GSM Wireless Security and Fire Alarm Control Panel "Lun-25"

User Manual

ortus
ORTUS Group

Table of contents

1 Quick reference

The "Lun-25" Control Panel can includes a different Indication and Control Devices (ICD) for security management as described in Section 2. TouchMemory key readers and RFID-card readers can indicate zones state, system faults and can system arming/disarming. When using a keypads, the Control Panel additionally uses shortcut keys to access most options or features.

NOTES: Some features must be enabled by installer.

[*] – If configured by installer.

Lun-25T or Lun-25E (built-in TouchMemory or RFID-card reader), **Lind-EM** (additional RFID-card reader)

Status Light	
Green	Group #1 is **disarmed** and **ready to arm**
off	Group #1 is **disarmed**, some **zones are violated**
Flashes yellow every 3 seconds	Group #1 is **disarmed**, with some **system faults**
Flashes red every second	Group #1 is **armed**, arming event is sending to CMS
Red	Group #1 is **armed, no system faults**
Red with **yellow flashes** every 3 seconds	Group #1 is **armed,** with **some system faults**
Flashing red N times while try to arm	N = 1...5 – **zone** number N **is violated**, arming impossible N = 6 – **arming disabled** by Central Monitoring Station (CMS)

Lun-25TE (built-in TouchMemory + RFID reader) **/** "Lind-11TM", "Lind-7" (additional TouchMemory readers)

Status Lights		Faults display while the TROUBLE hold	
ZONE 1...10 / ZONE 1...8	**Red** – zone is violated, **Yellow** – zone is faulty / Red – zone is violated or faulty	ZONE1	**AC power** lost
		ZONE2	**Battery** absence/fault/discharge
AC POWER / AC 220V	Green, if AC power is present	ZONE3	**CMS** connection lost
	Off, if AC power is absent	ZONE4	**AM-11** connection lost
BATTERY / BATTERY	Green, if battery is charged	ZONE5	**Arming disabled** (from CMS)
	Off, if the battery is absent or discharged	ZONE6	**Radio receiver** connection lost
WIRELESS / –	Green, if radio system is normal or switched off	ZONE7	**WiFi module** connection lost (Lun-25TE only)
	Off, if radio system is failed		
SYSTEM / SYSTEM	_Blinking every 2 seconds_, if **no system faults**		
	Blinking twice per second, if some system faults		

"Lind-9M3" (additional keypad)

Status Lights			
READY	On indicates group ready to arm	POWER 220V	On indicate AC power fault
POWER	On indicates keypad works normal	BATTERY	On indicate battery fault
FIRE	On indicates "Fire" alarm state	CP CONNECTION	On indicate CP connection fault
ARMED	On indicates group is armed	CMS CONNECTION	On indicate CMS connection fault
ACCESS LEVEL	Flashes for admin or fire access	MODE 0	On for wireless sensors bind mode
ZONE 1...16	On for violated, flash for zone fault	MODE 1	On for admin/fire codes manage
MUTED	On if sound for faults disabled	MODE 2	On for under duress manage mode
INPUT	On if the code partially entered	MODE 1 + MODE 2	On for users codes manage mode
FAULT	On indicates some system faults	BYPASS	On indicate bypass zones mode

Faults Lights (displayed while Hold ⊛)			
ZONE 1	**AC power** lost	ZONE 9	Arming disable by CMS command
ZONE 2	**Battery** absence/fault/discharge	ZONE 10	**CMS** connection lost
ZONE 4	**Lind-11TM** connection lost	ZONE 11	**Radio receiver** connection lost
ZONE 5	**AM-11** connection lost	ZONE 15	**WiFi module** connection lost
ZONE 6	**Lind-9M3** connection lost	ZONE 16	GPRS/GSM **signal jamming**

Function Keys			
(*)	ENTER, confirm	🔔̸	FAULT – display faults while hold or MUTE – sound for faults off (as #+MUTE)
(#)	CANCEL, discard, exit to normal mode	📶	SIGNAL LEVEL of GPRS/WiFi while hold or FIRE RESET (*see below*)
🔇	STAY HOME (press before entering the code)	☀	TEST INDIC. – test LEDs/buzzer while hold or BACKLIGHT on/off (as #+BACKLIGHT)

Action	Keys (+ for press and hold first key then press second then release both)	Section
Arming and Disarming		
Arm	Enter 4 digit user "normal" code	3.2.1
Arm in Stay Home mode	🔇 , then enter 4 digit user "normal" code, **STAY HOME** LED lights up	3.2.2
Disarm	Enter 4 digit user "normal" code	3.9
Disarm under duress	Enter 4 digit user "under duress" code	3.9
Bypassing	(#) + (8) , *admin code* to enter bypassing mode, **BYPASS** LED lights up	
Bypass zone on/off	Enter zone number **01...16**, ZONE LED lights up if zone bypassed	3.7
Fire subsystem commands	(#) + (5) , *fire code* to enter this mode, **ACCESS LEVEL** LED lights up	
Fire state reset	📶	4.3
Fire siren off	🔔̸	4.2.1
Fire siren on	🔇	4.2.1
Management Functions		
Normal codes manage	(#) + (3) , *admin code* to enter this mode, **MODE 1** lights up	6.1.1
Under duress codes manage	(#) + (4) , *admin code* to enter this mode, **MODE 2** lights up	6.1.1
User keys management	(#) + (6) , *admin code* to enter, **MODE 1** and **MODE 2** lights up	6.1.1
Group Functions		
Select group*	(*) , *group number*, (*)	8.2
View current group number	Hold (#) + (9)	8.2.1
View groups arm state	Hold (#) + (2)	8.2.2
Common Functions		
View system faults	Hold 🔔̸	7
View GPRS/WiFi signal level	Hold 📶	9.1.1
Test LEDs and buzzer	Hold ☀	9.1.2
Keypad hardware version	Hold (#) + (0)	9.1.4
Sound for faults off/on	(#) + 🔔̸ . If sound off, **MUTED** LED lights up. New fault turns on sound	7.1.1
Backlight on/off	(#) + ☀ . If on, all key LEDs flash once, else – flash twice	9.1.3

2 About your Security System

2.1 The Lun-25 Control Panel

Your Lun-25 has been designed to provide you with the most comfort and flexibility. Read this manual carefully and have the installer inform you on how to use your system and which features have been switched on in your Control Panel. Fill out Section 13 information with your access codes and zone information, then store this manual in a safe place.

2.2 General Control Panel Operation

Your Security System consists of a Control Panel Lun-25, various sensors (wired or wireless) and may contain one or two external Indication and Control Devices (ICD). If the ICD used in your Security System, the Control Panel is mounted out of the way (as a utility closet). The Control Panel housing contains the main PCB, fuses and standby battery. Depending of the model, the Control Panel front can contained built-in TouchMemory key reader or RFID-cards reader.

Every ICD have a sound buzzer, zone and system status lights. Every ICD is used for group arming/disarming and display alarms and system faults. ICD is mounted in convenient place near the entry/exit door.

