DSC®

Installation Manual

• W A R N I N G •

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.

DSC®

PC6820 Software Version 2.0

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.

Installer's Lockout

Any products returned to DSC which have the Installer's Lockout option enabled and exhibit no other problems will be subject to a service charge.

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.

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.

PC6820 Programming Worksheet

You can record your PC6820 module programming here. If you have more than one PC6820 module to install, record your programming in the PC6010 Programming Worksheets instead.

PC6820 Options

PC6820 Module Number: |__|__|

Select Reader Type   Default: 00 |__|__|

Select Door Number:

	Door 01		Door 02	
Toggle Options:	Default		Default	
Lock Reversed?	N	|__|	N	|__|
Unlock on REX?	Y	|__|	Y	|__|
Flash When Arm?	Y	|__|	Y	|__|
Relock on Arm?	N	|__|	N	|__|
Two Readers?	N	|__|		|__|
Code Required?	N	|__|	N	|__|
LED Reversed?	N	|__|	N	|__|
Lock on Close?	N	|__|	N	|__|
Arm Disable?	N	|__|	N	|__|
Access Shunt?	N	|__|	N	|__|

Arm/Disarm Mask:

Area:
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
N N N N N N N N N N N N N N N N

17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
N N N N N N N N N N N N N N N N

Area:
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
N N N N N N N N N N N N N N N N

17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32
N N N N N N N N N N N N N N N N

	Door 01		Door 02	
Door Times:				
Door Unlock Time	010	|__|__|__|	010	|__|__|__|
Door Open Time	030	|__|__|__|	030	|__|__|__|
Lock Delay Time	000	|__|__|__|	000	|__|__|__|
Zone Assignment	000	|__|__|__|	000	|__|__|__|
Delay AutoArm Schedule	01	|__|__|	01	|__|__|
Arm Request Schedule	01	|__|__|	01	|__|__|
Door Unlock Schedule	00	|__|__|	00	|__|__|
REX Schedule	01	|__|__|	01	|__|__|
Second Card Schedule	00	|__|__|	00	|__|__|
Disarm Request Schedule	00	|__|__|	00	|__|__|

Access Level (enter 02 - 63) Default (all levels): [00]

Access Level	Schedule Number	Access Level	Schedule Number	Access Level	Schedule Number	Access Level	Schedule Number	Access Level	Schedule Number	Access Level	Schedule Number
02	|__|__|	23	|__|__|	44	|__|__|	02	|__|__|	23	|__|__|	44	|__|__|
03	|__|__|	24	|__|__|	45	|__|__|	03	|__|__|	24	|__|__|	45	|__|__|
04	|__|__|	25	|__|__|	46	|__|__|	04	|__|__|	25	|__|__|	46	|__|__|
05	|__|__|	26	|__|__|	47	|__|__|	05	|__|__|	26	|__|__|	47	|__|__|
06	|__|__|	27	|__|__|	48	|__|__|	06	|__|__|	27	|__|__|	48	|__|__|
07	|__|__|	28	|__|__|	49	|__|__|	07	|__|__|	28	|__|__|	49	|__|__|
08	|__|__|	29	|__|__|	50	|__|__|	08	|__|__|	29	|__|__|	50	|__|__|
09	|__|__|	30	|__|__|	51	|__|__|	09	|__|__|	30	|__|__|	51	|__|__|
10	|__|__|	31	|__|__|	52	|__|__|	10	|__|__|	31	|__|__|	52	|__|__|
11	|__|__|	32	|__|__|	53	|__|__|	11	|__|__|	32	|__|__|	53	|__|__|
12	|__|__|	33	|__|__|	54	|__|__|	12	|__|__|	33	|__|__|	54	|__|__|
13	|__|__|	34	|__|__|	55	|__|__|	13	|__|__|	34	|__|__|	55	|__|__|
14	|__|__|	35	|__|__|	56	|__|__|	14	|__|__|	35	|__|__|	56	|__|__|
15	|__|__|	36	|__|__|	57	|__|__|	15	|__|__|	36	|__|__|	57	|__|__|
16	|__|__|	37	|__|__|	58	|__|__|	16	|__|__|	37	|__|__|	58	|__|__|
17	|__|__|	38	|__|__|	59	|__|__|	17	|__|__|	38	|__|__|	59	|__|__|
18	|__|__|	39	|__|__|	60	|__|__|	18	|__|__|	39	|__|__|	60	|__|__|
19	|__|__|	40	|__|__|	61	|__|__|	19	|__|__|	40	|__|__|	61	|__|__|
20	|__|__|	41	|__|__|	62	|__|__|	20	|__|__|	41	|__|__|	62	|__|__|
21	|__|__|	42	|__|__|	63	|__|__|	21	|__|__|	42	|__|__|	63	|__|__|
22	|__|__|	43	|__|__|			22	|__|__|	43	|__|__|		

	Default		Default	
Code Schedule	01	|__|__|	01	|__|__|
Access Log Schedule	00	|__|__|	00	|__|__|

Section 4: Diagnostics

4.1 Hardware Reset

On occasion, it may be necessary to perform a reset of the PC6820 to factory default programming. To perform a hardware reset of an PC6820 module, do the following:

1. Power down the PC6010 by removing both AC and battery power from the control panel.

2. Power down the PC6820 module by removing both AC and battery power from the unit.

3. Remove all connections from the following PC6820 terminals: OUT (for OUT DOOR 1), Door (for INPUTS DOOR 1) and AUX+.

4. On the selected PC6820, connect a short from the terminals marked as OUT (for OUT DOOR 1) and Door (for INPUTS DOOR 1). Next connect a 5600 ohm resistor from the Door input to the AUX+ terminal.

