

# ***FORCE Series***

Advanced Intruder Alarm Systems



## **User Guide**

Version: 1.3.X



**Table of Contents**

<b>Chap. 1 Introduction .....</b>	<b>4</b>
1.1 Main features .....	4
1.1 System comparison table .....	5
1.2 Technical specifications .....	6
<b>Chap. 2 Keypads.....</b>	<b>7</b>
2.1 KLT/KLR500 .....	7
2.1.1 Main features.....	7
2.1.2 Technical specifications .....	7
2.1.3 Quick guide .....	7
2.1.4 Operation keys and keypad alarms.....	8
2.1.5 Keypad settings .....	8
2.1.6 Other indications .....	9
2.2 How to enter text and characters.....	9
2.3 KLA500 arming station.....	10
2.3.1 Main features.....	10
2.3.2 Technical specifications .....	10
2.3.3 Quick guide .....	10
<b>Chap. 3 System Programming .....</b>	<b>11</b>
3.1 Menus and codes .....	11
3.1.1 Code setting guidelines .....	11
3.1.2 How to enter the menu and change the default codes .....	11
3.2 The user menu .....	12
<b>Chap. 4 Arming and Disarming .....</b>	<b>13</b>
4.1 Arm Away .....	13
4.2 Arm in Home 1-4 .....	13
4.3 Disarming .....	14
4.3.1 Disarming partitions.....	14
<b>Chap. 5 Bypass Zones.....</b>	<b>15</b>
5.1 How to bypass on-the-fly .....	15
5.2 How to bypass before arming.....	15
<b>Chap. 6 Event Memory.....</b>	<b>16</b>
<b>Chap. 7 Users and Codes .....</b>	<b>16</b>
7.1.1 Users.....	16
<b>Chap. 8 Communication.....</b>	<b>18</b>
8.1 Contacts .....	18
8.1.1 Communication and Backup Paths.....	18
8.1.2 Communication Test .....	19
8.2 PIMA Cloud .....	19
8.3 Phone Notifications.....	19
8.4 Remote Service .....	19
8.5 CMS Registration .....	20
<b>Chap. 9 System Options .....</b>	<b>21</b>
9.1 Override Faults .....	21
9.2 Zone Information .....	21
9.3 Armed Partitions .....	22
9.4 Time and Date.....	22
9.5 Chime Zones .....	22
9.6 Auto Arming.....	23
9.7 Reset Smoke Detector .....	23
9.8 Technician Permit.....	24

9.9	System Information.....	24
<b>Chap. 10</b>	<b>Partitioning .....</b>	<b>25</b>
10.1	Optional uses .....	25
10.2	How to clean the LCD screen .....	26

## Appendixes

<b>Appendix A</b>	<b>Troubleshooting Faults.....</b>	<b>27</b>
<b>Appendix B</b>	<b>Glossary .....</b>	<b>29</b>
<b>Appendix C</b>	<b>Zone Number and Location.....</b>	<b>31</b>

### Safety Instructions. Read Carefully!

- Hazards of fire and electric shock exist in this alarm system. To reduce the risk of fire or electric shock, do not expose this alarm system to rain or moisture. Pay attention: Telephone cords could be a good conductor for lightings energy.
- 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.
- Dangerous high voltages are present inside the control panel's enclosure. Refer servicing to qualified personnel only.
- This alarm system should be used with 230VAC/110VAC, 50/60Hz, protected by anti-electric shock breaker. Use only the power supply provided with this equipment. Use of unauthorized power supplies may cause damage.
- Do not spill liquid of any kind onto the unit. If liquid is accidentally spilled onto the unit, immediately consult a qualified service.
- Disposal of used batteries must be made in accordance with local waste recovery and recycling regulations.

### Default Codes

Master User: 5555

Master Installer: 1234

### Signs in this guide



**Warning**



Note



Enter sub-menu, select/deselect, save selection.



Menu with sub-menus (on the display)



Menu with sub-menus (in this guide)



Options menu



Return/Esc, Cancel



Selectable parameter (enabled/disabled)



Scroll between zones, partitions, users, etc.

# Chap. 1 Introduction

Dear customer

Congratulations on your purchase of PIMA Electronic Systems' highly reliable **FORCE Series** (hereinafter, **FORCE**) intruder alarm system. This guide will introduce you with the alarm series that includes the **FORCE**, **FORCE Lite** and **FORCE 32**.

**FORCE**'s 7-line, LCD screen keypads are menu-driven. The Technician and User subject menus make programming and navigating the **FORCE** menus fast and easy. Help screens reduce the need to look in this guide on every servicing.

Using a wireless receiver, various wireless peripherals can be used, including detectors, key fobs, and a panic button.

With PimaLink 3.0 smartphone application (for Android and iOS) and cloud service you can receive notifications, and arm and disarm your alarm system from anywhere.

Note: This alarm system must be checked by a qualified technician at least once a year.

This User guide refers to the **FORCE** alarm system, version 1.3.X. The system is supplied with two guides:

- This guide that includes the user-programming guide and the system maintenance instructions. Read this guide
- The Installation guide that includes the system and accessories installation and wiring instructions, as well as the technician-programming guide.

## 1.1 Main features

### **FORCE**

- Zones: eight onboard, expandable to 144 (including zone doubling), including up to 64 wireless<sup>1</sup>.
- Users: up to 144, with a unique code for each, up to 64 of which with a remote control.
- Contacts: up to 32, for receiving alarm and other notifications.
- Partitions: up to 16, with a separate keypad for each.
- Expanders for 8 and 16 zones, with one or two relays on each
- Multi-channel communications: Ethernet, 3G, Cellular Data, PSTN and Radio.
- Up to two CMSs (Central Monitoring Station) with password protection for each
- Remote operations via PIMAlink 3.0 cloud and smartphone application
- Graphic, LCD, 7-line keypad display with various menus.
- Detailed tests and diagnostics menu
- Remote and local upload/download using the Force Manager software, via Ethernet/Cellular.
- Remote firmware update via the Force Manager software
- Encrypted CMS reporting

<sup>1</sup> Requires a wireless receiver

**FORCE Lite**

- Zones: eight onboard, expandable to 32, and 24 wireless<sup>2</sup> (a total of 64, including zone doubling).
- Users: up to 64, with a unique code for each.
- Contacts: up to 16, for receiving alarm and other notifications.
- Up to eight true partitions, with separate keypads (up to eight) for each.
- Multi-channel communications: Ethernet, 2G/3G/4G, Cellular Data, and Radio.
- One siren output
- One tamper input

**FORCE 32**

- Zones: eight onboard, expandable to 32 (including zone doubling), including 24 wireless<sup>3</sup>.
- Users: up to 32, with a unique code for each.
- Contacts: up to 16, for receiving alarm and other notifications.
- Up to four true partitions/eight keypads
- Multi-path communications: cellular (2-4G), PSTN, radio, and network (limited). The network connection only allows connecting with the FORCE Manager up/download software.
- PIMALink 3.0 app including system notifications, when using cellular modem.
- One siren output
- One tamper input

**FORCE 32C**

The **FORCE 32C** has the same features as the **FORCE 32**, except that it has full network capacity (Ethernet) as in the **FORCE**.

