

## INSTALLATION AND SETUP GUIDE

### INTRODUCTION

The 5883 RF Transceiver Module:

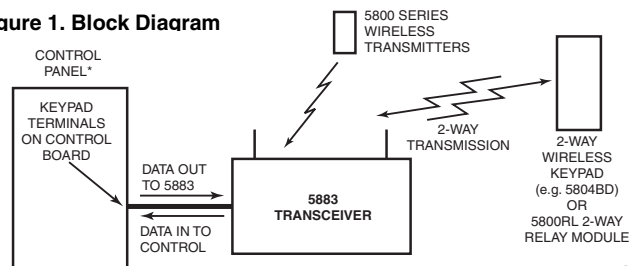
- contains an RF receiver and a transmitter,
- is intended for use with 5800 series RF transmitters, including bi-directional wireless units (e.g. 5804BD), and the 5800RL Wireless Relay Module (see Fig. 1),
- receives alarm, status, and control messages from 5800 transmitters, and passes these messages to the control panel via wired connections, which then responds accordingly (arm/disarm the system, initiate an alarm, etc.),
- transmits system status and other conditions to bi-directional devices (e.g., 5804BD),
- emulates the functions of a 5800TM module, and can control the relays on the 5800RL Wireless Relay Module,
- features a Spatial Diversity system that virtually eliminates the possibility of "Nulls" and "Dead Spots" within the coverage area,
- incorporates new high-security encryption technology (UL-864 and RF Jam Detect),
- supports the number of zones shown in the chart at right.

### RF Zones Supported

|       |  |
|-------|--|
| 5883M | Up to 16 zones   |
| 5883H | Depends on the control with which it is used. See the control panel's instructions for specific details. |

If "SET UP ERROR" (alpha keypads) or "E4 or "E8"" (fixed-word keypads) is displayed on the system's keypad, it indicates that more than the permitted number of wireless zones have been programmed, and none of the zones will be protected.

Figure 1. Block Diagram



\*CONTROL MUST BE CAPABLE OF SUPPORTING A 5800 RF SYSTEM

5883-003-10

### MOUNT THE MODULE OR PC BOARD

The 5883 can be mounted remotely, or, with some controls, can be mounted inside the control's cabinet. When mounting, make sure the antennas do not touch any metal surfaces.

**First, Check for RF Interference:** Before mounting permanently, use the red RF Interference LED (see figure 3) to check for strong local radio frequency interference at the intended mounting location. If this LED is continuously lit, the 5883 module should be relocated.

#### Removing the Cover

Remove the 5883's cover by inserting and twisting a screwdriver blade in the slot at the center of the cover's lower edge.

Replace the cover when installation is complete if unit is not mounted within a cabinet.

#### Mounting inside the control's cabinet (refer to Fig. 2):

- Remove the 5883's circuit board from its base by bending back the two flexible plastic tabs that hold the board's lower edge. Discard the 5883's unused plastic cover and base.
- In the control's cabinet, unfasten and move the control circuit board downward (if already installed).
- Hang two short (black) mounting clips (provided) on the raised cabinet tabs in the cabinet, as shown in Detail B of Figure 2.
- Insert the top of the 5883's board into the supporting slots at the top of the cabinet (Detail A). Swing the bottom of the board into the two short (black) mounting clips installed in step 3, and secure it to the cabinet with the accompanying screws. See Detail B.
- Insert the top of the control's board into the slot in the black clips holding the lower edge of the 5883 board (see Detail B); position two long (red) clips at the lower edge of the board (see Detail C).
- Swing the lower edge of the control board into place, and secure with two additional screws.
- Insert the grounding lugs (provided) through the top of the cabinet and into the left-hand terminals of the antenna blocks (at the upper edge of the 5883's circuit board). Secure it to the cabinet with the two screws provided. See Detail D.
- Insert the 5883's two antennas through the two openings in the top of the cabinet, one into each block's right-hand terminal, and tighten the screws to secure them.
- Affix the 5883's Summary of Connections label to the inside of the control's cabinet door.

