MAXSYS™

PC4020 v3.0 • Instruction Manual

WARNING: *This manual contains information on limitations regarding product use and function and information on the limitations as to liability of the manufacturer. The entire manual should be carefully read.*

Table of Contents

Introduction 2

Section 1: General System Operation 3

1.1 Getting to Know Your System ... 3
1.2 How to Arm ... 4
1.3 Alternate Arming Methods ... 5
1.4 Disarming ... 6
1.5 Alarm Memory ... 6
1.6 If An Alarm Sounds ... 7
1.7 Zone Bypassing ... 7
1.8 Trouble Conditions ... 8

Section 2: Access Codes 9

2.1 Program A New Access Code ... 9
2.2 Modify an Existing Code ... 11
2.3 Change User Code Options ... 12
2.4 Access Code Label Options ... 12
2.5 Delete an Existing Code ... 14
2.6 Special Codes ... 14
2.7 Installer Programmed Codes ... 15

Section 3: System Administration 16

3.1 Quick Arm ... 16
3.2 Quick Exit ... 16
3.3 Auto Arm Control ... 16
3.4 Setting the Time and Date ... 18
3.5 Activating Door Chime ... 18
3.6 View Event Buffer ... 18
3.7 [*][7] Command Outputs 1-8 ... 19
3.8 Keypad Control ... 19
3.9 Downloading Options ... 19

Section 4: Access Control 21

4.1 Access Card Readers ... 21
4.2 Access Card Programming ... 22
4.3 Search Using Access Card Numbers ... 24

Section 5: Testing and Maintenance 25

5.1 Walk Test ... 25
5.2 System Test ... 26
5.3 Lamp Test (PC4216) ... 26
5.4 System Maintenance ... 26

Section 6: Fire Safety 27

6.1 Fire Alarm Operation ... 27
6.2 Guidelines for Locating Smoke Detectors ... 27
6.3 Household Fire Safety Audit ... 29
6.4 Fire Escape Planning ... 29

Appendix A – Special Characters 31

Introduction

About Your Security System

Your DSC security equipment has been designed to give you the greatest possible flexibility and convenience. The LCD keypad will guide you through each operation with English language prompts. The keypad provides audible feedback each time a key is pressed; with unique audible sequences, it will also signal system troubles and other indications of system status.

Read this manual carefully and have your installer instruct you on your system's operation. Become familiar with the features that have been implemented on your system. All users of this system should be equally instructed in its use.

About this Manual

This manual is a thorough explanation of all system functions, including troubleshooting and programming access codes in addition to performing basic system functions. Most users of the system will not need to know all of this information. The first section of this manual, titled "General System Operation," explains general system concepts and instructs the user on how to arm and disarm the system and bypass zones. Photocopy this section and distribute it to general users of the system. The remaining sections of the manual are reserved for more detailed system information.

Fire Detection

This equipment is capable of monitoring fire detection devices such as smoke detectors and providing a warning alarm if a fire condition is detected. Good fire detection depends on having adequate numbers of fire detectors placed in appropriate locations. This equipment should be installed in accordance with NFPA 72 (NFPA, 1 Batterymarch Park, Quincey MA 02269). Carefully review the "Fire Escape Planning" guidelines in this manual.

NOTE: *Your installer must enable the fire detection portion of this equipment before it will work.*

Monitoring

This system is capable of transmitting alarms, troubles, and emergency information over telephone lines to a monitoring station. If you inadvertently initiate an alarm, immediately call the monitoring station to prevent an unnecessary response.

NOTE: *Your installer must enable the monitoring function before it will work.*

Section 1: General System Operation

1.1 Getting to Know Your System

Your security system is made up of a control panel, one or more keypads and various detectors and sensors. The control panel will be mounted out of the way in a utility room or basement. The metal control cabinet contains the system's electronics and stand-by battery. There is normally no reason for anyone except an installer or service person to have access to the control panel.

The keypads each have an audible indicator, an alphanumeric liquid crystal display (LCD), status lights and command entry keys. The keypad is used to send commands to the system and to display the current system status. Each keypad will be mounted in convenient locations inside the protected premises, near designated points of entry / exit.

Zones and Partitions

The protected premises has been divided by your installer into zones and partitions. A zone is an area of protection that has one or more detection sensors connected to it (motion detectors, glassbreak detectors, door contacts or shock sensors). A single zone might be a room, a hallway or a door or window. Two or more of these zones will be linked together by the control panel to form a partition.

A partition is a region of the protected premises. A partition can be armed and disarmed independently from other partitions. All of the partitions together form the entire system.

Some zones will belong to more than one partition, such as points of entry / exit and hallways. These are called **global zones** because they are not assigned to a single partition.

Access Codes

As a user of the system, you will be assigned a 4- or 6-digit access code. Access codes are used to arm and disarm the partition(s) to which they are assigned. Some access codes can perform additional system functions, such as programming system options and bypassing zones.

Your access code may not allow you to access certain system functions.For instance, if your code is only allowed to arm and disarm Partition 1, you will not be able to arm or disarm other partitions, or the entire system.

Keypads

Several LCD keypads will be installed throughout the protected premises, usually one at each entry / exit door. Some keypads are programmed only to access a single partition. These are called partition keypads.

If required, the system may have a **global keypad**. A global keypad can access any partition. When you enter your access code at a global keypad, you will be asked which partition you would like to arm. The keypad will only offer the partitions available for your access code.

The keypad will display the message "Enter Your Access Code" when it is not in use. Sometimes, it may display the time and date. Whatever the display, entering a valid access code on an idle keypad will access the system.

1.2 How to Arm

Prepare the partition to be armed by closing all protected doors and windows. Also, cease any movement in areas covered by motion detectors.

If the time and date appears on the LCD keypad display, press the [#] key. The "Enter Code to Arm System" message should appear. If the display reads "Secure System Before Arming," ensure that all doors and windows have been shut and that all motion has ceased.

Once the "Enter Code to Arm System" message has appeared, enter your 4- or 6-digit access code. If the access code was entered incorrectly, the keypad will beep steadily for two seconds.

For Single-Partition Access Codes

When a single-partition access code is entered, the system will select to arm the partition your code has access to. The "Exit delay in Progress" message will be displayed and the keypad will beep three times quickly. The exit delay will begin, providing a window of up to two minutes for you to exit the partition without causing an alarm.

Exit the premises through the designated exit/entry door. A timer will appear in the right side of the LCD keypad display indicating the remaining time in the exit delay period. When the allowed exit time expires, the partition will be armed. The message "Enter Code to Disarm System" will appear on the keypad.

For Multi-Partition Access Codes

When a multi-partition access code is entered, you must tell the system which partition(s) you wish to arm. The system will only offer to arm the partitions for which your code is programmed. Once you have entered your code, the display will read:

```
(0) TO ARM      < >
(Partition Label)  R
```

The lower right hand corner of the display will show the partition status using the letter "R" for the partitions which are Ready to be armed, "A" for the partitions which are already Armed and "N" for those partitions which are not yet secured. To arm the partition indicated on the display, press the number in parentheses (in this case, [0]) or press the [*] key. The exit delay will begin, providing a window of up to two minutes for you to exit the partition without causing an alarm. Once the exit delay has expired, the partition will be armed.

