***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.*

ioPass™

IoPass™
Stand-Alone Door Controller
Installation Manual

KANTECH | access control and integrated systems

DN1445-0303 / V.2.22

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 access 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

An access system must be installed properly in order to provide adequate protection. Every installation should be evaluated by a qualified professional to ensure that every access point is adequately controlled to the building owner's or facility management's expectations. Electric solenoid locks, magnetic locks and gate controllers should be secure and operate as intended. All latches used with the system should have adequate holding power (lbs of force) and latch cavity size for the door weight type (glass, wood, steel) used. A reevaluation must be done during and after construction activity. An evaluation by the fire and/or postal carrier is recommended if this service is available. All authorized emergency personnel should be able to gain immediate access to the premises when required.

■ 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, disconnecting a device, immediately following a person through the controlled gate or door, or interfering with 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.

■ System Users

A user may not be able to operate the system due to permanent or temporary physical disability, inability to reach the keypad, or unfamiliarity with the correct operation. It is important that all system users be trained in the correct operation of the system and that they know how to respond when prompted.

■ 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 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.

■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.

■Security and Insurance

Regardless of its capabilities, a system is not a substitute for property or life insurance. A 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.

Limited Warranty

Kantech Systems 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, Kantech Systems 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 Kantech Systems 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 Kantech Systems 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 Kantech Systems must first obtain an authorization number. Kantech Systems 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 Kantech Systems 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 Kantech Systems);
- 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.

Kantech Systems'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 Kantech Systems 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 Kantech Systems 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 state of California, U.S.A.

WARNING: Kantech Systems 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

Kantech Systems 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 Kantech Systems must first obtain an authorization number. Kantech Systems will not accept any shipment whatsoever for which prior authorization has not been obtained.

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

Products which Kantech Systems 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.

Table of Contents

Section 1 • Introduction to IoPass™ 7

1.1 Product Overview 7
1.2 About this Manual 7
1.2.1 - New in this Version 7
1.2.2 - Record Sheet and Worksheet 7
1.3 Features 7
1.4 Specifications 8

Section 2 • Installing and Wiring IoPass™ 9

2.1 Unpacking the IoPass Unit 9
2.2 Required Equipment 9
2.3 Selecting a Mounting Location 9
2.4 Typical Mounting Diagram 9
2.5 Mounting the IoPass Unit 9
2.6 Mounting the IoProx P100 Reader 10
2.7 Connecting the Door Locking Device 10
2.8 Connecting the T.Rex Exit Detector or Exit Button ...10
2.9 Connecting the Door Contact 10
2.10 Connecting the Alarm Annunciator 10
2.11 Setting Relay 1 Functions 11
2.12 Connecting the Power 11

General Wiring Diagram 12

Section 3 • Programming IoPass™ - Introduction 13

3.1 IoPass Programming Mode 13
3.2 IoPass Factory Defaults 13

Section 4 • Programming IoPass™ - Features 15

4.1 Access Mode Selection 15
4.2 System Passwords 15
4.3 Card Management 15
4.4 Relay-1 Functions 15
4.5 Alarm Relay Functions 15
4.6 Tamper Alarm Function 15
4.7 Forced Entry Alarm Function 15
4.8 Door Ajar Alarm Function 16
4.9 PIN Error Alarm Function 16
4.10 Beeper Key Tone Function 16
4.11 Loop Type Selection 16
4.12 Strike Relay Activation Timer 16
4.13 Reset to Factory Default 16
4.14 Selecting the System Language 16

Section 5 • Programming IoPass™-Step by Step 17

5.1 Selecting the System Language 17
5.2 Selecting the Access Mode 17
5.3 Managing Passwords 17
5.3.1 - Modifying the Master Password 17
5.3.2 - Modifying the Main Password 18
5.3.3 - Modifying the Auxiliary Password 18
5.3.4 - Modifying the Guard Password 18
5.4 Adding & Deleting Cards 19
5.4.1 - Single Add/Single Deletion 19
5.4.2 - Batch Add/Batch Deletion 19
5.4.3 - Adding & Deleting Auxiliary Cards 20
5.5 Viewing Cards 20
5.6 Verifying a Card Number 21
5.7 Guard Function Configuration (Relay-1) 21
5.7.1 - Enabling the Guard Function 21
5.7.2 - Arming / Disarming Quick Reference 21
5.7.3 - Viewing the Audit Trail 22
5.8 Auxiliary Function Configuration (Relay-1) 22
5.8.1 - Enabling the Auxiliary Function 22
5.9 Configuring the Duress Function (Relay-1) 23
5.9.1 - Enabling the Duress Function 23
5.9.2 - Setting the Duress Relay Timer 23
5.9.3 - Using the Duress Function 23
5.10 Configuring the Tamper Alarm Function 23
5.10.1 - Enabling the Tamper Alarm Function 23
5.10.2 - Using the Tamper Alarm Function 24
5.11 Configuring the Forced Entry Alarm 24
5.11.1 - Enabling/Disabling the Force Entry Alarm Function 24
5.11.2 - Using the Force Entry Function 24
5.12 Configuring the Door Ajar Function 24
5.12.1 - Enabling/Disabling the Door Ajar Function .24
5.12.2 - Activating the Alarm Relay on Door Ajar 25
5.12.3 - Setting the Door Ajar Timer 25
5.12.4 - Using the Door Ajar Function 25
5.13 PIN Error Function Configuration 25
5.13.1 - Enabling the PIN Error Function 25
5.13.2 - Enabling Auto-Deletion on PIN Error 25
5.14 Beeper Key Tone Configuration 26
5.15 Loop Type Configuration 26
5.16 Alarm Relay Timer Configuration 26
5.17 Setting the Strike Relay Timer 27
5.18 Resetting the IoPass Unit to Factory Defaults 27

Quick Reference Programming Table 28

Programming Worksheet 29

Card Information Record Sheet 30

Using the IoPass™ System 31

Section 1 • Introduction to IoPass™

1.1 Product Overview

The IoPass is a fully programmable stand-alone access control system that allows entry using proximity technology, keypad or both, for up to 5,000 users. Compact and surface mount, the IoPass is programmed directly from the keypad. The system is available in two models: with integrated or external proximity reader.

Easy Programming

Programming is performed directly from the keypad with visual confirmation of each operation on the 16-character, 2-line LCD display.

Custom Language

IoPass lets you select the system operating language. Messages are displayed in English, French, Spanish, German and Dutch.

Lockout on Invalid Password

To prevent unauthorized persons from gaining password entry by trial and error, the system activates an alarm relay and/or automatically deletes the card number after five tries, once the option is selected in the system.

Integrated or External IoProx Proximity Reader

Two IoPass models are available. The integrated proximity reader model is used for indoor installations. The external proximity reader model provides a vandal and weather resistant feature.

Higher Security Provided by Concealed Relay Module

The IoPass relay module is separate from the unit and can be concealed inside a wall or ceiling. The relay module acts as a connecting module between the IoPass unit and the system devices. Devices (door contact, strike, exit button or detector, alarm annunciator, power, etc.) are connected to this module.

1.2 About this Manual

This Installation Manual provides installation and programming instructions for IoPass installers. Please read this manual carefully before installing or programming the IoPass unit.

1.2.1 - New in this Version

This version of the manual was released to support the new revision of the IoPass firmware (as of version 2.22 The new features include:

1. **Reset** function: you can clear the IoPass memory and reset it to factory default values.
2. **View** function: you can view the next and previous card (access and auxiliary card) programmed in the system.
3. Custom language selection: the IoPass unit can be operated in five languages (English, French, Spanish, German and Dutch).
4. More transaction in the **Audit trail**: 380 last transactions (instead of 10).
5. User PIN required for arming/disarming the unit.

1.2.2 - Record Sheet and Worksheet

You can find the **Card Information Record Sheet** on page 30. Please photocopy this form as reference material so you can keep a record of the cards that are programmed in the IoPass unit.

You can also find a **Programming Worksheet** to record the settings that were modified within the unit. For more information, refer to the “ Quick Reference Programming Table”, page 28.