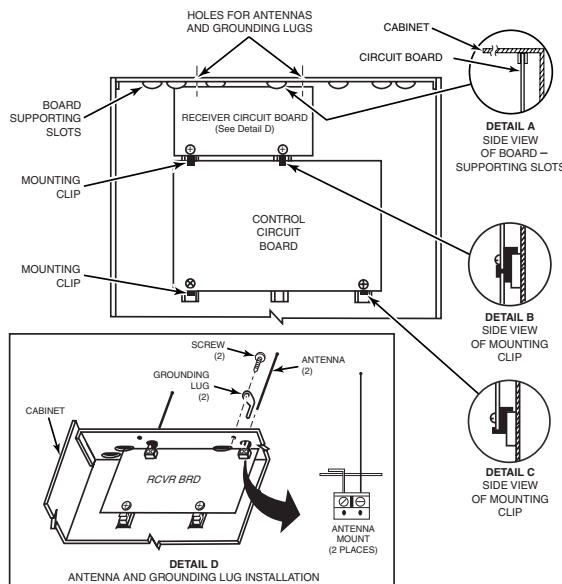


Figure 2. Installing the 5883 Board in the Control's Cabinet (Check the control's Installation and Setup Guide for applicability.)

#### Mounting the 5883 remotely

NOTE: If mounting the 5883 in its own enclosure, the supplied PCB mounting clips, grounding lugs, and screws are not needed.

- All wiring between the 5883 and the control panel must be located in a conduit.
- For concealed wiring, route wires through the rectangular opening at the rear of the base before mounting. For surface wiring entry, a thin breakaway area is provided along the base's right edge.
- Mount the module in the selected location. For greatest security, use all four mounting holes (two keyslot holes and two round holes) in the plastic base. (Refer to Detail D in Figure 2 above.)
- Install each antenna in the respective right-hand terminal of the two terminal blocks at the upper edge of the 5883's circuit board, and tighten the screws to secure them.
- Affix the 5883's Summary of Connections label to the inside of the housing cover.

## Mounting for Commercial Fire Applications (in separate cabinet)

For Commercial Fire applications, the 5883 module must be mounted in a separate cabinet (N4868V4-BE), using the ADEMCO Cam Lock (N6277), and Retainer Clip (N6277-1). Refer to the control's instructions for installing the Cam Lock and Retainer Clip.

The cabinet containing the module must be located no more than 20 feet from the alarm control cabinet (maximum wire run length 20 feet in a conduit), with no intervening walls or barriers.

**IMPORTANT:** If mounting the 5883 in a separate cabinet in a Commercial Fire installation, do not use the antenna grounding lugs.

## SET THE DIP SWITCHES

Use the DIP switches to set the 5883's device address, to activate Commercial Fire usage (if applicable), to enable the built-in transmitter, and to check or delete encrypted keys.

**Addresses:** The 5883 Transceiver has two device addresses: one for the receiver (addresses 1-7) and one for the transmitter (addresses 27-30, similar to the 5800TM device addresses; see notes 5 and 6 below). First, select a pair of addresses from the table below, making sure that neither address is currently being used in the alarm system, then use DIP switches 2-4 to set the address pair. The addresses should then be programmed in the control. Do not program the transmitter's address in the control if the 5883 is not being used with 5800TM compatible devices, such as the 5804BD.

### DIP Switch Functions

| Sw.                            | Function   |     |     |     |     |     |     |    |
|--------------------------------|--|-----|-----|-----|-----|-----|-----|----|
| 1                              | Check/deactivate high-security keys (see High-Security Keys paragraph)   |     |     |     |     |     |     |    |
| <b>Device Address Settings</b> |  |     |     |     |     |     |     |    |
| Transmitter:                   | Non-Addr.*   | 28  | 29  | 30  | 27  | 28  | 29  | 30 |
| Receiver:                      |  | 1   | 2   | 3   | 4   | 5   | 6   | 7  |
| 2                              | OFF  | OFF | OFF | OFF | ON  | ON  | ON  | ON |
| 3                              | OFF  | OFF | ON  | ON  | OFF | OFF | ON  | ON |
| 4                              | OFF  | ON  | OFF | ON  | OFF | ON  | OFF | ON |
| 5                              | <b>Commercial/Non-commercial Fire Installation:</b><br>ON = commercial fire system (see Notes for Commercial Fire Apps.)<br>OFF = non-commercial fire system                         |     |     |     |     |     |     |    |
| 6                              | ON = enable transmitter (if using 5800TM compatible devices)<br>NOTE: If using more than one 5883 in a system, enable the transmitter in only one 5883.<br>OFF = disable transmitter |     |     |     |     |     |     |    |
| 7                              | Not used; leave in OFF position  |     |     |     |     |     |     |    |
| 8                              | Used when removing RF keypads (see Removing RF Keypads paragraph); otherwise leave OFF   |     |     |     |     |     |     |    |

\* also address "0." See VISTA-15P/20P note at right.