If you wish to arm another partition, use the arrow (< >) keys to scroll though the partitions available to be armed by your access code. To select a partition, enter the number indicated in parentheses, or press the [*] key. If you have selected another partition, the keypad will display the following message:

Select (0) < >
Arm Partition R

To arm the partition, enter the number indicated in parentheses, or press the [*] key. The exit delay will begin in the other partition and the keypad will read:

Exit Delay
In Progress

This display will remain for a few seconds until the keypad returns to the previous "(0) To Arm…" display.

1.3 Alternate Arming Methods

Away Arming

Arming the system in the Away mode will have all interior zones and perimeter zones active. If motion is detected in the interior zones, or if one of the perimeter zones is violated, the alarm sequence will begin. To arm in the Away mode, enter your access code, select the partition(s) to be armed and exit the premises through a designated exit/entry door. The system will recognize that you have left the premises. Once the exit delay expires, the system will be armed in the Away mode.

Stay Arming

This feature, if enabled, will allow you to arm the perimeter zones while leaving some interior zones inactive so that you can remain on the premises while the system is armed. When you enter your access code to arm the system and *do not* exit the premises through a designated exit/entry door, the system will arm in the Stay mode, automatically bypassing the interior zones.

The interior zones can be reactivated at any time by entering [*][1] at any keypad. If you reactivate the interior zones, be sure to only inhabit areas not covered by motion detectors. To access areas protected by motion sensors, you must enter your security code to disarm the system.

Arming Without Entry Delay

The entry delay is the period during which someone may enter an armed area without causing an alarm, providing time to get to a keypad to disarm the system. If you wish to arm your system without the entry delay, enter [*][9] then your access code. The Armed light will flash as a reminder that the system is armed and has no entry delay. The system will bypass the interior zones. An entry through any exit/entry door will create an instant alarm.

Quick Arm

When the Quick Arm feature is enabled, the system may be armed by simply pressing [*][0] instead of your access code. Please note that pressing [*][0] will only allow you to arm the system; to disarm, you must enter a valid access code. Your system administrator will inform you if the Quick Arm feature has been enabled on your system.

1.4 Disarming

Enter the premises through a designated exit/entry door. Entering the premises through any door not designated as a point of entry will cause an immediate alarm. As soon as the exit/entry door is opened, the keypad sounder will beep and the entry delay will begin. The entry delay provides a window of up to 255 seconds to disarm the system.

Go to the keypad and enter your access code. **If an error is made entering the code, press the [#] key and enter the code again.** The Armed light will turn off and the keypad buzzer will stop. A valid access code must be entered before the entry delay time expires.

If an alarm occurred while the panel was armed, the "View Memory" message will be on the display with the zone name for the zone that caused the alarm. The display will keep those messages on for two minutes or until the [#] key is pressed. The keypad will then return to it's idle state.

Disarming Another Partition

If you have a multi-partition access code, you can disarm other partitions before entering them. To disarm another partition, enter your access code. The keypad display will read:

```
(0) TO ARM      < >
(Partition Label)  R
```

Use the arrow (< >) keys to scroll to the partition you wish to disarm. Remember that only partitions to which your access code is assigned will be displayed. If the partition you have selected is armed, the letter "A" will appear on the bottom right-hand corner of the display, as in the following example:

```
(2) TO SELECT   < >
(Partition Label)  A
```

To disarm the partition, press the number in parentheses (in this case, [2]) or press the [*] key.

1.5 Alarm Memory

To view alarms that occurred while the system was armed, press [*] then [3]. Alarms caused during the last armed period will be displayed. Press [#] when you have finished viewing alarms to exit the alarm memory mode.

***NOTE**: Tamper alarms will not be shown in alarm memory display.*

1.6 If An Alarm Sounds

Fire Alarm

If your system has been installed with fire detectors, a fire alarm will be indicated by a pulsing siren. If you hear a fire alarm, follow your emergency evacuation plan immediately (see Section 6.5 “Fire Escape Planning”).

Intrusion Alarm

An intrusion alarm will be indicated by a continuous bell or siren. An intrusion alarm may be silenced by entering a valid access code. If the alarm was unintentional, call local authorities immediately to avoid an unnecessary response.

You can determine the source of the alarm by entering the alarm memory mode. Once the source of the alarm has been corrected, the panel can be restored to its original armed state.

1.7 Zone Bypassing

You can use zone bypassing when access is needed to part of the protected area while the system is armed. Zones which are temporarily out of service due to damaged wiring or contacts may be bypassed to allow system arming until repairs can be made. Armed zones cannot be bypassed.

Bypassed zones will not cause an alarm. Zones cannot be bypassed once the system is armed. Bypassed zones are automatically canceled each time the system is disarmed and must be reapplied before the next arming.

NOTE: *For security reasons, your system administrator may program the system to prevent you from bypassing certain zones.*

Bypassing zones reduces your security protection. If you are bypassing a zone due to damaged wiring or contacts, please notify your system administrator or call a service technician immediately so that the problem can be resolved and your system returned to proper working order.

NOTE*: Your installer may have included the ability to bypass fire zones on your system. Ask your installer for more information.*

If fire zone bypassing is possible, when you bypass a fire zone the panel will indicate a fire trouble until the bypass is turned off. You cannot turn off fire zone bypasses by disarming and / or arming the system. You must turn off the bypass manually, as described below.

To bypass zones, enter [*] [1]. You may be required to enter your access code. A menu will appear outlining the various bypassing options. Use the arrow (< >) keys to scroll through each option and press the [*] key to select it, or press the corresponding number in parentheses. The bypassing options are as follows:

[0] Bypass Open Zones – This section will only display the zones which are currently open or bypassed. Use the arrow (< >) keys to scroll through these zones. Zones that are open will be indicated by an exclamation (!) mark in the lower right hand side of the keypad display. To select a zone to be bypassed, press the [*] key. A “*” will appear next to the zone label to indicate that the zone has been bypassed.

[1] Bypass Zones – This selection takes you immediately to bypassing zones. Use the arrow (< >) keys to find the zone to be bypassed and press the [*] key to select it. A "*" will appear next to the zone label to indicate that the zone has been bypassed.

[2] Clear Bypasses – This selection will allow you to turn bypassing off for all of the zones in your partition.

[3] Recall Bypasses – This selection will automatically bypass the same group of zones which were bypassed the last time the partition was armed.

[4] Previous Menu – This selection will return the display to "Enter Code to Arm System." From here, you will be able to arm the system.

1.8 Trouble Conditions

The alarm control panel continuously monitors a number of possible trouble conditions. If one of these conditions occurs, the keypad Trouble light will turn on and a beeping sound will be heard every 10 seconds. Press the [#] key to silence the keypad. The Trouble light will stay on until the trouble is cleared.

To view which trouble conditions are present, enter [*] [2] at any keypad. Use the arrow (< >) keys to scroll through the list of trouble conditions:

If **AC Trouble** is present, the system has lost its power. This trouble may be due to a power outage and should be cleared once the power is restored. If the power on the premises is running normally and the trouble condition persists, call your installer for service.

If **TLM Trouble** is present, the is a problem with the telephone line. If the telephones on the premises are running normally and the trouble condition persists, call your installer for service.

Any other trouble condition will require the assistance of your installer. As soon as a trouble condition occurs, call your installer to have the problem corrected as soon as possible.

Section 2: Access Codes

Access codes are used to arm and disarm the system as well as to access system functions. There are many different codes available on the system.

