NAPCO®
333 Bayview Avenue
Amityville, New York 11701
For Sales and Repairs, (800) 645-9445
For Technical Service, (800) 645-9440

GEM-ACM1D
Access Control Accessory
USER'S GUIDE

OI293 4/04

The GEM-ACM1D and GEM-2D Access Control Accessory adds integrated Access Control to your GEM-X255 burglary control panel. This guide contains important information about the operation of your access control system. Read it carefully and keep it handy for future reference.

ACCESS CONTROL

Access control allows you to extend or restrict admittance to a secured area of a protected premises. Cards with proper credentials that are presented to a card reader(s) will release a door locking mechanism (magnetic lock or electric strike). If the cards do not have proper credentials, the system will prevent access (exit or entry). The access control system described in this guide is integrated with the burglary functions of your control panel, and thus can be used to arm and disarm the system and to generate audible alarms that can be reported to a Central Station monitoring service. In addition, door activity can be mapped to several zones for the recording of log events.

ACCESS CONTROL READERS

To enter a secured area through an access controlled door, place an access card (such as ProxCards® or ProxKey® keyfobs) within a few inches in front of the card reader. Proximity card readers receive their power from radio frequency waves transmitted by a low power antenna inside the reader. The card contains a small antenna and a small chip. The card reader will examine the individual code embedded into the circuitry of the card, and if the code is programmed to allow access, the system will grant access, unlocking the protected door. If the card is disabled or an unidentified card is presented to the reader, the door will remain locked.

Card Reader Status LED Lights

Many access card readers contain a status light on the face of the reader which will change depending on the access status of the card. The Steady RED LED indicates a docked door. The steady GREEN LED indicates that the card has been read, as follows: If the card is disabled or invalid, the GREEN LED will remain on for only a few seconds; if the card is enabled and valid, the GREEN LED will remain on only while the door is unlocked.

Because the status lights within card readers can reveal internal aspects of the security system, there may be installations where the status lights must be disabled. **Stealth Mode** disables the status lights when the light's feedback is not desired (such as for card readers located outside the protected premises) but will light for 1 minute for the following events:

- Press a Request to Exit button
- Press a Request to Arm button
- Present a valid ARM/DISARM or ARM card to the card reader

Card Reader Sounder

Some card readers have audible sounders that provide status feedback to users. The reader may sound when access cards are presented and read, and if a door has remained open too long or if forced open.

ACCESS CARD ARMING AND DISARMING

You may be able to arm and disarm an area within the system using a card, if enabled. Before arming the area, ensure that the area is secured--all protected doors are closed and there is no movement within areas protected by motion sensors.

Arming the system with a card can be performed in two ways: (1) in conjunction with a Request to Arm button, and (2) with the Two Swipe Arming method, as follows:

Request to Arm Button: Press the Request to Arm button and present the access card to the card reader to begin the exit delay. Exit the premises within the exit delay time.

Two-Swipe Arming: With Two-Swipe Arming, the programmed card is presented to the card reader twice, the two presentations transpiring within a certain time period. The presentations must be separate and distinct; present the card to the reader once and remove, then present the card a second time, and remove. The card reader may provide visual and audible feedback to aid in the distinction between separate card presentations.

Disarming: Access cards may be configured to allow access to an armed system, with disarming allowed via a keypad mounted inside the protected area. If so, then present your access card to the reader, unlocking the door. Enter the premises and disarm within the entry delay time.

Access cards may be configured to allow for disarming outside the protected premises, via the card reader. If so configured, simply present the access card to the card reader to simultaneously disarm the area and unlock the door.

PROGRAMMING ACCESS CARDS

Before programming access cards, please be aware of the

Note: ProxCard® and ProxKey® are trademarks of the HID© Corporation.

following important warnings:

IMPORTANT

- YOU MUST KEEP A USER LIST when programming or distributing user access cards. Use the blank form at the end of this guide to photocopy. Write down the Access Group, embossed card number, user name and all other information. You will need this information later, if you need to delete a card.

Before you start programming Cards

1. **How many cards must be programmed?** If you have more than 25 cards, you may wish to have your installer program the cards during the system installation. This way, you can keep a set of pre-programmed cards in a secure location, and distribute them to users when needed. If you have less than 25 cards, you may wish to program them individually using the keypad. **Note:** Up to 195 cards can be programmed.
2. **What is the bit format, facility code, and embossed ID numbers on the cards?** Two card formats are supported: (1) NAPCO standard 36 bit format or (2) HID standard 26 bit format. The "embossed" number printed on the face of the card, up to 6 digits, must be manually entered as the user code (see Programming page 4). **Note:** When this embossed number is entered and configured in the system, the number cannot be entered at a system keypad for access.
3. **How many cards are already enrolled--and which User Locations are currently filled?** The User List is needed to determine the next available User Location numbers into which new cards can be programmed.
4. **Concept of an Access Group.** Useful when designing an access control system, an *Access Group* is a collection of people who all have similar attributes; they all enter and exit the same access door, and all keep to the same basic schedule when using the system. To keep the system organized, these users can be given a group name and assigned to a specific range of user numbers (total range is 1-195). Thus when deactivating and activating cards is required, errors as to scheduling and other attributes can be minimized. The "Users Chart" on page 4 should be photocopied and used to record this user information and kept in a secure location. **Note:** The GEM-X255 control panel is limited to a maximum of 195 users that can be programmed using the keypad. For more users, use the PCD-Windows Download software.

