VPKEYPADS

USER'S MANUAL

2023

PTI SECURITY SYSTEMS

VER 11042025

VPKEYPADS

USER'S MANUAL

TABLE OF CONTENTS

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio TV technician for help.
- This Class A digital apparatus complies with Canadian ICES-003 - Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

TECHNICAL SPECIFICATIONS

Power Supply:

Voltage:	12 – 18 VDC or AC
Current Consumption:	300mA Maximum

Relay Specifications:

Maximum Switching Voltage*:	30 VAC / 24VDC
Maximum Switching Current*:	1A (NO / NC)

* Resistive Load

Environmental:

Ambient Temperature:	-40°C to +85°C (-40°F to 185°F)
Ambient Humidity:	0 to 85% (non-condensing)

WARNINGS

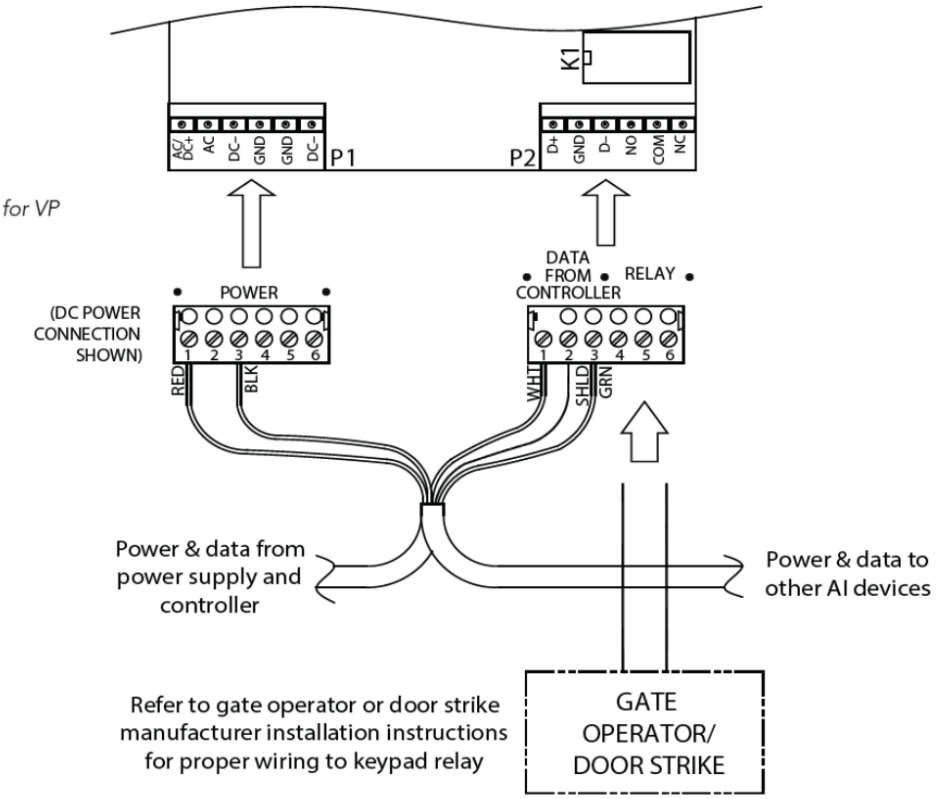
- This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference in which case the user, at his/her own expense, will be required to take whatever measures may be required to correct the interference.

- The system will not operate properly if the voltage is below 12VDC. Extreme care should be taken when choosing a power supply voltage and current rating. Long distance runs may require a remote power supply to be installed in line with an RB5 relay to ensure proper operation.

- The User should follow all installation, operation, and maintenance instructions. The User is strongly advised to conduct product and systems tests at least once each week. Changes in environmental conditions, electric or electronic disruptions and tampering may cause the product to not perform as expected.

- PTI Security Systems warrants its Product to the User. The User is responsible for exercising all due prudence and taking necessary precautions for the safety and protection of lives and property wherever PTI Security Systems products are installed. PTI Security Systems does not authorize the use of its products in applications affecting life safety.