Your Security System has some zones of space protection and each of them is linked to one (or more) sensors. Every sensor violation is displayed by the corresponding zone LED lit.

NOTE: Only the Security Company installer/engineer shall have access to the Control Panel.

2.3 Fire Detection

Your Control Panel can to monitor a fire detectors and provide a fire state warning. Quality fire detection depends of the fire sensors quantity and its placement. If you planned to use this features, the Control Panel should be installed in accordance with NFPA 72 (N.F.P.A., Batterymarch Park, Quinsey MA 02269).

NOTE: Must be enabled and configured by installer.

2.4 Testing your external ICD and System

WARNING:

- To ensure that your external ICD works properly, you must test it weekly.
- If any ICD test failed, you should contact your Security Company immediately.
- All smoke detectors must be tested by your installer once per year to ensure proper operation.

To perform an external "Lind-11TM"/"Lind-7" ICD Test

Press and hold **RESET** key. The ICD buzzer and all LEDs will be activated. If all LEDs is lit and you hear the sound tone – the test was successful. To go back – release the key.

To perform an external "Lind-9M3" ICD Test

Press and hold ⊛ key. The ICD buzzer and all LEDs will be activated. If all LEDs is lit and you hear the sound tone – the test was successful. To go back – release the key.

2.5 Monitoring

Your Security System can transmit security events, faults and alarms to the Central Monitoring Station (CMS) depends of the operating mode selected by installer. If you turn on the alarm by mistake, immediately call to CMS to prevent an unwanted response.

NOTE: The CMS mode must be configured by installer.

2.6 Maintenance

With normal use, your Control Panel requires minimum maintenance. Remember the next:
- Do not wash any equipment with a wet cloth. The slightly moistened cloth should be used for regular dust removal.
- The standby battery should be replaced every 1-2 years.
- For the third party equipment, as a sensors, TouchMemory keys, RFID tags and others, read the manufacturer's guides for any testing and maintenance information.

3 Securing the House

All your premises may be divided by 2 independent groups (partitions) by security reasons. Every group can arming/disarming independently.

The Security System provides the two arming modes:

Away arming   It uses when all leaved the house. In this mode activates all perimeter and interior sensors.

Stay Home   This mode uses when anyone are staying home and someone may use the entrance door later. In this case some interior sensors are still deactivated but all perimeter sensors will be armed.

NOTE: The Stay Home mode may be enabled and configured by installer.

Depending on your system configuration, you can use the next methods to arm Control Panel group:

- By keypad code;
- By TouchMemory key or a RFID card;
- By wireless key fob;
- By the arming switch.
- By the phone call (only phone numbers configured by your installer will be permitted to contact your system).
- By the iOS or Android application command.

3.1 Group Arming with the TouchMemory or RFID card readers

Away arming current group with the TouchMemory or RFID card readers:

1. Ensure all windows and doors are closed.
2. Check all **ZONE** LEDs on the reader face are off. If the reader is installed in the optical sensor zone detection, you shall stop and stand still until the sensor returns to the normal state.
   If your system is equipped with the built-in reader, its LED will be **lit green** for all zones closed. If this LED is off, then some zones are violated or faulted. And it's yellow flashing every 3 second if there are some system faults.
3. Touch to Touch Memory key reader port with the authorized key or bring your RFID-card closer to RFID reader.
4. If the arming process started successfully, then:
   - The **ARMED** LED and remote LED will be flashing up to the arming event sent to CMS;
   - Exit Delay timer countdown begins;
   - Reader's buzzer begins beeping once per second up to Exit Delay timer expired.
5. Immediately after the **ARMED** LED starts flashing, you should leave the facility through the entrance door (until the Exit Delay expires).
6. To cancel the arming process, touch to Touch Memory key reader or bring your RFID-card again. The **ARMED** LED will be turned off immediately.
7. Once the Exit Delay timer expires, the group is armed; the reader beeps stops and **ARMED** LED and remote LED remain on (lit red).

Stay Home arming current group with the TouchMemory or RFID card readers:

All steps are the same to Away arming **excluding the step 5** – do not open any door for Stay Home Arm.

NOTES: Build-in reader arms a group (partition) to which key is assigned.

The built-in reader's LED assigned to the **first Control Panel's group** only.

3.2 Group Arming with the Keypad Lind-9M3

3.2.1 Away Arming

Away arming current group with the Keypad:

8. Ensure all windows and doors are closed.

9. Check the current group number the keypad assigned to by press and hold (#) + (9);

10. You can switch the group you need by press (*), **_group number_**, (*), if this provided by your System configuration;

NOTE: If the keypad is configured to assign to one group only, then the steps 2 and 3 can be skipped.

11. Check all **ZONE** LEDs on keypad are off and the **READY** LED is lit. If the Keypad is installed in the optical sensor zone detection, you shall stop and stand still until the sensor returns to the normal state.
12. To group Away Arm, enter the 4-digits "normal" user's code.
13. If the arming process started successfully, then:
    • The **ARMED** LED and remote LED will be flashing up to the arming event sent to CMS;
    • Exit Delay timer countdown begins;
    • Keypad buzzer begins beeping once per second up to Exit Delay timer expired.
14. Immediately after the **ARMED** LED starts flashing, you should leave the facility through the entrance door (until the Exit Delay expires).
15. To cancel the arming process, enter the 4-digits "normal" user's code. The **ARMED** LED will be turned off immediately.
16. Once the Exit Delay timer expires, the group is armed; the Keypad beeps stops and **ARMED** LED and remote LED remain on.

NOTE: The Exit Delay timer interval configured by installer.

3.2.2 Stay Home Arming

Stay Home arming current group with the Keypad:

1. Ensure all windows and doors are closed.

2. Check the current group number the keypad assigned to by press and hold (#) + (9);

3. You can switch the group you need by press (*), **_group number_**, (*), if this provided by your System configuration;

NOTE: If the keypad is configured to assign to one group only, then the steps 2 and 3 can be skipped.

4. Check all **ZONE** LEDs on keypad are off and the **READY** LED is lit. If the Keypad is installed in the optical sensor zone detection, you shall stop and stand still until the sensor returns to the normal state.

5. To group Stay Home Arm, press the (⌀), then enter the 4-digits "normal" user's code.
6. If the arming process started successfully, then:
    • The **ARMED** LED and remote LED will be flashing up to the arming event sent to CMS;
    • Exit Delay timer countdown begins;
    • Keypad buzzer begins beeping once per second up to Exit Delay timer expired.
7. To cancel the arming process, enter the 4-digits "normal" user's code. The **ARMED** LED will be turned off immediately.
8. Once the Exit Delay timer expires, the group is armed; the Keypad beeps stops and **ARMED** LED and remote LED remain on.

3.3 Group Arming with the wireless key fob

To arming current group with the wireless key fob:

Press the desired Arming mode button any time the **READY** LED is on and all **ZONE** LEDs are off.
If the group arming is started, then:
- The **ARMED** LED and remote LED will be flashing up to the arming event sent to CMS;
- Exit Delay timer countdown begins;
- One short siren squawk will hear as an arming confirmation sound.