1.3 Features

- Proximity type reader with a read range up to 10 cm (4");
- Capacity to store up to 5,000 user records;
- Large 2-line LCD of 16 characters with back light feature including power saver function: the backlight will turn off if inactive for more than 3 minutes;
- Three (3) access mode options:
  - Card only (default);
  - Card and PIN;
  - Card only **OR** main password.
- Relay 1 offers one of the three (3) following options:
  - Ability to arm and disarm an external alarm system;
  - Duress function;
  - Auxiliary card function.
- Cards can be enrolled/deleted in batch mode;
- The “Alarm Relay” can be activated if:
  - an incorrect password is entered five times consecutively within four (4) minutes;
  - the unit detects a forced entry;
  - the front cover of the unit is removed (tamper alarm function);
  - the door is opened longer than pre-set time (door ajar function).
- Last 380 Access Granted card numbers can be viewed on-screen;
- Audible key tones;
- Strike, alarm and duress relay have a selectable activation timer (1-255 seconds);
- Selectable door left open timer (1-255 seconds);
- Can be mounted on a standard flush mount electrical box (vertical or horizontal positioning of the box acceptable).

1.4 Specifications

- **Typical read range**—Up to 10 cm (4")[1];
- **Input voltage**—12VDC;
- **Current DC maximum**—300mA;
- **Display**—16 characters, 2 lines, LCD with backlight;
- **Cards**:
  - Access cards—5000 cards
  - Auxiliary cards—20 cards
- **Dimensions (H • W • D)**:
  - cm—15 x 11 x 4.5
  - in—5.9 x 4.3 x 1.8
- **Weight**—380g (13.5oz);
- **Case material**—Gray ABS (UL 94V-0);
- **LED indicator**—Bicolor (green/red);
- **Operating temperatures**—0°C to 50°C (32°F to 122°F);
- **Operating humidity**—5% to 95% (relative humidity non-condensing);
- **Door contact input**—NO or NC selectable;
- **Request-to-Exit input**—NO or NC selectable;
- **Relay output** (Strike, Alarm and Relay-1 relay)—Form C, NO and NC, 3A, 24VDC;
- **Strike, Alarm and Relay-1 timer**—1 to 255 sec.;
- **Door ajar timer**—1 to 255 sec.;
- **Audit trail**—On unit, last 380 transactions;
- **Compatible cards**—IoProx cards P10SHL, P20DYE and P40KEY;
- **PIN length**—4 digits;
- **Certifications**—CE and FCC.

[1] Reduced read range with keytag and Dye-Sub cards.

Section 2 • Installing and Wiring IoPass™

2.1 Unpacking the IoPass Unit

Check that the following parts are in your IoPass package:

- One (1) IoPass unit (SA-500 or SA-600);
- One (1) relay module (SA-RM56 including connectors);
- One (1) hardware kit;
- Ten (10) proximity keytags (P40KEY);
- One (1) IoProx P100 proximity reader (with SA-600 model only).

***NOTE:** The SA-RM56 relay module comes with all the necessary connectors to facilitate installation.*

2.2 Required Equipment

- Power supply—12VDC, 1A (required);
- Cables (required):
  - **Between IoPass and reader**
    2 twisted pairs, solid conductor #22AWG UNSHIELDED
  - **Between IoPass and relay module**
    2 twisted pairs, solid conductor, #22AWG UNSHIELDED
  - **Between relay module and power supply**
    1 pair, solid conductor #22AWG UNSHIELDED

***NOTE:** Maximum wiring distance between equipment—150m (500').*

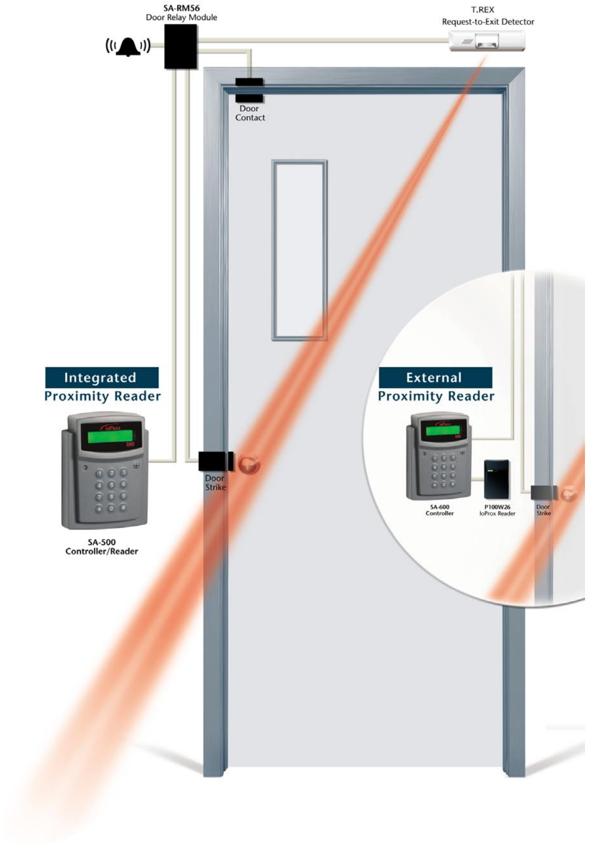
- Door contact (recommended);
- Locking device (required);
- Door alarm or annunciator (recommended);
- T.Rex Request-to-Exit detector (recommended).

2.3 Selecting a Mounting Location

Select a mounting location for the unit using the following guidelines:

- Close to the door being supervised;
- Away from areas with a large amount of background noise;
- It is recommended that you mount the unit so that the LCD is visible to users when requesting access. The top of the unit should not be higher than 45 to 50 inches from the floor.

2.4 Typical Mounting Diagram



2.5 Mounting the IoPass Unit

1. Remove the front panel by squeezing the sides of the unit and sliding forward;
2. Use the provided paper-sticker template to mark the position of the holes on the wall;
3. Mount the base unit to the wall using four (4) screws (provided) to secure the unit to the wall;
4. Replace the cover by gently sliding it back on the unit;
5. The unit offers a tamper alarm protection in case someone tries to remove the cover. For more information, please refer to "Configuring the Tamper Alarm Function" (page 23).

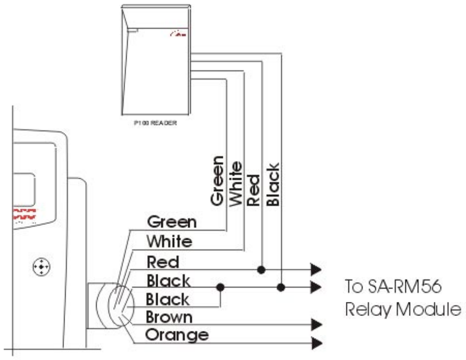
2.6 Mounting the IoProx P100 Reader

***NOTE:** For model SA-600 only.*

To mount the IoProx proximity reader, please refer to installation instructions provided with the reader.

***NOTE:** If the IoPass unit and P100 reader are not on the same side of the door, you will not be able to use the “card and PIN” mode since the keypad of the IoPass unit will not be accessible to cardholders when a valid card is presented to the P100 reader.*

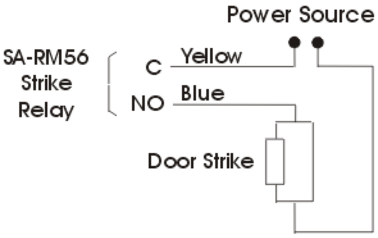
Wiring Diagram



2.7 Connecting the Door Locking Device

To install the door locking device, refer to the manufacturer’s instructions. To connect it, refer to the diagram below.

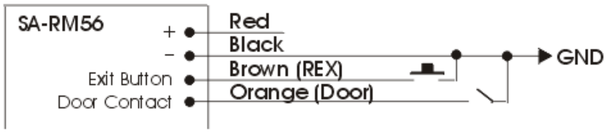
Wiring Diagram



2.8 Connecting the T.Rex Exit Detector or Exit Button

To install the T.Rex Exit Detector/push button, refer to the manufacturer’s instructions. To connect it, refer to the diagram below.

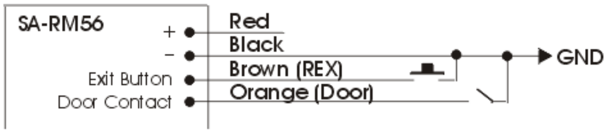
Wiring Diagram



2.9 Connecting the Door Contact

To install the door contact, refer to the manufacturer’s instructions. To connect it, refer to the diagram below.