VP ACCESS DEVICE INSTALLATION & OPERATOR MANUAL
› INSTALLATION INSTRUCTIONS



Drawing 5: Wiring for VP keypad

Never install any other devices in the same wire run as the APEX

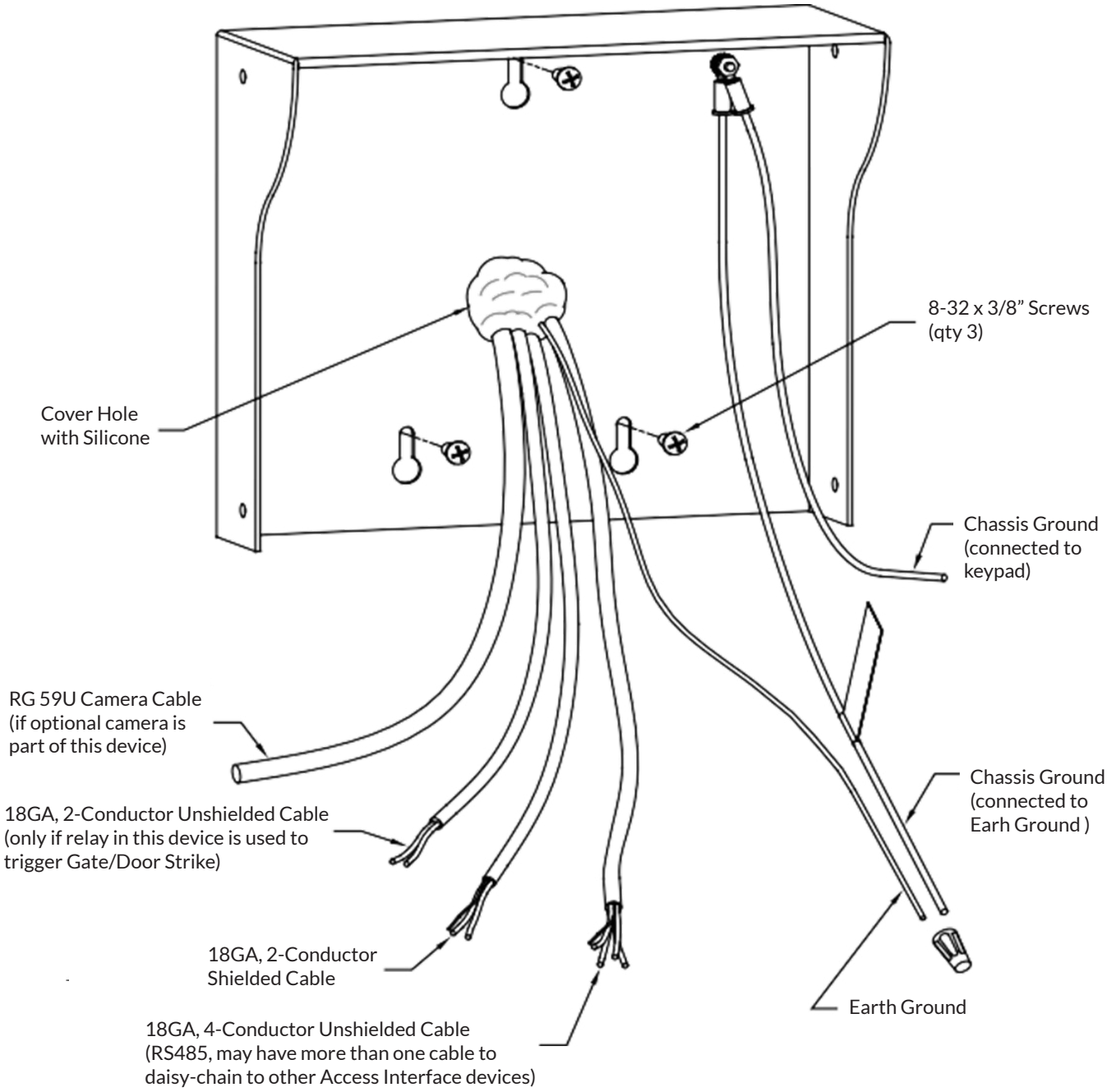
PTI recommends that power and data communication be run through a single 18 AWG, 4-conductor shielded cable. Some installations will require larger gauge wire. See “Wiring for VP keypad” (above) for details on connecting the wiringto the VP device.

The system will not operate properly if the voltage is below 12VDC. Extreme care should be taken when choosing a power supply voltage and current rating. Long distance runs may requre a remote power supply.