Once the Exit Delay timer expires, the group is armed; the sound beeps stops and **ARMED** LED and remote LED remain on.

NOTE: Siren confirmation sound may be enabled by installer.

3.4 Group Arming with the arming switch

To arming current group with the arming switch:

Turn the switch on any time the **READY** LED is on and all **ZONE** LEDs are off.
If the group armed, then **ARMED** LED and remote LED light on immediately.

NOTE: This function must be configured by installer.

3.5 Group Arming by the phone call

To group arming by the phone call:

1. Call the number of Control Panel.
2. Enter the next sequence on your phone keypad:

   [*group_number*] $\boxed{*}$ [*command*] $\boxed{\#}$

   As a [*command*] you can use:

   $\boxed{1}$ – for Away Arming.

Available answers:	**long** beep	– Done.
	5 short beeps	– Rejected.

   $\boxed{3}$ – for Arming state request.

Available answers:	**1 tone** beep	– Armed.
	2 tone beeps	– Disarmed.

   $\boxed{8}$ – for Stay Home Arming.
3. Enter another arming sequence or ends a call.

If the group armed, then **ARMED** LED and remote LED light on immediately.

NOTE: This function may be enabled and configured by installer.

3.6 Group Arming by the iOS or Android application command

To group arming by the iOS or Android application command:

1. Open the application "Mobile Keyboard" in your smartphone.
2. Log in to the application if this is required by application settings.
3. Select object (facility) number and group number you need.
4. Use the menu item **Commands**, then

Arm	for Away Arming or
Arm (Stay at home)	for Stay Home Arming.

If the group armed, then **ARMED** LED and remote LED light on immediately.

NOTE: This function may be enabled and configured by installer.

3.7 Bypassing Zones

WARNING: If a zone is not operating properly contact your service engineer immediately.

Bypassing zones intentionally unprotects specified zones the next time your group is armed.

NOTE: You can bypass zones by keypad **Lind-9M3** only.

Remember about zones bypassed:
- They must be configured before the group arming.
- Can be done using a keypad only.
- Reduce the facility's security level while the group is armed.
- Allow group arming if a zone is temporarily out of service.
- Will be automatically canceled when the group is disarmed.

To bypass zones by keypad Lind-9M3:

1. Press (#) + (8) , *admin password* to enter bypassing mode, then **BYPASS** LED lights up.
2. Enter 2 digits zone number **01...16** to bypass, then corresponding **ZONE** LED will be lit if zone bypassed. You can switch off zone bypassing mode by entering the same zone number.

3.8 Arming Errors and Exit Faults

The Control Panel notifies you by buzzer beeps of any errors when you are attempting to group arm.

3.8.1 Arming Errors

You will hear a long beep and the remote LED will flash quickly several times if the group can not be armed. Number of flashes corresponds to the number of zone violated (up to 5). Arming errors occur if:
- Group is not ready to arm (i.e. any zone violated).
- An unregistered key/card is used or incorrect user code is entered.
- Arming disabled by CMS command.

To Correct an Arming Error

1. Ensure all group sensors are restored. You can see the **ZONE** status LEDs on the most ICD's face plate. All **ZONE** LEDs should be off.
2. Try group arming again as described earlier.
3. If errors persist contact your Security Company.

3.9 Group Disarming

Depending on your system configuration, you can use the next methods to disarm Control Panel group:

- By keypad code
- By TouchMemory key or a RFID card
- By wireless key fob
- By the arming switch
- By the cell phone call (only phone numbers configured by your installer will be permitted to contact your system)
- By the iOS or Android application command.

To Group Disarm with a Keypad

1. Check the current group number the keypad assigned to by press and hold (#)+(9);

2. You can switch the group you need by press (*), **group number**, (*), if this provided by your System configuration;

NOTE: If the keypad is configured to assign to one group only, then the steps 1 and 2 can be skipped.

3. If you walk through the entry door the keypad will beep to indicate an Entry Delay starts.
4. Enter your 4-digit **"normal" access code** until this delay has expired.
5. If the group disarmed successfully, then:
   - The **ARMED** LED and remote LED will turn off;
   - Entry Delay timer countdown stops;
   - Reader's buzzer beep stops with the confirmation "thrill".

To Group Disarm Under Duress with a Keypad

You should use the **"under duress" access code** at the step 4 as described above.

WARNING: If you will use the "under duress" code, the alarm event will sent to CMS at the same time the group disarmed.

To Group Disarm by TouchMemory key or a RFID card

1. Touch to Touch Memory key reader port with the authorized key or bring your RFID-card closer to RFID reader.
2. If the group disarmed successfully, then:
   - The **ARMED** LED and remote LED will turn off;
   - Entry Delay timer countdown stops;
   - Reader's buzzer beep stops with the confirmation "thrill".

NOTES: Build-in reader disarms a group (partition) to which key is assigned.
The built-in reader's LED assigned to the **first Control Panel's group** only.

To Group Disarm by the phone call

1. Call the number of Control Panel.
2. Enter the next sequence on your phone keypad:

   [**group_number**] | ✶ | [**command**] | # |

   As a [**command**] you can use:

   | 2 | – for Group Disarming.

   Available answers: **long** beep – Done.
   5 short beeps – Rejected.

   | 3 | – for Arming state request.

   Available answers: **1 tone** beep – Armed.
   2 tone beeps – Disarmed.

   | 5 | – for Group Disarming Under Duress.

3. Enter another disarming sequence or ends a call.

To Group Disarm by the arming switch

      Turn the arming switch off.

To Group Disarm by wireless key fob

1. Press the Disarm key fob button.
2. If the group disarmed successfully, then:
   - The **ARMED** LED and remote LED will turn off;
   - Entry Delay timer countdown stops;
   - Reader's buzzer beeps stops with the confirmation "thrill".
   - Two short siren squawks will hear as a disarming confirmation sound.

NOTE: Siren confirmation sound may be enabled by installer.

To Group Disarming by the iOS or Android application command:

1. Open the application "Mobile Keyboard" in your smartphone.
2. Log in to the application if this is required by application settings.
3. Select object (facility) number and group number you need.
4. Use the menu item **Commands** – **Disarm**.

3.9.1 Disarming Error

If you entered an invalid keyboard access code or tried to use an unauthorized key/card, the group will not disarmed and long tone will sound. In this case re-enter a correct access code or use the pre-registered key/card for current group.

4 Emergency Keys and Alarms

4.1 Emergency Keys

IMPORTANT: EMERGENCY USE ONLY!

- You can use a **hardware button** installed in the convenient place to generate Panic Alarm.
- You can use a **key fob Panic button** to generate Panic Alarm.
- You can use the phone call to you Control Panel to generate Panic Alarm:
  1. Call the number of Control Panel.
  2. Enter $\boxed{9}$ $\boxed{1}$ $\boxed{1}$ on your phone keypad to generate Panic Alarm.
- You can use the **iOS or Android application** command with the same purpose:
  1. Open the application "Mobile Keyboard" in your smartphone.
  2. Log in to the application if this is required by application settings.
  3. Select object (facility) number and group number you need.
  4. Use the menu item **Commands**, then press the **Red Round Button** to generate Panic Alarm.