5. Restore AC power to the PC6820 module .

6. Wait for 10 seconds then remove AC power from the PC6820 module.

7. Remove the connections made in Step 4.

8. Any terminal connections removed in Step 3 can now be reconnected.

9. Restore AC and battery power to the PC6820 module.

10. Restore AC and battery power to the PC6010 control panel.

The PC6820 will now indicate to the PC6010 that a hardware default has been performed and the PC6010 will retransmit all programming information back to the PC6820 modules. All keypads on the system will beep quickly 16 times to indicate that the programmed information has been sent to the PC6820.

Be sure to remove all connections involved in the hardware default procedure when the hardware default has been completed.

NOTE: *When performing a hardware or software default of the PC6010 be sure to also perform a hardware default on the PC6820. This will ensure that all unwanted programming has been removed from the module.*

4.2 Diagnostics via VTAL LED (L1)

The VTAL LED (located on the right hand side of the circuit board) of the PC6820 is capable of providing diagnostics information for various conditions that may appear on the module.

- Steady flash (once per second) indicates normal operation.

- Fast flash indicates that communication to the PC6010 has been lost (Combus fault).

- On steady (1/2 second) indicates data is being received from an access card reader.

Table of Contents

PC6820 Access Control Module Wiring Diagram

- Battery and AC Connections
- Combus Connections

- Lock device and Reader Connections
- Typical Zone Circuits

PC6820

L1

ECM2 TAMP — READER PWR— RDR 1— RDR 2—
LK2 GND -IN+ GRN WHT GRN WHT

A C | + - | LK1- + LK2 | RED BLK YEL GRN | DOOR Ç REX POST Ç ARM | DOOR Ç REX POST Ç ARM | LED BUZ OUT | LED BUZ OUT
A U X   LCK PWR   COM BUS   — INPUTS DOOR 1 —   — INPUTS DOOR 2 —   OUT DOOR 1   OUT DOOR 2

Transformer
16.5 V @ 40 VA

16.5 VAC 40 VA

To PC6010
Control Panel

The REX, POST and ARM inputs are capable of being used with normally closed loops as well as single end of line resistors (5600Ω). When using Double end of line resistors, these inputs must still be used in the single end of line configuration.
Note: If these inputs are left unused, they must be terminated with a 5600Ω resistor.

Follow one of the end of line configurations for the door inputs (below). These inputs are capable of normally closed loops, single end of line or double end of line.

Note: If this input is left unused it must be terminated with a 5600Ω resistor.

BLK   RED

Battery 12 VDC
Minimum 7.0 Ah

Locking Device
These may be LK1 and LK2 electric strikes (12Vdc, 250mA max.) locking device. If the output is left unused, a 1000Ω resistor must be used to terminate the connection.

Typical Zone Circuits

Any Door Input | Any COM Terminal | Any Door Input | Any COM Terminal

Double end of line circuit, 2 normally closed contacts with 5600Ω end of line resistors.

Double end of line circuit, 1 normally closed contact with 5600Ω end of line resistors.

5600Ω Resistor Colour Band:
Green/Blue/Red/Gold

NOTES:
1. The connection to the mains supply must be made as per the local authorities' rules and regulations. In the UK, as per BS6701.
2. If during the installation a knockout is removed, it is the installer's responsibility to ensure that the same degree of protection for the cabinet is provided by the use of bushings, fittings, etc.
3. The cabinet must be secured to the building structure before operation.
4. The equipment is intended to be installed by SERVICE PERSONNEL ONLY or equivalent (e.g.: persons having appropriate technical training and experience necessary to be aware of hazards to which they are exposed in performing that task.

5. Internal wiring shall be routed in a manner that prevents:
   - excessive strain on wire and on terminal connections;
   - loosening of terminal connections;
   - damage of conductor insulation.
6. The power supply shall meet the applicable requirements of the Low Voltage Directive.

Disarm Request Schedule
This schedule will program the times when the selected areas may be disarmed by a user presenting their access card at the appropriate reader. Only areas which have the door's zone assigned to them, and that are selected in the arm/disarm mask will be affected.

To disarm the area(s), the user must present their access card and open the door. The area(s) will be disarmed if the Disarm Request schedule is active. If the user presents their card outside of the Disarm Request schedule time window, the door will be unlocked but the area(s) will not be disarmed when the door is opened. The user must then enter their access code at a keypad to disarm the area(s).

NOTE: *To disarm an area or enter an area which is armed, the user must be assigned to the area, and the user's disarm attribute must be enabled in access code and card programming. See your PC6010 Maintenance Manual for information on programming access codes and cards.*

The default date schedule is 00 (disabled).

Code Schedule
When this schedule is active, the door will not unlock until both an access card is presented AND a valid access code is entered on the keypad. When the schedule is inactive, the door will unlock when only an access card is presented.

If Schedule [00] is programmed into this section, the door will be unlocked by only an access card when the area(s) the door is assigned to are disarmed. When the areas are armed, an access code will also be required.

NOTE: *The Code Required option must be enabled in order for this feature to work.*

The default date schedule is 01.

Access Log Schedule
Program a schedule that determines when the system will log access granted events in the event buffer. The default date schedule is 00 (disabled).

3.8   Access Level
Access levels allow specific users to have access to areas of the system at various times of the day. Each door can have multiple access levels assigned to it. Each access level will follow one date schedule.

There are 63 access levels for each door. To program access levels, select an access level number (02-63) and then enter the date schedule that the access level will follow. The access level will only be valid for the door during the window provided by the date schedule. Access cards programmed with access level 01 always have access to all doors. Access levels 02 - 63 will be recognized by the card reader during the windows provided by the assigned date schedule.

Date Schedules 00 and 01
Access levels programmed with date schedule 01 will always be recognized by the door. Access levels programmed with date schedule 00 will never be recognized by the door. In order to disable an access level for a door, assign the access level to Date Schedule 00.

By default all access levels are assigned to Date Schedule 00 (disabled).