1. Open the device by removing the four stainless steel buttonhead machine screws on the side of the keypad case using the security hex key provided with the unit.

2. Mount the back plate to the desired keypad location using thethree-keyed holes. Seal around the back of each screw hole and around the back of the wire hole with an outdoor silicone sealant.

Drawing 7: Wires for VP Keypad



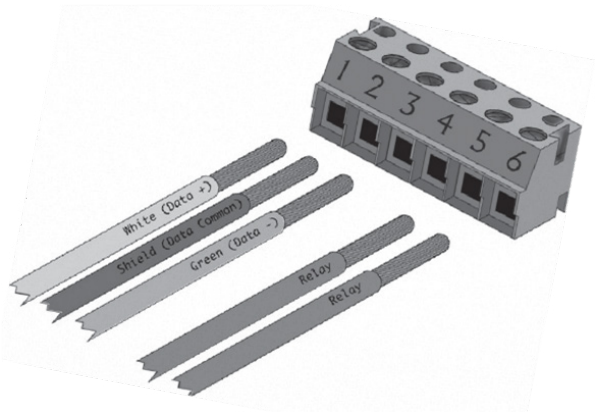
3. Pull the necessary wires through the wire hole on the back of the housing. Allow an extra 1 foot of wire to remain inside the housing. Each keypad should have the following wires as shown in "Drawing 7: Wires for the VP keypad" (above).

Drawing 8: Terminal Block P1 Wiring (Left)

1. Red DC + *
2. If using AC power, place the AC wires in slots 1 and 2. We recommend 12-18 VDC, but 12-18 VAC can be used.
3. Black DC -
4.
5.
6. Earth Ground if applicable

   * If using AC Power, place the AC wires in slots 1 & 2. We recommend 12-18 VDC but 12-18 VAC can be used.

4. For Terminal Block P1 wiring" (drawing 8 - above): Insert both red wires (coming in from the power supply and going out to the next AI device) into terminal slot 1 on the first terminal block (P1).



Drawing 9: Terminal Block P1 Wiring (Left)

1. White Data +
2. Shield *
3. Green Data -
4. Relay Normally Open Wire
5. Relay Common Wire

* Shield wire should be insulated with heat shrink or electrical tape

6. Ensure that both wires are seated all the way inside the slot. Use a flathead precision screwdriver to tighten down the terminal screw. Verify the terminal slot has tightened down on the copper wire and not on the rubber insulation.

7. Insert both black wires into terminal slot 3 on P1. Repeat this process with each of the remaining wire connections, placing them as shown in "Drawing 8: Terminal block P1 wiring" (above).

8. For Terminal block P2 “Drawing 9: Terminal block P2 wiring” (above). If a gate operator or door strike is being triggered directly from this keypad,use pins 4, 5, and 6 for the relay and the wires will connect to two of these three pins.

9. Refer to the gate or door strike manufacturer’s instructions to determine whether it needs to be connected to the normally open and common or to the normally closed and common.
   - An earth ground must be supplied either:
     - Through the mounting of the keypad to a conductive surface with an earth ground.
     - Using the earth ground wire and a proper earth ground connection.

10. The earth ground wire is connected in locations where the keypad is mounted on a wall that is wood, stone, or other nonconductive material.

11. To connect the ground wire, run a copper wire from a grounded water pipe or from a copper rod in the ground to the keypad and connect it to the green earth ground wire using a wire nut. Set Jumper J1 to NORMAL.

12. Connect any additional features such as an intercom, gate operator, or pinhole camera. The VP keypad may have additional features and functions. They need to be connected after steps 1 - 12.

