key holders of the situation and of potential resolutions;
- Should the alarm not be restored within 24 hours, follow-up calls shall be made each subsequent 24-hour period, unless notified in writing by the customer.

Other items:

Incidence of false alarms in residential fire monitoring can be significantly mitigated by the following actions taken by the installing company:

- Adhering to the manufacturer's installation instructions;
- Obtaining additional installation training from recognized training bodies (CANASA ATC, CFAA etc.);
- Scheduling annual inspections of the monitoring transmitter;
- Documenting records of equipment installation timeframes so expired equipment can be replaced;
- Training customers on system use.

Please note:

This best practice is not intended to apply to alarms which have a requirement to be monitored under a federally or provincially mandated code, which would (currently) fall under the requirements of CAN/ULC-S561.

When these types of systems are sold, the dispatch process should be clearly explained to the end-user, including all implications involving local fees for false alarms. It should also be emphasized to the end-user that a home fire escape plan should be developed in concert with the implementation of one of these systems, and that this system does not take the place of a home escape plan.

References/Resources:

NFPA 72 (2103) - National fire alarm and signalling code.

NFPA 1221 (2010) - Installation, maintenance, and use of emergency services communications systems.

NFPA 1710 (2010) - Organization and deployment of fire suppression operations, emergency medical operations, and special operations to the public by career fire departments.

UL (2012) - Analysis of Changing Residential Fire Dynamics and Its Implications on Firefighter Operational Timeframes. Northbrook, IL: Stephen Kerber.

Section 13: Carbon Monoxide Supervising Station Response Standard

Introduction

Like fire, an alarm generated from a carbon monoxide detector is potentially life threatening. However, whereas fire can be very apparent, the opposite is true for carbon monoxide: it is colourless and odourless (CDC, 2014), meaning that alarms received from these devices should be treated seriously and the customer should be educated as to the risk factors and implications of alarm by the installing company when these devices are installed. As false alarms from these devices are relatively rare, in comparison with other devices, we do not recommend any delay being set on these devices for alarm transmission. Build-up of carbon monoxide can reach dangerous to fatal levels in minutes (CDC, 1996), thus time is of the essence in reacting to these alarms.

The following best practice guidelines outline procedures to be taken by a supervising station in the event of the receipt of a carbon monoxide alarm at the protected premises, for either residential or commercial installations.

Recommended Best Practices

For the purpose of this document, NFPA 720 Standard for the Installation of Carbon Monoxide (CO) Detection and Warning Equipment is recommended. An abridged version follows and full reference to this standard can be found at http://www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=720

The installation, testing and maintenance of a Carbon Monoxide alarm system shall be in accordance with NFPA 720 Standard for the Installation of Carbon Monoxide (CO) Detection and Warning Equipment.

The Supervising Station response procedure shall be in accordance with NFPA 720 Standard for the Installation of Carbon Monoxide (CO) Detection and Warning Equipment and this standard.

Supervising Station Procedure

Unless otherwise required by the emergency response agency (organizations providing law enforcement, emergency medical, fire, rescue, communications, and related support services), upon receipt at the supervising station of a CO alarm signal, with or without a restored signal, the supervising station shall first call the premises and then proceed as outlined below.

If someone answers the telephone:

The occupants shall be instructed to leave the premises and move to fresh air. The supervising station shall ask the following questions of the individual answering the telephone:
a) Are all the occupants accounted for and are they out of the premises?
b) Is anyone nauseous, ill, have a headache or dizzy?

The supervising station shall instruct the occupants not to re-enter the premises until cleared by the responding fire service.

The supervising station shall then immediately call the appropriate emergency response agency to inform them of the alarm. The emergency response agency shall be informed that the occupants answered the telephone, were told to leave the premises and of any reported symptoms.

Recommended Best Practice

If no one answers the telephone:

The supervising station shall then immediately call the appropriate emergency response agency and report that a CO alarm was received from a particular premise and it was unable to reach an occupant.

If no one answers the telephone after dispatch, the supervising station shall contact the responsible party(s) in accordance with the notification plan.