3.9   Keypad/Reader Assignment
If you install an LCD6501 keypad next to a reader, you can program the system so that users will need to both enter an access code, and swipe their card, to gain entry to the user menu on the keypad. (See the "Code Required" PC6820 toggle option.) For this to work correctly, you will need to assign keypads used this way to a specific reader. When you enter this section, select the keypad you want to assign (01-16). Then, select the PC6820 module (01-16), and the reader (door 01-02) you want to assign the keypad to.

NOTE: *When you assign a reader to a keypad, you should not set up the reader to also control a door. The reader should only be used to grant access to the keypad.*

NOTE: *Only one keypad should be assigned to any one reader.*

When you assign a keypad to a reader, the keypad will prompt "Present Card" on the start screen, instead of "Enter Your Code". If a valid card is presented, the display will change to "Enter Your Code" . If no code is entered, the display returns to "Present Card".

NOTE: *Do not use the arm disable option for readers that are assigned to keypads.*

3.10 Programming Access Cards
In order for an access card to function on the PC6820 the card must first be programmed into the PC6010. This is done through user programming. See your PC6010 *Maintenance Manual* for more information on programming access codes and cards.

Door Open Time

Program the amount of time an access door can remain open before a Door Open Too Long event is generated. After half of the Door Open Time has expired, the reader buzzer will pulse on and off as a warning. At the end of the Door Open Time, the buzzer will sound steady to indicate that the door has been left open too long. The default setting is 030 seconds. Valid entries are from 001-255 seconds.

Lock Delay Time

The system will wait the programmed amount of time after the system is armed, before locking the door. Valid entries are 000-255 seconds. The default time is 000 seconds.

3.6   Zone Assignment for Access Doors

Assign each "door" to a zone on the PC6010. Any zone from Zone 017 to 256 may be used. Entering [000] disables zone assignment.

The PC6010 uses double end-of-line resistor zone supervision. The end of line resistors used for the door inputs are 5600Ω for the alarm contact. If you will be using DEOL resistors, the tamper contact is also 5600Ω.

Program the zone the door is assigned to as a Standard Delay, Auxiliary Delay, or a Force Arm Delay zone. See your PC6010 *Programming Manual* for information on programming zones.

3.7   Access Door Schedules

You can assign an PC6010 date schedule to each of the following access door features. Program the date schedules in the PC6010 Event Scheduling section. See the PC6010 *Programming Manual* for more information. A date schedule will include the start and end times for each event, the days of the week the schedule will be active for and any holiday groups the event will observe.

Date Schedules 00 and 01

If you program date schedule 00, the feature will be disabled (this schedule is never active). If you program date schedule 01, the feature will be always on (this schedule is always active). For more information regarding date schedule programming, please refer to your PC6010 *Programming Manual*.

You can assign date schedules to the following access door features:

Delay AutoArm Schedule

Program a date schedule that determines when the automatic arming sequence can be postponed by a user presenting their access card at the appropriate reader. Only the areas to which the door's zone are assigned and that are selected in the arm/disarm mask will be affected.

The user's access card must also be assigned to the appropriate areas, and have the disarming attribute enabled for the feature to work correctly. See your PC6010 *Maintenance Manual* for information on programming access codes and cards.

The default date schedule is 01.

Arm Request Schedule

Program a date schedule that determines when the selected areas may be armed by a user presenting their access card at the appropriate reader. Only the areas assigned to the door zone and selected in the arm/disarm mask will be affected.

The user's access card must also be assigned to the appropriate areas and have the arming attribute enabled in order for arming to occur. See your PC6010 *Maintenance Manual* for information on programming access codes and cards.

The default date schedule is 01.

Door Unlock Schedule

Program a date schedule that determines when the access door will be unlocked. When the door is unlocked, a user will not require an access card to open the door. The door will remain unlocked for the duration of the schedule. Opening the door will not cause a door forced open event.

When the area(s) to which the door zone is assigned are armed, the door will automatically lock at the beginning of the exit delay. If the Door Unlock schedule becomes active while the area(s) are armed, the door will not unlock. However, if the area is disarmed while the door unlock schedule is active, the door will unlock, and will remain unlocked until the scheduled end time.

NOTE: *If the door is assigned to more than one area, the door will only lock when the last area to be armed has begun its exit delay.*

The default date schedule is 00 (disabled).

Request To Exit (REX) Schedule

This schedule controls the Unlock on REX option. When the schedule is active, tripping a Request To Exit device will cause the door to unlock for the programmed Door Unlock time (see section 3.5 "Door Times"). If the schedule is not active, a Request To Exit will not cause the door to unlock.

The default date schedule is 01.

Second Card Schedule

This schedule determines when or whether the system will require a second access card to be presented before granting access. When the schedule is active, ALL users assigned to the door must have a second user present their card within the determined time before the user(s) is/are granted access to the area. The order of the presentation of the cards does not matter. When the first user presents their card, the LED on the card reader will flash slowly for 10 seconds. If during this time, the second card is presented, the door will be unlocked and the LED of the reader will turn a solid color.

To have the door grant access to a single card (i.e. a second card is never required), program schedule 00. Program schedule 01 to have a second card always required. Program a schedule from 02-99 to have a second card required only when the schedule is active. The default schedule is 00.

The PC6820 is a versatile Dual Card Reader Access Control module which will enable you to meet the most demanding access control requirements of an installation. The PC6820 is monitored and programmed via the PC6010 control panel. Up to 16 PC6820 modules can be connected to a PC6010 via a 4-conductor Combus, using standard, unshielded station wire.

Each PC6820 is capable of providing double end-of-line supervision for two door inputs which may to assigned to any PC6010 zone.

Each of the two PC6820 Access Card Readers can be programmed to function independently on different doors, or together controlling access for both sides of one door.

Control of the access points can be performed using a variety of equipment. The PC6820 supports four different types of card readers: the Polaris magnetic strip reader, the Shadow Prox proximity card reader, the HID proximity readers, and 26-bit standard Wiegand card readers. The PC6820 also supports the use of any request to exit device including the T-REX exit detector.