## CONNECT THE WIRING FROM THE CONTROL

1. Insert the wiring plug (with 4 flying leads) into the mating socket on the 5883 (see Figure 3 for socket location).
2. Connect the 4 wires to the control's corresponding remote keypad connection points as follows:

RED: 12VDC input (+) Aux Power  
 GREEN: Data to Control (control's data IN)  
 YELLOW: Data from Control (control's data OUT)  
 BLACK: Ground (-)

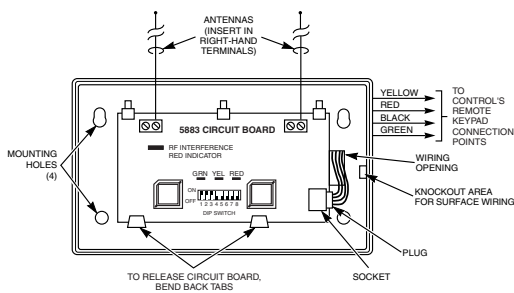


Figure 3. 5883 Transceiver

1. Remove the PC board by bending back the two flexible plastic tabs that hold the board's lower edge. Discard the 5883's unused plastic cover and base.
2. Insert the top of the board into the supporting slots at the top of the cabinet (see Detail A, Figure 2).  
Secure the bottom of the board with the 2 screws removed in step 1 above, using an insulating washer (supplied) between the head of each mounting screw and the PC board.
3. Affix the 5883's Summary of Connections label to the inside of the cabinet door.

## NOTES:

- If multiple 5883 Transceivers are used on one control, DIP switch 5 must be set to the same position on all receivers.
- DIP switch 5 reduces sensitivity during supervision message reception. For Commercial Fire applications (see note box), you must set DIP switch 5 to the ON position.
- DIP switches 2-4 select both an RF receiver and an RF transmitter device address.
- When used with 5800TM compatible (bi-directional) devices (e.g., 5800RL, 5804BD), the transmitter address must be enabled as a "keypad" in the control and DIP switch 6 must be set to "ON."
- If the 5883 is not being used with 5800TM compatible devices, the RF transmitter address should be ignored and DIP switch 6 should be set to OFF.
- If programming the control to supervise the 5883, program only the receiver address for supervision. Do not program the transmitter address for supervision.
- The 5883 does not support the 5827BD Wireless Keypad.

## Special Notes When Used With Certain Controls

VISTA-40: When using bi-directional devices (e.g., 5804BD), use device address setting 1/28 or 5/28 for devices used in partition 1; use device address setting 2/29 or 6/29 for devices used in partition 2 (this is necessary because the VISTA-40 automatically assigns address 28 or 29 depending on the programming in field 1\*48, wireless keypad partition assignment).

VISTA 32FB, VISTA-50P and higher: When using bi-directional devices (e.g., 5804BD), the Wireless Keypad Partition Assignment field (typically 1\*48) must be set to the partition in which the devices are used.

VISTA-15P/20P Series, FA168C Series: Use device address setting of "non-addressable," which is address 0 (sets the receiver address; the transmitter address (for bi-directional devices) is automatically set for 28).

## Notes for Commercial Fire Applications:

- DIP switch 5 must be in the ON position.
- All other system components, including the control, must be approved for use in Commercial Fire applications.
- When the 5883 is not used in a Commercial Fire application, switch 5 must be placed in the OFF position.

## LED FUNCTIONS (refer to Figure 3)

Red RF Interference LED: Lit Indicates local RF interference.

Green LED: Flickering indicates reception of messages (decoded and/or non-decoded).

Yellow LED: Occasional blinks occur under normal operation.

Red LED: Blinks indicate available space for high security keys; Steady ON indicates ready to deactivate high security keys or remove wireless (RF) keypads. See High Security Keys and Wireless Keypads section.

**IMPORTANT:** Take precautions against static discharge when handling the 5883 PCB. A static discharge can damage the module's EEPROM and/or cause unpredictable changes in its factory programming.