4.2 Alarms

The Control Panel can generate 2 different alarm sounds.

Priority	Type of alarm	Alarm sound
1	Fire	Temporal beeps
2	Intrusion (Burglary)	Continuous siren

4.2.1 Fire Alarm

Follow your emergency evacuation plan immediately!

If the Fire Alarm was accidental

1. Turn off the fire siren

   With the keyboard

   1. Press (#) + (5), then enter *fire_password* with keyboard for fire subsystem access.
      ACCESS LEVEL LED will lights up.
   2. Then press (⊛) to fire siren turn off.
      ACCESS LEVEL LED will turned off.

   With the TouchMemory or RFID reader

   Touch to Touch Memory key reader port with the authorized key or bring your RFID-card closer to RFID reader.
2. Call your Security Company to avoid a dispatch.

4.2.2 Intrusion (Burglary) Alarm – Continuous siren

WARNING! If you are unsure of the source of the alarm – approach with caution!

If the Intrusion Alarm was accidental

1. Turn off the Intrusion siren
   With the keyboard – enter your 4-digits "normal" access code.

   With the TouchMemory or RFID reader – touch to Touch Memory key reader port with the authorized key or bring your RFID-card closer to RFID reader.
2. Call your Security Company to avoid a dispatch.

4.3 Reset the Fire State

After having detected a fire alarm, smoke detectors require a "reset" to exit to the normal condition.

NOTE: Verify with you Security Company if this function is required on your system.

To Reset the Fire State with the keyboard

1. Press (#)+(5), then enter *fire_password* with keyboard for fire subsystem access.
   ACCESS LEVEL LED will lights up.

2. Then press ⊛ to reset the Fire State.
   ACCESS LEVEL LED will turned off.

If a smoke detector fails to reset, it may still be detecting an alarm condition, so the alarm will reactivate or continue.

5 Keys and other Devices

Your system can be controlled by a variety of devices:
- Keyboard
- Key fobs
- TouchMemory keys and RFID cards/tags
- Calling from cell phones (only phone numbers configured by your installer will be permitted to contact your system)
- iOS and Android application commands.

5.1 Using Key Fobs

Key fobs allow users in the close proximity of their house to easily group arm/disarm and to generate Panic Alarm.

NOTE: Every key fob should be enrolled previously by your installer.

1. Away Arm
2. Stay Home Arm
3. Disarm
4. Panic
5. LED
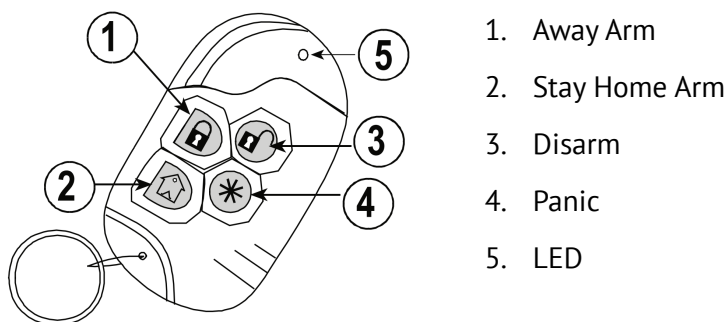
Figure 1. Visonic key fob

NOTE: The key fob shape, size and buttons layout in your system can vary.

5.2 Using TouchMemory Keys and RFID cards/tags

This kind of devices is very useful if you do not use the security system regularly. Besides, they do not required to remember security codes for arming/disarming action.

NOTE: Every key/card/tag should be enrolled previously by your installer.

These keys are used for:
- Fire Siren sound cancel
- Intrusion Siren sound cancel
- Group Arming/Disarming.

NOTE: The Siren sound canceled up to the next alarm event only.

For group arming/disarming you should touch to Touch Memory key reader port with the authorized key or bring your RFID card/tag closer to RFID reader.

6 Managing Users

Up to 16 users can have access to every Control Panel group (partition). Each user may have:
- Access to only operate specific group (partition)
- Unique pair of 4 digits access codes ("normal" and "under duress" in pair)
- TouchMemory key or RFID card/tag
- Access by cellular phone number
- iOS or Android application access

NOTE: All access codes/cards/tags/phone numbers/application logins and passwords – is configured by your installer.

6.1 Access Codes types

There are 5 access codes types:

Code	Add User	Delete User	Arm	Disarm	Access Codes
Administrator	Yes	Yes	Yes	Yes	Yes
Fire subsystem	No	No	No	No	Yes (Fire only)
Installer	Yes	Yes	No	No	Yes
User "normal"	No	No	Yes	Yes	No
User "under duress"	No	No	No	Yes	No

Administrator, Fire and Installer are system codes that can be changed only (not deleted). To every group (partition) may be assigned different Administrator and Fire codes.

Administrator   With this code can access to any function, arm/disarm and user management besides the system configuring function

Fire   With this code you can access to reset fire state and to fire siren on/off.

Installer   With this code can access to system configure.

User "normal"   Is used to arm/disarm assigned groups (partitions) only.

User "under duress"   Use if forced to access your keypad under threat. These codes are the same to "normal" codes, but they can used to disarm only and they send an Alarm event to CMS at the same time the disarming started.

6.1.1 Adding, Changing and Deleting Access Codes

Each configured user in the group (partition) is assigned a number 01...16.

To Add or Change User Access Codes

1. If the keypad are in normal mode operating, then press ⊛, *group number*, ⊛ to select group.

2. To enter to the codes change mode – press ⌗ + ③, *administrator code*
   - **MODE 1** LED will lights up.
   - Occupied user's codes appear **glowing** 1...16 **ZONE** LEDs, free – by **turned off ZONE** LEDs.

3. Enter the user's code number (the number 1...16) and press ⊛ to confirm.
   The **ZONE** LED is corresponding to a code number you enter will flashes.

4. Enter a new user's "normal" 4 digit code.
   - The corresponding **ZONE** LED will light continuously.
   - To add or change the another code – repeat steps 2 and 3.
   - If you don't need to change the code selected at step 2 – press ⌗.

5. To exit from codes change mode – press ⌗.

To Delete User Access Codes

1. If the keypad are in normal mode operating, then press (*), *group number*, (*) to select group.

2. To enter to the <u>codes change mode</u> – press (#) + (3), *administrator code.*

3. Enter the user's code number (the number 1...16) and press (*) to confirm.

4. Press (⊠) to delete user's code selected.
   • The corresponding **ZONE** LED will turned off.
   • To delete the another code – repeat steps 2 and 3.
   • If you don't need to delete the code selected at step 2 – press (#).

5. To exit from <u>codes change mode</u> – press (#).

To Change System Codes

1. If the keypad are in normal mode operating, then press (*), *group number*, (*) to select group.

2. To enter to the <u>codes change mode</u> – press (#) + (3), *administrator code.*

3. Press (※) to change **Administrator code** or

   (※) to change **Fire subsystem code.**
   All **ZONE** LEDs will flash.