The **Grand System Master Code** will be able to perform all system functions. This includes zone bypassing, activating outputs enabling user options and programming access codes. The Grand System Master Code is access code 0001. Normally, only your installer can change this code. Please ask your installer if you wish to be able to alter this code.

The following sections explain how to program new codes and modify existing codes. All access code options will also be described.

2.1 Program A New Access Code

This section describes three basic aspects to programming an access code:

- How to select a new access code for programming
- How to program the 4- or 6-digit code
- How to program the user's name to identify the code
- How to select the partitions the code will be active on

To select a new access code for programming, perform the following steps:

1. Enter [*][5] followed by a Master Code.
2. The display will read:

Select (0) < >
User No. Search

   Press [0] or [*].
3. The display will read:

Sel. Code (0001) < >
User 1

   User 1 (Access Code 0001) is the System Master Code. Your installer may already have programmed this code. Use the right arrow (>) key to scroll to the code you wish to program (for example, access code 0002). Press [*] to select the code.
4. The display will read:

Select (0) < >
Program Code

   This is the **Program Code menu**. Use the right arrow (>) key to scroll though each display in the Program Code menu. Each display pertains to a different aspect of access code programming, including the three listed below. To select any menu item for programming, press [*].

Program Code

To program the code for the new access code, perform the following:

1. From the Program Code menu, use the arrow keys to scroll to the first message: "Select (0) Program Code." Press [0] or [*] to program the access code.
2. The display will indicate "Enter Digits" followed by "AAAA." This is the default setting for the access code. Enter four digits for the new code.
3. Press [#]. The display will return to "Select (0) Program Code." The new code has been programmed.

6-digit access codes are available. Talk to your installer if you require 6-digit access codes on your system.

NOTE: *Do not program access codes that can be easily guessed and will compromise the security of your system (e.g. 1111 or 1234).*

Edit User Name

To program the user name for the new access code, perform the following:

1. From the Program Code menu, use the right arrow (>) key to scroll to the following display:

Select (2) < >
Edit User Name

2. Press [2] or [*].
3. The display will read "Program Name." For access code 0002, the default name will be "User 2." Enter the new access code name using the number keys in the following manner:

The letters of the alphabet have been divided up among the 1 to 9 number keys on the keypad as follows:

[1] = A, B, C, 1	[2] = D, E, F, 2	[3] = G, H, I, 3	[4] = J, K, L, 4
[5] = M, N, O, 5	[6] = P, Q, R, 6	[7] = S, T, U, 7	[8] = V, W, X, 8
[9] = Y, Z, 9, 0	[0] = Space		

For example, if you press the [4] key once, the letter "J" will appear above the cursor on the display. Press the [4] key again, the next letter "K" will appear, and so on. If a different number key is pressed, the cursor will automatically move to the right one space. To erase a character, use the [<] [>] keys to move the cursor under the character, then press the [0] key. (See section 2.4 for other options available when programming user names.)

---

4. Once the new name has been entered, press [#]. The display will return to "Select (2) Edit User Name."

Edit Partition Mask

Your installer has divided the system into partitions. The system may contain one or more partitions. In order for an access code to function, you must program which partitions the code will be active on. If your system only has one partition, you must activate the code for partition 1.

To program partition access for the new access code, perform the following:

1. From the Program Code menu, use the right arrow (>) key to scroll to the following display:

   ```
   Select (6) < >
   Edit Part. Mask
   ```

2. Press [6] or [*]. The display will read "Select Toggle < >." Partition 1 will be displayed, followed by the letter "N." This means that Partition 1 is not available for that code. Press [*] to select Partition 1 (Y). The [*] key will alternately enable (Y) and disable (N) the partition for the selected code.
3. Use the right arrow (>) key to scroll to the next partition on the system. Press [*] to enable or disable the partition. Repeat this step for the rest of the partitions on the system until the desired partition access has been granted for the selected code.
4. Press [#] once you have finished programming the partition mask for the code. The display will return to "Select (6) Edit Part. Mask."

2.2 Modify an Existing Code

To modify an existing code, you must first search for it using one of two methods: search by code number or by user name.

To search for the code by **user number**, perform the following:

1. Enter [*][5] followed by a Master code.
2. The display will read:

   ```
   Select (0) for
   User Number Search
   ```

   Press [0] or [*].
3. Enter the access code number and press [*] to continue programming. You can also use the arrow (< >) keys to scroll to the desired number.

To search for the code by **user name**, perform the following:

1. Enter [*][5] followed by a Master code.
2. The display will read "Select (0) for User Number Search." Use the right arrow (>) key to scroll to the following display:

   ```
   Select (1) for
   User Name Search
   ```

   Press [1] or [*].
3. The first letter of the access code name using the corresponding number key. For example, for John, enter the letter "J" by pressing the [4] key once.
4. The keypad will display the first available name starting with the selected letter. Use the right arrow (>) key to scroll through subsequent names.
5. Once the appropriate user name is displayed, press [*] to continue programming.

Once the code has been selected, the Program Code menu will be shown. Reprogram the access code, code label or partition access using the steps outlined in Section 2.1 “Program a New Code”.

2.3 Change User Code Options

User code options determine which system features the code will be able to access. Table 2-1 shows all of the available access code options. The table also indicates which options are enabled by default for each type of code.

To change the user options for a code from its default settings, perform the following:

1. Enter [*][5] followed by a Master code.
2. Locate the code using one of the code searching methods (see Section 2.2). Press [*] to select.
3. Use the right arrow (>) key to scroll to the following display:

Select (5) < >
Edit User Opt's

   Press [5] or [*].
4. Use the arrow (< >) keys to scroll through each option. Press [*] to turn each option on (Y) or off (N).
5. When the desired options have been programmed, press [#].

2.4 Access Code Label Options

In Section 2.1, you learned how to program the access code label (“Program User Name”). There are other options available when programming labels.

When programming the label, press the [*] key for the options menu. Use the arrow (< >) keys to scroll through each option. Press the [*] key to select.

The available options are:

- **Clear Display:** Selecting this option will clear the entire code label.
- **Clear to End:** This will clear the display from the character where the cursor was located to the end of the display.
- **Change Case**: This will toggle the letter entry between uppercase and lowercase letters.
- **ASCII Entry:** This is for entering uncommon characters. Use the arrow (< >) keys to scroll through the available characters. Each character will be displayed along with the corresponding 3-digit ASCII number. If you know the character’s 3-digit number, enter it. Press the [*] key to enter the character into the code label. See Appendix A at the back of this manual for a list of the available ASCII characters.

Table 2-1: Access Code User Options	Default Settings*				
	GM	2M	SM	S	AC
System Master Select this option to program a System Master Code			Yes		
Supervisor Select this option to program a Supervisor code. You must also program the partition mask for this code.			Yes✦	Yes	
Arm Allows arming of the assigned partition(s).	Yes	Yes	Yes	Yes	Yes
Disarm Allows disarming of the assigned partition(s).	Yes	Yes	Yes	Yes	Yes
Bypass Allows bypassing of zones on the assigned partition(s).	Yes	Yes	Yes	Yes	Yes
Command Output Allows activation of a [*][7][X] command output when an access code is required. For more information, ask your installer.	Yes	Yes	Yes	Yes	Yes
Duress Pulse Select option for Duress codes only (See "Special Codes")					
One-Time Use Select option for One-Time Use codes only (see "Special Codes")					
Escort4580 Access Allows access to the Escort4580 Audio Assistant, if installed.	Yes	Yes	Yes	Yes	Yes
Global Access Allows use of a Global keypad.	Yes	Yes	Yes	Yes	Yes
Partition Select Menu Allows all accessible partitions to be viewed when the code is entered.	Yes	Yes	Yes	Yes	Yes
Card Valid *(For Access Control Systems only. See Section 4.2 "Access Card Programming")*	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Privilege Card *(same as previous)*	*Yes*	*Yes*			
Wait for Prvl *(same as previous)*					
Silence Fire Allows the user to silence and reset any Fire Alarms on the selected partitions by entering their access code on the partition keypad.	Yes	Yes	Yes	Yes	Yes
* Code abbreviations: GM = Grand System Master; 2M = Second Master; SM = System Master; S = Supervisor; AC = Access Code (default).					
The options for the Grand System Master and Second Master codes cannot be changed from their default settings.					
✦For the System Master code, the supervisor option changes to Yes after you exit access code programming.					