CONNECTING THE INTERCOM

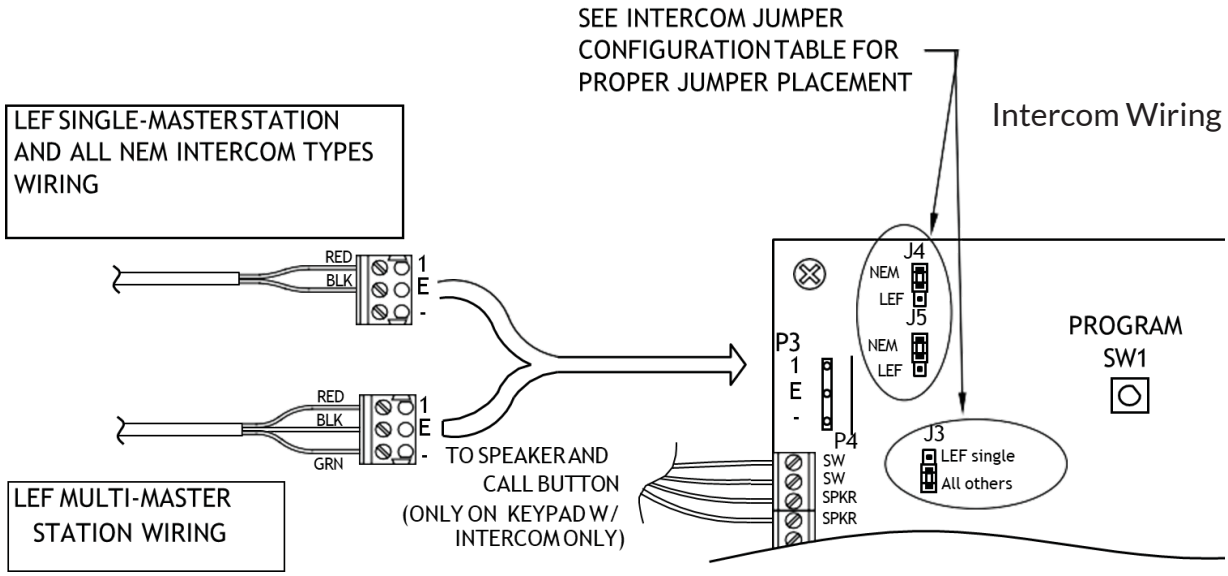
Connect the wires to terminal block P3 in the upper left corner of the board as shown in "Drawing 14: Intercom wiring and jumper configuration" (below). The connection and jumper settings will vary depending on whether the intercom is LEF Single Master Station, LEF Multiple Master Station, or NEM type intercom. Refer to the manufacturer's instructions.

The VP with Intercom can be connected to an Aiphone LEF or Aiphone NEM intercom.

- The intercom wiring must be separate from all other wiring to either keypad. Use 18 AWG, 2 or 3-conductor shielded cables for the intercom depending on the type of intercom being used. Refer to the Aiphone specifications for more detail.

- The intercom type jumpers on either keypad circuit board must be set to match the type of intercom that you are using.

INTERCOM JUMPER: CONFIGURATION TABLE (Drawing 14: Intercom Jumper Settings)			
INTERCOM TYPE	VP JUMPER CONFIGURATION		
NEM (ALL)	J4 NEM LEF	J5 NEM LEF	J3 LEF Single All Others
LEF (ALL BUT SINGLE MASTER STATION)	J4 NEM LEF	J5 NEM LEF	J3 LEF Single All Others
LEF (SINGLE MASTER STATION)	J4 NEM LEF	J5 NEM LEF	J3 LEF Single All Others



GATE OPERATORS

- Most electric gate operators require a 'normally open' contact (pins 4 & 5). Some electric door strikes require a 'normally closed' contact (pins 5 & 6).
- If door strikes are used it is recommended that they be 12V DC.
- Install a shunting diode across the solenoid to prevent ground spikes from disrupting the keypad communication.

Do not place a diode across AC strikes as it will short out the power supply for the strike.