4. Enter new 4 digits code.

5. To exit from <u>codes change mode</u> – press (#).

To Add or Change User Under Duress Codes

1. If the keypad are in normal mode operating, then press (*), *group number*, (*) to select group.

2. To enter to the <u>under duress codes change mode</u> – press (#) + (4), *administrator code*.
   • **MODE 2** LED will lights up.
   • Occupied user's codes appear **glowing** 1...16 **ZONE** LEDs, free – by **turned off ZONE** LEDs.
   • You can add or change "under duress" codes for <u>existing</u> "normal" user codes only.

3. Enter the user's code number (the number 1...16) and press (*) to confirm.
   The **ZONE** LED is corresponding to a code number you enter will flashes.

4. Enter a new user's "<u>under duress</u>" 4 digit code.
   • The corresponding **ZONE** LED will light continuously.
   • To add or change the another code – repeat steps 2 and 3.
   • If you don't need to change the code selected at step 2 – press (#).

5. To exit from <u>under duress codes change mode</u> – press (#).

To Delete User Under Duress Codes

1. If the keypad are in normal mode operating, then press (*), *group number*, (*) to select group.

2. To enter to the <u>under duress codes change mode</u> by press (#) + (4), *administrator code.*

3. Enter the user's code number (the number 1...16) and press (*) to confirm.

4. Press (⊠) to delete user's "under duress" code selected.
   • The corresponding **ZONE** LED will turned off.
   • To delete the another code – repeat steps 2 and 3.
   • If you don't need to delete the code selected at step 2 – press (#).

5. To exit from <u>under duress codes change mode</u> – press (#).

6.1.2 Enrolling and Deleting TouchMemory Keys and RFID cards/tags

To Enroll a TouchMemory Key or RFID card/tag

1. If the keypad are in normal mode operating, then press ⊛, *group number*, ⊛ to select group.

2. To enter to the <u>keys change mode</u> – press # + 6, *administrator code*.
   - **MODE 1** and **MODE 2** LEDs will lights up
   - Occupied user's keys appear **glowing** 1...16 **ZONE** LEDs, free – by **turned off ZONE** LEDs.

3. Enter the user's key number (the number 1...16) and press ⊛ to confirm.
     The **ZONE** LED is corresponding to a key number you enter will flashes.

4. Touch to TouchMemory key reader port with the new key or bring new RFID-card closer to RFID reader.
   - The corresponding **ZONE** LED will light continuously.
   - To add or change the another key – repeat steps 2 and 3.
   - If you don't need to change the code selected at step 2 – press #.

5. To exit from <u>keys change mode</u> – press #.

To Delete a TouchMemory Key or RFID card/tag

1. If the keypad are in normal mode operating, then press ⊛, *group number*, ⊛ to select group.

2. To enter to the <u>keys change mode</u> – press # + 6, *administrator code*.

3. Enter the user's key number (the number 1...16) and press ⊛ to confirm.

4. Press ⊠ to delete user's key/card/tag selected.

5. To exit from <u>keys change mode</u> – press #.

7 Managing Faults

Your Control Panel is monitored all system parameters continuously and notifies you about faults.

Any fault presence displayed by (depends of your system equipped):

- Keypad **FAULT** LED lights on.
- External **TouchMemory** key reader **SYSTEM** LED **flashes** twice per second.
- External **RFID** cards/tags reader **LED flashes yellow** every 3 seconds.
- Built-in reader **LED flashes yellow** every 3 seconds.

You can view a detail information about the fault kind on the keypad or Lind-7/11TM TouchMemory key readers as described in Table below.

Fault	Keypad LED		Lind-7/11TM LED		Description
	Directly	While hold ☎	Directly	While hold TROUBLE (up to 3 sec)	
AC POWER	**POWER 220V**	**ZONE 1**	**AC 220V**	**ZONE 1**	AC power was lost. Call for service
BATTERY	**BATTERY**	**ZONE 2**	**BATTERY**	**ZONE 2**	Battery trouble. Call for service
Lind-11TM link		**ZONE 4**			Link to external reader was lost. Call for service
AM-11 link		**ZONE 5**		**ZONE 4**	Link to external module was lost. Call for service
Keypad link		**ZONE 6**			Link to external keypad was lost. Call for service
CMS connection	**CMS CONNECTION**	**ZONE 10**		**ZONE 3**	Connection to CMS was lost. Check the cellular signal level as described in Section 9. If it does not restored within 5 minutes call for service
Wireless receiver link		**ZONE 11**		**ZONE 6**	Link to external module was lost. Call for service
WiFi module link		**ZONE 15**		**ZONE 7**	Link to external module was lost. Call for service
GSM signal jamming		**ZONE 16**			Cellular signal was lost or jamming. Call for service
CP connection	**CP CONNECTION**		**ZONE 1...8** "running light"		Link of this device to Control Panel was lost. Call for service
Arming disabled		**ZONE 9**		**ZONE 5**	Current group (partition) arming disabled by CMS command. Call your Security Company

7.1.1 Switching Faults Sound off/on

As new fault occurs the ICD built-in buzzer will sounds every 30 second.

To Switching Faults Sounds off/on

Press ⌗ + ☎.

- If sound off, **MUTED** LED lights up.
- New fault turns on the sound again.

8 Managing Groups (Partitions)

A group is a limited area of the facility which operates independently from other areas.

Groups in Security System may be useful when some areas required different arming conditions as other areas or if your home has a separate apartment.

Your Control Panel supports up to 2 groups (partitions).

Each group can have it's own ICD (keypad or TouchMemory/RFID reader) for access control. But the keypad may be programmed to access to both groups.

User access to groups is controlled via access codes or keys/cards/tags.

NOTE: Every ICD must be assigned to some group by installer.

8.1 Single Group Operation

Every ICD provide access to security functions for an assigned group only.

Single Group Keypad functions

- Displays the armed state of the group.
- Displays first 16 zones violated or fault state.
- Arming/disarming.
- Allows user codes/keys/cards/tags managing.
- Allows zone bypassing.
- Displays system faults.
- Test it's own LEDs and buzzer.

Single Group TouchMemory Key External Reader functions

- Displays the armed state of the group.
- Displays first 8 zones violated or fault state.
- Arming/disarming.
- Displays system faults.
- Test it's own LEDs and buzzer.

8.2 Switching Keypad to Another Group (Partition)

If the keypad is configured for access to both groups, you can switch it to another group any time. When a keypad is switched from either group, she starts to displays armed state and zones state for current group.

To Switch the Keypad to Another Group

Press ⊛, *group number*, ⊛.

8.2.1 Verify Current Group Number

To Verify Current Group Number

Hold ⌗+⑨
- Corresponding **ZONE** LED lights on as a current group number.

8.2.2 View the Armed Status for All Assigned Groups

To View the Armed Status by Group

Hold ⌗+②
- Corresponding **ZONE** LED lights on if the group armed.