## 1.1 System comparison table

<b>Feature</b>	<b>FORCE</b>	<b>FORCE Lite</b>	<b>FORCE 32/32C</b>
Hardwired zones	8-144	8-64	8-32
Wireless zones (max.)	64	24	24
Users	144	64	32
Contacts	32	16	16
Partitions	16	8	4
Onboard network connection	✓	✓	✓ <sup>4</sup>
Communication paths	Network, PSTN, cellular, radio	Network, cellular, radio	PSTN, cellular, radio, network (limited <sup>4</sup> )
Output current	1.1A	750mA	750mA
Siren outputs	2	1	1
Relay output	1	-	1

<sup>2</sup> Requires a wireless receiver

<sup>3</sup> Requires a wireless receiver

<sup>4</sup> See the limited network connection features for each system above the table.

## 1.2 Technical specifications

- AC power input: 11-18V
- Backup battery input: 13.8VDC
- Relay: 1A max.
- On/Off and Alarm outputs (minus, open drain): 10A max., external power: +25V max.
- Output current
  - Max: +13.8VDC, 1.1A. **FORCE Lite/32**: +13.8VDC, 750mA
  - Idle: 50mA
- EOL resistors (up to two): programmable
- Operating temperature: -10 to +50 °C
- Humidity (max.): 93% R.H., non-condensing

## Chap. 2 Keypads

### 2.1 KLT/KLR500

**FORCE's** LCD keypads are the KLT500 with touch keys, and KLR500 with rubber keys. Both keypads connect to the control panel's bus and have 7-line LCD screen with a graphic display.

#### 2.1.1 Main features

- Graphic LCD screen
- 4 system status LEDs
- Uses PIMA proprietary communication protocol
- Tamper switch protection

#### 2.1.2 Technical specifications

- Screen size: 128X64 pixel
- Communication voltage levels: 0, +12V
- Operating Voltage Range: 9-14 VDC
- Current Consumption: 50mA idle, 90mA max.
- Sizes: 15 x 12 x 2cm
- Weight: 235gr
- CE compliance
- Operating Temperature: -10 to +55 °C
- Humidity (max.): 93% R.H., non-condensing

#### 2.1.3 Quick guide

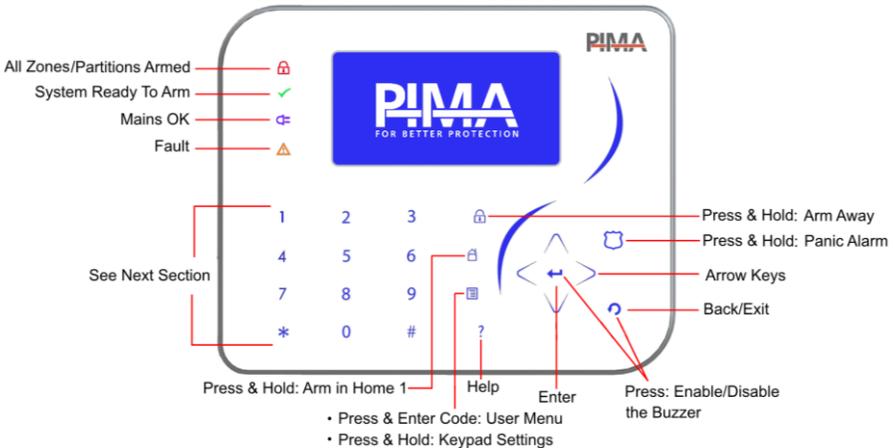


Figure 1. KLR/KLT500 keypad keys

LED	Type	Status	Indication
Red 	Arm	Steady On	System armed Away or in Home/All partitions are armed
		Off	All zones/partitions are disarmed
		Flashes once every 1 second	Exit delay in progress (including in a partition)
		Flashes once every 2 seconds	One or more partitions are armed

LED	Type	Status	Indication
Green ✓	Ready To Arm	Steady On	No alarm or fault exist, all non-delayed zones are closed.
		Off	A zone is open, or a fault exists.
Blue ⚡	AC Power	Steady On	AC power OK
		Flashes	Faults exist
Orange ⚠	Fault	Flashes	Faults exist
		Off	No fault exist, or the system is armed.

## 2.1.4 Operation keys and keypad alarms

### Quick access keys

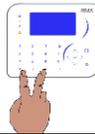
Press and hold the keys described in the next table, for the following operations:

Key	Operation
1-4	Arm in <i>Home 1-4</i>
5	Zones' status
6	<i>Remote Service</i> menu (+ user code) <sup>5</sup>
7	Partitions' status (+ user code) <sup>6</sup>
8	Pair to cloud menu (+ user code) <sup>6</sup>
0	Display the service provider and the control panel's version
*	Turn the chime on/off (toggle)

### Keypad alarms

You can trigger 3 alarms at the keypad: *Panic*, *Fire*, and *Medical*. When these alarms are triggered, **FORCE** activates the programmed responses, including triggering the sirens and reporting the CMS (where relevant), and the contacts.

Alarm	Press & hold
Medical	4 + 6
Fire	7 + 9
Panic	* + #



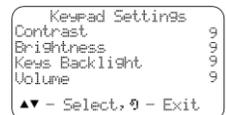
## 2.1.5 Keypad settings

To view the *Keypad Settings* screen press and hold the menu key .

In this screen you can set the audio-visual parameters of the keypad, which are *Contrast*, *Brightness*, *Keys Backlight*, and the *Volume* of the buzzer. Each parameter is scaled 0-9. Settings are per keypad.