1.1   PC6820 Access Control Module Specifications

Two Zone Inputs

- Two programmable supervised zones (5600Ω EOL resistors)
- Zones may be programmed as Standard, Auxiliary, or Force Arm delay zone types
- PC6010 v2.0Y: up to 16 PC6820 can be added (up to 32 access points)

Non Volatile RAM (internal memory)

- Does not lose any system programming when the module is powered down.

Low Current Outputs

- Six low current outputs (open collector outputs switched to ground 25mA max.) :
- Two LED terminals - To the LED input of the reader
- Two BUZ terminals - To the Buzzer input of the reader
- Two OUT terminals - Reserved for future use

Regulated Power Supply (1.5 Amp max.)

- Electronic shutdown protection of the battery, auxiliary output, 5 and 12 V reader power supplies, and lock device power output
- Auxiliary output supply: 12V$_{DC}$, 125mA Max
- LK1 and LK2 Door Strike power: 12V$_{DC}$, 250mA Max
- Reader Power 5V$_{DC}$, 125mA Max
- Reader Power 12V$_{DC}$, 125mA Max

Reader Technology

- Polaris, Shadow Prox, HID Proximity and 26-bit Standard Weigand format

Access Card Compatibility

- Polaris POL-C1CN - Polaris Magnetic Cards
- Shadow Prox, Module Numbers:
  SH-C1 - Shadow Prox Card
  SH-K1 - Shadow Prox Keytag
- HID Proximity:
  HID-C1325KSF - Proximity Card
  HID-C134KSP - Proximity Keytag
- Weigand - Standard 26 bit formats

Battery

- 12V$_{DC}$ 7.0Ah recommended rechargeable gel-cell

Transformer

- 16.5 V$_{AC}$, 40VA

Operating Environment

- 2°C to 40°C (35°F to 110°F) operational Temperature Range
- 90% non-condensing humidity

Output Voltage

- Output voltage = 13.8V$_{DC}$ (with normal AC and a fully charged battery). Devices that require power from the PC6820 should be capable of operation over the voltage range of 10 to 14V$_{DC}$.
- 5V Power Supply - Devices connected to the 5V supply should be capable of operation between 4 and 6V.

Section 2: Installation and Wiring

2.1 Plan Your Installation

When designing a security system with access control, you should first lay out the system on paper. This will help determine the total number of zones, additional expanders, access control points and other system components that you will need to complete the installation.

When you know the location of all points of access, you can choose appropriate points for access control. When working from the layout, be sure to locate the PC6820 module so that the wire runs from each door will be as short as possible.

When deciding the placement of the access points and module, remember to check the capacitance limit for the wire you are using for the Combus. Follow the steps outlined in your PC6010 *System Manual*.

NOTE: *Do not run the Combus to the PC6820 in shielded cable.*

2.2 Installation Steps

Once you have determined the location of the PC6820 and each access point, follow the installation steps outlined below.

1 Installation of PC6820 and accessories:

The PC6820 controller cabinet has been designed for surface mounting. The cabinet is large enough to accommodate the battery backup supply and the necessary wiring connections for most applications. The cabinet should be mounted indoors, in a dry, secure location providing normal temperature, humidity levels, and access to an earth ground connection. The location should be easily accessible for servicing the equipment, and it is recommended that each PC6820 module be near the doors it controls. If the PC6820 is within the access controlled area, keys for the controlled doors must be made available so that the PC6820 can be accessed for servicing.

Connect the various devices for each access door according to the diagram below:
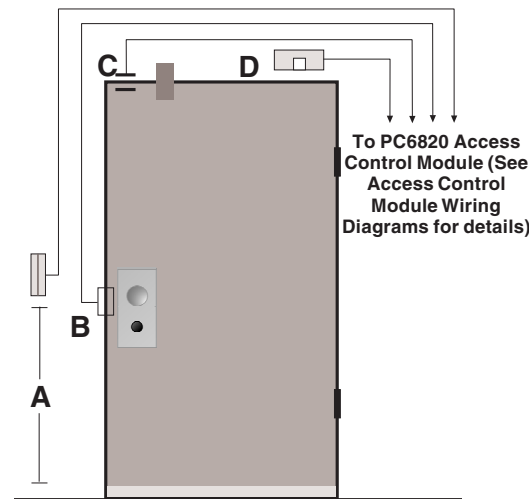
A. Access card readers should be located 107cm (42") from the floor.

B. Connect door strikes using standard 18-gauge cable. Recommended door strikes are electric "Continuous Duty" devices which, when power is cut, will remain in a locked or "secured" state. When using magnetic locks, follow local regulations on the use of these devices.

CAUTION – *Local regulations may prohibit "Lock on Power Failure" if the door is used as a Fire Escape route.*

C. Door contact must be hardwired directly to the PC6820. Wireless or addressable contacts *may not* be used.

D. Install a T-REX exit detector and door alarm (optional) inside of the protected area. (See T-REX Installation Instructions for details on wiring and proper mounting locations.)

2 Tamper protection

A tamper switch may be installed on the cabinet to protect it from unauthorized entry. The normally closed tamper switch is connected to the TAMP and GND (on right side of the PC6820). If the tamper switch is not used, the TAMP terminal must be terminated to any GND terminal with a wire.

3 Connect all inputs, outputs, door locking devices and card readers

Follow the instructions outlined in the sections below for installing each type of device.

4 Power requirements

Install a 16-18V$_{AC}$/40VA transformer outside the cabinet. Connect the red battery lead to the positive terminal and the black battery lead to the negative terminal.

NOTE: *Do not apply power until all wiring is complete. Both the AC and battery connections must be made in order for the PC6820 to function properly.* **Connect the battery before connecting the AC.**

2.3 Inputs – POST, ARM and REX

The door inputs are only capable of following double end-of-line supervision.

The POST, ARM and REX inputs are for Auto-arm postponement, Arming buttons and Request to Exit devices, respectively. These inputs will only be capable of Normally Closed Loops or Single End of Line resistors. When using Double End of Line supervision, these inputs must only be wired for Single End of Line configuration. Please see section 3.5 "Zone Assignment for Access Doors" for information on door input zone programming.