## PROGRAM THE CONTROL FOR RF OPERATION

Proceed with any control panel programming that may be necessary for RF operation and the installation of the system's wireless transmitters, as described in the control's Installation And Setup Guide. In addition, note the following:

- Enable the appropriate control data field for RF usage.
- Enroll the wireless keypad address(es), if used (see instructions provided with keypad).
- Wireless key buttons must first be enrolled in the control panel via zone programming, and, where applicable, assigned to a user number. Enroll each wireless key in the 5883 by pressing the appropriate buttons according to the instructions provided with the key.
- Upon the successful enrollment of an encrypted key, the red LED blinks the number of available spaces remaining for additional encrypted key enrollment (see Checking Available Space For High Security Keys paragraph).
- If more than one receiver is being used and you are using encrypted wireless keys, we recommend that you:
  - a. Enter the GO/NO GO mode.
  - b. Disconnect one receiver.
  - c. Enroll all encrypted keys into the connected receiver.
  - d. Reconnect the disconnected receiver.
  - e. Exit the GO/NO GO mode.
  - f. Repeat steps a-e for the receiver that was disconnected.

Notes for UL Commercial Burglary Installations:

- Program the control panel to transmit Low Battery, AC Loss, Tamper, and RF Communication loss trouble signals to the central station.
- The 5883 Transceiver Module must be mounted at ceiling height. If the ceiling is higher than 10-feet, Module must be mounted at a minimum height of 10-feet. Module must also be located at least 4-feet away from any fixed construction that could provide access for an intruder.

## HIGH SECURITY KEYS & WIRELESS KEYPADS

Depending on the control panel used, the 5883 can support up to 16 high-security (encrypted) wireless keys and up to 16 wireless keypads (e.g., 5839). The following paragraphs describe how to:

- Check available space for high-security keys
- How to deactivate all keys
- How to remove all wireless keypads.

**IMPORTANT:** Take precautions against static discharge when handling the 5883 PCB. A static discharge can damage the module's EEPROM and/or cause unpredictable changes in its factory programming.

See the Control's instructions and the appropriate device instructions for procedures on enrolling high security keys and wireless keypads.

### Checking Available Space for High Security Keys

The RED LED (above the DIP switch) shows (by blinking) how many high-security keys may be enrolled into the transceiver.

1. Remove power from the transceiver and set DIP switches:  
DIP 1 = ON  
DIP 8 = OFF
2. Apply power and observe one of the following RED LED indications:
  - a. Blinks, indicating the number of available spaces for additional high-security key enrollment, and then lights steady ON.
  - b. Immediate Steady ON (no blinks), indicating that high-security key enrollment is full.
  - c. Off, indicating that no encrypted keys are enrolled.
3. Set DIP switch 1 back to the OFF position to return to normal receiver operation (leave DIP 8 in OFF position).

### Deactivating High-Security keys

This procedure deactivates all enrolled high-security keys and is required only if previously enrolled high-security keys are being replaced and there is not enough available space left for them in the receiver. Once this procedure is performed, all desired high-security keys must be re-enrolled to activate high-security operation.

1. Perform steps 1 and 2 in Checking Available Space procedure above.
2. Wait until the RED LED lights steady ON then:
  - a. Record the positions of DIP switches 1 through 8.
  - b. Set DIP switches 1 through 8 to the opposite positions of their current settings and wait a few moments.
  - c. Set DIP switches 1 through 8 back to their original positions as recorded in step a. All enrolled high-security keys will be deactivated.
3. Set DIP switch 1 back to the OFF position to return to normal receiver operation (leave DIP 8 in OFF position).

### Removing All Wireless Key pads

This procedure removes all wireless keypad from the transceiver.

1. Remove power from the transceiver and set DIP switches:  
DIP 1 = OFF  
DIP 8 = ON
2. Apply power and observe the RED LED lights steady ON, then:
  - a. Record the positions of DIP switches 1 through 8.
  - b. Set DIP switches 1 through 8 to the opposite positions of their current settings and wait a few moments.
  - c. Set DIP switches 1 through 8 back to their original positions as recorded in step a. All enrolled wireless keypads will be removed from the transceiver.
3. Set DIP switch 8 back to the OFF position to return to normal receiver operation (leave DIP 1 in OFF position).

NOTE: If unsure that correct RF keypad (5839) addresses are enabled in the receiver, you should perform the RF keypad delete procedure, then enable RF keypad addresses as described in the instructions included with the RF keypad. Otherwise, erroneous ecp device "check" messages may occur.