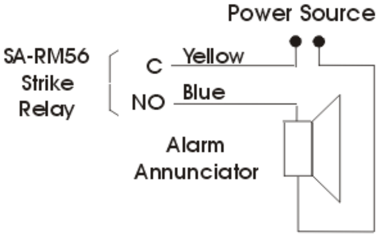
Wiring Diagram



2.10 Connecting the Alarm Annunciator

To install the alarm annunciator, refer to the manufacturer’s instructions. To connect the annunciator (i.e.: horn, bell, etc.), refer to the diagram below.

Wiring Diagram



2.11 Setting Relay 1 Functions

Depending on how you intend to use Relay-1, you will need to configure the jumpers, located on the SA-RM56 relay module, before you mount it inside the wall.

NOTE: *For more information on the relay function, please refer to "Relay-1 Functions" (page 15).*

Jumper Settings:

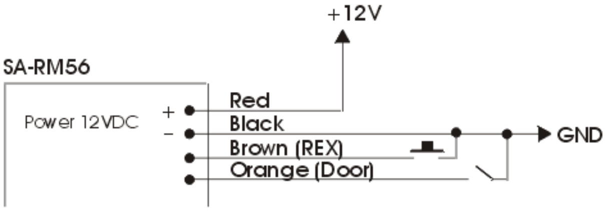
Relay-1 Function

Function	1	2	3
DURESS	**ON**	OFF	OFF
GUARD	OFF	**ON**	OFF
AUX. CARD	OFF	OFF	**ON**

2.12 Connecting the Power

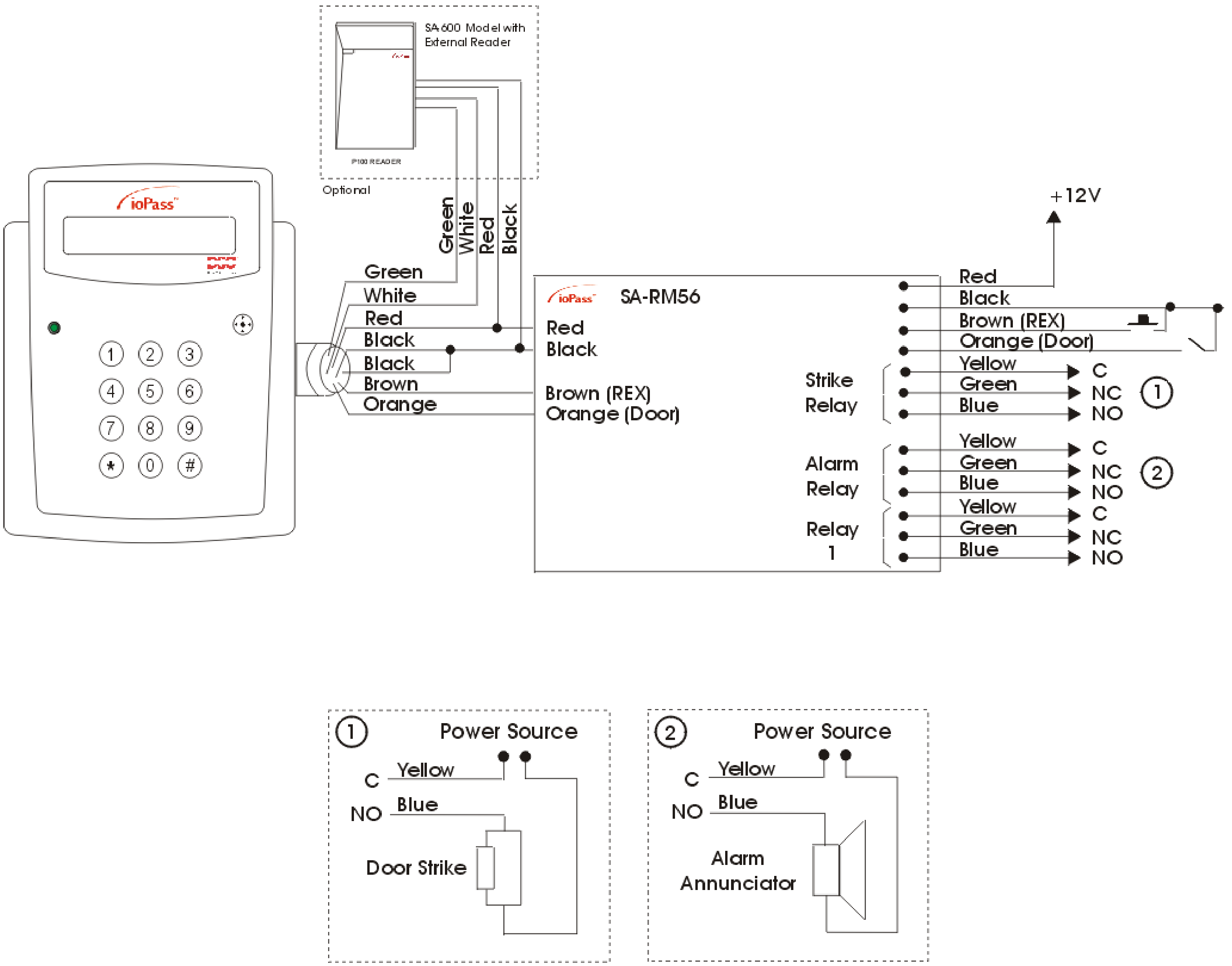
Once all other wiring is complete, power up the unit.

Wiring Diagram



NOTE: *Once all connections are finished, you may start to program the unit. Before you do so, we recommend you read the section called "Programming IoPass™ - Introduction" (page 13).*

General Wiring Diagram



Section 3 • Programming IoPass™ - Introduction

3.1 IoPass Programming Mode

To enter the programming mode, you have to enter the 6-digit Master Password followed by the [#] key. The default Master Password is [111111].

The LCD will display the following information:

```
1. ENROLL   2. PASSWD
3. TIMER    4. SYSTEM
```

From these basic functions, more options are available.

When programming the unit, you need to know that:

- The **[*]** key is used to either go back to the previous menu, or delete what was entered.
- The **[#]** key is used to accept, save the data that was modified or programmed in the system and quit.

3.2 IoPass Factory Defaults

The factory defaults consists of a series of options that are automatically set up in the unit as the “basic” system configuration and can be modified.

Description	Factory Default	To Modify
Access mode	Card only (mode 0)	See p. 17
Master password	111111 (always enabled)	See p. 17
Main password	1234 (always enabled)	See p. 18
Duress function	Disabled	See p. 23
Auxiliary function	Disabled	See p. 22
Auxiliary password	1234567 (default) when enabled	See p. 18
Guard function	Disabled	See p. 21
Guard password	123 (default) when enabled	See p. 18
Tamper alarm function	Disabled	See p. 23
Forced entry alarm function	Enabled	See p. 24
Door ajar	Enabled	See p. 24
Alarm relay activated on door ajar	Disabled	See p. 24
Incorrect PIN keyed in incorrectly five times activates alarm relay (P-ERR)	Disabled	See p. 25
Card auto-deletion on PIN error (5 times)	Disabled	See p. 25
Beeper key tones	Enabled	See p. 26
Alarm relay activation timer when door left open more then the preset time (door ajar)	30 seconds (has to remain open more than 30 seconds to trigger alarm relay—if the function is enabled)	See p. 24
Duress relay active time (Relay-1)	10 seconds (when enabled)	See p. 23
Auxiliary relay active (Relay-1) time	3 seconds	Cannot be modified
Guard relay active time (Relay-1)	Remains activated until deactivated manually	Cannot be modified
Alarm relay active time	240 seconds (4 min.)	See p. 26
Strike relay active time	10 seconds	See p. 27
Exit button input type	Normally Open (NO)	See p. 26
Door contact type	Normally Open (NO)	See p. 26

Section 4 • Programming IoPass™ - Features

4.1 Access Mode Selection

Before you start registering cardholders, you **must select the suitable access mode** for your installation.

This function allows the system administrator to decide how access will be granted to cardholders (card only, with PIN, etc.). The default access mode is set to **"Mode 0 - Card Only"**.