POST Inputs

When enabled, this PC6820 input allows postponement of autoarm of the PC6010 for the partitions selected in the Arm/Disarm mask. To postpone an autoarm, the user must present their access card (during the autoarm pre-alert) and activate the device connected to the POST input. Typically the POST input will be a push button device mounted next to the access card reader (107cm (42") from the floor) which is assigned to the area(s).

The PC6010 will send an Autoarm Abort reporting code to the central station if the reporting code is programmed. The autoarm will restart at the end of the Postpone Arm time unless the area has been manually rearmed. The autoarm may be postponed from the reader as many times as desired.

NOTE: *To postpone an autoarm, the user must be assigned to the area(s) being armed, and the user's access card must have the disarm attribute enabled. See your PC6010 Maintenance Manual for information on programming access codes and cards.*

NOTE: *This option can only be enabled for Door 1.*

If disabled, doors 1 and 2 will have their own zone and area assignments. (Default = No)

- **Code Required**: When this option is enabled the PC6820 will not allow access to the door, or to the assigned keypad, until the user enters an access code. When a user passes their access card, the LED on the reader will flash twice every second to indicate to the user that the reader is waiting for a code to be entered. The user then has 15 seconds to enter their code. If the access code is entered successfully, the reader will grant access. The access code entered must match the code for the user card. Access will not be granted if the access code does not match the code for the access card, even if the code is valid on the system.
  When access is denied to the user due to a wrong/invalid code being entered, or if time has expired waiting for the access code, the LED on the reader will flash 3 times every second and the buzzer will give an audible beep 3 times every second. If an error is made when entering the access code, the user can press the [#] key and re-enter their access code.
  If disabled, no access code will be required. (Default = No)

NOTE: *A reader that requires a code will follow the Total Bad Codes and Lockout Duration programmed in the Keypad Lockout Options section.*

NOTE: *Only use this feature if you have installed either readers with built-in keypads, or where you have installed LCD6501 keypads near each reader. If you have installed keypads near the readers, you should also assign them to the readers in the Keypad/Reader Assignment section. When you assign a reader to a keypad, you should not set up the reader to also control a door. The reader should only be used to grant access to the keypad.*

- **LED Reversed**: If enabled, the normal state of the LED output on the PC6820 will be energized (on). If disabled, the output's normal state will be de-energized (off). (Default = No)

- **Lock On Close**: If enabled, a door unlocked by an access card or by a REX device will lock once the zone is opened and then closed. If disabled, a door unlocked by an access card or by a REX device will relock once the zone is opened. (Default = No)

- **Arm Disable:** If enabled, when all areas assigned in the Arm/Disarm Mask are armed, the reader will be disabled. The LED will not function and access will never be granted until at least one area is disarmed. If disabled, the reader will always function regardless of the arm status of any area. (Default = No)

NOTE: *To use this feature, at least one area must be assigned in the Arm/Disarm mask. See section 3.3, below.*

- **Access Shunt:** If enabled, when the system grants access to a user, the system will bypass the zone that the door is assigned to, for the Door Unlock time. If the door is forced open, the zone will go into alarm (or start an entry delay). If the door is left open past the Door Open time, the zone will go into alarm (or start an entry delay). If disabled, the system will not bypass the zone that the door is assigned to after access is granted. (Default = No)

3.4 Arming and Disarming with Access Cards

The PC6820 can be set up so that users may arm and disarm, or postpone the autoarm of any active area on the system. To set up areas to be armed and disarmed from an access control module, you must program the following:

1. The user's access card must be assigned to the appropriate area(s). An access level must also be assigned to the access card (see section 3.8 "Programming Access Cards").
2. The access door must be assigned a PC6010 zone (see section 3.5 "Zone Assignment for Access Doors"), and the zone must be assigned to the appropriate areas (see below).
3. The Arm/Disarm mask must be programmed to include the area(s) that are to be armed/disarmed from that access card reader (see below).
4. The Postpone Arm, Arm Request and Disarm Request schedules must be programmed with a date schedule other than [00] (see section 3.6 "Access Door Schedules").

TIP: When setting up the arming/disarming options of the PC6820, use a Bell Squawk and a Area Status output to give users a clear indication of the armed status of the area(s). These options can be enabled/disabled on each area (see your PC6010 *Programming Manual* for more information on programming areas).

Arm/Disarm Area Mask

In this section select the area(s) which users will be able to arm and/or disarm when they present the appropriate access card at the reader for the access door.

NOTE: *The zone assigned to the door must be assigned to the same areas selected in the Arm/Disarm Area Mask.*

To program the Arm/Disarm Mask:

1. Scroll to Arm/Disarm Mask, then press [*].
2. Use the arrow (< >) keys to scroll through each area. Press the [*] key to toggle a selected area on or off in the mask.

3.5 Door Times

You can program different times for each door. Scroll to the section you want to program, and press [*].

Door Unlock Time

Program the amount of time that the door will remain unlocked after a valid access card has been presented. This is also the Request To Exit time period. Program the Door Unlock Time to be twice as long as the Lock Delay Time, plus an adequate amount of time for a person to pass through the doorway. [Example: if the Lock Delay Time is 3 seconds, program the Door Unlock Time to be at least 16 seconds - 2 x 3 sec., plus 10 sec. for a person to pass through the door.] You must do this because the door cannot be opened during the Lock Delay Time (because the lock motor is active). The lock motor will be active two times during this time period - once for unlocking and once for locking.

The default setting is 10 seconds. Valid entries are from 001-255 seconds.

The programming for the PC6820 is contained in the main PC6010 installer's programming. You can program the PC6820 from any system keypad, or using DLS-3 downloading software. Refer to the "How to Program" section of the PC6010 *System Manual* for instructions.