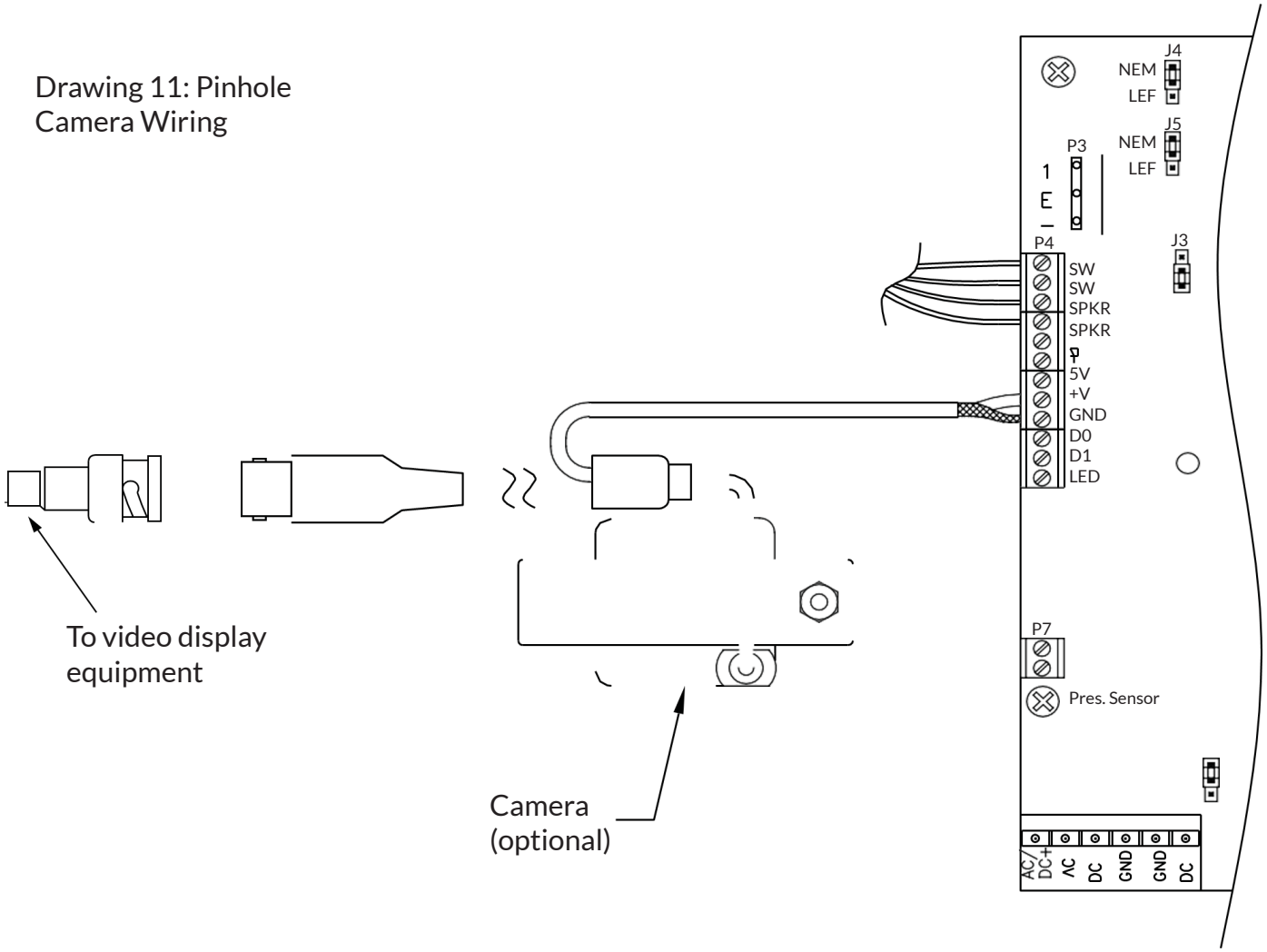
- The VP has a presence sensor function that allows the keypad to be connected to a loop detector, or pressure mat requiring a 'presence' in order to use the keypad.
- This function is often used in connection with a gate operator and loop detector. Loop detector output wires are connected to terminal block P7 in the keypad. The keypad is then programmed with the Presence Required 'ON'. see 'Setup Functions' for information on setting up this feature.

Check the voltage level. Relay voltage must not exceed 30 volts. Wiring the relay to the operating device introduces the operating device control voltage into the keypad housing.

PINHOLE CAMERA

- Connect the video signal cable using RG59U cable and BNC type connectors. The keypad circuit board provides pinhole camera power.
- In some situations, it may be necessary to install a video amplifier or a video isolator depending on how the video system is installed.
- See Drawing 11 on page 10 for wiring information.

Drawing 11: Pinhole Camera Wiring



› TESTING THE KEYPAD

1. Test the display by supplying power to the keypad.

   - The default date and time should appear on the display. If the controller is configured correctly, it will update the date and time on the keypad display automatically.

2. To verify that the backlight is working:

   - Press the * key. The backlight should light up and then the display will read **Please Enter Access Code**.

   - If no keys are pressed within 10 seconds, the display will return to the Date/Time and the backlight will shut off.