If an answering machine or voicemail is encountered:

The supervising station shall leave a message including the date, time and alarm event and instruct that all occupants evacuate the building.

The supervising station shall then immediately call the appropriate emergency response agency and report that a CO alarm was received from a particular premise and it was unable to reach an occupant.

Premises Access

All buildings with a CO system or detector monitored at a supervising station shall be equipped with a means of providing emergency access to all areas of the premises as required by the authority having jurisdiction.

References/Resources:

Central Station Alarm Association: Carbon Monoxide Supervising Station Response Standard - ANSI/CSAA CS-CO-01-2008

NFPA 720 Standard for the Installation of Carbon Monoxide (CO) Detection and Warning Equipment, 2009 Edition

NFPA 720 Standard for the Installation of Carbon Monoxide (CO) Detection and Warning Equipment.
www.nfpa.org/codes-and-standards/document-information-pages?mode=code&code=720

Section 14: Global Positioning Systems (GPS)

Introduction

GPS: A system of earth-orbiting satellites, transmitting signals continuously towards the earth, that enables the position of a receiving device on or near the earth's surface to be accurately estimated from the difference in arrival times of the signals GPS.

GPS technology has been around for many years, but it is in its infancy stage for people tracking. As the technology has just begun to be used within the industry outside of traditional mobile tracking applications, manufacturers are in the early stages of implementing GPS hardware to track mobile individuals. Examples: Patient wandering, Special Needs children. This brings a new set of issues and challenges to the monitoring station regarding notification process.

The security industry needs to come to a consensus about how these events will be tracked and dispatched. There is currently no agreement with authorities to respond to these types of situations. In addition, there is no Canadian registry or map overlay for the monitoring community to use that would allow a mobile system to be dispatched on. As a result, there is a need for a framework that will work for the client, authorities, and monitoring stations. There are also privacy issues that need to be addressed to ensure that client rights are adhered to.

General Requirement of GPS Use (Employer)

1. Any forum of data collection must be rationalized and within reason.
2. Only personal information deemed necessary for operational purpose should be collected.
3. The organization is responsible for protecting any personal information they collect.
4. Individuals have the right to access their own personal information and request revisions as deemed necessary.

General Requirement of GPS Use (Business, NGO, Associations)

1. Any forum of data collection must be rationalized and within reason.
2. The employer is responsible for limiting the amount of data collected to the purposes identified (corporate policy).
3. Privacy and security (data collection) should be balanced and never compromise each other.
4. Data collection used for employee management and discipline should be established and communicated prior to the use of GPS.
5. GPS should not be used to routinely gauge employee performance.
6. It is recommended that the company establish a GPS policy to clearly define terms and conditions.
7. The GPS policy should be communicated to all employees and managers who control or use the system. This communication process then ensures that privacy obligations and appropriate usage of information guidelines are established.

At present, the Federal Government has not established a legislative framework to standardize the use of GPS systems. Before establishing a national model (incorporating GPS usage), the Federal Government requires more research related to distracted driving. In other words, before GPS can be legalized, the issues associated with distracted driving need to be resolved. Currently the Federal Government is in agreement with vehicle manufacturers through a Memorandum

of Understanding to abide by voluntary safety standards. Since newer vehicles appear to be moving into more autonomous functionality, it is likely that the lack of a national standard will be short-lived. Some provinces have taken initiatives to legislate GPS use through distracted driving Laws.

With respect to the issues of privacy, Privacy Commissioner, Jennifer Stoddart provided a brief overview of the use of GPS at the 2010 Association of Labour Relations Agencies Annual Conference:

"…In 2006, my Office investigated a case in which several workers complained that their employer, a telecommunications company, was using GPS to improperly collect information about their movements while on the job.

In our findings, we noted that using GPS to track the location of a vehicle might not be overly privacy invasive. Routinely evaluating worker performance based on assumptions drawn from GPS data, however, can be.

We felt that employers should not use GPS to constantly monitor their workers. If it is used as a surveillance tool, employers need to be clear on when, why and how, and communicate this to staff beforehand.