To change a parameter, do as follows:

1. Press an arrow key and select a parameter.
2. Enter a number between 0-9.
3. Press  to save and exit.



<sup>5</sup> Version 1.2 and higher

<sup>6</sup> Version 1.3 and higher



**Warning: if you set the buzzer's Volume to 0, no alerts will be sounded from the keypad, including from chime zones.**

## Silencing the keypad

To silence the keypad's buzzer (including the chime) and keys completely, press together the Back/Exit ↶ and Enter ↵ keys. Press again to re-activate the buzzer (toggle).

### 2.1.6 Other indications

Letters displayed on the keypad's upper line indicate the following:

Letter	Indication
G	Cellular/data communication
M	SMS message
N	Network communication (including with PIMA cloud)
P	PSTN communication
R	Relay (device) is activating
S	The siren is currently sounding
T	Radio transmission
V	Cellular/Voice communication

## 2.2 How to enter text and characters

Text in the **FORCE** is entered like in a telephone: each key is assigned with several characters; pressing a key repeatedly replaces the characters. For example, pressing key 8 once displays the letter T. Pressing it immediately once more displays the letter U.

The keystrokes and characters are listed in the table and image below. To move between the letter sets, press the pound key (#). Set 3 is useful for entering IP addresses.

Key	Set 1	Set 2	Set 3
1	1.,?!( )/*:-+#@'	1.,?!( )/*:-+#@'	1.:
2	ABC2	abc2	2
3	DEF3	def3	3
4	GHI4	ghi4	4
5	JKL5	jkl5	5
6	MNO6	mno6	6
7	PQRS7	pqrs7	7
8	TUV8	tuv8	8
9	WXYZ9	wxyz9	9
0	Space, 0		
#	Delete, return to default		
*	Uppercase/lowercase/digits		

1.,?!( )/*:-+#'	ABC2	DEF3
1	2	3
GHI4	JKL5	MNO6
4	5	6
PQRS7	TUV8	WXYZ9
7	8	9
Letter Case	Space, 0	
*	0	#

## 2.3 KLA500 arming station

The KLA500 is a wired arming station. It is used for arming and disarming, and activating devices (using *Operation codes*; see page 17). The keypad connects to the control panel's bus and has touch keys.



*In addition to the KLA500, we recommend using a minimum of one LCD keypad on every premises.*

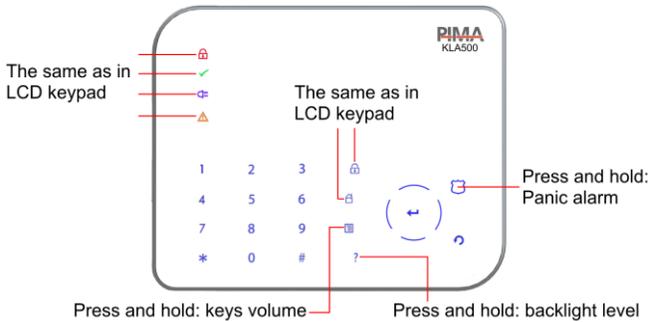
### 2.3.1 Main features

- Arming and disarming using only user codes (the Master user code is not in use).
- 4 status LEDs
- Uses PIMA proprietary communication protocol
- Back tamper

### 2.3.2 Technical specifications

- Communication voltage levels: 0, +12V
- Operating Voltage Range: 9-14 VDC
- Current Consumption: 50mA idle, 90mA max.
- Sizes: 15 x 12 x 2cm
- Weight: 163gr
- CE compliance
- Operating Temperature: -10 to +55 °C
- Humidity (Max.): 93% R.U., Non-condensing.

### 2.3.3 Quick guide



- For the system status LEDs, refer to page 7.
- For *Keypad alarms*, see section 2.1.5 above.

### Silencing the keypad

To silence the keypad's buzzer (including the chime) and keys completely, press together the and keys. Press again to re-activate the buzzer (toggle).

### Operation keys

Press and hold the keys described in the next table, for the following operations:

Key	Operation
1-4	Arm to <i>Home 1-4</i> modes
*	Turn on/off the chime

## Chap. 3 System Programming

### 3.1 Menus and codes

**FORCE** has two separate menus, User and Technician, with two matching Master codes. In addition, there are up to 144 user codes (**FORCE Lite**: up to 64). The Master user code allows setting all the user menus. Other user codes can be restricted by permissions.

The Master technician code allows entering the Technician menu. Monitoring stations' menus can have lock codes. Refer to the technician.

#### 3.1.1 Code setting guidelines

Note the following, when setting codes:

- All codes are made of four to six digits, except the Quick Arm (two-digit) code.
- Codes cannot start with the digits of other defined code, including the Quick Arm 2-digit code. For example, a five-digit user code cannot start with the digits of a four-digit user code.
- Every code must be unique.
- After saving a code, it can not be revealed or restored in any way.
- The codes 1234 and 5555 are reserved.

#### 3.1.2 How to enter the menu and change the default codes

To enter the **FORCE** menus for the first time, you must change the default Master user (5555) code. This is usually done by the installer of the alarm system.

Do as follows to change the codes:

1. In the main screen, press 5555. The code changing screen is displayed.
2. Press ← - the cursor moves to the right.
3. Enter a new 4-6 digit Master code.

```
11 May Sun 08:12
Master Code:--
Technician Code:--
```

```
Press 0 to Exit
```



*Write down the code and keep it in a safe place.*

4. Press ← - the cursor moves back to the left.
5. If only the Master code field is displayed, press ↻ to save and return to the main screen. The new code has now been saved.
6. If the *Tech. Code* field is displayed, press the arrow down key, press ← and enter a new 4-6 digit Technician code. Write down the code and keep it in a safe place.
7. Press ←.
8. Press ↻ to save and return to the main screen. The new code has now been saved.
9. Set the system time - see section 9.4, on page 22.

## 3.2 The user menu

The user menu includes the users and contacts settings, and some system parameters. As mentioned before, the Master user can enter all the sub-menus of the User menu and set every parameter. The access of other users can be limited, using access permissions.

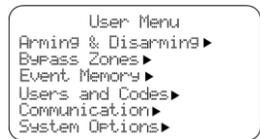
To enter the user menu, do as follows:

1. Enter the Master code, **or**
2. Press the menu key  on a keypad, and enter a user code in the code screen (the user must have a permission to enter the menu - see section 7.1.1, on page 16).

Navigate in the **FORCE** menus as follows:

- Press **←** to select, save, or enter a sub-menu.
- Press **↻** to exit a sub-menu without saving (except in the *Keypad Settings* screen).
- Press the upwards and downwards **^** **v** arrows to scroll accordingly.
- Press **#** to scroll to the next screen.