9 Additional Features

Your Control Panel supports some additional features.

9.1.1 Check the Cellular and WiFi Signal Level

To Signal Level Check by Keypad

Hold ⊛
- **ZONE 1...8** LEDs display **GSM/GPRS** signal level.
- **ZONE 9...16** LEDs display **WiFi** signal level.
- Eight lighted LEDs correspond to the maximum level.

To Signal Level Check by TouchMemory Key Reader

Press **RESET+TROUBLE**
- **ZONE 1...8** LEDs display **GSM/GPRS** signal level for 30 seconds.

9.1.2 Test ICD LEDs and buzzer

To test Keypad LEDs and buzzer

Hold ⊛
- All keypad LEDs will lights up and buzzer will sounds up to 10 seconds for test.

To test TouchMemory Key Reader LEDs and buzzer

Hold **RESET**
- All reader LEDs will lights up and buzzer will sounds for test.

9.1.3 Keypad Backlight on/off

To Keypad Backlight on/off

Press ⓗ + ⊛.
- If on – all key LEDs flash once, else – flash twice.

9.1.4 ICD Hardware Version

To View a Keypad Hardware Version

Hold ⓗ + ⓪
- Hardware Version displays by **ZONE** LEDs in binary code
  (**ZONE 1** corresponds to the least significant bit)

To View an External TouchMemory Key Reader Hardware Version

Hold **TROUBLE**
- Hardware Version displays by **ZONE** LEDs in binary code
  (**ZONE 1** corresponds to the least significant bit)

10 Installer Warning

WARNING Please Read Carefully

Note to Installers

This warning contains vital information. As the only individual in contact with system users, it is your responsibility to bring each item in this warning to the attention of the users of this system.

System Faults

This system has been carefully designed to be as effective as possible. There are circumstances, however, involving fire, burglary, or other types of emergencies where it may not provide protection. Any alarm system of any type may be compromised deliberately or may fail to operate as expected for a variety of reasons. Some but not all of these reasons may be:

Inadequate Installation

A security system must be installed properly in order to provide adequate protection. Every installation should be evaluated by a security professional to ensure that all access points and areas are covered. Locks and latches on windows and doors must be secure and operate as intended. Windows, doors, walls, ceilings and other building materials must be of sufficient strength and construction to provide the level of protection expected. A reevaluation must be done during and after any constructing activity. An evaluation by the fire and/or police department is highly recommended if this service is available.

Criminal Knowledge

This system contains securi feature which were known to be effective at the time of manufacture. It is possible for persons with criminal intent to develop techniques which reduce the effectiveness of these features. It is important that a security system be reviewed periodically to ensure that its features remain effective and that it be updated or replaced if it is found that it does not provide the protection expected.

Access by intruders

Intruders may enter through an unprotected access point, circumvent a sensing device, evade detection by moving through an area of insufficient coverage, disconnect a wanting device, or interfere with or prevent the proper operation of the system.

Power Failure

Control units, intrusion detectors, smoke detectors and many other security devices require an adequate power supply for proper operation. If a device operates from batteries, it is possible for the batteries to fail. Even if the batteries have not failed, they must be clawed, in good condition and installed correctly. if a device operates only by AC power, any interruption, however brief, will render that device imperative while it dos not have power. Power interruptions of any length are often accompanied by voltage fluctuations which may damage electronic equipment such as a security system. Alter a power interruption has occurred, immediately conduct a complete system test to ensure that the system operates as intended.

Failure of Replaceable Batteries

This system's wireless transmitters have been designed to provide several years of battery life under normal conditions. The expected battery life is a function of the device environment, usage and type. Ambient conditions such as high humidity, high or low temperatures, or large temperature fluctuations may reduce the expected battery life. While each transmitting device has a low battery monitor which identifies when the batteries need to be replaced, this monitor may fail to operate as expected. Regular testing and maintenance will keep the system in good operating condition.

Compromise of Radio Frequency (Wireless) Devices

Signals may not reach the receiver under all circumstances which could include metal objects placed on or near the radio path or deliberate jamming or other inadvertent radio signal interference.

System Users

A user may not be able to operate a panic or switch possibly due to permanent or temporary physical disability, inability to reach the device in time, or unfamiliarity with the correct operation. It is important that all system users be trained in the correct operation of the alarm system and that they know how to respond when the system indicates an alarm.

Smoke Detectors

Smoke detectors that are apart of this system may not properly alert occupants of a fire for a number of reasons, some of which follow. The smoke detectors may have been improperly installed or positioned. Smoke may not be able to reach the smoke detectors, such as when the fire is in a chimney, walls of roofs, or on the other side of closed doors. Smoke detectors may not detect smoke from fires on another level of the residence or building.

Every fire is different in the amount of smoke and the rate of building. Smoke detectors cannot sense all types of fires equally well. Smoke detectors may not provide timely warning of fires caused by carelessness or safety hazards such as smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits, children playing with matches or arson.

Even if the smoke detector operates as intended, there may be circumstances when there is insufficient warning to allow all occupants to escape in time to avoid injury or death.

Motion Detectors

Motion detectors can only detect motion within the designated areas as shown in their respective installation instructions. They cannot discriminate between intruders and intended occupants. Motion detectors do not provide volumetric area protection. They have multiple beams of detection and motion can only be detected in unobstructed areas covered by these beam. They can not detect motion which occurs behind walls, ceilings, floor, closed doors, glass partitions, glass doors or windows. Any type of tampering whether intentional or unintentional such as masking, painting, or spraying of any material on the lenses, mirrors, windows or any other part of the detection system will impair its proper operation.

Passive infrared motion detectors operate by sensing changes in temperature. However their effectiveness can be reduced when the ambient temperature rises near or above body temperature or if there are intentional or unintentional sources of heat in or near the detection area. Some of these heat sources could be heaters, radiators, stoves, barbecues, fireplaces, sunlight, steam vents, lighting and so on.

Warning Devices

Warning device such as sirens, bells, horns, or strobes may not warn people or waken someone sleeping if there is an intervening wall or door. if warning devices are located on a different level of the residence or premise, then it is less likely that the occupants will be alerted or awakened Audible warning devices may be interfered with by other noise sources such as stereos, radios, televisions, air conditioners or other appliances, or passing traffic. Audible warning devices, however loud, may not be heard by a herring-impaired person.

Telephone Lines

If telephone line are used to transmit alarms, they may be out of service or busy for certain periods of time. Also an intruder may cut the telephone line or defeat its operation by more sophisticated means which may be difficult to detect.

Insufficient time

There may be circumstances when the system will operating as intended, yet the occupants will not be protected from the emergency due to their inability to respond to the warnings in a timely manner. If the system is monitored, the response may not occur in time to protect the occupants or their belongings.

Component Failure

Although every effort has been made to make this system as reliable as possible, the system may fail to function as intended due to the failure of a component.

Inadequate Testing

Most problems that would prevent an alarm system from operating as intended can be found by regular testing and maintenance. The complete system should be tested weekly and immediately after a break-in, an attempted break-in, a fire, a storm, an earthquake, an accident, or any kind of construction activity inside or outside the premises. The testing should include all sensing devices, keypads, consoles, alarm indicating devices and any other operational devices that are part of the system.