We recommended that the company draw up a detailed policy on its use of GPS in managing employees."

The company also committed to training its managers on the appropriate use of GPS data.

For Monitoring Stations that use GPS for Lone Worker

The Criminal Code holds liability on organizations and representatives responsible for any act of negligence, which can include directors, partners, members, agents and contractors as well as employees. It is strongly recommended that monitoring stations collaborate with third party service that provides non – core policing services, in circumstances where traditional authorities do not respond.

For Monitoring Stations that use GPS for Fleet Vehicles

The Privacy Commissioner of Canada accepts the usage of GPS for safety, efficiency and productivity, but deems the frequent monitoring of employee performance as unacceptable. Monitoring stations may want to consider establishing guidelines of what they will and will not monitor for GPS. It is also strongly recommended that monitoring stations collaborate with third party service that provides non – core policing services, in circumstances where traditional authorities do not respond.

References/Resources:

Collins English Dictionary, 2012

Canadian Centre of Occupational Health and Safety:
http://www.ccohs.ca/oshanswers/information/govt.html
http://www.ccohs.ca/oshanswers/hsprograms/workingalone.html

Underwriters Laboratories, 2013, P. 184
Underwriters Laboratories. 2013. Guide Information For Canadian Certified Equipment The Canadian White Book 2013. (Catalog No. N/A) Underwriters Laboratories: Global Entity. Accessed July 18, 2014

CBC. 2010. "No Regulations for GPS Use Despite Safety Risk." CBC News. Jan. 31. Accessed July 21, 2013. http://www.cbc.ca/news/no-regulations-for-gps-use-despite-safety-risk-1.933654

Collins English Dictionary. 2012. Complete Unabridged 2012 Digital Edition. © HarperCollins Publishers. <Dictionary.com>. Accessed August 26, 2014. http://dictionary.reference.com/browse/global%20positioning%20system

Stoddart, Jennifer. 2010. New Technologies and the Protection of Privacy. (N/A). Ottawa, Ontario: Remarks at the Association of Labour Relations Agencies Annual Conference. Accessed August 15, 2014. www.priv.gc.ca/media/sp-d/2010/sp-d_20100726_e.asp

Transport Canada. 2003. Strategies for Reducing Driver Distraction from In-Vehicle Telematics Devices: A Discussion Document. (Cat. No. TP 14133 E). Ottawa, Ontario: Standards Research and Development Branch & Road Safety and Motor Vehicle Regulations Directorate. Accessed July 21, 2014.
https://www.tc.gc.ca/media/documents/roadsafety/tp14409e-tp14409.pdf

Section 15: Lone Worker Guidelines

Introduction

In March 2004, the Canadian Federal Government included provisions to the Criminal Code holding employers liable for failing to enact lone worker safety measures. Though each province enacts different regulatory frameworks, these general lone worker guidelines apply:

1) A point of contact between the employer and the employee (via device)
2) A Lone Worker Strategy (documentation)
3) Risk Assessments (incidence report and or annual evaluations)
4) Training & Information (employee and employer)
5) Alleviation of isolated work conditions (buddy system, don't work alone).

Some jurisdictions have designed checklists and assessment guides to help employers design a lone worker protocol. Please note, some provinces are in partnership with Non-Government Organizations, and therefore may require verification and/or approval to enact a corporate lone worker policy. For general information on Lone Worker Policy by province, please refer to the reference guide below:

Lone Worker Resources

Province	General Contact Information
British Columbia	
Work Safe BC	1-888-621-7233
Alberta	
Government of Alberta Employment and Immigration	1-866-415-8690
Workers' Compensation Board (Alberta)	
• Edmonton	1-780-498-3999
• Calgary	1-403-517-6000
• Toll Free	1-866-922-9221
Workplace Health and Safety Contact Centre	1-866-415-8690
Saskatchewan	
Government of Saskatchewan	
Department of Labour Relations and Workplace Safety	
• Occupational Health and Safety Division	1-800-567-7233
• Saskatchewan Workers' Compensation Board	1-800-667-7590
Manitoba	
Manitoba Labour and Immigration Workplace Safety and Health	1-866-626-4862
The Workers Compensation Board of Manitoba (crown corporation)	1-204-954-4321
Manitoba Workplace Health and Safety	1-204-957-SAFE (7233)
	1-204-726-6361