On the right is the user menu main screen. To select and enter a sub-menu, scroll using the arrow keys **^** **v** and press **←**.



## Chap. 4 Arming and Disarming



Note

- You can find detailed information on the arming modes in the Glossary, on page 29.
- From here onwards, in addition to the Master code you can use any user code with permissions.

### 4.1 Arm Away

Arming *Away* is used when the premises is left vacant and all the detectors should be activated. Check that the message "Ready to Arm" is displayed - if open zones are displayed, see Chap. 5, on page 15; if faults are displayed, see section 9.1, on page 21.

1. Press and hold the  key, until the keypad sounds a long beep; the alarm system is immediately armed, while the *Exit Delay*<sup>7</sup> starts running, and the keypad sounds beeps and displays a progress bar timer. During the delay, passing through delayed zones will not trigger the alarm and will allow you to leave the premises.
2. If one key arming is not enabled (by the technician), you will have to enter a user code.  
*User Menu* ► *Arming & Disarming* ► *Arm Away*
3. You can also arm via the menu: press , enter a *User code* → *Arming & Disarming* → *Arm Away*.



Note

The technician can set the siren to sound beeps, to indicate on arming and disarming.

### 4.2 Arm in Home 1-4

The *Home 1-4* arming modes are used in defined parts of the premises - floors, separate rooms, perimeter detectors, etc. - when it is partially occupied, or during night time. As the alarm system is armed in one of these modes, only the *Home* mode zones (detectors) are armed, while all the other zones are not; triggering an armed zone sets off the alarm, while people can stay in the zones that are not armed at the same time.

The technician can define up to 4 *Home* modes.

1. To arm in *Home 1*, press and hold the  key, until the keypad sounds a long beep. To arm in *Home 1-4*, press and hold the 1-4 keys; the Home zones are immediately armed, while the *Exit Delay*<sup>7</sup> starts running, and the keypad displays a progress bar timer. During the delay you can stay in delayed zones, without setting off the alarm<sup>7</sup>. Entering an instant zone will set off the alarm.
2. If *One Key Arming* is not enabled (by the technician), press  and enter a user code.  
*User Menu* ► *Arming & Disarming* ► *Arm Home 1-4*
3. You can also arm via the menu: press , enter a *User code* → *Arming & Disarming* → *Arm in Home 1-4*.

<sup>7</sup> See the Glossary, on page 29.

## 4.3 Disarming

User Menu ► Arming & Disarming ► Disarming

To disarm the alarm system, enter an authorized user code; if the alarm system is not disarmed, the user may not have a disarming permission, or is out of its disarming window of time (see section 7.1.1, on page 16). If you enter the Master code, press *Arming & Disarming* → *Disarm*.

### 4.3.1 Disarming partitions

When partitions are in use (see *Partitioning*, on page 25), a user can only disarm the partitions he/she is allocated to. When disarming at a keypad, the user partitions will be disarmed only when the keypad is allocated to the same partitions (when disarming using the PIMALink app, there is no such limit).

For example: a user that is allocated to partitions no. 2, 3 and 4, disarms the alarm system in a keypad that is allocated to partitions no. 1, 4, and 6. As a result, only partition no. 4 will be disarmed, being the only partition that both the user and the keypad are allocated to.

## Chap. 5 Bypass Zones

Open zones - doors, windows, moving objects - must be closed, or you cannot arm the alarm system. When there is no other option, you can bypass the zone and arm the system. Bypassing is a one-time operation and time limited - A bypassed zone is automatically un-bypassed as the alarm system is disarmed and you will need to repeat it any time you want to arm, as long as the zone is at fault.



- **A bypassed zone does not trigger the alarm when opened, and can breach the security of the premises.**
- **Bypass a zone only when it cannot be closed. If the problem persists, consult a technician.**

### 5.1 How to bypass on-the-fly

To bypass a zone while arming the alarm system, do the following.

1. Enter user code to arm; if you enter the Master code, press *Arming & Disarming* → *Arm Away/ Home*.
2. The *Zone Bypass* menu is displayed - press ← to bypass the zone and scroll (press \* or #) to other open zones, if there are any. The exit delay starts running immediately and when elapsed, the system is armed.

### 5.2 How to bypass before arming

User Menu ► Bypass Zones

To bypass zones some time before arming, do as follows.

1. Press , enter a *User code* → *Bypass Zones*, and press ←.
2. Press # or \* and select the zone number.
3.  Bypassed: press ← to select and bypass the zone.
4. Repeat steps 3-2 with other open zone, if there are any.
5. Press ↻ to exit.



*Because of security considerations, bypassing a zone before arming is limited in time. Refer to the technician.*

# Chap. 6 Event Memory

The *Event Memory* displays the last 1024 system events, chronologically. You can scroll between the events by pressing the arrow keys, and see the details that follows.



Figure 2. The event memory screen

# Chap. 7 Users and Codes

Set the codes and definitions of the users of the alarm system, and system codes. All codes, except the *Short Code* are four to six digit long. See the *Code setting guidelines* on page 11.

The menu includes the sub-menus that follows.

1. ← Users: see the next sub-section.
2. Master Code: the Master user code
3. Quick arm code: a two-digit code, used for arming only. This code can be used by anyone who does not have a user code.
4. Duress code: see the *Glossary*, on page 29.
5. Home Auto.: a code for home automation systems<sup>8</sup>
6. ← Operation codes: see next page.

## 7.1.1 Users

User Menu ► Users and Codes ► Users

To scroll between users, press # or \*.

Parameter	Description
Code	A unique 4-6 digit user code
Name	User text, up to 16 characters.
Keyfob	<p>Enroll wireless key fobs or panic buttons (one per user). The key fob is used for arming and disarming, and activate devices. A wireless module is required; refer to the technician.</p> <ol style="list-style-type: none"> <li>1. Press * or # to select a user.</li> <li>2. ☉ Enrolled: indicates whether a key fob or a panic button is enrolled to the user.</li> <li>3. Enroll                             <ol style="list-style-type: none"> <li>a. Manual: use it only with PIMA peripherals.                                     <ul style="list-style-type: none"> <li>• Serial no.: enter the device's serial number.</li> </ul> </li> </ol> </li> </ol>

<sup>8</sup> Only systems that are approved by PIMA Electronic Systems.