2.5 Delete an Existing Code

An access code may be erased in two parts. First, all data pertaining to the code may be deleted (access code, user options, partition access, etc.). The access code label is erased separately.

To delete all access code data from an existing code, perform the following:

1. Enter [*][5] followed by a Master code.
2. Locate the code using one of the code-searching methods (see Section 2.2 “Modifying an Existing Code”). Press [*] to select.
3. Use the right arrow (>) key to scroll to the following display:

Select (1) < >
Erase Data

4. Press [1] or [*]. All data pertaining to the access code, except the access code name, will be erased.

To delete the access code name from an existing code, perform the following:

1. Enter [*][5] followed by a Master code.
2. Locate the code using one of the code-searching methods (see Section 2.2 “Modifying an Existing Code”). Press [*] to select.
3. Use the right arrow (>) key to scroll to the to “Select (2) Edit User Name” and press [*].
4. The display will indicate the current name. Press [*].
5. The display will read “Select (0) Clear Display.” Press [*]. The access code name will be erased.
6. Follow the instructions outlined in Section 2.1 to program a new label, or press [#] until you have exited access code programming.

2.6 Special Codes

The following four codes are special codes. Selecting the corresponding user option will program each code (see Section 2.3 “Change User Code Options”).

System Master Codes

System Master codes have access to all partitions on the system. These codes can be used to program other access codes, except for other System Master codes. For a list of the other user options that are enabled for this code, see Table 2-1.

Supervisor Codes

The supervisor code can be used to program other access codes that are only to be active on the supervisor’s partition. Users with Supervisor codes cannot program other Supervisor codes, or System Master codes. For a list of the other user options that are enabled for this code, see Table 2-1.

Duress Codes

If the "Duress" user option is enabled, the code will become a Duress code. When this code is entered, the system will send a duress signal to the monitoring station. Make sure that the Arm and Disarm user options are also enabled for this code.

One-time Use Codes

If the "One-time Use" option is enabled, the code will become a One-time Use code. The code can be used to disarm assigned partitions. When a user arms the system using a One-Time Use code, the panel will erase the code once the Exit Delay expires; after this time, the code cannot be used again. Make sure that the Arm and Disarm user options are also enabled for this code.

Log Only Codes

A "Log Only" code will onlycreate an entry in the event buffer when entered at a keypad. Example: a log-only code may be used by a guard to record the time that they checked each area of the premises.

To create a log-only code, disable all the access code options for the code.

2.7 Installer Programmed Codes

These are access codes that are programmed by your installer. Talk to your installer for more information regarding these codes.

- **Second Master Code:** This code has the same properties as the System Grand Master code. Only your installer can program this code.
- **Walk Test Code:** The Walk Test code is used to access to the walk test mode. See Section 5.1 "Walk Test" for instructions on performing a walk test.
- **Guard Code:** This code is only valid when a partition is disarmed and for a programmed amount of time after a partition is armed using the Guard code. Only your installer can program the Guard code.

Section 3: System Administration

3.1 Quick Arm

Keypad Command: [*][6][Access Code]

This option will allow the system to be armed by entering [*] [0] at any keypad instead of entering an access code. This option must be enabled in order for the Stay or Away function keys to work. To turn this feature on, perform the following:

1. Press [*] [6], then enter a valid access code which has the "System Master" or "Supervisor" option enabled. The display "System Functions Menu" should appear.
2. Use the arrow keys (< >) to scroll to the message "Quick Arm." Press [*].
3. To enable or disable quick arming, press the [*] key to select [Y]es or [N]o.

3.2 Quick Exit

Keypad Command: [*][6][Access Code]

This option will allow a user to exit an armed system through a designated entry / exit point by entering [*] [0] at a keypad. The system gives the user 2 minutes to exit the premises. Once the user has exited the premises, the system will continue to be armed. This option must also be enabled in order for the Exit function key to work.

1. Press [*] [6], then enter a valid access code which has the "System Master" or "Supervisor" option enabled. The display "System Functions Menu" should appear.
2. Use the arrow keys (< >) to scroll to the message "Quick Exit." Press [*].
3. To enable or disable Quick Exit, press the [*] key to select [Y]es or [N]o.

3.3 Auto Arm Control

Daily Auto Arming

Keypad Command: [*][6][Access Code]

This option will allow the system to be automatically armed at the same time each day. Auto arming can occur at the same time every day. In order for this function to work, you must enable the Auto Arm function and program the Auto-Arm Time (follow the steps below).

To enable auto arming at the same time each day, perform the following:

1. Press [*] [6], then enter a valid access code which has the "System Master" or "Supervisor" option enabled. The display "System Functions Menu" should appear.

2. Use the arrow keys (< >) to scroll to the message "Auto Arm Control." Press [*].
3. Use the arrow keys to scroll to the message "Auto Arm." Press [*]. This option turns auto arming on or off. To turn the auto arm feature on, press the [*] key to select [Y]es. To turn it off, press the [*] key to select [N]o. Press [#].
4. Use the arrow keys to scroll to the message "Auto Arm Time." Press [*].This is the time at which the partition will automatically arm itself every day. Once you have selected this option, enter the time using the 24 hour format (HHMM). Press [#].

Scheduled Auto Arming

Auto arming can also occur according to a schedule. Schedules can only be programmed by your installer. If you wish to know more information regarding scheduling and your security system, please consult your installer.

To enable auto arming according to a schedule, perform the following:

1. Press [*] [6], then enter a valid access code which has the "System Master" or "Supervisor" option enabled. The display "System Functions Menu" should appear.
2. Use the arrow keys (< >) to scroll to the message "Auto Arm Control." Press [*].
3. Use the arrow keys to scroll to the message "Auto Arm." Press [*]. This option turns auto arming on or off. To turn the auto arm feature on, press the [*] key to select [Y]es. To turn it off, press the [*] key to select [N]o. Press [#].
4. Use the arrow keys to scroll to the message "Schedule Arm." This option, when enabled, will program the partition to automatically arm according to a schedule programmed by your installer. To turn the schedule arm feature on, press the [*] key to select [Y]es. Press the [*] key to select [N]o to disable the feature. Press [#].
5. Use the arrow keys to scroll to the message "Sched. Disarm." When this option is enabled, the partition will follow the auto disarming schedule programmed by your installer.

When Auto Arming Occurs

At the selected auto arm time, the keypad will beep and the bell or siren will pulse once every 10 seconds to alert anyone on the premises that the system is about to arm. The bell/siren pulse can be programmed by the installer to be silent.