3. To test touch pad operation:

   - Press the * key. When the display shows “Please Enter Access Code, press 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Each digit should appear on the display as it is pressed (if Secure Entry is enabled an X for each digit appears)

   - Press the # key to transmit the code to the controller. The display will show **Please Wait** until a response is returned from the controller. If the keypad is communicating with the controller, the display will show either **Entry Granted** or another corresponding message.

4. Test for communications with the controller

   - Power up the controller. The date and time at the controller will automatically update on the keypad and appear in the display. This verifies communications from the controller to the keypad.

   - Test communications from the keypad to the controller by entering an access code into the keypad and pressing the # key.

5. If the keypad display responds with anything other than **Please Wait** before returning to the date and time, the keypad has successfully communicated with the controller.

6. If the keypad display **Please Wait** then returns to 12:00 (the power-up default time), recheck the wiring, baud rate settings, and address settings. Also ensure that the controller is set to the correct number of remotes.

› SETUP FUNCTIONS

To enter **Setup Mode**:

1. Press the *, 0 and # simultaneously
2. Enter the factory password 8898
3. Press the # key

In the event the password is changed and then forgotten, you can disconnect power from the keypad and then hold the program button while reconnecting power. This will bypass the password prompt and enter the setup mode directly. When using this method, you will also be prompted to **Restore Factory Defaults**.

> √ **It is highly recommended that the factory password be changed after installation for security reasons.**

Select **YES** to restore all default factory settings including the password.

Press the # key to advance through each setup parameter.

- A parameter is automatically saved when you press # and move to the next parameter.
- A time-out is built into the system that will exit Setup mode if there is no input on the keypad for an extended period of time
- If a time-out occurs, the current parameter WILL NOT be saved.

Numeric values are entered directly into the unit using the number keys. When an option is presented, use the * key to scroll through the available settings.

There are two (2) ways to exit Setup mode:

- Press the 7, 8, and 9 keys simultaneously
- Go through all of the setup functions

Setup Parameters in the Order Displayed by the VP Access Device:

KEYPAD DISPLAY	EXPLANATION
Restore Defaults *=Yes #=No	This prompt only occurs if the program button is held while powering the device. Pressing the * key to select YES will restore all of the factory defaults. WARNING: This will overwrite all setup parameters including the setup password.
Setup Menus *=change #=next	Identifies how to use the keys: the * key is used to change a parameter and the # key is the enter key to move to the next menu.
Current Add: 001 New (1-127):	Polling address used by the controller. **The number 22 cannot be used.** Each device connected to the controller must have a unique address. Factory default is 1.
* to Change Baud: 9600	The controller communications baud rate. Scroll through the list of available rates by pressing the * key. Factory default is 9600.

At this point, the basic parameters required for operation have been entered. If no other options are active or required, you can exit the setup mode. Following are optional parameters to customize the feel of the site.

› OPTIONAL SETUP FUNCTIONS

KEYPAD DISPLAY	EXPLANATION
Setup Password * =Change #=No	Change the setup password from the factory default of 8898. New passwords must be entered twice for verification before it changes.
Tamper Switch: Enabled	Controls the use of the tamper sensor. If enabled, the keypad will not function and an alarm will occur from the controller if the unit is tampered with. Factory default is Enabled.
Secure Entry: Disabled	Controls the characters displayed during code entry. When set to Enabled, the display will show only an X for each key pressed. When set to Disabled, the numbers pressed will be echoed to the display. Factory default is Disabled.
Beep with Key: Enabled	Controls the internal buzzer used to provide audio feedback for any key press. When set to Enabled, the buzzer will produce a short beep when a key is depressed. When set to Disabled, the buzzer will not sound with key presses. Factory default is Enabled.
Beep with Access: Enabled	Causes the internal buzzer to sound when an access is granted. A valid access will cause the buzzer to sound one long beep. All other attempts will cause the buzzer to sound four short beeps. Factory default is Enabled.
Beep with Alarm: Disabled	Controls the internal buzzer used to provide audible feedback when a system alarm occurs. When set to Enabled, the internal buzzer will sound whenever an alarm occurs and remain on until the alarm resets from the controller. When set to Disabled, the internal alarm buzzer will not sound with an alarm event. Factory default is Disabled.
Language XX.XX: English	Language display for user messages. Options are English, French, Italian, German, Danish and Dutch. Factory default is English.
Date Format: US	Controls the date display on screen. Options are US and European. Factory default is US.
Time Format: 12 Hour	Controls how the time is displayed. Factory default of 12-hour.