NOTE: *By default, before you can enroll modules, or change any system programming, a user must tell the system to "Allow System Service". The system will then allow access to Installer's Programming for 60 minutes. Any user with a Master code can tell the system to allow service at a system keypad. The default Master code is [1234]. See the Maintenance Manual for more information. See the Programming Manual – "Download Section" for more information on the "User Allows Serv" toggle option.*

Before you can program the PC6820, you must enroll it on the system. See the section 4 "Module Enrollment" in the PC6010 *System Manual* for instructions. Be sure to record the module number of each PC6820 you enroll, so that you have a record of how each module has been programmed.

The control panel will transfer all necessary information (access codes, scheduling, etc.) to each PC6820 module whenever one of the following occurs:

1. the main panel is powered up
2. installer's mode is exited
3. an PC6820 loses and then restores communication with the control panel
4. an PC6820 is hardware defaulted
5. an PC6820 is enrolled
6. a downloading session has disconnected.

The data transfer can take up to 2.5 minutes per PC6820 module. When the transfer is completed, all keypads will beep 16 times. Changes to PC6820 programming will not take effect until the data transfer is complete.

You must program the following sections for each PC6820 enrolled on the system. To select a module, scroll to PC6820 options, press [*], then scroll to the number of the PC6820 you want to program and press [*]. Use the arrow (< >) keys to scroll through each programming section. To select a section, press [*].

3.1   Programming Reader Types

The PC6820 is capable of supporting different types of access card readers. The same type of reader must be used on both doors of an access card module, but different modules may use different reader types. To program the reader type for the PC6820:

1. Select the PC6820 module, then press [*].
2. Scroll to "Reader Type", then press [*].
3. Enter the 2-digit code for the reader type you are installing on the selected zone.

   00 Polaris 1- Magnetic card reader. 7 Digits with clock and data.

   01 Shadow Prox - Extended range proximity reader SH5, SH6, SH7, SH-VR 32 Bits.

   02 26 Bit Standard Wiegand reader, HID Proximity readers

   The default access card reader type is **00** (Polaris 1).

NOTE: *Use reader type 01 when using Kantech Secure Format (KSF) devices.*

3.2   Door Options

You can program each "door" on the PC6820 module with different options. Sections 3.2 to 3.7 describe the programming sections available for each door. To program door options:

1. Select which of the two doors to program. Use the arrow (< >) keys to scroll to either Door 1 or Door 2, and then press [*].
2. Use the arrow (< >) keys to scroll through each programming section. To select a section to program, press [*]. For example to program the toggle options for a door, press [*] to select Toggle Options. A series of toggle options will be available for each door. Use the arrow (< >) keys to scroll through each option. Press the [*] key to turn the selected option on or off.

3.3   Toggle Options

The options available for each door are as follows:

- **Lock Reversed**: If enabled, power will be applied to lock the door. The lock will remain closed when idle and will deactivate when a valid access card is used to open the door. The programming for this option is dependent on the type of locking device being used. Check the installation sheet provided with the locking device to see what is required for power.

  If disabled, power will be applied to unlock the door. This option is for use with "Fail Secure" devices such as electronic door strikes. (Default = No)

- **Unlock on REX**: If enabled, tripping a Request To Exit device will cause the door to unlock for the programmed Door Unlock time (see Section 3.4 "Door Times"). If disabled, tripping the Request To Exit device will not cause the door to unlock. (Default = Yes)

- **Flash When Arm**: If enabled, the armed status of the assigned area(s) will be indicated by the light on the reader assigned to the door. The LED will flash slowly for the duration of the armed period.

NOTE: *The area(s) to which the door's zone is assigned must also be selected in the Arm/Disarm Mask for this function to work.*

  If disabled, the LED on the access card reader will not indicate the armed status. (Default = Yes)

- **Relock On Arm**: If enabled, a Request To Arm will relock the door when the arm input is activated. If disabled, a Request to Arm will not relock the door. (Default = No)

- **Two Readers**: If enabled, both "doors" (card readers) will be assigned to the same zone. This will allow the PC6820 to control access both into and out of a secured area at a single access point. The zone and area assignment of both doors on the PC6010 must be the same. (See section 3.5 "Zone Assignment for Access Doors" and your PC6010 *Programming Manual* for information on zone and area programming.)

  Any time an access card is presented at one reader to open the door, the second reader will also allow access. This will prevent a door forced open event (both lock outputs will unlock).

  Each door can still be programmed to have its own access levels (allowing the ability to control both entry and exit permissions for each door on the system), and schedules.

ARM Inputs

When enabled, this PC6820 input will allow designated users to arm the selected areas on the PC6010. To arm the area, the user must first ensure that the area(s) to be armed are secure (close all protected doors and stop movement in areas covered by motion detectors). The user should present their access card and activate the device connected to the ARM input. The exit delay will begin. Typically the ARM input will be connected to a push button device and should be mounted next to the access card reader (107cm (42") from the floor) which is assigned to the area(s).

NOTE: *To arm areas, the user must be assigned to the area(s) being armed, and the user's access card must have the Arm attribute enabled. See your PC6010 Maintenance Manual for information on programming access codes and cards.*

REX Inputs

A Request to Exit device can be used on the inside of the secured area to provide a method of unlocking the door without the need for an access card reader on the inside of the door. When the REX device is tripped, the door will unlock. This will also allow the door to be opened without the door being "Forced open." There are many different types of request to exit devices. Be sure to read the installation sheets provided with each unit for proper installation of the REX devices.

2.4   Outputs – LED, BUZ and OUT Terminals

LED Outputs

The LED outputs for Out Door 1 and Out Door 2 are used for controlling the LED on the access card readers. This allows the PC6820 to provide visual feedback when the access card is presented to the reader. Connect the wire from the reader indicated as LED to the LED terminal of the selected output.

When using this output to switch an external device, the negative terminal of the device must be connected to the LED output terminal. The positive terminal of the external device must be connected to the AUX+ terminal.