Parameter	Description
	<ul style="list-style-type: none"> <li>• Enroll: press to enroll the device.</li> </ul>
	<p>b. Auto:</p> <ul style="list-style-type: none"> <li>• Status <ul style="list-style-type: none"> <li>○ Waiting: the system is waiting for a signal. Press one of the key fob's buttons, or the panic button for 5 seconds.</li> <li>○ Received: a signal was received. The keypad will sound beeps. If more than one device is received, press the right arrow key until the desired one is displayed.</li> </ul> </li> <li>• Serial no.: the selected device's number</li> <li>• Signal: the selected device's signal strength - <i>Strong, Good, or Poor</i>. If the signal is poor, change the location of the device.</li> <li>• Enroll: press to enroll the selected device.</li> </ul>
	<p>4. Delete</p> <ul style="list-style-type: none"> <li>• Delete: select a user (press # or *) and delete its device.</li> </ul>
↵ Disarming Window	<p>Set a daily window of time, only during which the user is allowed to disarm the alarm system. This is a security measure against unauthorized action.</p> <ol style="list-style-type: none"> <li>1) Set the <i>Start</i> and <i>End</i> times (the same for all the selected days).</li> <li>2) Days: select the days to apply the window.</li> </ol> <p>Example: Monday through Friday, 07:30-10:00. If the user will try to disarm the system anytime else, it will be rejected with <i>Access Denied!</i> message. However, anyone can arm the system at any time.</p>
↵ Permissions	<p>Define the special permissions of each user of the alarm system. A user that will try to enter a menu it is not permitted to, will be rejected with <i>Access Denied!</i> Message.</p> <p>The permissions are as follows: Disarm, Event Memory, Communication, Users and Codes, Time and Date, Bypass Zones, Auto Arming, Technician Permit, Control Remotely, Use All Keypads.</p>
↵ Partitions	<p>If partitions are in use<sup>9</sup>, assign each user with one or more partitions - he/she will only be able to view and arm/disarm these partitions.</p> <p>Select the assigned partitions: a selected number (partition) is steady on. Make sure the un-assigned partitions are flashing.</p>
↵ Reset User	<p>Delete all the user definitions, including the password.</p>

## Operation codes

**FORCE** offers 8 *Operation codes*, for activating different devices such as electric gates, garage shutter doors, and floodlights. You activate the peripheral (switch on/off, open/close) by entering an activation code (toggle) in a keypad, or in the PIMALink app. Refer to the technician to use these codes.

*Operation codes* are subject to keypad and user partitioning (where relevant).

- 1) Press # or \* to select a code.
- 2) Press ←, enter a 4-6 digit code and press → to save.

<sup>9</sup> See Chap. 10, on page 21.

# Chap. 8 Communication

The sub-menus in this menu are as follows:

- 1) ↵ Contacts
- 2) ↵ PIMA Cloud
- 3) ↵ Phone Notifications
- 4) ↵ Remote Service
- 5) ↵ CMS Registration

## 8.1 Contacts

User Menu ► Communication ► Contacts

Contacts receive notifications on alarms and other events. Here you set which contact will receive what notification and in what medium. Contacts are allocated to partitions the same as system users (where relevant).

Note, that contacts of the PIMALink 3.0 app are different from the **FORCE's** contacts, and that each contact can set its notifications in the app.

- Press \* or # to select a contact.

Parameter	Description
Phone	The phone no. of the contact. If <b>FORCE</b> is connected to a phone line over a phone system, make sure the technician sets it accordingly.
Name	User-defines text, up to 16 characters.
↵ Comm. Paths	See below.
↵ Notifications	Select the events that will be notified to the contacts. The options are: Alarms from <i>Burglary, Panic, Fire, Duress, Medical</i> , and <i>Tamper/Anti-Mask</i> zones (detectors), and <i>Custom Zone 1-5, Faults, Invalid Code<sup>10</sup></i> , and <i>Arming/Disarming</i> events.  The control panel notifies, by sounding an alarm sound over the phone, or sending a text message.
↵ Partitions	Select the partitions that will report the contact on events (where relevant).

### 8.1.1 Communication and Backup Paths

User Menu ► Communication ► Contacts ► Comm. Paths

Set the communication path/s to the contact, and the backup path/s, if the main path is at fault.

- Press \* or # to select a contact.
- Comm. Paths 1-2: select the communication path/s of the contact:
  - *Over Landline*: notifications will be sent over landline telephone (**FORCE Lite**: unavailable).
  - *Over Cellular*: notifications will be sent over cellular phone<sup>11</sup>.
  - *Over SMS*: notifications will be sent as text messages over cellular phone<sup>11</sup>.
- ↵ Backup Paths: select a path different from the main path, as a backup. For example, if you have selected *Over Cellular* as the main path, you can select *Over Landline* as a backup. The

<sup>10</sup> Exceeding the programmed limit of keystrokes, when trying to enter any code.

<sup>11</sup> Requires a cellular expander.

control panel will first try to notify the contact through the main path, and will use the backup path if it fails.

### 8.1.2 Communication Test

→ Path: select a contact's path to be tested.

← Press to Start: press and check that a notification is received by the contact.

## 8.2 PIMA Cloud

User Menu ► Communication ► PIMA Cloud

To use the PIMAlink 3.0 app to control the alarm system remotely, you will need to pair it with the cloud, receive a pairing code and use it for pairing the mobile phones of whoever will use the application. The pairing process is short. Before you pair the alarm system, make sure all the app users download and install it on their phones.

The pairing code must be used within 10 minutes, or you will have to repeat the process and receive a new code (for mobile phones that have not been paired).

- 1) ← Pair to PIMAlink: press and wait (shortly) for the code to appear on the screen. Immediately enter the code in the pairing screen of the PIMAlink app, in every phone.
- 2) ← Unpair: press and disconnect **FORCE** and all your mobile phones from the cloud.

## 8.3 Phone Notifications

User Menu ► Communication ► Phone Notifications

When the alarm is set off, **FORCE** calls the contact that is set to receive notifications, and sounds an alarm sound over the phone.

Parameter	Description	Default	Range (sec)
Alarm Sound	The length of the alarm sound	30 sec	5-120
Repeat Message	No. of times to redial and sound the notification	2	1-8

## 8.4 Remote Service

User Menu ► Communication ► Remote Service

Use the *Remote Service* menu when the service technician or CMS need to connect to the alarm system remotely. Go directly to this menu by pressing and holding key '6' on the main menu<sup>12</sup>.