To prevent the system from auto arming, press any key on the partition keypad during this pre-alert period. If desired, your installer can program the system so that a valid access code will be required to prevent the system from auto arming. Swiping an access card on one of the partition's readers—if installed—will also prevent auto arming.

3.4 Setting the Time and Date

Keypad Command: [Master Code][9]

To set the time and date on the system, perform the following:

1. Enter a Master code and press [9]. The display will read "System Master Menu."
2. Use the keypad arrow keys (< >) to scroll to the display "Set System Time." Press [*].
3. Enter the current time in 24 hour format (HHMM). For instance, to program 3:51 p.m., type in "1551."
4. Next, use the keypad arrow keys to scroll to the display "Set System Date." Press [*].
5. Enter the current date (MMDDYY). For example, to program May 31, 1997 type "053197."
6. Once the date and time have been programmed, press [#] to return the partition to its normal disarmed state.

3.5 Activating Door Chime

Keypad Command: [*][4]

When the door chime feature is enabled, the keypad will emit five quick beeps when a zone is opened or closed. The keypad will only beep for zones which have the door chime zone attribute enabled. Often this feature is applied to entry doors so that you are notified when someone enters or exits the premises.

To enable door chime, enter [*] [4] at any keypad. To program the chime zone attribute for a particular zone, please ask your installer.

***NOTE**: The door chime feature will not work on bypassed zones.*

3.6 View Event Buffer

Keypad Command: [Master Code][9]

Each system event is stored in an event buffer which can be viewed from any keypad. To view the event buffer, perform the following:

1. Enter a System Master code and press [9]. The display will read "System Master Menu."
2. Use the keypad arrow keys (< >) to scroll to the display "View Event Buffer." Press [*].
3. The event buffer can now be viewed, starting with the most recent event. When an event is presented, the first line of the display will show the event number and the partition on which the event occurred; the second line of the display will show the date and time of the event. Press the [*] key to display a description of the event. Use the arrow keys to scroll through the list of all events in the event buffer.
4. To stop viewing events, press [#].

3.7 [*][7] Command Outputs 1-8

Keypad Command: [*][7][1-8]

These outputs must be programmed by your installer. Up to eight command outputs can be added to your system. These outputs will operate sets of lights, door strikes and various other items depending on what you and your installer have decided to add to your system.

To activate the output, enter [*] [7] followed by the output number, from 1-8. For more information regarding the [*] [7] command outputs, please ask your installer.

3.8 Keypad Control

Keypad Command: [*][6][Master Code]

The brightness of the keypad backlighting and the contrast of the keypad display can be adjusted. To alter the brightness and contrast from their default settings, perform the following:

1. Press [*] [6], then enter a valid access code which has the "System Master" or "Supervisor" option enabled. The display "System Functions Menu" should appear.
2. Use the arrow keys (< >) to scroll to the message "Keypad Setup." Press [*].
3. The display should read "Bright Control." Press [*]. Use the arrow keys to scroll through eight different settings of backlighting levels and press [*] to select the desired setting.
4. Use the arrow keys to scroll to "Contrast Control." Press [*].Use the arrow keys to scroll through eight different settings of display contrast and press [*] to select the desired setting.

Press [#] when you have finished programming to return the partition to its normal disarmed state.

3.9 Downloading Options

Keypad Command: [Master Code][9]

Enable DLS Window

This option will allow the downloading computer to access the system. This DLS window will last for 60 minutes after the option is selected. This function can only be disabled by your installer. To enable downloading, perform the following:

1. Enter a System Master code and press [9]. The display will read "System Master Menu."
2. Use the keypad arrow keys (< >) to scroll to the display "Enable DLS Window." Press [*]. Downloading will be enabled for one hour.
3. To exit the menu, press [#].

User Call Up

When this option is activated, the alarm control panel will call the downloading computer. The downloading computer must be waiting for the call in order for downloading to begin.

To start user call up, perform the following:

1. Press [*] [6], then enter a valid access code which has the “System Master” or “Supervisor” option enabled. The display “System Functions Menu” should appear.
2. Use the arrow keys (< >) to scroll to the message “User Call Up.” Press [*] and the panel will call the downloading computer.

NOTE: *This option must be enabled by your installer in order for it to become functional.*

Section 4: Access Control

NOTE: *This section only applies to systems that have the PC4820 Access Control module installed. Talk to your installer for information regarding the access control capabilities of your system.*

4.1 Access Card Readers

To gain access to an area via a door with an access card reader, present your access card through the reader. Depending on how your card has been programmed, the system will either grant or deny you access to the protected area.

Most access card readers will have a status light. This light will indicate your access status once the card is presented. The light will appear according to the following conditions:

- Steady red light: The door is locked.
- Steady green light: The door is unlocked.
- Slowly flashing from red to green: The partition is armed.
- Flashing from red to green twice per second: The reader is waiting for a Privilege card to be swiped.
- Flashing from red to green three times per second: Access is denied.

Some access card readers also have audible indicators which beep under certain conditions. The reader may beep when an access control door has been left open too long, or when a door has been forced open.

Arming and Disarming Using an Access Card

You may be able to automatically arm or disarm your partition using your access card. Ask your installer if this feature has been enabled.

To arm a partition using an access card, ensure that the partition area is secured. Close all protected doors and cease movement in areas covered by motion detectors. Swipe the access card in the reader. Push the "Arm" button. The exit delay will begin.

To disarm a partition, present the access card to the reader. The partition may disarm if the system allows. If disarming is granted, the door will unlock. When you open the door, the system will disarm the partition.

A NOTE FOR PROGRAMMING ACCESS CARDS:

To arm or disarm a partition using an access card, the following access code options must be programmed:

- *User Code Options: Arming and Disarming Options*
- *Edit Partition Mask: Partition access must be granted.*

See Section 3 "Access Codes" for instructions on programming these options.

4.2 Access Card Programming

Access card programming is a part of access code programming. An access card is assigned to a single user of the system. A user can have both an access code and an access card to provide two different means of accessing the system.

Two methods of programming access cards are described below:

- Programming access cards for existing users
- Programming access cards for new users

Three different areas require programming for each access card: the access card number, the user's access level and the access code user options that pertain to access card operation.

The access card number is a serial number printed on the back of each card. This number is usually between five and seven digits.

Programming Access Cards for Existing Users

1. Enter [*][5] followed by a Master code.
2. Search for existing access code by user number or user name (methods outlined in Section 2.2 "Modify and Existing Code"). Once you have found the correct access code, press [*].
3. The display will read "Select (0) Program Code." Using the right arrow (>) key, scroll to the following display:

Select (3) < >
User Card Number

   Press [*] or [3].
4. The display will read "User Card Number Enter #" followed by "0000000." Enter the access card number using the number keys.
5. Press [#] when the access card number has been entered. The display will return to "Select (3) User Card Number."

Programming Access Cards for New Users

If there is the user has not yet been programmed on the system, follow the steps outlined in Section 2.1 "Program a New Access Code." Once you have programmed such information as the user name, continue programming from steps 3-5 from above.

Some access card numbers may have the letters A-F as either the first or second digits. To enter these letters into the access card number, press the [*] key followed by the number key corresponding to the letter. The corresponding number keys are the following:

1 = A 2 = B 3 = C 4 = D 5 = E 6 = F

Access Level

Once the access card has been programmed, an access level can be assigned to the user. The access level will determine when the user has access to certain areas. Your installer will have to work with you to set up various access levels on the system, depending on the access times required.