Using a keypad, the procedure for programming an access card and a User Code are similar because the access card information interpreted by the card reader is programmed into the same location as a User Code. The same user can possess a User Code and an access card, thus providing two means of accessing a protected area.

Before programming access cards, you must first enter User Program Mode via keypad address 1.

User Program Mode

Your Installer has programmed into your system a special *User Program Code* which can be used not only to arm and disarm the system, but also to enter the User Program Mode, where you can program other User Codes, card access codes, Zone Descriptions and also set the system Time and Date. The following explains how you will use this code to program or erase additional access cards. **Note:** Two types of keypads can be used with your system: "Classic RP Series" keypads and "K Series" keypads. Programming is the same for both keypads--only the button names have changed. In User Program Mode with either keypad, the [FUNCTION] and the [MENU] buttons operate identically and the [ON/OFF] and [ENTER] buttons operate identically. The instructions in this manual are depicted using the GEM-K1CA "K Series" keypad.

Programming / Reprogramming an Access Card

1. Enter User Program Mode as follows: First enter your User Code, then press [MENU] to enter the Function Mode.
2. Answer NO until "ACTIVATE PROGRAM Y/N" is displayed, then press YES. "ENTER USER CODE" will display indicating that the system is ready for User Code programming.
3. Enter the digits of the user number (1-195) to be programmed (representing individual users), followed by [MENU] [MENU]. (Example: For User 4, enter "004 [MENU] [MENU]").
4. Enter the "embossed" number printed on the face of the proximity card to be assigned to that user number, and if there is a Facility Code, use the least significant digit as the first number of the Code. For example, if the embossed card number is 78799 and the Facility Code is 12, enter 278799 for the user selected. **Note:** Complete codes may be up to 6 digits in length.
5. Press [ENTER] to save the new card access code. Duplicate codes are not allowed; therefore a duplicate code entered in the LCD Window will erase when [ENTER] is pressed. Repeat Steps 1 through 3 for each card access code to be programmed.

Deleting an Access Card

1. Enter User Program Mode as follows: First enter your User Code, then press [MENU] to enter the Function Mode.
2. Answer NO until "ACTIVATE PROGRAM Y/N" is displayed, then press YES. "ENTER USER CODE" will display indicating that the system is ready for User Code programming.
3. Enter the digits of the user number (1-195) to be programmed (representing individual users), followed by [MENU] [MENU]. (Example: For User 4, enter "004 [MENU] [MENU]").
4. Press [*] [0] to erase each digit of the card ac-

cess code and then press [ENTER].

- Example: Erase User 3's 5-digit User Code: (For the GEM-X255 panel, enter all three digits of the User #). Press:
[0] [0] [3] [MENU] [MENU] [✱] [0] [✱]
[0] [✱] [0] [✱] [0] [✱] [0] [ENTER].

Disable a Card
You may also wish to populate the card access code with all zero's in order to disable the card without deleting the other user options associated with the user number.

Reviewing a Programmed Card Access Code
To review an existing card access code, enter the user number (1-195) and the corresponding card access code will display.

Exiting the User Program Mode
When you have completed programming card access codes, press [RESET] to exit the User Program Mode.

Programming Example
A new employee was hired at your company, and you wish to add a new proximity card to the system for the new employee to use. The card is embossed with the number 33784, and has a facility code of 18. The new employee will join a department within your company for which an Access Group was created. According to your Users Chart (see page 4), this Access Group reserved user numbers 1-77 (out of 195) for its members, and user number 5 is currently unoccupied. To keep the system organized, add the proximity card access code to this location.

1. Enter your User Code, followed by [MENU].
2. Answer NO repeatedly until "ACTIVATE PROGRAM Y/N" is displayed, then press YES. The display will read: "ENTER USER CODE"
3. Press [0] [0] [5] for User No. 5, then press [MENU] [MENU] [MENU], followed by [8A] [3] [3] [7F] [8A] [4]. Because the facility code is 18, use the least significant digit, "8" as the first digit of the card access code.
4. Press [ENTER] to save the code. **Note:** Duplicate Codes are not allowed; therefore a duplicate Code entered in the LCD Window will erase when [ENTER] is pressed. Press [RESET] to exit the User Program Mode.

Notes:
- If the system contains more than one keypad, only the keypad designated "No. 1" may be used for programming (if in doubt which is No. 1, ask your installer).
- While in Program Mode, the ARMED and STATUS lights remain off and burglar and fire alarm functions are disabled.
- If the keypad detects no Program Mode activity for more than 4 minutes, a tone will sound. Press [RESET] to silence.