› OPTIONAL SETUP FUNCTIONS

KEYPAD DISPLAY	EXPLANATION
Max. #Attempts:00 (0-10,0=off):	Sets the maximum number of attempts within a one minute period before the keypad prevents further code entry. The lockout will remain active for 60 seconds and will reset a maximum of 10 times. Use 000 to disable the lockout feature. The factory default is 000.
Presence In Req.: Disabled	When this feature is Enabled, a presence must be detected before a code or card can be used Factory default is Disabled
Card Format: 26 Bit	Set the format of the cards being used for access. Options are 26, 30, 31 and 34 Bits. See the card manufacturer specifications to determine the Bits of the card. Factory default is 26 Bit.
Trip Relay NoCom: Disabled	After any code has been entered the display will read Access Granted and the relay will be tripped to allow access. When Enabled, the keypad will allow the relay to be triggered when the communications are offline. Enabling this setting compromises site security. Factory default is Disabled.
Com Off Time:005 (1-25 sec):	Sets the amount of time the keypad should wait before deciding it has lost communication with the controller. Factory default is 5 seconds.
Setup Complete Press # key	Message displayed when exiting setup mode. Pressing the # key will return the device to normal operation. If no key is pressed, the device will return to normal operation after a few seconds and all information will be automatically saved.

Standard Keypad Messages

KEYPAD DISPLAY	EXPLANATION
Fri, 05/01/23 12:13 PM	When the user approaches the keypad, the standard display message will be shown on the display The display and keypad are backlit at a low level to conserve power when the device is not in use. This low level of light is sufficient to read the display at night. As soon as a customer presses the * key, the display returns to full brightness.
PLEASE ENTER ACCESS CODE	To enter an access code, the user presses *. The following message will be displayed.
PLEASE WAIT VERIFYING ACCESS	The user enters their access code using the touch pad and presses the # key. The keypad sends the code to the controller and waits for a response while the keypad goes through the security checks described in “Security Checks” on page 17 .
SORRY - TRY CARD AGAIN	If there is an error on the card, the following message will be displayed.
PLEASE WAIT	The controller is waiting for a response.

When the keypad receives a response from the controller it will display the response message. The messages received from the controller vary depending on the type of response. The various response messages are shown in the Access Response Messages section.

Security Checks

The VP performs a series of security checks before allowing entrance. These checks are used to prevent unauthorized access attempts. When a customer uses an access code, the checks are performed as soon as the code is entered.

SECURITY CHECK	EXPLANATION
Communications Check ***Please Wait***	When the keypad is not communicating with the controller and the Trip Relay NoComm is disabled, the unit will display PLEASE WAIT and revert back to the date and time.
Tamper Check: ***Sorry - Tamper Lockout***	The VP performs a tamper check to see if the tamper switch has been enabled. If it is enabled, the VP checks that the switch is secure. If either condition is true or the tamper is disabled, the VP will proceed to the next security check. If the VP detects tampering, it will display the following message and no further access attempts will be allowed.
Presence Required Check ***Sorry –No Presence Det***	After checking the tamper, the VP will check to see if the Presence is Req option has been selected. If it has been selected, the VP will check the input to see if a presence has been detected. If this option has been turned off, or if a presence has been detected, the keypad will continue with the next security check. If the VP does not detect a required presence, it will display the following message and no further access attempts will be allowed.
Maximum Attempts Check ***Sorry….* See Manager ****	The maximum attempts check is designed to discourage a user from entering random numbers to enter the site. If the Max # Attempts feature is set to a value between 1-10, the VP will check to see if the user has tried a code more than the permitted number of times. If not, the VP will allow the user to enter an access code. If a user exceeds the maximum number of unsuccessful attempts, the VP displays the following message and disables any further access.
Trip Relay Offline Check ***Access Granted***	After the customer has entered their code, the VP checks to see if the Trip Relay NoCom option has been enabled. If it has been enabled and the keypad is not in communication with the controller, then the VP will display thefollowing message and further access attempts will be allowed.

Access Response Messages

There are several standard messages built in to the VP. The types of messages the VP receives in response to an access request vary depending on the conditions. The following briefly describes the conditions and the displayed message.