BUZ Outputs

The BUZ outputs for Out Door 1 and Out Door 2 are used for controlling the buzzer of the access card readers. This will allow the PC6820 to provide audible feedback to indicate error conditions. Connect the wire indicated as buzzer to the BUZ terminal of the selected output.

When using this output to switch an external device, the negative terminal of the device must be connected to the BUZ output terminal. The positive terminal of the external device must be connected to the AUX+ terminal.

OUT Outputs

Reserved for future use.

2.5   Door Locking Devices – LK1 & LK2 Terminals

Connect door locks to LK1 and LK2. Each lock output can provide up to 250mA at 12Vᴅᴄ. Always check local regulations concerning the installation of magnetic locking devices.

These door locking device outputs can operate DC-powered locking devices such as electromechanical strikes and can be configured to operate in fail-safe or fail-secure modes (normal or reverse action). The typical maximum DC for each lock output is 250mA.

You can program options on the PC6820 for allowing access to doors, or unlocking the doors according to schedules. See section 3 "Programming the PC6820" for more information.

WARNING: *According to local regulations, there may be strict limitations to installing magnetic locks or other similar locking devices on doors used for exit. Be sure to check local regulations before installing any door locking device.*

2.6   Access Card Readers

Each PC6820 module can control two access card readers. The readers can both be installed on one door to control both entry and exit, or on two separate doors to control access in one direction only. Using the proper cable, the readers may be located up to 150 meters (500 feet) from the PC6820 module. Mount the access card readers 107cm (42") from the floor.

WARNING: *Connecting the Red wire lead (or power lead) of a 5VDC reader to the 12VDC terminal may damage the reader. See reader installation procedure for proper power connection.*

Using Two Readers to Control One Door

When using the Two Readers option, the PC6820 can use both readers to control entry and exit from a single access control point. Each reader can be programmed to have its own access levels (allowing the ability to separately control entry and exit permissions for each door on the system), and schedules. See section 3.2 "Door Options" for programming information.

NOTE: *When using the Two Reader option, terminate the Door 2 input to any COM terminal.*

Access Card / Keypad Readers

You can use access card readers with integrated keypads with the PC6820. In order to use this reader type, the user must first present their access card. The LED on the reader will flash twice every second to indicate to the user that the reader is waiting for an access code to be entered. The user will have 15 seconds to enter their access code. If the code is entered successfully, the door will be unlocked. The access code entered must be the correct code for the access card used, otherwise access will not be granted, even if the code entered is a valid code on the system. When access is denied to the user due to a wrong/invalid code being entered, or time has expired waiting for the access code, the LED on the reader will flash 3 times every second and the buzzer will give an audible beep 3 times every second to indicate that access was denied.

Reader LED Flash Rates

Most access card readers will have an LED output to provide visual feedback when the access card is presented to the reader. The light will flash in different ways to indicate the following conditions:

LED State	Access Condition
Steady Red	Door is locked
Steady Green	Door is unlocked – Access granted
Slow flash (state changes every half second)	The area that the Arm/Disarm mask is assigned to is armed
Medium Flash (state changes three times every second)	Waiting for a second card to be presented
Fast flash (State change four times every second)	Access denied/Time expired waiting for a second card.

Buzzer Operation

Most access card readers will have a buzzer output to provide audible feedback. The buzzer output may be connected to operate local warning devices for the following conditions:

- The access controlled door has been forced open. The buzzer will turn on and remain on until the door has been closed.
- The access controlled door has been left open too long. The buzzer will turn on and remain on until the door has been closed. The buzzer will pulse on and off for the last half of the programmed Door Open Time to indicate that the Door Open Too Long event is about to occur.

PC6820 Connection Chart

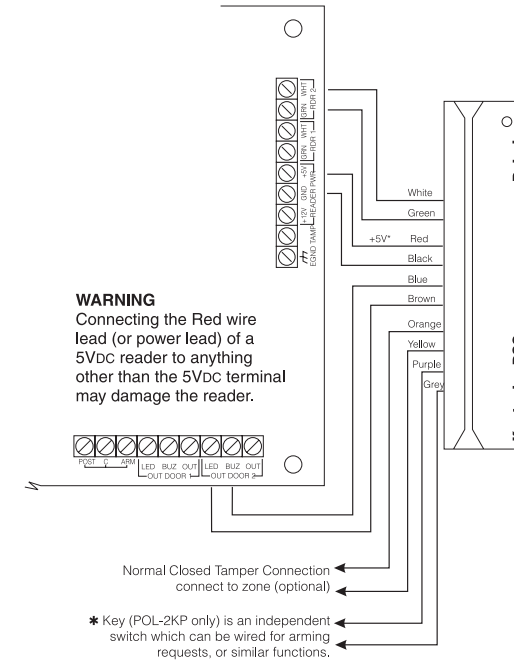| Reader Connection		Function	PC6820 Terminal
Polaris / Shadow Prox	HID		
Green	Green	Data 0	GRN
White	White	Data 1	WHT
Red	Red	+ V_{DC} or +12V_{DC}	+5V or +12V
Black	Black	Ground	GND
Blue	Yellow	Buzzer	Buzz
Brown	Brown (Red LED)	LED	LED
Orange/Yellow (Polaris only)	Terminals marked as Tamper Common & Tamper Select*	Tamper Switch	To PC6010 zone or connected in series with the assigned door input on this module (optional)
————	Blue	Hold	Not used
————	Orange	Green LED	Not used
————	Violet	Return	GND
Purple/Grey (POL-2KP only)	--------	Independent Switch	Can be used for Arm or Post inputs. See PC6820 Wiring Diagram for wiring instructions.