About Lost Cards
A lost card is a security breach. If a cardholder tells you that their card has been stolen or lost, its access code should be disabled or deleted immediately to prevent any unauthorized persons from accessing the system.

NAPCO LIMITED WARRANTY

NAPCO SECURITY SYSTEMS, INC. (NAPCO) warrants its products to be free from manufacturing defects in materials and workmanship for thirty-six months following the date of manufacture. NAPCO will, within said period, at its option, repair or replace any product failing to operate correctly without charge to the original purchaser or user.

This warranty shall not apply to any equipment, or any part thereof, which has been repaired by others, improperly installed, improperly used, abused, altered, damaged, subjected to acts of God, or on which any serial numbers have been altered, defaced or removed. Seller will not be responsible for any dismantling or reinstallation charges.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, WHICH EXTEND BEYOND THE DESCRIPTION ON THE FACE HEREOF. THERE IS NO EXPRESS OR IMPLIED WARRANTY OF MERCHANTABILITY OR A WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE. ADDITIONALLY, THIS WARRANTY IS IN LIEU OF ALL OTHER OBLIGATIONS OR LIABILITIES ON THE PART OF NAPCO.

Any action for breach of warranty, including but not limited to any implied warranty of merchantability, must be brought within the six months following the end of the warranty period.

IN NO CASE SHALL NAPCO BE LIABLE TO ANYONE FOR ANY CONSEQUENTIAL OR INCIDENTAL DAMAGES FOR BREACH OF THIS OR ANY OTHER WARRANTY, EXPRESS OR IMPLIED, EVEN IF THE LOSS OR DAMAGE IS CAUSED BY THE SELLER'S OWN NEGLIGENCE OR FAULT.

In case of defect, contact the security professional who installed and maintains your security system. In order to exercise the warranty, the product must be returned by the security professional, shipping costs prepaid and insured to NAPCO. After repair or replacement, NAPCO assumes the cost of returning products under warranty. NAPCO shall have no obligation under this warranty, or otherwise, if the product has been repaired by others, improperly installed, improperly used, abused, altered, damaged, subjected to accident, nuisance, flood, fire or acts of God, or on which any serial numbers have been altered, defaced or removed. NAPCO will not be responsible for any dismantling, reassembly or reinstallation charges.

This warranty contains the entire warranty. It is the sole warranty and any prior agreements or representations, whether oral or written, are either merged herein or are expressly canceled. NAPCO neither assumes, nor authorizes any other person purporting to act on its behalf to modify, to change, or to assume for it, any other warranty or liability concerning its products.

In no event shall NAPCO be liable for an amount in excess of NAPCO's original selling price of the product, for any loss or damage, whether direct, indirect, incidental, consequential, or otherwise arising out of any failure of the product. Seller's warranty, as hereinabove set forth, shall not be enlarged, diminished or affected by and no obligation or liability shall arise or grow out of Seller's rendering of technical advice or service in connection with Buyer's order of the goods furnished hereunder.

NAPCO RECOMMENDS THAT THE ENTIRE SYSTEM BE COMPLETELY TESTED WEEKLY.

Warning: Despite frequent testing, and due to, but not limited to, any or all of the following: criminal tampering, electrical or communications disruption, it is possible for the system to fail to perform as expected. NAPCO does not represent that the product/system may not be compromised or circumvented; or that the product or system will prevent any personal injury or property loss by burglary, robbery, fire or otherwise; nor that the product or system will in all cases provide adequate warning or protection. A properly installed and maintained alarm may only reduce risk of burglary, robbery, fire or otherwise but it is not insurance or a guarantee that these events will not occur. CONSEQUENTLY, SELLER SHALL HAVE NO LIABILITY FOR ANY PERSONAL INJURY, PROPERTY DAMAGE, OR OTHER LOSS BASED ON A CLAIM THE PRODUCT FAILED TO GIVE WARNING. Therefore, the installer should in turn advise the consumer to take any and all precautions for his or her safety including, but not limited to, fleeing the premises and calling police or fire department, in order to mitigate the possibilities of harm and/or damage.

NAPCO is not an insurer of either the property or safety of the user's family or employees, and limits its liability for any loss or damage including incidental or consequential damages to NAPCO's original selling price of the product regardless of the cause of such loss or damage.

Some states do not allow limitations on how long an implied warranty lasts or do not allow the exclusion or limitation of incidental or consequential damages, or differentiate in their treatment of limitations of liability for ordinary or gross negligence, so the above limitations or exclusions may not apply to you. This Warranty gives you specific legal rights and you may also have other rights which vary from state to state.

USERS CHART

USER (1-195)	ACCESS GROUP NAME	CODE	EMBOSSED NUMBER	FACILITY CODE	LAST NAME	FIRST NAME	COMMENTS