ACTION	KEYPAD DISPLAY
For a valid Entry:	* Welcome * Entry is Granted
For a valid Exit:	* Thank You * Exit is Granted
When the area is closed (outside of allowed time zone hours):	Sorry – Area Denied
When the customer's code has expired:	Sorry –Code Expired
When the customer's card has expired:	Sorry – Card Expired
When the customer has been suspended:	Sorry – Access Suspended
When the code the customer entered is not valid:	Sorry – Access Denied
When the card the customer used is not valid or not read properly:	Sorry –Try Card Again

Cleaning the Housing and Touch Pad

Inspect and clean the housing and touch pad at least twice per year.

- To clean the housing, spray the unit with a mild household cleaner then wipe it with a soft cloth.
- Do not use harsh chemicals, abrasives, or petroleum-based products as they can damage the finish on the device.
- Do not immerse the device in water or use a pressure washer.
- A small, soft brush (a toothbrush works well) can be used to clean between the keys on the touch pad.
- Remove the VP from the housing to inspect and clean the inside of the unit.
- When inspecting the inside of the housing and the VP, look for the following items:
  - » Dirt or dust that has collected on the inside of the housing and the circuit board
  - » Signs of water damage or corrosion caused by prolonged contact to water
  - » Insects or insect droppings
- Wipe out the inside of the housing with a soft cloth to remove any debris that has collected.
- A small can of compressed air can be used to remove insects and dust from the circuit board.
- Do not use cleaners of any kind, including water, to clean inside the housing or on the circuit board.

Warranty

PTI Security Systems warrants its products and equipment to conform to its own specifications and to be free from defects in materials and workmanship, under normal use and service, for a period of one year from the date of shipment. Within the warranty period, PTI Security Systems will repair or replace, at its option, all or any part of the warranted product which fails due to materials and/ or workmanship. PTI Security Systems will not be responsible for the dismantling and/or re-installation charges. To utilize this warranty, the customer must be given a Return Materials Authorization (RMA) number by PTI Security Systems. The customer must pay all shipping costs for returning the product.

This warranty does not apply in cases of improper installation, misuse, failure to follow the installation and operating instructions, alteration, abuse, accident, tampering, natural events (lightning, flooding, storms, etc.), and repair by anyone other than PTI Security Systems. This warranty is exclusive and in lieu of all other warranties, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. PTI Security Systems will not be liable to anyone for any consequential or incidental damages for breach of this warranty or any other warranties.

This warranty will not be modified or varied. PTI Security Systems does not authorize any person to act on its behalf to modify or vary this warranty. This warranty applies to PTI Security Systems products only. All other products, accessories, or attachments used in conjunction with our equipment, including batteries, will be covered solely by their own warranty, if any. PTI Security Systems will not be liable for any direct, incidental, or consequential damage or loss whatsoever, caused by the malfunction of product due to products, accessories, or attachments of other manufacturers, including batteries, used in conjunction with our products. This warranty does not cover the replacement of batteries that are used to power PTI Security Systems products.

The customer recognizes that a properly installed and maintained security system may only reduce the risk of events such as burglary, robbery, personal injury, and fire. It does not ensure or guarantee that there will be no death, personal damage, and/or damage to property as a result. PTI Security Systems does not claim that the 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.

PTI Security Systems products should only be installed by qualified installers. The customer is responsible for verifying the qualifications of the selected installer. PTI Security Systems shall have no liability for any death, injury, or damage, however incurred, based on a claim that PTI Security Systems Products failed to function. However, if PTI Security Systems is held liable, directly or indirectly, for any loss or damage arising under this limited warranty or otherwise, PTI Security Systems's maximum liability will not in any case exceed the purchase price of the Product, which will be fixed as liquidated damages and not as a penalty, and will be the complete and exclusive remedy against PTI Security Systems.

PTI SECURITY SYSTEMS

SHAPING THE INDUSTRY SINCE 1979

Since 1979, PTI Security Systems™ has provided the self-storage industry with proven security and access control systems. Known for our complete and innovative solutions that deliver advanced and cost-effective security systems, self-storage owners and operators can efficiently manage their facility from anywhere, lower operating costs, and enhance the tenant experience.

For more information about PTI Security Systems or StorLogix, please contact a PTI representative or visit our website.

ptisecurity.com sales@ptisecurity.com 800.523.9504