Your installer will customize access levels 02-63 to suit your purposes. Assigning access level 00 means that the user will never have access to a given area. Assigning access level 01 means that the user will always have access to a given area.

To program access level, perform the following. Your starting point should be from the Program Code menu (from Step 3 above):

1. Use the right arrow (>) key to scroll to the following display:

Select (4) < >
Access Level

   Press [*] or [4].
2. The display will read "Access Level Enter 00-63." The numbers "01" will be in the bottom right-hand corner of the display. This means that the system has assigned Access Level 01 by default to the user and the user will always have access. To assign another access level, enter a 2-digit number from 00-63, corresponding to the new access level.
3. Once the access level has been entered, press [#]. The display will return to "Select (4) Access Level."

User Options

Once the access level has been programmed, three different user options must be programmed. These options are the following:

Card Valid: This option allows the user's access card to become active on the system. Make sure the access card number is also programmed.

Prvleged Card: A privilege card user will be able to access areas via an access card entry point when general access is prohibited. This option, when enabled, will also give the user the ability to grant access to users who have a "Wait for Privilege" access card (see next option).

Wait for Prvl: This option will restrict the user's access to areas via an access card entry point when access is prohibited. A Wait for Privilege user, however, can gain access to the system under the following condition: A Privilege cardholder must present their card after the Wait for Privilege user swipes theirs.

Table 2-1 shows which codes have these options turned on by default. To change the user option settings for these features, follow the directions outlined in Section 2.3 "Change User Code Options."

4.3 Search Using Access Card Numbers

In Section 2.2 “Modify an Existing Code,” two methods were outlined for searching for existing users: by access code number and by user name. You may also search by access card number. To do so, perform the following:

1. Enter [*][5] followed by a Master code.
2. The display will read “Select (0) for User Number Search.” Use the right arrow (>) key to scroll to the following display:

Select (2) for
User Card Search

   Press [2] or [*].
3. Enter the access card number. If the first one or two digits are letters, press [*] followed by the number key corresponding to that letter (A = 1, B = 2, etc.).
4. Once you have entered the access card number, press [*]. If the number is not available, the keypad will sound an error tone and ask you to enter a new number.

Section 5: Testing and Maintenance

IMPORTANT NOTE: *Test your system on a weekly basis and have any system trouble conditions corrected by your installer or service technician.*

5.1 Walk Test

Keypad Command: [*][6][Walk Test Code]

The Walk Test feature allows you to test if the detectors on a partition are in proper working order. There are six options in the walk test menu. To access the walk test options, perform the following:

1. Press [*] [6] followed by the Walk Test code. If you do not know the Walk Test code, ask your installer.
2. Use the arrow (< >) keys to scroll to the walk test option you wish to execute and press [*]. The test will begin once the [*] key is pressed.

Each test must be initiated separately by performing Steps 1 and 2. The five test options are as follows:

- **Local Walk Test (No Bell)**: This option will operate the same as the Local Walk Test except that the bell will not sound when each zone is activated.
- **Local Walk Test:** When this option is selected, the keypad will sound three quick beeps and return to the normal disarmed display. You can then test each detector on the partition. For motion detectors, create movement in the detected area. For door and window contacts, open and close protected doors and windows. Any zone violated will cause the bell or siren to sound for two seconds, confirming that the detectors are working properly.

  During walk test mode, no alarms on that partition will be transmitted to the monitoring station. However, if a PC4400 printer module is installed, the violated zones will be printed.

  Consult each device's manufacturer's instructions for proper ways to test them.
- **Local + Communications Test:** This option will operate the same as Local Walk Test except that alarms will be transmitted to the monitoring station in order to test communications.
- **AML Smoke Test:** This option will test all AMS-220 smoke detectors enrolled on the system. This option will also restore any troubles which were fixed by a service technician. The test will perform itself and will take a few minutes to complete. Once the test is finished, the partition will return to its normal disarmed state.
- **Fire Insp. Test:** This test is only to be performed by your installer or fire inspector.

Disable Walk Test

To end every walk tests—except the "AML Smoke Test"—this option must be selected. Once you have completed your test, enter [*] [6] [Walk Test Code]. Use the arrow keys to scroll to this option and press [*]. The partition will return to its normal disarmed state. The walk test mode will also be automatically disabled if the partition is armed.

Press the [#] key to exit the walk test menu.

5.2 System Test

This option will test the system. This bell/siren will activate for two seconds and system will send a test code transmission to the monitoring station. To start the System test, perform the following:

1. Press [*] [6], then enter a valid access code which has the "System Master" or "Supervisor" option enabled. The display "System Functions Menu" should appear.
2. Use the arrow keys (< >) to scroll to the message "System Test." To start the test, press [*].

5.3 Lamp Test (PC4216)

This test will activate all outputs on the PC4216 output module for two seconds. To execute this test, perform the following:

1. Press [*] [6], then enter a valid access code which has the "System Master" or "Supervisor" option enabled. The display "System Functions Menu" should appear.
2. Use the arrow keys (< >) to scroll to the message "Lamp Test 4216." Press [*]. All outputs connected to the PC4216 output module will activate for two seconds. Once the test is complete, the partition will return to its normal, disarmed state.

5.4 System Maintenance

With normal use, the system requires minimum maintenance. The following points should be observed.

1. Do not wash the keypad with a wet cloth as water will damage the keypad circuits. Light dusting with a slightly moistened cloth should remove normal accumulations of dust.
2. The battery/bell test is designed to determine battery condition. We recommend, however, that the stand-by batteries be replaced every three years. Contact your installation company for service.
3. Do not attempt to replace the small round lithium battery on the control panel circuit board. It is not replaceable. If you suspect there is a problem with your equipment, call your installation company for service.
4. For other system devices such as smoke detectors, passive infrared, ultrasonic or microwave motion detectors and glassbreak detectors, consult the respective manufacturer's literature for testing and maintenance instructions.

Section 6: Fire Safety

6.1 Fire Alarm Operation

The following explains the fire alarm function of this system.

1. Fire Bells Sound

Upon a fire alarm, the bells or sirens will sound. They will pulse on and off in a programmed pattern. The keypad will display the following:

```
First Fire Alarm
[Zone Label]
```

The display will indicate the first fire zone in alarm, followed by any subsequent fire zones in alarm.

2. Bells Silenced

The fire bells or sirens will automatically silence after a programmed period. To manually silence the fire bells, enter a valid access code. A valid access code in this case has the Fire Silence user code option turned on (see Section 2.3 “Change User Code Options” for details).

Once the bells or sirens are silenced, the keypad will display the following:

```
Fire Bell Has
Been Silenced
```

Keypad trouble beeps will sound and the keypad Trouble light will be on. This is a Fire Bell Silence trouble. This trouble cannot be silenced.

3. Reset Fire Zones

In order to clear the Fire Bell Silence trouble and restore the system to normal operation, enter a valid access code. This will reset all fire zones. If there is no fire condition once the system has reset, the system will return to normal operation.

If a fire condition is present once the system has reset, the fire alarm function will restart (1. Fire Bells Sound).

6.2 Guidelines for Locating Smoke Detectors

Experience has shown that all hostile fires in residential units generate smoke to a greater or lesser extent. Experiments using typical fires in residential units indicate that detectable quantities of smoke precede detectable levels of heat in most cases. For these reasons, smoke detectors should be installed outside of each sleeping area and on each additional story of the dwelling.