Security and insurance

Regardless of its capabilities, an alarm system is not a substitute for property or life insurance. An alarm system also is not a substitute for property owners, renters, or other occupants to act prudently to prevent or minimize the harmful effects of an emergency situation.

11 Safety Instructions

WARNING: This equipment has no mains on/off switch. the plug of the direct plug-in power supply is intended to serve as the disconnecting device if the equipment must be quickly disconnected.

It is imperative that access to the mains plug and associated mains socket/outlet, is never obstructed.

WARNING: When using equipment connected to the mains and/or to the telecommunication network, there are basic safety instructions that should always be followed. Refer to the safety instructions provided with this product and save them for future reference. To reduce the risk of fire, electric shock and/or injury, observe the following:

- Do not attempt to service this product yourself. Opening or removing the cover may expose you to dangerous voltage or other risk. Refer servicing to qualified service persons. Never open the device yourself.
- Any servicing shall be referred to Service Persons only.
- Dispose the used batteries according to the local rules and regulations.
- Do not leave and/or deposit any object on the top of the equipment cabinet. The cabinet, as installed, is not designed to support any supplementary weight.
- Do not spill any liquids on the cabinet.
- Do not touch the equipment and its connected cables during an electrical storm; there may be a risk of electric shock.
- Never touch uninsulated wires or terminals unless the Direct Plug In transformer has been disconnected.
- Ensure that cables are positioned so that accidents cannot occur. Connected cables must not be subject to excessive mechanical strain. Do not spill any type of liquid on the equipment.
- Do not use the Security System to report a gas leak if the system is near a leak.
- The equipment is stationary/fixed and direct plug-in connected to the mains and shall be installed and serviced by service persons only.

11.1 Regular Maintenance and Troubleshooting

Keep your Control Panel in optimal condition by following all the instructions that are included within this manual and/or marked on the product.

11.1.1 Cleaning

- Clean the units by wiping with a damp cloth only.
- Do not use abrasives, thinners, solvents or aerosol cleaners (spray polish) that may enter through holes in the Control Panel and cause damage.
- Do not use any water or any other liquid.
- Do not wipe the front cover with alcohol.

11.1.2 Troubleshooting

Occasionally, you may have a problem with your Alarm Controller or telephone line. If this happens, your Control Panel will identify the problem and displays an error message. Refer to the provided list when you see an error message on the display. If additional help is required, contact your distributor for service.

NOTE: There are no parts replaceable by the end-user within this equipment.

12 Locating Detectors and Escape Plan

The following information is for general guidance only and it is recommended that local fire codes and regulations be consulted when locating and installing smoke and CO alarms.

12.1 Smoke Detectors

Research has shown that all hostile fires in homes generate smoke to a greater or lesser extent. Experiments with typical fires in homes indicate that detectable quantities of smoke precede detectable levels of heat in most cases. For these reasons, smoke alarms should be installed outside of each sleeping area and on each floor of the home.

The following information is for general guidance only and it is recommended that local fire codes and regulations be consulted when locating and installing smoke alarms.

It is recommended that additional smoke alarms beyond those required for minimum protection be installed. Additional areas that should be protected include: the basement; bedrooms, especially where smokers sleep; dining rooms; furnace and utility rooms; and any hallways not protected by the required units. On smooth ceilings, detectors may be spaced 9.1m apart as a guide. Other spacing may be required depending on ceiling height, air movement, the presence of joists, uninsulated ceilings, etc. Consult National Fire Alarm Code NF PA 72, CAN/ULC-SSS3-02 or other appropriate national standards for installation recommendations.
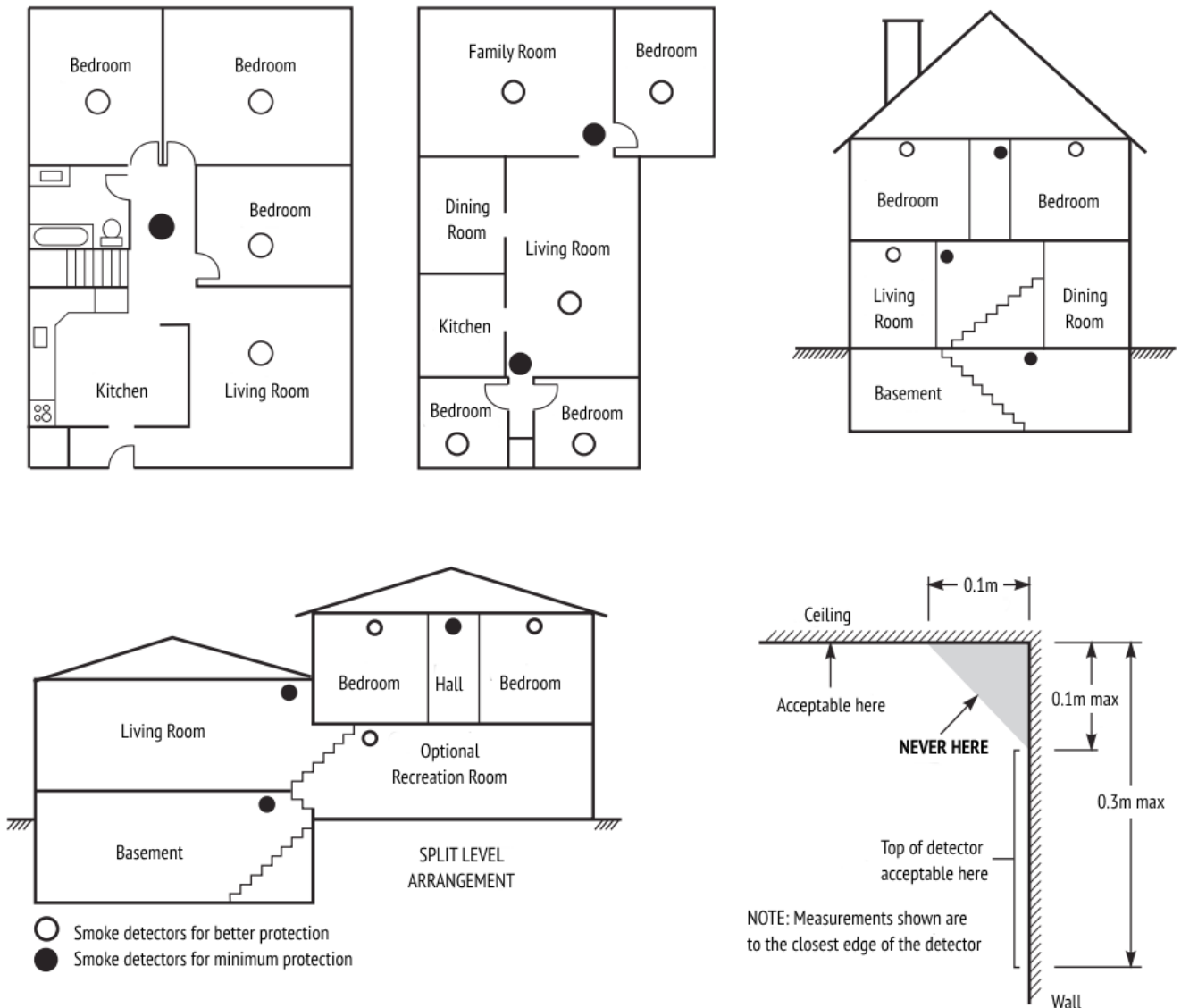