- **"Remote Service" and "CMS Registration" (next) allow connecting and controlling the alarm system. Only allow authorized technician to use these options!**
- **The CMS/Technician can connect to the system remotely only using a remote connection code.**

Parameter	Description
← Allow Access Now	When you press this menu, you allow a (authorized) technician to connect to the alarm system and control it remotely.
← Over Network	1) IP/URL: enter the data in the form of IP:Port (no space) when asked by a (authorized) technician.
← Over Cellular	

<sup>12</sup> System version 1.2 and higher

Parameter	Description
	2) Connect: the alarm system allows the technician to connect remotely with a special software.

## 8.5 CMS Registration

In this menu, **FORCE** is registered at the CMS (where relevant) via network.

## Chap. 9 System Options

The *System Options* are as follows:

- 1) Override Faults: see below.
- 2) Zone Information: zone names, location, and status: see below.
- 3) Armed Partitions: see next page.
- 4) Time and Date: see page 22.
- 5) Chime Zones: see page 22.
- 6) Auto Arming: see page 23.
- 7) Reset Smoke Detector: see page 23.
- 8) Technician Permit: see page 24.
- 9) System Information: see page 24.

### 9.1 Override Faults

*User Menu* ► *System Options* ► *Override Faults*

As with open zones, you cannot arm the alarm system if a fault exists, and it must be fixed. Only when there is no other option it can be overridden<sup>13</sup>. Overriding is valid for one arming session and needs to be repeated every time you want to arm, as long as the fault exists.



**Faults can breach the security of your alarm system and may also indicate on burglary setup. Use the fault overriding option only when there is no other option, fix the fault immediately or call for service technician.**

To override a fault before or while you arm the alarm system, do as follows:

1. Enter the *Master* code.
2. Scroll to *System Options* and press ←.
3. Press *Override Faults* - the current faults are displayed.
4. ⦿ Press ← to select the displayed faults.
5. Press ↻ to exit. You can now arm the alarm system.

### 9.2 Zone Information

*User Menu* ► *System Options* ► *Zone Information*

View information about the zones (detectors) and their status - open or closed, alarming, and more, detailed below. If partitions are in use (see the *Glossary*, on page 29), only those allocated with both the keypad and the user will be displayed.

Press and hold the ↻ key to exit. Press \* or # to scroll between zones.

- 1) ↵ Name & Location: zone name and location. This information is set by the technician.
- 2) Zone Status: the status of each defined zone is represented by letters, listed in the table below.

<sup>13</sup> If a fault cannot be overridden, call a service technician.

Zone	Description
No., steady on	Closed zone (normal mode)
No., flashing	Open zone - you must close or bypass to arm.
No. missing	The zone is permanently disabled by the technician
A	The zone is alarming now, or was violated when the alarm system was armed.
B	The zone has been bypassed by a user, or during auto arming.
C	Chime zone (door or window)
F	Zone fault. May indicate on burglary setup - call service immediately!
M	Anti-mask alarm; triggered when a wireless anti-mask detector is blocked (masked) with a material such as paper, tape, film, or spray. The zone is alarming now, or was violated when the alarm system was armed. Remove the blocking material or call service immediately - may indicate on burglary setup!
O	Armed zone (24H zone, or all the allocated partitions of the zone are armed)
T	Test mode (set by the technician. The zone will not trigger the alarm). The zone will be reinstated automatically after few days.

## 9.3 Armed Partitions

User Menu ► System Options ► Armed Partitions

View the numbers and names of the partitions that are currently armed. Only the keypad's allocated partitions are displayed.

## 9.4 Time and Date

User Menu ► System Options ► Date and Time

The system time must be set after a prolonged power failure (when the backup battery is discharged). If the alarm system is connected to PIMA cloud, time can be automatically updated (see below). Make sure system time is always accurate: *Auto-Arming* and *Disarming Window of Time* are time-based, and so is the event memory.

Parameter	Description
Time	Set the current time in hh:mm
Date	Set the current date in dd:MM
Year	Set the current year in 2 digits
☉ Cloud	If the alarm system is paired with the PIMAlink cloud, and the <i>Time Zone</i> is set auto-update in the application, time will automatically be updated by the cloud.
Day	Set automatically

## 9.5 Chime Zones

User Menu ► System Options ► Chime Zones

Chime is a feature, in which the keypad buzzer sounds a series of beeps when a protected door or window is opened. The chime is active only while the alarm system is disarmed.

- 1) ☉ Chime Active/Inactive: globally set if the chime is active or not.
- 2) ↵ Set per Zone: press # or \* to select a zone; press ← to activate the chime.

## 9.6 Auto Arming

User Menu ► System Options ► Auto Arming

The alarm system can be auto armed without the need to enter any code. Auto arming can be in *Away* or *Home* modes. If partitions are in use, each partition can be armed in a different time and have a separate no-movement period.

There are two auto-arming options:

- Timed: daily, at a certain time.
- No Movement: when no movement is detected in any of the detectors for a given period, probably because the premises is vacant and the alarm system was not armed<sup>14</sup>.

When the auto-arming starts, the keypad buzzer sounds a series of beeps for a period of 45 seconds, after which the exit delay runs and the system is armed. If a user stops the process by entering a user code, **FORCE** will try to re-arm itself, according to the parameters you set in this menu.

The technician can set the alarm system to bypass open zones on auto-arming (they will be reinstated when the system is disarmed).

1) Timed: select a partition (or stay in Partition 1 for no-partition system):

Definition	Description
↵ Daily Hour	For every day of the week, set the time of the day for auto-arming.
Retry Interval	If a user stops the auto-arming process by entering a user code, set an interval in hours and minutes for arming retries. <b>FORCE</b> will try to re-arm itself according to the interval and the retry period (next).
→ Retry Period	If a user stops the auto-arming process by entering a user code, set the period in hours (1-12) for the <b>FORCE</b> to re-arm itself. If you do not set any period, <b>FORCE</b> will try to re-arm itself until midnight of the same day, in accordance with the previous <b>Retry Interval</b> .
Arming Mode	Select in which arming mode <b>FORCE</b> will be auto-armed: <i>Away</i> or <i>Home</i> 1-4.

2) ↵ No-movement:

- Select a partition (or stay in Partition 1 for no-partition system) and set the time in minutes (up to 255), that if no detector detects any movement at all, the auto-arming process will start.
  - Period: no-movement time in minutes (up to 255).
  - Arming Mode: see above.
- 3) ⊙ Timed-All Partitions: apply the definitions of partition #1 to all partitions.
- 4) ⊙ No-Movement-All Partitions: apply the definitions of partition #1 to all partitions.