The following information is for general guidance only. The smoke detector manufacturer’s literature should be consulted for detailed installation instructions.

Additional smoke detectors beyond those required should be installed for increased protection. The added areas include: basement, bedrooms, dining rooms, furnace room, utility room and hallways not protected by the required detectors.

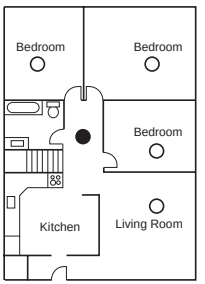

Figure 1

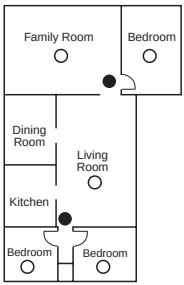

Figure 2

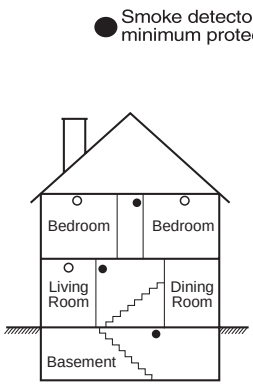

Figure 3

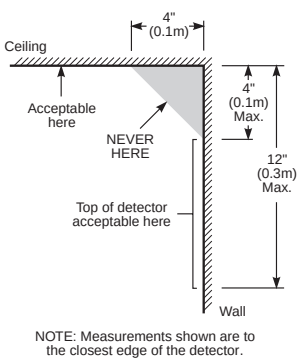

Figure 4

Figure 1: A smoke detector should be located between the sleeping area and the rest of the family unit.

Figure 2: In residential applications, a smoke detector should be located to protect each sleeping area.

Figure 3: A smoke detector should be located on each story of the dwelling.

Figure 4: Smoke Detector Mounting – Dead Air Space: The smoke from a fire generally rises to the ceiling, spreads out across the ceiling surface and begins to bank down from the ceiling. The corner where the ceiling and wall meet is an air space into which the smoke may have difficulty penetrating. In most fires, this "dead" air space measures about 4 in. (0.1m) along the ceiling from the corner and about 4 in. (0.1m) down the wall as shown in Figure 4. Detectors should not be placed in the dead air space.

6.3 Household Fire Safety Audit

Most fires occur in the home. To minimize this danger, a household fire safety audit should be conducted and a fire escape plan should be developed and practised.

1. Are all electrical appliances and outlets in a safe condition? Check for frayed cords, overloaded lighting circuits, etc. If you are uncertain about the condition of your electrical appliances or household service, have a professional evaluate these units.
2. Are all flammable liquids stored safely in closed containers in a well ventilated cool area? Cleaning with flammable liquids should be avoided.
3. Are fire hazardous materials (matches) well out of reach of children?
4. Are furnaces and wood burning appliances properly installed, clean and in good working order? Have a professional evaluate these appliances.

6.4 Fire Escape Planning

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

1. Every person who occupies the building should participate in developing the escape plan.
2. Study the possible escape routes from each location within the premises. In residential applications, special attention should be given to the escape routes from sleeping quarters since many fires occur at night. Escape from a bedroom must be possible without opening the interior door.

Consider the following when making escape plans:

- Make sure that all perimeter doors and windows are easily opened. Ensure that they are not painted shut, and that their locking mechanisms operate smoothly.
- If opening or using the exit is too difficult for children, the elderly or handicapped, plans for rescue should be developed. This includes making sure that those who are to perform the rescue can promptly hear the fire warning signal.
- If the exit is above the ground level, an approved fire ladder or rope should be provided as well as training in its use.
- Exits on the ground level should be kept clear. Be sure to remove snow from exterior doors in winter; outdoor furniture or equipment should not block exits.
- Each person should know of a predetermined assembly point where everyone can be accounted for i.e.: across the street or at a neighboring building. Once everyone is out of the building, call the fire department.

- A good plan emphasizes quick escape. Do not investigate or attempt to fight the fire, and do not gather belongings or pets as this wastes valuable time. Once outside, do not re-enter the house. Wait for the fire department.
- Write the fire escape plan down and rehearse it frequently so that should an emergency arise, everyone will know what to do. Revise the plan as conditions change, such as the number of people on the premises, or if there are changes to the building's construction.
- Make sure your fire warning system is operational by conducting weekly tests (see "Fire Alarm Operation" above). If you are unsure about system operation, contact your alarm installer.

Contact your local fire department to request further information on fire safety and escape planning. If available, have your local fire prevention officer conduct an on-site fire safety inspection.

Appendix A – Special Characters

Below is a chart indicating the available ASCII characters and the 3-digit number required for each character. Instructions on programming ASCII characters is outlined in Section 2 “Access Codes.”

LIMITED WARRANTY

Digital Security Controls Ltd. warrants the original purchaser that for a period of twelve months from the date of purchase, the product shall be free of defects in materials and workmanship under normal use. During the warranty period, Digital Security Controls Ltd. shall, at its option, repair or replace any defective product upon return of the product to its factory, at no charge for labour and materials. Any replacement and/or repaired parts are warranted for the remainder of the original warranty or ninety (90) days, whichever is longer. The original owner must promptly notify Digital Security Controls Ltd. in writing that there is defect in material or workmanship, such written notice to be received in all events prior to expiration of the warranty period.

International Warranty

The warranty for international customers is the same as for any customer within Canada and the United States, with the exception that Digital Security Controls Ltd. shall not be responsible for any customs fees, taxes, or VAT that may be due.

Warranty Procedure

To obtain service under this warranty, please return the item(s) in question to the point of purchase. All authorized distributors and dealers have a warranty program. Anyone returning goods to Digital Security Controls Ltd. must first obtain an authorization number. Digital Security Controls Ltd. will not accept any shipment whatsoever for which prior authorization has not been obtained.

Conditions to Void Warranty

This warranty applies only to defects in parts and workmanship relating to normal use. It does not cover:

- damage incurred in shipping or handling;
- damage caused by disaster such as fire, flood, wind, earthquake or lightning;
- damage due to causes beyond the control of Digital Security Controls Ltd. such as excessive voltage, mechanical shock or water damage;
- damage caused by unauthorized attachment, alterations, modifications or foreign objects;
- damage caused by peripherals (unless such peripherals were supplied by Digital Security Controls Ltd.);
- defects caused by failure to provide a suitable installation environment for the products;
- damage caused by use of the products for purposes other than those for which it was designed;
- damage from improper maintenance;
- damage arising out of any other abuse, mishandling or improper application of the products.

Digital Security Controls Ltd.'s liability for failure to repair the product under this warranty after a reasonable number of attempts will be limited to a replacement of the product, as the exclusive remedy for breach of warranty. Under no circumstances shall Digital Security Controls Ltd. be liable for any special, incidental, or consequential damages based upon breach of warranty, breach of contract, negligence, strict liability, or any other legal theory. Such damages include, but are not limited to, loss of profits, loss of the product or any associated equipment, cost of capital, cost of substitute or replacement equipment, facilities or services, down time, purchaser's time, the claims of third parties, including customers, and injury to property.