NOTE: *For more information on access modes, refer to "5.2 Selecting the Access Mode", page 17.*

4.2 System Passwords

Four passwords can be programmed in the IoPass unit:

- The **master password**: it is used to program the IoPass unit, to access the programming mode as well as to protect the parameters of the unit. For security purposes, you should modify the master password before you start programming the IoPass unit.
- The **main password** is a "global" password that can be used when access mode "2" is selected.
- Auxiliary password: it used to activate an auxiliary relay when the auxiliary function is enabled in the IoPass unit. This password will automatically be enabled when you enable the auxiliary function.
- The **guard password** is used to arm or disarm the connected security system when the guard function is enabled in the unit. This password will automatically be enabled when you enable the guard function.

NOTE: *For more information on passwords and how to modify them, refer to "5.3 Managing Passwords", page 17.*

4.3 Card Management

Up to 5,000 user cards (plus 20 auxiliary cards) can be registered in the IoPass unit. Depending on how many cards you need to program, you can simply add them one at a time or use the batch process to add a pre-selected batch of cards in the unit.

For more information on cards, auxiliary cards and all functions related to cards, refer to one of the following sections:

- "5.4 Adding & Deleting Cards", page 19:
  - "5.4.1 - Single Add/Single Deletion", page 19;
  - "5.4.2 - Batch Add/Batch Deletion", page 19;
  - "5.4.3 - Adding & Deleting Auxiliary Cards", page 20.
- "5.5 Viewing Cards", page 20;
- "5.6 Verifying a Card Number", page 21;

4.4 Relay-1 Functions

The "Relay-1" (located on the relay module) function depends on your requirements.

There are three (3) possibilities, but **ONLY ONE** can be configured. Depending on your choice, the jumpers of the relay module need to be set up accordingly.

- **Guard Function**—This function is used to arm/disarm the connected security system. Either by using a password and card, or simply a password to arm the system.
- **Auxiliary Function**—This function provides the ability to activate an external device without unlocking the door. This relay can be used to activate the lighting control, an HVAC control, or simply to unlock an auxiliary door.
- **Duress Function**—In general, this relay would be connected to an external alarm system's panic input. When the duress relay is activated, it triggers the panic input on the alarm system, sending a signal to the central station to dispatch the police.

NOTE: *For more information on how to configure and use these features, refer to "5.7 Guard Function Configuration (Relay-1)", page 21; to "5.8 Auxiliary Function Configuration (Relay-1)", page 22, and to "5.9 Configuring the Duress Function (Relay-1)", page 23.*

4.5 Alarm Relay Functions

An alarm relay is provided on the relay module. This alarm relay can be activated by the following events:

- Tamper Alarm (if enabled);
- Forced Entry (enabled by default);
- Door Ajar (if enabled);
- Incorrect Password keyed in five times consecutively within four (4) minutes (if enabled).

NOTE: *The alarm relay is always "enabled", but users can configure options that can trigger this relay as detailed in section "5.16 Alarm Relay Timer Configuration", page 26 (default 240 seconds).*

4.6 Tamper Alarm Function

When enabled, the tamper alarm function automatically activates the "Alarm Relay" and sound the internal buzzer when the front panel of the unit is removed.

NOTE: *Please refer to "5.10 Configuring the Tamper Alarm Function", page 23 for more information.*

4.7 Forced Entry Alarm Function

The Forced Entry Alarm Function is already enabled in the unit. This function automatically activates the "Alarm Relay" when the door contact detects unauthorized access (without card or password or both). When this occurs, a "door forced open" type of event is generated.

NOTE: *For more information refer to "5.11 Configuring the Forced Entry Alarm", page 24.*

4.8 Door Ajar Alarm Function

Already enabled in the unit, this function activates the "Alarm Relay" when the door is opened longer than the pre-set time following an access granted operation.

The user can decide if the alarm relay needs to be activated when this situation occurs.

NOTE: *Please refer to "5.12 Configuring the Door Ajar Function", page 24 for more information.*

4.9 PIN Error Alarm Function

This function, if enabled, will automatically activate the "Alarm Relay" when a cardholder keys in his PIN incorrectly five (5) times consecutively within four (4) minutes.

Furthermore, the card can automatically be deleted (from the unit's memory) when this situation occurs.

NOTE: *Please refer to "5.13 PIN Error Function Configuration", page 25 for more information.*

4.10 Beeper Key Tone Function

This function, already enabled in the unit, provides an audible "beep" tone when the keys of the keypad are used.

NOTE: *Please refer to "5.14 Beeper Key Tone Configuration", page 26 for more information.*

4.11 Loop Type Selection

The IoPass unit allows the installer to modify the loop type of the exit button and door contact.

These normally open contacts can be modified to normally closed to suit installer's requirements.

NOTE: *For more information refer to "5.15 Loop Type Configuration", page 26.*

4.12 Strike Relay Activation Timer

By default, the locking device relay is pre-set to 10 seconds, meaning that the door will remain unlocked for that period of time.

The timer can be modified from 1-255 seconds.

NOTE: *For more information refer to "5.17 Setting the Strike Relay Timer", page 27.*

4.13 Reset to Factory Default

A reset function is available in the unit. It is used to clear all configured options and cards from the unit memory which will bring back the IoPass unit to factory defaults.

To clear the memory, the master password is required.

NOTE: *For more information refer to "Resetting the IoPass Unit to Factory Defaults" (page 27).*

4.14 Selecting the System Language

IoPass offers users the ability to select the System operating language. You can operate the system in English, French, Spanish, German and Dutch.

NOTE: *For more information on setting the system language, refer to "Selecting the System Language" (page 17).*

Section 5 • Programming IoPass™-Step by Step

5.1 Selecting the System Language

IoPass offers users the ability to select the System operating language. To select the system language:

1. Enter the master password (default is [111111]), followed by the [#] key.
2. The LCD displays the following:

```
1. ENROLL   2. PASSWD
3. TIMER    4. SYSTEM
```

3. Press [4-System]. The LCD displays:

```
1. ALARM    2. CHECK
3. MODE     4. OTHER
```

4. Press [4-Other]. The LCD displays:

```
1. TONE     2. DURESS
3. MORE     4. LANGUAGE.
```

5. Press [4-Language]. The LCD displays the current language. For example, if the IoPass is set to display messages in English, it will display:

```
ENGLISH
Press ’1’---Change
```

6. Press [1] until the desired language is displayed, then press the [*] or the [#] key. The IoPass unit will start displaying messages in the selected language.

***NOTE:** Pressing the [#] key brings you back to the Welcome message (Ready for card). Pressing the [*] key changes the display language in the selected language without going back to the Welcome message.*

5.2 Selecting the Access Mode

The access mode is the most important function of the system. **Before** you start enrolling cards, you need to determine how access will be granted to users.

Three (3) access modes are available in the system:

- **Mode “0” - Card only - DEFAULT:** This mode only requires the user to present his card to be granted access.
- **Mode “1” - Card and PIN:** This mode requires that the user presents his card and then enters his PIN on the keypad. Make sure the keypad can be accessed by cardholders if you are using this mode.
- **Mode “2” - Card only OR main password only:** This mode will require that the user presents his card to the reader to be granted access **OR** enters his main password using the keypad to be granted access.

To Select an Access Mode:

1. Enter the master password (default is [111111]), [#].

***NOTE:** It is strongly recommended to modify the default password before programming the unit. To modify the master password, refer to “Managing Passwords” (page 17).*

2. The LCD displays the following:

```
1. ENROLL   2. PASSWD
3. TIMER    4. SYSTEM
```

3. Press [4-System]. The LCD displays:

```
1. ALARM    2. CHECK
3. MODE     4. OTHER
```

4. Press [3-Mode]. The LCD displays:

```
1-ACCESS MODE
2-DOOR_INPUT
```

5. Select [1-Access mode]. The LCD displays:

```
CURRENT: MODE ? (?=0,1 or 2)
PRESS ’1’ --] CHANGE
```

6. Press [1] until desired mode is displayed. Pressing this key will toggle between selections;
7. When the required mode is displayed (0, 1 or 2), press [#] to save and exit.

5.3 Managing Passwords

Four (4) passwords can be programmed in the IoPass unit. It is recommended to record system passwords on the “Quick Reference Programming Table” (page 28), and keep it in a secure location.