Figure 2

- Do not locate smoke detectors at the top of peaked or gabled ceilings; the dead air space in these locations may prevent the unit from detecting smoke.
- Avoid areas with turbulent air flow, such as near doors, fans or windows. Rapid air movement around the detector may prevent smoke from entering the unit.
- Do not locate detectors in areas of high humidity.
- Do not locate detectors in areas where the temperature rises above +38°C or falls below +5°C.
- Smoke detectors should always be installed in USA in accordance with Chapter 11 of NF PA 72, the National Fire Alarm Code: 11.5.1.1.

Where required by applicable laws, codes, or standards for a specific type of occupancy, approved single- and multiple- station smoke alarms shall be installed as follows:

1. In all sleeping rooms and guest rooms.
2. Outside of each separate dwelling unit sleeping area, within 6.4m of any door to a sleeping room, the distance measured along a path of travel.
3. On every level of a dwelling unit, including basements.
4. On every level of a residential board and care occupancy (small facility), including basements and excluding crawl spaces and unfinished attics.
5. In the living area(s) of a guest suite.
6. In the living area(s) of a residential board and care occupancy (small facility).

12.2 Fire Escape Planning

There is often very little time between the detection of a fire and the time it becomes deadly. It is thus very important that a family escape plan be developed and rehearsed.

1. Every family member should participate in developing the escape plan.
2. Study the possible escape routes from each location within the house. Since many fires occur at night, special attention should be given to the escape routes from sleeping quarters.
3. Escape from a bedroom must be possible without opening the interior door.

Consider the following when making your escape plans:

- Make sure that all border doors and windows are easily opened. Ensure that they are not painted shut, and that their locking mechanisms operate smoothly.
- If opening or using the exit is too difficult for children, the elderly or handicapped, plans for rescue should be developed. This includes making sure that those who are to perform the rescue can promptly hear the fire warning signal.
- If the exit is above the ground level, an approved fire ladder or rope should be provided as well as training in its use.
- Exits on the ground level should be kept clear. Be sure to remove snow from exterior patio doors in winter; outdoor furniture or equipment should not block exits.
- Each person should know the predetermined assembly point where everyone can be accounted for (e.g., across the street or at a neighbor's house). Once everyone is out of the building, call the fire department.
- A good plan emphasizes quick escape. Do not investigate or attempt to fight the fire, and do not gather belongings as this can waste valuable time. Once outside, do not re-enter the house. Wait for the fire department.
- Write the fire escape plan down and rehearse it frequently so that should an emergency arise, everyone will know what to do. Revise the plan as conditions change, such as the number of people in the home, or if there are changes to the building's construction.
- Make sure your fire warning system is operational by conducting weekly tests. If you are unsure about system operation, contact your installer.

We recommend that you contact your local fire department and request further information on fire safety and escape planning. If available, have your local fire prevention officer conduct an in-house fire safety inspection.

12.3 Carbon Monoxide Detectors

Carbon monoxide is colorless, odorless, tasteless, and very toxic, it also moves freely in the air. CO detectors can measure the concentration and sound a loud alarm before a potentially harmful level is reached. The human body is most vulnerable to the effects of CO gas during sleeping hours; therefore, CO detectors should be located in or as near as possible to sleeping areas of the home. For maximum protection, a CO alarm should be located outside primary sleeping areas or on each level of your home. Figure 3 indicates the suggested locations in the home.

Figure 3

Do NOT place the CO alarm in the following areas:

- Where the temperature may drop below -10°C or exceed +40°C.
- Near paint thinner fumes.
- Within 1.5m of open flame appliances such as furnaces, stoves and fireplaces.
- In exhaust streams from gas engines, vents, flues or chimneys.
- Do not place in close proximity to an automobile exhaust pipe; this will damage the detector.

PLEASE REFER TO THE CO DETECTOR INSTALLATION AND OPERATING INSTRUCTION SHEET FOR SAFETY INSTRUCTIONS AND EMERGENCY INFORMATION.
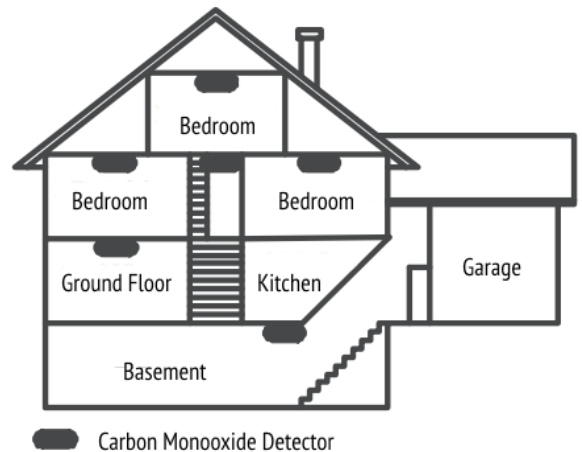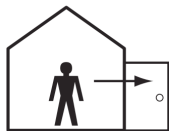
13 Reference

Fill out the following information for future reference and store this guide in a safe place.

13.1 System Information

Mark if Alarm Buttons are Enabled

☐ Fire   ☐ Panic

The Exit Delay Time is _____ seconds.
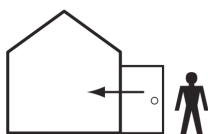
The Entry Delay Time is _____seconds.

13.2 Service Contact Information

Central Monitoring Station

Telephone: _____

Installer Information

Company: _____ Telephone: _____

Battery INSTALLATION / Service Date:

_____   _____   _____

_____   _____   _____

_____   _____   _____

WARNING: If you suspect a false alarm signal has been sent to the Central Monitoring Station, call the station immediately to avoid an unnecessary response.

13.3 Access Code and Zone Information

Administrator Code _____ Fire Code: _____

Table 1. Group #1 Access Code Reference

Code #	Access Code	Code #	Access Code	Code #	Access Code	Code #	Access Code
01		05		09		13	
02		06		10		14	
03		07		11		15	
04		08		12		16	

Table 2. Group #2 Access Code Reference

Code #	Access Code	Code #	Access Code	Code #	Access Code	Code #	Access Code
01		05		09		13	
02		06		10		14	
03		07		11		15	
04		08		12		16	

Table 3. Sensor / Zone Information

Sensor #	Protected Area	Sensor Type	Sensor #	Protected Area	Sensor Type
01			18		
02			19		
03			20		
04			21		
05			22		
06			23		
07			24		
08			25		
09			26		
10			27		
11					
12					
13					
14					
15					
16					
17					