Disclaimer of Warranties

This warranty contains the entire warranty and shall be in lieu of any and all other warranties, whether expressed or implied (including all implied warranties of merchantability or fitness for a particular purpose) And of all other obligations or liabilities on the part of Digital Security Controls Ltd. Digital Security Controls Ltd. neither assumes nor authorizes any other person purporting to act on its behalf to modify or to change this warranty, nor to assume for it any other warranty or liability concerning this product.

This disclaimer of warranties and limited warranty are governed by the laws of the province of Ontario, Canada.

WARNING: Digital Security Controls Ltd. recommends that the entire system be completely tested on a regular basis. However, despite frequent testing, and due to, but not limited to, criminal tampering or electrical disruption, it is possible for this product to fail to perform as expected.

Out of Warranty Repairs

Digital Security Controls Ltd. will at its option repair or replace out-of-warranty products which are returned to its factory according to the following conditions. Anyone returning goods to Digital Security Controls Ltd. must first obtain an authorization number. Digital Security Controls Ltd. will not accept any shipment whatsoever for which prior authorization has not been obtained.

Products which Digital Security Controls Ltd. determines to be repairable will be repaired and returned. A set fee which Digital Security Controls Ltd. has predetermined and which may be revised from time to time, will be charged for each unit repaired.

Products which Digital Security Controls Ltd. determines not to be repairable will be replaced by the nearest equivalent product available at that time. The current market price of the replacement product will be charged for each replacement unit.

DSC™
Security Products

©1998 Digital Security Controls Ltd.
Printed in Canada 29002614 R0

AVIS: L'étiquette de l'Industrie Canada identifie le matériel homologué. Cette étiquette certifie que le matériel est conforme à certaines normes de protection, d'exploitation et de sécurité des réseaux de télécommunications. Industrie Canada n'assure toutefois pas que le matériel fonctionnera à la satisfaction de l'utilisateur.

Avant d'installer ce matériel, l'utilisateur doit s'assurer qu'il est permis de le raccorder aux installations de l'entreprise locale de télécommunication. Le matériel doit également être installé en suivant une méthode acceptée de raccordement. L'abonné ne doit pas oublier qu'il est possible que la conformité aux conditions énoncées ci-dessus n'empêchent pas la dégradation du service dans certaines situations.

Les réparations de matériel homologué doivent être effectuées par un centre d'entretien canadien autorisé désigné par le fournisseur. La compagnie de télécommunications peut demander à l'utilisateur de débrancher un appareil à la suite de réparations ou de modifications effectuées par l'utilisateur ou à cause de mauvais fonctionnement.

Pour sa propre protection, l'utilisateur doit s'assurer que tous les fils de mise à la terre de la source d'énergie électrique, les lignes téléphoniques et les canalisations d'eau métalliques, s'il y en a, sont raccordés ensemble. Cette précaution est particulièrement importante dans les régions rurales.

AVERTISSEMENT: L'utilisateur ne doit pas tenter de faire ces raccordements lui-même; il doit avoir recours à un service d'inspection des installations électriques, ou à un électricien, selon le cas.

L'indice de charge (IC) assigné a chaque dispositif terminal indique, pour éviter toute surcharge, le pourcentage de la charge totale qui peut être raccordée à un circuit téléphonique bouclé utilisé par ce dispositif. La terminaison du circuit bouclé peut être constituée de n'importe quelle combinaison de dispositifs, pourvu que la somme des indices de charge de l'ensemble des dispositifs ne dépasse pas 100.

L'Indice de charge de ce produit est 0.1B.

NOTICE: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. Industry Canada does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

User should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The Load Number (LN) assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the total of the Load Numbers of all the devices does not exceed 100.

The Load Number of this unit is 0.1B.

MAXSYS™

PC4020 v3.0 • Instruction Manual

WARNING: *This manual contains information on limitations regarding product use and function and information on the limitations as to liability of the manufacturer. The entire manual should be carefully read.*

FCC COMPLIANCE STATEMENT

CAUTION: Changes or modifications not expressly approved by Digital Security Controls Ltd. could void your authority to use this equipment.

This equipment has been tested and found to comply with the limits for a Class B 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:

- Re-orient 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/television technician for help.

The user may find the following booklet prepared by the FCC useful: "How to Identify and Resolve Radio/Television Interference Problems". This booklet is available from the U.S. Government Printing Office, Washington D.C. 20402, Stock # 004-000-00345-4.

IMPORTANT INFORMATION

This equipment complies with Part 68 of the FCC Rules. On the side of this equipment is a label that contains, among other information, the FCC registration number of this equipment.

NOTIFICATION TO TELEPHONE COMPANY The customer shall notify the telephone company of the particular line to which the connection will be made, and provide the FCC registration number and the ringer equivalence of the protective circuit.

FCC Registration Number: F53CAN-20836-AL-E
Ringer Equivalence Number: 0.1B
USOC Jack: RJ-31X

TELEPHONE CONNECTION REQUIREMENTS Except for the telephone company provided ringers, all connections to the telephone network shall be made through standard plugs and telephone company provided jacks, or equivalent, in such a manner as to allow for easy, immediate disconnection of the terminal equipment. Standard jacks shall be so arranged that, if the plug connected thereto is withdrawn, no interference to the operation of the equipment at the customer's premises which remains connected to the telephone network shall occur by reason of such withdrawal.

INCIDENCE OF HARM Should terminal equipment or protective circuitry cause harm to the telephone network, the telephone company shall, where practicable, notify the customer that temporary disconnection of service may be required; however, where prior notice is not practicable, the telephone company may temporarily discontinue service if such action is deemed reasonable in the circumstances. In the case of such temporary discontinuance, the telephone company shall promptly notify the customer and will be given the opportunity to correct the situation.

ADDITIONAL TELEPHONE COMPANY INFORMATION The security control panel must be properly connected to the telephone line with a USOC RJ-31X telephone jack.

The FCC prohibits customer-provided terminal equipment be connected to party lines or to be used in conjunction with coin telephone service. Interconnect rules may vary from state to state.

CHANGES IN TELEPHONE COMPANY EQUIPMENT OR FACILITIES The telephone company may make changes in its communications facilities, equipment, operations or procedures, where such actions are reasonably required and proper in its business. Should any such changes render the customer's terminal equipment incompatible with the telephone company facilities the customer shall be given adequate notice to the effect modifications to maintain uninterrupted service.

RINGER EQUIVALENCE NUMBER (REN) The REN is useful to determine the quantity of devices that you may connect to your telephone line and still have all of those devices ring when your telephone number is called. In most, but not all areas, the sum of the RENs of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices that you may connect to your line, you may want to contact your local telephone company.

EQUIPMENT MAINTENANCE FACILITY If you experience trouble with this telephone equipment, please contact the facility indicated below for information on obtaining service or repairs. The telephone company may ask that you disconnect this equipment from the network until the problem has been corrected or until you are sure that the equipment is not malfunctioning.
Digital Security Controls Ltd. 160 Washburn St., Lockport, NY 14094

WARNING **Please Read Carefully**

Note to Installers

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

System Failures

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

■ Inadequate Installation

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

■ Criminal Knowledge

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

■ Access by Intruders

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

■ Power Failure

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

■ Failure of Replaceable Batteries

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

■ Compromise of Radio Frequency (Wireless) Devices

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

■ System Users

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

■ Smoke Detectors

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

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

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

■ Motion Detectors

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

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

■ Warning Devices

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

■ Telephone Lines

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

■ Insufficient Time

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

■ Component Failure

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

■ Inadequate Testing

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

■ Security and Insurance

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