5.3.1 - Modifying the Master Password

The master password is used to access the programming mode and to protect the parameters of the IoPass controller.

To Modify the Master Password

1. Enter the master password (default is [111111]), then [#].
2. The LCD displays the following:

```
1. ENROLL   2. PASSWD
3. TIMER    4. SYSTEM
```

3. Press [2-Passwd]. The LCD displays the following:

```
1. MASTER   2. MAIN
3. AUX.CR   4. GUARD
```

4. Press [1-Master]. The LCD displays:

```
Current: 111111
    New:
```

5. Enter the new master password. This password must be 6 characters.
6. Press [#] to save and exit.

5.3.2 - Modifying the Main Password

The main password is a "global" password that can be used when **Access mode "2"** is selected. This access mode offers two options:

- Users present the card to the reader, OR
- They enter the main password to gain access.

To Modify the Main Password:

1. Enter the master password (default is [111111]) then [#]. The LCD displays the following:

```
1. ENROLL   2. PASSWD
3. TIMER    4. SYSTEM
```

2. Press [2-Passwd]. The LCD displays the following:

```
1. MASTER   2. MAIN
3. AUX.CR   4. GUARD
```

3. Press [2-Main]. The LCD displays the default Main password:

```
Current: 1234
    New:
```

4. Enter the new main password. This password must be 4 characters.
5. Press [#] to save and exit.

5.3.3 - Modifying the Auxiliary Password

The auxiliary password is used to activate an auxiliary relay when the auxiliary function is enabled in the IoPass unit.

You can either use the auxiliary card OR the auxiliary password to activate the auxiliary relay.

To Modify the Auxiliary Password:

1. Enter the master password (default is [111111]) then [#]. The LCD displays the following:

```
1. ENROLL   2. PASSWD
3. TIMER    4. SYSTEM
```

2. Press [2-Passwd]. The LCD displays the following:

```
1. MASTER   2. MAIN
3. AUX.CR   4. GUARD
```

3. Press [3-Aux.Cr]. The LCD displays the default password and invites you to enter a new one:

```
Current: 1234567
    New:
```

4. Enter the new auxiliary password. This password must be 7 characters.
5. Press [#] to save and exit.

5.3.4 - Modifying the Guard Password

The guard password is used to arm or disarm the connected security system when the guard function is enabled. The Guard password is automatically enabled when you enable the guard function.

To Modify the Guard Password

1. Enter the master password (default is [111111]) then [#]. The LCD displays the following:

```
1. ENROLL   2. PASSWD
3. TIMER    4. SYSTEM
```

2. Press [2-Passwd]. The LCD displays the following:

```
1. MASTER   2. MAIN
3. AUX.CR   4. GUARD
```

3. Press [4-Guard]. The LCD displays the default password and invites you to enter a new one:

```
Current: 123
    New:
```

4. Enter the new guard password. This password must be 3 characters.
5. Press [#] to save and exit.

5.4 Adding & Deleting Cards

Up to 5,000 cards can be stored in the unit (plus 20 auxiliary cards).

NOTE: *Once you have selected the "Access Mode", you may start enrolling cards. Otherwise, please refer to "Access Mode Selection" (page 15).*

Use the provided "Card Information Record Sheet" (page 30) to store user information (card number, name and PIN if applicable). Also, if you are using the PIN feature, you may want to gather the PIN from cardholders in advance.

All new cards must be enrolled into the unit before access is allowed. Up to 5,000 cards can be stored in the unit (plus 20 auxiliary cards).

Cards are stored based on their programming sequence within the unit. If a card that is not enrolled is presented to the reader, the message INVALID CARD is displayed.

NOTE: *Depending on how many cards you need to program, you can simply add them one at a time or use the batch process to add a pre-selected batch of cards in the unit.*

If the maximum number of cards (access/auxiliary) has been reached, the message NO SPACE will be displayed each time you attempt to add a new card:

5.4.1 - Single Add/Single Deletion

To add/delete a single card:

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

```
1. ENROLL   2. PASSWD
3. TIMER    4. SYSTEM
```

2. Press [1-Enroll]. The LCD displays:

```
1-ACCESS CARD
2-AUX. CARD
```

3. Press [1-Access Card]. The LCD displays:

```
1. PROGRAM CARDS
2. VIEW CARDS
```

4. Press [1-Program Cards]. The LCD displays:

```
1. S_ADD    2. S_DEL
3. B_ADD    4. B_DEL
```

5. Press:

- [1-S_Add] to add a new card, or
- [2-S_Del] to delete a card from the unit.

The LCD displays:

```
TOTAL CARDS: XX (xx=# of cards in
unit)
CARD NO.__:______
```

6. There are two ways to enter the card number in the system:

- You can simply present the card to the reader and the number will automatically be entered.
- You can type in the number (XX:XXXXX) printed on the card followed by the [#] sign using the keypad. If you need to enter special characters (hexadecimal) see "Special Characters (Hexadecimal)" below, OR

7. Once you have entered the card number, you will see the following screen:

```
CARD NO. XX:XXXX
PIN:
```

OR

```
ALREADY USED
PIN:
```

8. To enter the PIN, enter the 4-digit code using the keypad. Use the [#] key to accept;

NOTE: *If you leave the PIN blank, the unit will assume that no PIN was entered and the user will not be prompted for his PIN.*

9. Once the card has been accepted, the system will display:

```
ACCEPTED
```

10. Following the acceptance message, the unit will display the add/delete card screen. To add/delete another card simply repeat steps 5 and up.

11. To exit the programming mode press [#], [#].

Special Characters (Hexadecimal)

When inputting the card number using the keypad, you may need to program special characters. You can do this using hexadecimal digits. The following hexadecimal digits will insert special characters into the card number. To program a hexadecimal digit press [*], then press the number corresponding to the hexadecimal digit.

- For A press [0]
- For B press [1]
- For C press [2]
- For D press [3]
- For E press [4]
- For F press [5]

If another hexadecimal digit is required, press [*] again, then press the corresponding number. The IoPass will return to decimal programming on the next digit.

Example: To program "4E", you would enter:

- [4] - programs a "4"
- [*][4] - programs an "E"

5.4.2 - Batch Add/Batch Deletion

Before you can use the batch mode to enroll new cards, it is essential that the group of cards be numbered sequentially.

To Add/Delete a group of cards:

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

   ```
   1. ENROLL   2. PASSWD
   3. TIMER    4. SYSTEM
   ```

2. Press [1-Enroll]. The LCD displays:

   ```
   1-ACCESS CARD
   2-AUX. CARD
   ```

3. Press [1-Access Card]. The LCD displays:

   ```
   1. PROGRAM CARDS
   2. VIEW CARDS
   ```

4. Press [1-Program Cards]. The LCD displays:

   ```
   1. S_ADD    2. S_DEL
   3. B_ADD    4. B_DEL
   ```

5. Press [3-B_Add] to add cards or [4-B_Del] to delete a batch of cards. The LCD displays:

   ```
   TOTAL CARDS: XX (xx=#cards in unit)
   CARD NO.__:______
   ```

6. There are two ways to enter the card number in the system:

   - You can simply present the card to the reader and the number will automatically be entered.
   - enter the card number manually followed by the [#]. To enter special characters (hexadecimal) refer to the section “Special Characters (Hexadecimal)” (page 19).

7. Once you have entered the first card number, the LCD will display the following screen:

   ```
   CARD NO. XX:XXXXX
   TOTAL:
   ```

8. Enter the total number of sequential cards that you wish to add/delete followed by the [#] key to accept. The LCD will display:

   ```
   Processing...xx
   ```

   For example if you wanted to add 250 cards that are sequentially numbered you would enter the first card (lowest) number and then select 250 for the total. If for example you enter [01:00001] as the first card number, the system would automatically program cards [01:00001] to [01:00250] into the system.

NOTE: *Cards that were enrolled in the unit using the “batch mode” will function without having to enter the PIN, even if the mode is selected. You will have to enter the PINs using the Single Add feature. When you delete a card, the PIN associated with the card is also deleted.*

5.4.3 - Adding & Deleting Auxiliary Cards

Auxiliary cards are used to activate an external device without unlocking the door. For more information, refer to “5.8 Auxiliary Function Configuration (Relay-1)”, page 22.