## 9.7 Reset Smoke Detector

User Menu ► System Options ► Reset Smoke Detector

When a smoke detector detects smoke, it remains in detection mode and cannot reset itself. If the detector was activated because of the presence of smoke, read its instructions guide. If there was no smoke, press here to reset the detector.

<sup>14</sup> Someone may be sleeping also.

## 9.8 Technician Permit

*User Menu ▶ System Options ▶ Technician Permit*

Press this parameter according to the options that follow.

1. During the installation of the alarm system, when the technician needs to enter the *Technician menu*. In this way you, as the owner give the technician a permission to change parameters and definitions. From now on, the technician will not need your approval to enter its menu.
2. **FORCE** allows you to be serviced by several CMS's. The settings of each CMS are set separately and are protected by a password. Only the Master technician can enter the Technician menu without your approval (except for the first time) - other technicians will have to ask you to press *Technician Permit* every time they want to service the **FORCE** (and will be able to view and change only the parameters of their CMS).
3. In some cases, when the technician needs to connect remotely via PIMA cloud.

## 9.9 System Information

*User Menu ▶ System Options ▶ System Information*

View information about the control panel and the peripherals of your alarm system. The *System Reboot* menu is to be used when you are asked by a certified technician.

# Chap. 10 Partitioning

A partition is made of some zones. When the premises is large and has floors, wings, shops or so, it can be divided into independent groups of zones called partitions. This lets you operate each partition separately from other partitions, and have separate users.

When using partitions, users and keypads are also partitioned, meaning that a user can only arm and disarm the partitions he/she and the keypad are allocated to. Users and keypads can be allocated to one or more partition.

Zone and keypad allocation is done by the technician. User allocation is done in the definitions of each user.

You can set up to 16 partitions. The max number of keypads is also 16.

## 10.1 Optional uses

### Example A

A two-floor house with a single keypad, each floor is defined as a separate partition.

In this example, the zones on the first floor are allocated to partition 1 and those on the second floor to partition 2. The keypad is allocated to the two partitions and so are the users, who can therefore arm and disarm the two floors (partitions).



Figure 3. Partitions, example A

### Example B

A two-floor house, each floor is defined as a separate partition and has a keypad.

In this example, the same as in the previous example, the zones on the first floor are allocated to partition 1, and those on the second floor to partition 2. However, while



Figure 4. Partitions, example B

keypad 1 is allocated only to partition 1, keypad 2 is allocated to the two partitions. While all the users are allocated to partition 1, only some users are allocated to partition 2. The result is that all the users can arm and disarm partition 1 from keypad 1, and some users can arm the two partitions from keypad 2.

### Example C

A commercial center with multiple shops, each is defined a separate partition and has its own keypad. In this example, the partitions match the shops, each with its own detectors and users.

If the center has a lobby (or an entrance door) that serves all

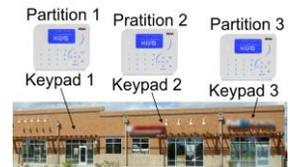


Figure 5. Partitions, example C

the shops, its keypad can be allocated to all the partitions (shops) and allow some users (such as the shop owners), to view the status of the partitions.

If a detector (such as the door magnet) in this area is allocated to all the partitions, it will arm only when all the partitions will be armed.

## 10.2 How to clean the LCD screen

To keep your keypad screen clean and without scratches, follow the next instructions:

- When you clean your monitor, do not press down on the screen.
- Do not spray any kind of liquid directly onto the screen. Only use a cleaning solution specifically made for cleaning LCD screens.
- Do not use paper towels or abrasive pads.
- Gently wipe the surface using a clean, dry microfiber cloth.



# Appendix A Troubleshooting Faults

The **FORCE Series** alarm systems are constantly monitoring the status of the control panel, the detectors, and the peripherals. When a fault occurs, this is what happens:

- The fault LED  starts flashing
- The keypad buzzer starts sounding beeps. To silence it, press and hold the  key.
- A description of the fault is displayed
- The fault is logged in the event memory
- **FORCE** reports the CMS (where relevant) and the contacts, and may activate peripherals (set by the technician).



***Some faults may indicate on burglary setup. Consider consulting with your service technician.***

Below is the description of common faults.

Fault	Description
AC Power	Power outage. As long as the backup battery has enough power, the alarm system will function normally.
Low Battery	The backup battery is draining. Either there is a long power outage, or the battery is exhausted and needs to be replaced.
	 <p><b><i>An exhausted battery will not backup your alarm system if AC power is lost!</i></b></p>
Tamper 1-2, Expander/Keypad tamper	<ul style="list-style-type: none"> <li>• Tamper 1: the tamper switch of the box of the control panel is at fault or open. Check that the box is closed.</li> <li>• Tamper 2, Expander Tamper, Keypad Tamper: the tamper switch of one of the peripherals<sup>15</sup> is at fault or open.</li> </ul>
Auxiliary Voltage	May indicate on burglary setup.
Telephone-DC, Dial Tone ( <b>FORCE Lite</b> : unavailable)	The telephone line is disconnected or at fault. If other telephone sets are connected to the <b>FORCE</b> , check them too.
Low DC	Internal power fault
Local/Zone/Outputs Expander (various faults)	Power or communication fault in a zone expander (some detectors) or Outputs expander (some peripherals).
Keypad (various faults)	Power or communication fault in a keypad
CMS	Communication fault with the monitoring station
Contact (various faults)	Notification error
Modem (various faults)	Communication fault
SIM (various faults)	SIM card fault (cellular add-on)

<sup>15</sup> Depending on the setting of the technician.

<b>Fault</b>	<b>Description</b>
Network	Local network (LAN) connection fault
Anti-mask	Anti-mask detector at fault or open box
Invalid Code	Code keystrokes exceeded limit (keypad is locked out for a period set by the technician)
Internal/External Siren	Fault or open tamper switch
System Time Not Set	Occurs after a prolonged power outage, when the back battery is exhausted.

**Installer details:**

Name \_\_\_\_\_ Mobile: \_\_\_\_\_

Company: \_\_\_\_\_

Tel.: \_\_\_\_\_

Date of installation: \_\_\_\_\_

Service expiration date: \_\_\_\_\_

## Appendix B Glossary

- **Arm Away**

When arming in Away mode all the detectors are armed and will set off the alarm if any movement (or whatever the detector is design to detect) is detected.

When entering a user code, the exit delay that allows you to leave the premises without triggering a detector, starts. When the delay time elapses, all the zones are armed.