Section 15: Lone Worker Guidelines (continued)

Province	General Contact Information
Ontario	
Public Service Health and Safety Association	1-877-250-7444
Infrastructure Health and Safety Association	1-905-212-7933
Safe Workplace Promotion Services Ontario	1-888-478-6772
Workplace Safety North	1-705-474-7233
Workers Health and Safety Centre (WHSC)	1-416-441-1939
The Workplace Safety and Insurance Board	1-800-387-0750
Quebec	
Commission de la santé et de la sécurité du travail du Quebec (Occupational Health and Safety Commission)	1-866-302-CSST (2778)
New Brunswick	
Government of New Brunswick	
• Department of Human Resources	1-506-453-2264
• Work Safe New Brunswick (crown corporation)	1-800-222-9775
Nova Scotia	
Ministry of Labour and Advanced Education	1-800-670-4357
Workers' Compensation Board of Nova Scotia	
• Halifax	1-800-870-3331
• Sydney	1-800-880-0003
Prince Edward Island	
Government of PEI	
• Department of Labour and Justice	1-800-333-4362
• Workers Compensation Board of PEI	1-866-460-3074
Newfoundland & Labrador	
Government of Newfoundland and Labrador	
• Department of the Human Resource Secretariat	1-709-729-2476
Nunavut & Northwest & Yukon Territories	
Workers' Safety & Compensation Commission	1-867-979-8500

Section 15: Lone Worker Guidelines (continued)

Province	Work Safety Web Resources/Training
British Columbia	
Working Alone A Handbook for Small Business	www.worksafebc.com/en/health-safety/hazards-exposures/working-alone
OH&S Training Providers	http://www.ohstrainingbc.com/
Work Safe BC - Safety at Work	https://www.worksafebc.com/en/health-safety/education-training-certification
Work Safe BC - Work Safe Magazine	https://www.worksafebc.com/en/about-us/news-events/worksafe-magazine
Alberta	
Alberta Human Services	http://humanservices.alberta.ca/working-in-alberta/268.html
Working Alone Safely: A Guide for Employers and Employees	http://www.work.alberta.ca/documents/WHS-PUB_workingalone.pdf
Workplace Health and Safety Bulletin (Working Alone)	http://work.alberta.ca/documents/WHS-PUB_wa001.pdf
Workplace Health and Safety Bulletin (Reporting Injuries and Incidents)	http://work.alberta.ca/occupational-health-safety/report-an-incident.html
Alberta Human Services - Occupational Health & Safety Magazine	http://work.alberta.ca/occupational-health-safety/resources.html
Quebec	
Commission de la santé et de la sécurité du travail du Québec	http://www.cnesst.gouv.qc.ca/Pages/accueil.aspx

Section 16: Security Employee Education and Training Resources

Introduction

Training and education are the building blocks of any successful career in any industry. Although opportunities can be found via many channels, we have compiled a list below of some educational/training courses or sites that have relevant information.

TMA Central Station Operator Level 1 – Online

The Central Station Operators course teaches employees the skills and knowledge that is crucial for taking a call. Trainees are presented with policies and procedures to assist in handling the wide variety of situations they will face as station operators; and are given the chance to test their knowledge at every level of the content. Student results are measured and tracked in a state-of-the-art learning management system that includes a full transcript for employer evaluation.