To Add/delete Auxiliary Cards:

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

   ```
   1. ENROLL   2. PASSWD
   3. TIMER    4. SYSTEM
   ```

2. Press [1-Enroll]. The LCD displays:

   ```
   1-ACCESS CARD
   2-AUX.CARD
   ```

3. Press [2-Aux.Card]. The LCD displays:

   ```
   1. PROGRAM CARDS
   2. VIEW CARDS
   ```

4. Press [1-Program Cards]. The LCD displays:

   ```
   1. S_ADD
   2. S_DEL
   ```

5. Press [1-S_Add] to add a card or [2-S_Del] to delete a card. The LCD displays:

   ```
   TOTAL CARDS: XX
   CARD NO.__:______
   ```

6. Enter the card number in the system by simply presenting the card to the reader, or by entering the card number manually followed by the [#]; to enter special characters refer to “Special Characters (Hexadecimal)” (page 19).

7. Once you have entered the card number, the LCD will display:

   ```
   ACCEPTED
   ```

8. Once the card has been accepted, the system will return to the add/delete card screen. To add or delete another card simply repeat steps 5 and up. To exit the programming mode press [#], [#].

5.5 Viewing Cards

You may view the cards that are programmed in the unit’s memory. These are sorted based or their programming order within the unit. For example, if cards numbered 01:00000 to 01:00005 are programmed and you delete the card number 01:00004, when you add a new card (for example 01:00009), it is placed where the last card was deleted: 01:00000, 01:00001, 01:00002, 01:00003, ***01:00009***, 01:00005.

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

   ```
   1. ENROLL   2. PASSWD
   3. TIMER    4. SYSTEM
   ```

2. Press [1-Enroll]. The LCD displays:

   ```
   1-ACCESS CARD
   2-AUX. CARD
   ```

3. Press [1-Access Card] to view access cards OR press [2-Aux. Card] to view auxiliary cards . The LCD displays:

```
1. PROGRAM CARDS
2. VIEW CARDS
```

4. Press [2-View Cards]. The LCD displays:

```
XXXX     ID_XX:XXXXX
1.NEXT   2.PREV.
(XXXX indicates the cards programming
sequence in the unit’s memory)
```

5.6 Verifying a Card Number

This feature is particularly useful when the card number is no longer visible on the card.

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

```
1. ENROLL   2. PASSWD
3. TIMER    4. SYSTEM
```

2. Press [4-System]. The LCD displays:

```
1.ALARM  2.CHECK
3.MODE   4.OTHER
```

3. Press [2-Check]. The LCD displays:

```
1.CHECK CARD NO.
2.RECORD CHECK
```

4. Press [1-Check Card No.]. The LCD displays:

```
CARD PLEASE
CARD NO.
```

5. Present the card to the reader. The LCD displays the associated card number:

```
CARD PLEASE
CARD NO.: XX:XXXXX
```

6. To exit and return to the main menu, press the [#] key.

5.7 Guard Function Configuration (Relay-1)

NOTE: *Are your jumpers configured correctly to use this function? For more information, please refer to “Jumper Settings:” (page 11).*

This function is used to arm/disarm the connected security system. Either by using a password and card, or simply a password to arm the system.

NOTE: *The relay will be triggered and will remain activated until the system is disarmed.*

Recommended Configuration Procedures

- Jumper setup (relay module). Refer to “Jumper Settings:” (page 11);
- Enable guard function. Refer to “Enabling the Guard Function” (page 21);
- Modify guard code. Refer to “ To Modify the Guard Password”, page 18;

5.7.1 - Enabling the Guard Function

To enable the guard function:

1. Enter the master password (default is [111111]) followed by the [#] key. The unit displays the following:

```
1. ENROLL   2. PASSWD
3. TIMER    4. SYSTEM
```

2. Press [4-System]. The LCD displays:

```
1.ALARM  2.CHECK
3.MODE   4.OTHER
```

3. Press [4-Other]. The LCD displays:

```
1.TONE   2.DURESS
3.MORE   4. LANGUAGE
```

4. Press [3-More]. The LCD displays:

```
1.GUARD  2.AUX.CR
3.A_DEL  4.RESET
```

5. Press [1-Guard]. The LCD displays:

```
1.GUARD FUNCTION
2.STRIKE ACTIVE
```

6. Select [1-Guard Function]. The LCD displays:

```
CURRENT: ENABLE
PRESS ’1’ --] CHANGE
```

7. Press [1] until the desired mode is displayed, then press [#] to save and exit.

5.7.2 - Arming / Disarming Quick Reference

Only cards that are associated with a PIN can be used for arming/disarming the unit.

NOTE: *You have 20 seconds to arm/disarm the system. Passed this delay, the LCD displays a “Time-Out” message and returns to the normal greeting screen.*

To arm the IoPass unit:

1. Enter the **Guard code** (default is [123]) then press **[#]**. The LCD will prompt:

```
CARD PLEASE
```

2. Present a card to the reader.
3. Enter the cardholder’s PIN (any card associated with a PIN and that has been programmed in the unit will do). Once you have presented the card and entered the PIN, the relay will be triggered (and will remain activated until disarmed). The LCD displays:

```
ARMED
```

4. The LED will blink RED to indicate the armed status.

To disarm the IoPass unit:

The system has to be disarmed in order to grant access. When a card is presented to the reader when the system is still armed, an “invalid card message” is displayed. Users have to enter the system Guard code, then present their card and enter their PIN.

To disarm the system:

1. Enter the **Guard code** [123] followed by the [#] key.
2. The LCD prompts for a card:

```
CARD PLEASE
```

3. Present a card to the reader then enter the cardholder's PIN (any card associated with a PIN and that has been programmed in the unit will do).
4. The relay will be triggered and the system will disarm. Depending on how the system is set up, the strike may activate or deactivate.

The LCD will return to the normal greeting display and the red LED will not flash. When the door unlocks, access is granted instantly. When the door remains locked, you must present your card to the reader to be granted access.

5.7.3 - Viewing the Audit Trail

1. Enter the master password [111111, default]. The LCD displays the following:

```
1. ENROLL   2. PASSWD
3. TIMER    4. SYSTEM
```

2. Select [4. System]. The LCD displays:

```
1. ALARM 2. CHECK
3. MODE  4. OTHER
```

3. Select [2. Check]. The LCD displays:

```
1. CHECK CARD NO.
2. RECORD CHECK.
```

4. Select [2. Record check]. Then scroll the audit trail by using [1] or [2]. The events will appear as follows:

[1 ACC 41:4118]	for access granted
[1.Up 2 Down]	
[2 ARM 41:4118]	for arming
[1.Up 2.Down]	
[3 DIS 41:4118]	for disarming
[1.Up 2. Down]	

5.8 Auxiliary Function Configuration (Relay-1)

The auxiliary function is used to trigger a device without unlocking the door. The auxiliary relay can be used to activate such devices as lighting control, HVAC control, or to unlock an auxiliary door.

The system will **either** accept an auxiliary card or the auxiliary code to activate the relay.

NOTE: *The relay will be activated for a period of 3 seconds, then will deactivate automatically (this delay cannot be modified).*

Recommended Configuration Procedure

- Jumper set up (relay module). See "Jumper Settings:" (page 11);
- Enable auxiliary function;
- Modify auxiliary password. See " To Modify the Auxiliary Password:", page 18;
- Enroll auxiliary cards (if required). See "5.4.3 - Adding & Deleting Auxiliary Cards", page 20.

5.8.1 - Enabling the Auxiliary Function

1. To enter the programming mode, enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

```
1. ENROLL   2. PASSWD
3. TIMER    4. SYSTEM
```

2. Press [4-System]. The LCD displays:

```
1.ALARM  2.CHECK
3.MODE   4.OTHER
```

3. Press [4-Other]. The LCD displays:

```
1.TONE   2.DURESS
3.MORE   4.LANGUAGE
```

4. Press [3-More]. The LCD displays:

```
1.GUARD  2.AUX.CR
3.A_DEL  4.RESET
```

5. Press [2-Aux. Cr]. The LCD displays:

```
CURRENT: ENABLE
PRESS '1' --> CHANGE
```

6. Press [1] until desired mode is displayed. Pressing this key will toggle between selections. When required mode is displayed (in this case "Enable"), press [#] to save and exit.