The **FORCE** can be armed only if the message "Ready to Arm" is displayed and the green  LED illuminates. **FORCE** is ready to armed, when there are no *Open Zones* (detectors) or *Faults*. A zone is "Open" when it is in detection or alarm modes. To close (reinstate) a zone, you need to remove the cause for the detection - moving objects, open protected door, etc. **FORCE** cannot be armed if there are open zones.

Existing faults also prevent arming, but some faults can be overridden in a special menu<sup>16</sup>. To override faults before arming the **FORCE**, go to *User Menu* → *System Options* → *Overriding Faults*, select the fault and exit the menu. Overriding faults is a one-time operation and needs to be repeated every time you want to arm the alarm system. Call service if the fault cannot be fixed.

- **Arm Home**

When arming **FORCE** to a Home mode, only some detectors (zones) are armed, while some are not. This mode is used for arming defined areas like floors, perimeter detectors, shops, etc. It allows you to be in areas that are not armed, while entering Home armed zones will trigger the alarm. The technician can set up to four Home modes (areas).

- **Backup battery**

The backup battery enables the alarm system to continually safeguard the premises for a limited time, at AC power fault. Cutting power cords is common among burglars, and the backup battery ensures that the alarm system will continue to protect the premises. When a "Low Battery" message appears with no previous power fault, replace the battery.

- **Chime and chime zones**

Chime is a feature by which the alarm system supervises doors and windows, and sounds a series of beeps any time one of these is opened. The chime is active only when the alarm system is disarmed. The chime feature is useful with toddlers and in shops, but also when door or window are away from you.

The technician, together with you, define the chime zones that will trigger the keypad buzzer when opened.

- **Duress code**

A code used when a user is forced to disarm the alarm system. When this code is entered, the alarm system is disarmed, but also sends a silent distress signal to the CMS (where relevant) and the contacts, without giving any indication to that.

Tip: to remember the code easily, use the Master (or user) code, but switch around the last two digits. For example, if the original code is 280961, set the Duress code to 280916

- **Entry and exit delays**

After arming or disarming the alarm system, the exit and entry delays give you the needed time to exit or enter the premises without triggering the alarm, by crossing only delayed zone (set by the technician). These zones will not set off the alarm as long as the delay timer is in progress (but will if are still open when the delay elapses).

<sup>16</sup> The technician sets which faults you can override and which you cannot.

- **Partitions**

Partitions allow dividing the premises into separate areas, with detectors, keypads, and users for each partition. Users can be allocated to one or more partitions, so they can arm and disarm only these partitions. Keypads are also allocated to partitions.

Normally, a partition can be a house floor, a shop, a perimeter zone, etc. The technician defines the zones and keypads partition allocation, while the Master user defines the users' allocation.

- **Zone**

A zone is an input of the alarm system, to which one or more detectors are connected and monitored. Each zone covers a defined area in the premises. The alarm system is made of zones, each triggers the alarm when it detects a movement or other changes. There are various zone types, such as Burglary, Panic, Medical, Flood, etc.

A zone is normally "closed", and is "open" when in detection mode. The detection mode can be easily identified, by passing near the detector - a red LED illuminates as an indication.

Immediate zones triggers the alarm as they are opened, while delayed zones only triggers the alarm when a delay expires. See "Exit and entry delays".

- **Zone Bypass**

Zones (detectors) can be temporarily bypassed, so when the alarm system is armed, they stay in "normal" mode. This feature is used when the detector is at fault and it is valid for one-time arming only.

# Appendix C Zone Number and Location

Zone	Name/Location	Zone	Name/Location	Zone	Name/Location
1		49		97	
2		50		98	
3		51		99	
4		52		100	
5		53		101	
6		54		102	
7		55		103	
8		56		104	
9		57		105	
10		58		106	
11		59		107	
12		60		108	
13		61		109	
14		62		110	
15		63		111	
16		64		112	
17		65		113	
18		66		114	
19		67		115	
20		68		116	
21		69		117	
22		70		118	
23		71		119	
24		72		120	
25		73		121	
26		74		122	
27		75		123	
28		76		124	
29		77		125	
30		78		126	
31		79		127	
32		80		128	
33		81		129	
34		82		130	
35		83		131	
36		84		132	
37		85		133	
38		86		134	
39		87		135	
40		88		136	
41		89		137	
42		90		138	
43		91		139	
44		92		140	
45		93		141	
46		94		142	
47		95		143	
48		96		144	

## Limited Warranty

PIMA Electronic Systems Ltd. does not represent that its Product may not be compromised and/or circumvented, or that the Product will prevent any death, personal and/or bodily injury and/or damage to property resulting from burglary, robbery, fire or otherwise, or that the Product will in all cases provide adequate warning or protection. The User understands that a properly installed and maintained equipment may only reduce the risk of events such as burglary, robbery, and fire without warning, but it is not insurance or a guarantee that such will not occur or that there will be no death, personal damage and/or damage to property as a result.

PIMA Electronic Systems Ltd. shall have no liability for any death, personal and/or bodily injury and/or damage to property or other loss whether direct, indirect, incidental, consequential or otherwise, based on a claim that the Product failed to function.

Please refer to a separate warranty statement found on PIMA website at: [www.pima-alarms.com/help-support/pima-product-warranty/](http://www.pima-alarms.com/help-support/pima-product-warranty/)

Warning: The user should follow the installation and operation instructions and among other things test the Product and the whole system at least once a week. For various reasons, including, but not limited to, changes in environment conditions, electric or electronic disruptions and tampering, the Product may not perform as expected. The user is advised to take all necessary precautions for his/her safety and the protection of his/her property.

This document may not be duplicated, circulated, altered, modified, translated, reduced to any form or otherwise changed unless PIMA's prior written consent is granted.

All efforts have been made to ensure that the content of this manual is accurate. Pima retains the right to modify this manual or any part thereof, from time to time, without serving any prior notice of such modification.

Please read this manual in its entirety before attempting to program or operate your system. Should you misunderstand any part of this guide, please contact the supplier or installer of this system.

Copyright © 2019 by PIMA Electronic Systems Ltd. All rights reserved. E&OE



Manufactured by:

PIMA Electronic Systems Ltd.

[www.pima-alarms.com](http://www.pima-alarms.com)

5 Hatzoref Street, Holon 5885633, ISRAEL

Tel: +972.3.6506414

Fax: +972.3.5500442

Email: [support@pima-alarms.com](mailto:support@pima-alarms.com)

P/N: 4410460



Revision: XX en, B3, Dec 2019