* Tamper connection not available on the MiniProx detector

PC6820 List of Supported Readers and Cards

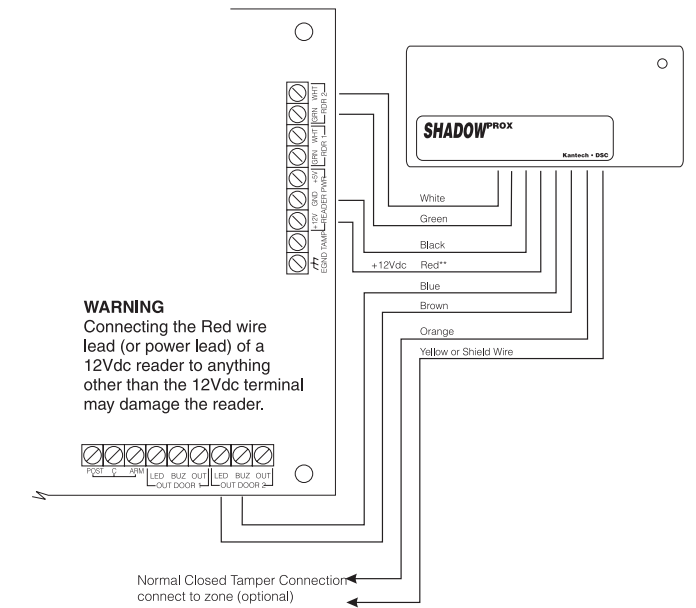| Reader Type	Reader Part Numbers	Supply Voltage	Card Part Numbers
Magnetic Stripe	POL-1, POL-1W, POL-2, POL-2KP	+5Vdc	POL-C1CN
Bar Code	BC-201		
Proximity: Shadow Prox	SH-1, SH-2, SH-2KP	+5Vdc to 14Vdc	SH-C1, SK-K1, SH-CMG1, SH-CMG2
	SH-4, SH-5	+12Vdc	
	SH-6, SH-7	+24Vdc to 28Vdc	
HID	HID-MP5365 - MiniProx	+12Vdc	HID-1365KSF, HID-1335KSF, HID-1334KSF, HID-1365KSF, HID-1385KSF
	HID-PR5355, HID-PR5355KP - ProxPro	+10Vdc to 15Vdc	
	HID-MX5375 - MaxiProx	+14Vdc to 28.5Vdc	

Polaris Readers (POL-1, POL-2, POL-2KP)

WARNING Connecting the Red wire lead (or power lead) of a 5Vdc reader to anything other than the 5Vdc terminal may damage the reader.

Normal Closed Tamper Connection connect to zone (optional)

✱ Key (POL-2KP only) is an independent switch which can be wired for arming requests, or similar functions.

NOTE: Only use the +5V power supply when using Polaris Readers.

Shadow Prox Readers

WARNING Connecting the Red wire lead (or power lead) of a 12Vdc reader to anything other than the 12Vdc terminal may damage the reader.

Normal Closed Tamper Connection connect to zone (optional)

†*NOTE: Only use the +12V power supply when using the Shadow Prox Reader.*

HID Readers

WARNING Connecting the Red wire lead (or power lead) of a 12Vdc reader to anything other than the 12Vdc terminal may damage the reader.

Normal Closed Tamper Connection connect to zone (optional)
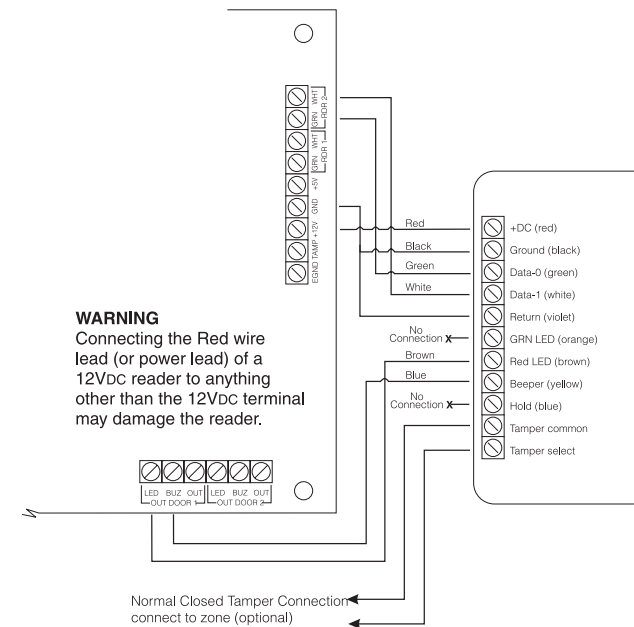
Connecting External Power Supplies
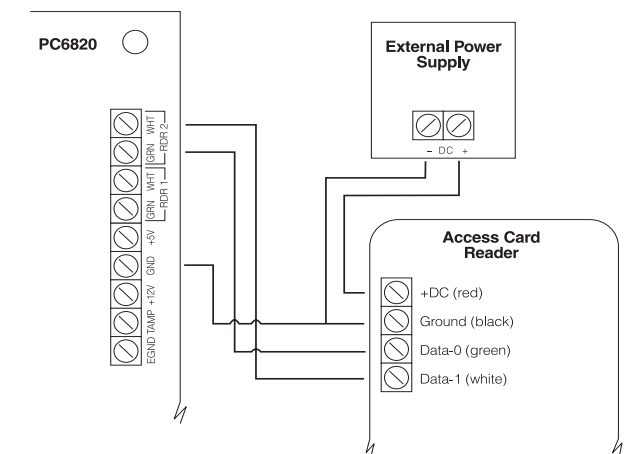
NOTE: Refer to notes listed in main wiring diagram on page ii.

Cabling Specifications

Component	Maximum Wire Length	Cable Description
Reader 5V	150m (500ft)	3 Pair, #18 AWG, stranded, overall shield with extra drain conductor
Reader 12V	150m (500ft)	3 Pair, #22 AWG, stranded, overall shield with extra drain conductor
Inputs (Door, REX, Post, Arm)	300m (1000ft)	2 pair, #22 AWG, twisted pairs
AC Transformer	8m (25ft)	1 pair, #18 AWG Ground 8m (25ft) 1 conductor, #18 AWG, Solid