5.9 Configuring the Duress Function (Relay-1)

The duress function is used to provide added security to personnel. In situations of duress, a cardholder enters his code (PIN) with a trailing digit [9] and the duress relay will be activated (timer can be modified) to drive the require device.

NOTE: *This function can only be used when the system is programmed to use access mode 1 or 2. The number [9] can be inserted at the end of the PIN or the main password.*

NOTE: *The relay will be activated and access will be granted normally. The relay activation timer can be modified (normally set to 10 seconds).*

Recommended Configuration Procedure

- Jumper set up (relay module). See “Jumper Settings:” (page 11);
- Enable duress function;
- Modify duress active timer setting (if required).

5.9.1 - Enabling the Duress Function

1. To enter the programming mode, enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

   ```
   1. ENROLL   2. PASSWD
   3. TIMER    4. SYSTEM
   ```

2. Press [4-System]. The LCD displays:

   ```
   1.ALARM  2.CHECK
   3.MODE   4.OTHER
   ```

3. Press [4-Other]. The LCD displays:

   ```
   1.TONE   2.DURESS
   3.MORE   4. LANGUAGE
   ```

4. Press [2-Duress]. The LCD displays:

   ```
   CURRENT: ENABLE
   PRESS '1' --> CHANGE
   ```

5. Press [1] until desired mode is displayed. Pressing this key will toggle between selections. When required mode is displayed (in this case “Enable”), press [#] to save and exit.

5.9.2 - Setting the Duress Relay Timer

By default, the relay-1 timer for the duress function is set to be activated for 10 seconds.

If required, you can modify this setting and program a value between 1-255 seconds.

1. To enter the programming mode, enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

   ```
   1. ENROLL   2. PASSWD
   3. TIMER    4. SYSTEM
   ```

2. Press [3-Timer]. The LCD displays:

   ```
   1.STRIKE 2.ALARM
   3.DURESS 4.AJAR
   ```

3. Press [3-Duress]. The LCD displays:

   ```
   CURRENT: 10 SEC.
       NEW:
   ```

4. Using the keypad, enter the number of seconds during which the duress relay will remain activated. Enter digits in “seconds”. Press [#] to save and exit.

5.9.3 - Using the Duress Function

Once the function is enabled in the system, follow this procedure to use the duress function:

1. Present your card at the reader (skip this step if you are using mode 2);
2. Key in your PIN (if mode 1) immediately followed by the digit [9].

   Example:

   `55559` followed by [#]
3. The door will open normally (access granted) and the relay will activate for the pre-set period of time.

5.10 Configuring the Tamper Alarm Function

This tamper alarm will activate the alarm relay when the front cover of the IoPass unit is removed.

Recommended Configuration Procedure

- Enable tamper function;
- Modify alarm relay timer activation (if required). See “5.16 Alarm Relay Timer Configuration”, page 26 for more information.

5.10.1 - Enabling the Tamper Alarm Function

1. To enter the programming mode, enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

   ```
   1. ENROLL   2. PASSWD
   3. TIMER    4. SYSTEM
   ```

2. Press [4-System]. The LCD displays:

   ```
   1.ALARM  2.CHECK
   3.MODE   4.OTHER
   ```

3. Press [1-Alarm]. The LCD displays:

   ```
   1.TAMPER 2.FORCE
   3.D_AJAR 4.P_ERR
   ```

4. Press [1-Tamper]. The LCD displays:

   ```
   CURRENT: DISABLE
   PRESS '1' --> CHANGE
   ```

5. Press [1] until desired mode is displayed. Pressing this key will toggle between selections. When required mode is displayed (in this case “Enable”), press [#] to save and exit.

5.10.2 - Using the Tamper Alarm Function

Once the function is enabled in the system, follow this procedure to STOP the tamper alarm if it has been activated.

1. When the tamper alarm has been activated, the alarm relay will be triggered (usually an annunciator) and the LCD will display:

```
READY FOR CARD
TAMPER ALARM (blink)
```

2. This "Tamper Alarm" message is displayed (and blinking) and will remain on the LCD until an "access granted" operation is processed by the unit;
3. Present your card and enter your PIN or master password (depending on the system set up), access will be granted and the message will disappear.

5.11 Configuring the Forced Entry Alarm

This function, **already enabled in the unit (default)**, will automatically activate the "Alarm Relay" when the door contact detects unauthorized access (without card or password or both), a "door forced open" type of event.

Recommended Configuration Procedure

- Since this function is already enabled in the unit, follow the procedure below if you need to disable it (not recommended);
- Modify alarm relay timer activation (if required). See "5.16 Alarm Relay Timer Configuration", page 26 for more information.

5.11.1 - Enabling/Disabling the Force Entry Alarm Function

1. To enter the programming mode, enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

```
1. ENROLL   2. PASSWD
3. TIMER    4. SYSTEM
```

2. Press [4-System]. The LCD displays:

```
1.ALARM  2.CHECK
3.MODE   4.OTHER
```

3. Press [1-Alarm]. The LCD displays:

```
1.TAMPER 2.FORCE
3.D_AJAR 4.P_ERR
```

4. Press [2-Force]. The LCD displays:

```
CURRENT: ENABLE
PRESS '1' --> CHANGE
```

5. Press [1] until desired mode is displayed. Pressing this key will toggle between selections. When required mode is displayed, press [#] to save and exit.

5.11.2 - Using the Force Entry Function

Follow this procedure to STOP the force entry alarm if it has been activated.

1. When the force entry has been activated, the alarm relay will be triggered (usually an annunciator) and the LCD will display:

```
READY FOR CARD
 FORCE ENTRY
```

2. This "Force Entry" message is displayed (and blinking) and will remain on the LCD until an "access granted" operation is processed by the unit;
3. Present your card and enter your PIN or master password (depending on the system set up), access will be granted and the message will disappear.

5.12 Configuring the Door Ajar Function

This function, already enabled in the unit (default), **can** activate the "Alarm relay" when the door is opened longer than the pre-set time following an access granted operation.

By default, the IoPass warning device will sound until the door is closed correctly.

The user can decide if the alarm relay needs to be activated when this situation occurs.

5.12.1 - Enabling/Disabling the Door Ajar Function

To enable/disable the door ajar function:

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

```
1. ENROLL   2. PASSWD
3. TIMER    4. SYSTEM
```

2. Press [4-System]. The LCD displays:

```
1.ALARM  2.CHECK
3.MODE   4.OTHER
```

3. Press [1-Alarm]. The LCD displays:

```
1.TAMPER 2.FORCE
3.D_AJAR 4.P_ERR
```

4. Press [3-D_Ajar]. The LCD displays:

```
1.DOOR TIMER
2.ALARM RELAY
```

5. Press [1-Door Timer] to enable or disable the door ajar function. The LCD displays:

```
CURRENT: ENABLE
PRESS '1' --> CHANGE
```

6. Press [1] until desired mode is displayed. Pressing this key will toggle between selections. When required mode is displayed, press [#] to save and exit.
7. If you want the alarm relay to be activated when a "door ajar" situation occurs, follow the procedure below.

5.12.2 - Activating the Alarm Relay on Door Ajar

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

   ```
   1. ENROLL  2. PASSWD
   3. TIMER   4. SYSTEM
   ```

2. Press [4-System]. The LCD displays:

   ```
   1.ALARM  2.CHECK
   3.MODE   4.OTHER
   ```

3. Press [1-Alarm]. The LCD displays:

   ```
   1.TAMPER 2.FORCE
   3.D_AJAR 4.P_ERR
   ```

4. Press [3-D_Ajar]. The LCD displays:

   ```
   1.DOOR TIMER
   2.ALARM RELAY
   ```

5. Press [2-Alarm Relay] to enable (trigger) or disable (not trigger) the alarm relay when the door is left open longer than pre-set time. The LCD displays:

   ```
   CURRENT: DISABLE
   PRESS '1' --> CHANGE
   ```

6. Press [1] until desired mode is displayed. Pressing this key will toggle between selections. When required mode is displayed, press [#] to save and exit.