Operational Course Overview:

- The Role of the Central Station Operator
- Alarm Verification
- Communication Equipment
- Telephone and Radio Skills
- Underwriter's Laboratories/FM Approvals
- Emergency Procedures

http://www.csaaintl.org/education/operator-online/

TMA Central Station Operator Level 2 - Online

Modules include subject matter such as communications paths, alarm receiver formats, dealing with difficult customer situations, enhanced customer service skills and managing false alarms:

- Module 1. Dealing with Difficult Customer Situations – Specific tactics for dealing with customers who are irate, scared, confused, or experiencing any type of extreme emotion; and for controlling a conversation without appearing abrupt.
- Module 2. Enhanced Customer Service Skills – A review of the customer's experience with the station and overall impression that could impact the entire company. This module focuses on how to improve listening skills to enhance the customer's experience.
- Module 3. Specialty Alarms – A review of the various signal/event types that merit a response by the station. Various specialty activation descriptions are reviewed and background on equipment used in these applications is provided.
- Module 4. Receiver Formats – Understanding how to interpret a received printout is not only necessary in the event of a system failure, but can be of equal value when troubleshooting a field services problem. This module discusses various receiver formats and how they report.
- Module 5. Communication Paths – Discussion about the various traditional communications paths (T1, radio or POTS), as well as some basics on IP technology and new communications challenges/opportunities facing the security industry.
- Module 6. Managing False Dispatches – This module helps operators understand the false alarm problem and what can be done to assist the company in identifying problems and solutions.

http://www.csaaintl.org/education/operator-online-level-ii/

TMA False Alarm Online Training

An exclusive online course dedicated to educating users about the dangers of false alarms and the solutions to prevent them. Encourage your customers, employees and local agencies to take this online course.

http://www.csaaintl.org/education/false-alarm/alarm-company/

SIA Central Station Operators Course ("Train the Trainer")

Newly revised in 2011, the Operator Course can introduce new employees to a station or serve as an effective refresher for experienced operators. This is a 40-hour course and concludes with SIA's certification test.

http://thecsu.org/

ULC's Fire and Security Alarm System Certificate Programs

ULC's Fire and Security Alarm System certificate programs provide Authorities Having Jurisdiction (AHJs), Insurance Companies, and Municipalities/Governments with a convenient, reliable way to identify code complying fire alarms and security systems. These programs take the widely recognized ULC mark and place it on an installed system in the form of a certificate. A variety of AHJs, government bodies and insurers across Canada have found these programs to be a great benefit when assessing risk and determining ongoing code compliance. Programs include:

- Burglar alarm installation and monitoring – commercial, financial and residential
- Protective signalling systems (sprinkler and fire panels)
- Fire alarm testing and inspection
- Alarm response (guard) service
- Station automation software

http://canada.ul.com/ulcprograms/fireandsecurityalarmcertificateprograms/

CANASA Alarm Technician Course - Online

This course is ideal for all alarm installers currently active in the industry. The participant should have programming knowledge of all control panel types and have independently installed at least one system. ATC covers a wide range of topics and trends relevant to today's alarm technician and current industry requirements, including new technologies such as networking, and wireless and extensive false alarm prevention. Designed by top security experts, the course promotes best practices and the highest possible standards in the industry. Course content has recently been updated and now covers:

- Controls
- Detection (inputs)
- Notification/communication (outputs)
- Basic networking
- System design
- Job planning
- Field wiring
- Power and grounding
- Wireless
- Safety
- Metering
- False alarm management
- Commissioning

www.canasa.org

SIA's Certified Security Project Manager (CSPM®) Credential

A Certified Security Project Manager (CSPM®) is a professional experienced in managing a security project, which typically entails installing and integrating various components of a security system into a physical building structure. In order to become certified, you must take a 2-hour examination that covers the following domains:

- Security Industry-Specific Knowledge and Initiation
- Planning
- Execution
- Monitoring
- Project Closing
- Management Skills

To be eligible for the CSPM® examination, a candidate must have a minimum of 6,000 hours (about three years) of hands-on project management experience, of which a minimum of 3,000 hours must have been in direct security project management experience.

www.siaonline.org/Pages/Certification/CSPM-Certification.aspx

CANASA's False Alarm By-law Repository

CANASA's False Alarm By-law Repository includes a summary of false alarm by-laws, registration requirements and fees across Canada. Accessible and free-of-charge to all CANASA Members, this is an easily searchable, online library of by-law information.

Visit www.canasa.org. Login and select the "Members Only" button on the left sidebar, then select "False Alarm Repositories" under the heading "Repositories".