### RADIO FREQUENCY EMISSIONS

#### Federal Communications Commission (FCC) Part 15

#### FCC ID: CFS8DL5883

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

#### Industry Canada

This Class B digital apparatus complies with Canadian ICES-003. Cet Appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

## SPECIFICATIONS

Dimensions:

7-3/8" W x 4-3/8" (10-7/8" w/antennas) H x 1-7/16" D

188mm W x 112mm H (277mm w/antennas) x 37mm D

Input Voltage: 12VDC (from control's remote keypad terminals)

Current: 80mA typical

Range: 200ft (60m) nominal indoors from wireless devices (actual range is determined with the control in TEST mode)

### TO THE INSTALLER

Regular maintenance and inspection (at least annually) by the installer and frequent testing by the user are vital to continuous satisfactory operation of any alarm system. The installer should assume the responsibility of developing and offering a regular maintenance program to the user, as well as acquainting the user with the proper operation and limitations of the alarm system and its component parts. Recommendations must be included for a specific program of frequent testing (at least weekly) to insure the system's operation at all times.

## **WARNING**

### **THE LIMITATIONS OF THIS WIRELESS ALARM SYSTEM**

While this System is an advanced wireless security system, it does not offer guaranteed protection against burglary, fire or other emergency. Any alarm system, whether commercial or residential, is subject to compromise or failure to warn for a variety of reasons. For example:

- Intruders may gain access through unprotected openings or have the technical sophistication to bypass an alarm sensor or disconnect an alarm warning device.
- Intrusion detectors (e.g., passive infrared detectors), smoke detectors, and many other sensing devices will not work without power. Battery-operated devices will not work without batteries, with dead batteries, or if the batteries are not put in properly. Devices powered solely by AC will not work if their AC power supply is cut off for any reason, however briefly.
- Signals sent by wireless transmitters may be blocked or reflected by metal before they reach the alarm receiver. Even if the signal path has been recently checked during a weekly test, blockage can occur if a metal object is moved into the path.
- A user may not be able to reach a panic or emergency button quickly enough.
- While smoke detectors have played a key role in reducing residential fire deaths in the United States, they may not activate or provide early warning for a variety of reasons in as many as 35% of all fires, according to data published by the Federal Emergency Management Agency. Some of the reasons smoke detectors used in conjunction with this System may not work are as follows. Smoke detectors may have been improperly installed and positioned. Smoke detectors may not sense fires that start where smoke cannot reach the detectors, such as in chimneys, in walls, or roofs, or on the other side of closed doors. Smoke detectors also may not sense a fire on another level of a residence or building. A second floor detector, for example, may not sense a first floor or basement fire. Finally, smoke detectors have sensing limitations. No smoke detector can sense every kind of fire every time. In general, detectors may not always warn about fires caused by carelessness and safety hazards like smoking in bed, violent explosions, escaping gas, improper storage of flammable materials, overloaded electrical circuits, children playing with matches, or arson. Depending on the nature of the fire and/or location of the smoke detectors, the detector, even if it operates as anticipated, may not provide sufficient warning to allow all occupants to escape in time to prevent injury or death.
- Passive Infrared Motion Detectors can only detect intrusion within the designed ranges as diagrammed in their installation manual. Passive Infrared Detectors do not provide volumetric area protection. They do create multiple beams of protection, and intrusion can only be detected in unobstructed areas covered by those beams. They cannot detect motion or intrusion that takes place behind walls, ceilings, floors, closed doors, glass partitions, glass doors, or windows. Mechanical tampering, masking, painting or spraying of any material on the mirrors, windows or any part of the optical system can reduce their detection ability. Passive Infrared Detectors sense changes in temperature; however, as the ambient temperature of the protected area approaches the temperature range of 90° to 105°F (32° to 40°C), the detection performance can decrease.
- Alarm warning devices such as sirens, bells or horns may not alert people or wake up sleepers if they are located on the other side of closed or partly open doors. If warning devices are located on a different level of the residence from the bedrooms, then they are less likely to waken or alert people inside the bedrooms. Even persons who are awake may not hear the warning if the alarm is muffled by noise from a stereo, radio, air conditioner or other appliance, or by passing traffic. Finally, alarm warning devices, however loud, may not warn hearing-impaired people.
- Telephone lines needed to transmit alarm signals from a premises to a central monitoring station may be out of service or temporarily out of service. Telephone lines are also subject to compromise by sophisticated intruders.
- Even if the system responds to the emergency as intended, however, occupants may have insufficient time to protect themselves from the emergency situation. In the case of a monitored alarm system, authorities may not respond appropriately.
- This equipment, like other electrical devices, is subject to component failure. Even though this equipment is designed to last as long as 10 years, the electronic components could fail at any time.

The most common cause of an alarm system not functioning when an intrusion or fire occurs is inadequate maintenance. This alarm system should be tested weekly to make sure all sensors and transmitters are working properly. The security console (and remote keypad) should be tested as well.

This system's wireless transmitters are designed to provide long battery life under normal operating conditions. Longevity of batteries may be as much as 7 years, depending on the environment, usage, and the specific wireless device being used. External factors such as humidity, high or low temperatures, as well as large swings in temperature, may all reduce the actual battery life in a given installation. This wireless system, however, can identify a true low battery situation, thus allowing time to arrange a change of battery to maintain protection for that given point within the system.

Installing an alarm system may make the owner eligible for a lower insurance rate, but an alarm system is not a substitute for insurance. Homeowners, property owners and renters should continue to act prudently in protecting themselves and continue to insure their lives and property.

We continue to develop new and improved protection devices. Users of alarm systems owe it to themselves and their loved ones to learn about these developments.

### **LIMITED WARRANTY**

Honeywell International Inc., acting through its Security & Custom Electronics business ("Seller") 165 Eileen Way, Syosset, New York 11791, warrants its product(s) to be in conformance with its own plans and specifications and to be free from defects in materials and workmanship under normal use and service for 24 months from the date stamp control on the product(s) or, for product(s) not having a manufacturer's date stamp, for 12 months from date of original purchase unless the installation instructions or catalog sets forth a shorter period, in which case the shorter period shall apply. Seller's obligation shall be limited to repairing or replacing, at its option, free of charge for materials or labor, any product(s) which is proved not in compliance with Seller's specifications or proves defective in materials or workmanship under normal use and service. Seller shall have no obligation under this Limited Warranty or otherwise if the product(s) is altered or improperly repaired or serviced by anyone other than Honeywell factory service. For warranty service, return product(s) transportation prepaid, to Honeywell Factory Service, 165 Eileen Way, Syosset, New York 11791.

THESE ARE NO WARRANTIES, EXPRESS OR IMPLIED, OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OR OTHERWISE, WHICH EXTEND BEYOND THE DESCRIPTION ON THE FACE HEREOF. IN NO CASE SHALL SELLER BE LIABLE TO ANYONE FOR ANY CONSEQUENTIAL OR INCIDENTAL DAMAGES FOR BREACH OF THIS OR ANY OTHER WARRANTY, EXPRESS OR IMPLIED, OR UPON ANY OTHER BASIS OF LIABILITY WHATSOEVER, EVEN IF THE LOSS OR DAMAGE IS CAUSED BY THE SELLER'S OWN NEGLIGENCE OR FAULT. Seller does not represent that the product(s) it sells may not be compromised or circumvented; that the product(s) will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; or that the product(s) will in all cases provide adequate warning or protection. Customer understands that a properly installed and maintained alarm system may only reduce the risk of a burglary, robbery, fire, or other events occurring without providing an alarm, but it is not insurance or a guarantee that such will not occur or that there will be no personal injury or property loss as a result. CONSEQUENTLY, SELLER SHALL HAVE NO LIABILITY FOR ANY PERSONAL INJURY, PROPERTY DAMAGE OR OTHER LOSS BASED ON A CLAIM THAT THE PRODUCT(S) FAILED TO GIVE WARNING. HOWEVER, IF SELLER IS HELD LIABLE, WHETHER DIRECTLY OR INDIRECTLY, FOR ANY LOSS OR DAMAGE ARISING UNDER THIS LIMITED WARRANTY OR OTHERWISE, REGARDLESS OF CAUSE OR ORIGIN, SELLER'S MAXIMUM LIABILITY SHALL NOT IN ANY CASE EXCEED THE PURCHASE PRICE OF THE PRODUCT(S), WHICH SHALL BE THE COMPLETE AND EXCLUSIVE REMEDY AGAINST SELLER.

This warranty replaces any previous warranties and is the only warranty made by Seller on this product(s). No increase or alteration, written or verbal, of the obligations of this Limited Warranty is authorized.



K3791 3/04 Rev. B

# **Honeywell**

**165 Eileen Way, Syosset, New York 11791**  
Copyright © 2004 Honeywell International, Inc.

[www.honeywell.com/security](http://www.honeywell.com/security)