5.12.3 - Setting the Door Ajar Timer

The door ajar timer is set to 30 seconds. If the door remains open longer than 30 seconds, after an "access" event, an alarm will sound until the door is closed correctly. If required, you can modify this setting and program a value between 1-255 seconds.

To set the door ajar timer:

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

   ```
   1. ENROLL  2. PASSWD
   3. TIMER   4. SYSTEM
   ```

2. Press [3-Timer]. The LCD displays:

   ```
   1.STRIKE 2.ALARM
   3.DURESS 4.AJAR
   ```

3. Press [4-Ajar]. The LCD displays:

   ```
   CURRENT: 30 SEC.
       NEW:
   ```

4. Using the keypad, enter the number of seconds during which the alarm will sound. Enter digits in "seconds". Press [#] to save and exit.

5.12.4 - Using the Door Ajar Function

Depending if the door ajar function is configured to trigger the alarm relay, follow this procedure to STOP the warning device.

1. When the door is left opened, the alarm relay will be triggered OR the unit's piezo will sound. The LCD will display:

   ```
   READY FOR CARD
    DOOR OPEN
   ```

2. The "Door Open" message is displayed (and blinking) and will remain on the LCD until the door is closed properly.

5.13 PIN Error Function Configuration

This function, when enabled, will automatically activate the "Alarm Relay" when a cardholder keys in his PIN incorrectly five (5) times consecutively within four (4) minutes.

Furthermore, the card can automatically be deleted (from the unit's memory) when this situation occurs.

NOTE: *This function can only be used when access mode "1" is used (card and PIN).*

5.13.1 - Enabling the PIN Error Function

To enable the PIN error function:

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

   ```
   1. ENROLL  2. PASSWD
   3. TIMER   4. SYSTEM
   ```

2. Press [4-System]. The LCD displays:

   ```
   1.ALARM  2.CHECK
   3.MODE   4.OTHER
   ```

3. Press [1-Alarm]. The LCD displays:

   ```
   1.TAMPER 2.FORCE
   3.D_AJAR 4.P_ERR
   ```

4. Press [4-P_Err]. The LCD displays:

   ```
   CURRENT: DISABLE
   PRESS '1' --> CHANGE
   ```

5. Press [1] until desired mode is displayed. Pressing this key will toggle between selections. When required mode is displayed, press [#] to save and exit.

5.13.2 - Enabling Auto-Deletion on PIN Error

Enable this function if you wish to delete a card from the unit's memory when a cardholder enters the PIN incorrectly five (5) times consecutively within four (4) minutes.

To enable the auto-deletion feature on PIN error:

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

```
1. ENROLL  2. PASSWD
3. TIMER   4. SYSTEM
```

2. Press [4-System]. The LCD displays:

```
1.ALARM  2.CHECK
3.MODE   4.OTHER
```

3. Press [4-Other]. The LCD displays:

```
1.TONE   2.DURESS
3.MORE   4. LANGUAGE
```

4. Press [3-More]. The LCD displays:

```
1.GUARD  2.AUX.CARD
3.A_DEL  4.RESET
```

5. Press [3-A_Del]. The LCD displays:

```
CURRENT: DISABLE
PRESS '1' --> CHANGE
```

6. Press [1] until desired mode is displayed. Pressing this key will toggle between selections. When required mode is displayed, press [#] to save and exit.

5.14 Beeper Key Tone Configuration

This function, already enabled in the unit (default), provides an audible "beep" tone when the keys of the keypad are used.

This function is convenient when the cardholder must key in his PIN.

To disable the beeper:

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

```
1. ENROLL  2. PASSWD
3. TIMER   4. SYSTEM
```

2. Press [4-System]. The LCD displays:

```
1.ALARM  2.CHECK
3.MODE   4.OTHER
```

3. Press [4-Other]. The LCD displays:

```
1.TONE   2.DURESS
3.MORE   4. LANGUAGE
```

4. Press [1-Tone]. The LCD displays:

```
CURRENT: ENABLE
PRESS '1' --> CHANGE
```

5. Press [1] until desired mode is displayed. Pressing this key will toggle between selections. When required mode is displayed, press [#] to save and exit.

5.15 Loop Type Configuration

The IoPass unit allows the installer to modify the loop type of the exit button and door contact.

These normally open contacts can be modified to normally closed to suit installer's requirements.

To configure the loop type:

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

```
1. ENROLL  2. PASSWD
3. TIMER   4. SYSTEM
```

2. Press [4-System]. The LCD displays:

```
1.ALARM  2.CHECK
3.MODE   4.OTHER
```

3. Press [3-Mode]. The LCD displays:

```
1.ACCESS MODE
2.DOOR_INPUT
```

4. Press [2-Door_Input]. The LCD displays:

```
1.EXIT BUTTON
2.DOOR
```

5. Press [1-Exit Button] to modify the exit button's polarity OR press [2-Door] to modify the door contact's polariy. In either cases, the LCD displays:

```
CURRENT: NC
PRESS '1' --> CHANGE
```

6. Press [1] until desired mode is displayed. Pressing this key will toggle between selections. When required mode is displayed, press [#] to save and exit.

5.16 Alarm Relay Timer Configuration

By default, the alarm relay is pre-set to 240 seconds, meaning that the connected annunciator will remain activated for that period of time.

The timer can be modified from 1-255 seconds.

The alarm relay can be activated by the following events:

- Tamper alarm (if enabled);
- Forced entry (enabled by default);
- Door ajar (if enabled);
- Incorrect password keyed in five times consecutively within four (4) minutes (if enabled).

***NOTE:** This relay is always "enabled", but options that can trigger this relay can be customized by the user.*

To configure the relay timer:

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

```
1. ENROLL  2. PASSWD
3. TIMER   4. SYSTEM
```

2. Press [3-Timer]. The LCD displays:

```
1.STRIKE 2.ALARM
```

```
3.DURESS 4.AJAR
```

3. Press [2-Alarm]. The LCD displays:

```
CURRENT: 240 SEC.
    NEW:
```

4. Using the keypad, enter the number of seconds during which the alarm will sound. Enter digits in “seconds”. Press [#] to save and exit.

5.17 Setting the Strike Relay Timer

By default, the locking device relay is pre-set to 10 seconds, meaning that the door will remain unlocked for that period of time following an “access granted” event. The timer can be modified from 1-255 seconds.

To set the strike relay timer:

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

```
1. ENROLL  2. PASSWD
3. TIMER   4. SYSTEM
```

2. Press [3-Timer]. The LCD displays:

```
1.STRIKE 2.ALARM
3.DURESS 4.AJAR
```

3. Press [1-Strike]. The LCD displays:

```
CURRENT: 10 SEC.
    NEW:
```

4. Using the keypad, enter the number of seconds during which the locking device will be unlocked. Enter digits in “seconds”. Press [#] to save and exit.

5.18 Resetting the IoPass Unit to Factory Defaults

The reset to factory default option is used to clear all configured options and cards from the IoPass memory and bring back the unit to factory defaults.

To clear the memory, the master password is required. A double confirmation is used to confirm memory deletion.

1. Enter the master password (default is [111111]) followed by the [#] key. The LCD displays the following:

```
1. ENROLL  2. PASSWD
3. TIMER   4. SYSTEM
```

2. Press [4-System]. The LCD displays:

```
1.ALARM  2.CHECK
3.MODE   4.OTHER
```

3. Press [4-Other]. The LCD displays:

```
1.TONE   2.DURESS
3.MORE   4. LANGUAGE
```

4. Press [3-More]. The LCD displays:

```
1.GUARD  2.AUX.CR
3.A_DEL  4.RESET
```

5. Press [4-Reset]. The LCD displays:

```
PRESS 1
TO RESET THE UNIT
```

6. Press [1]. The LCD displays:

```
PASSWORD:
```

7. Enter the master password (default is [111111]) followed by the # key. The LCD displays:

```
PRESS 1
TO RESET THE UNIT
```

8. Press [1] to confirm your action. If you are not sure, press the [*] to cancel.

   All cards will be deleted from the memory and settings will return to factory defaults. While processing, the LCD displays:

```
EEPROM ERASING
```

9. When completed, the unit will return to the welcome screen.

NOTE: *If power is removed from unit during the process before the above message is displayed, the following message will be displayed when unit is powered again:*

```
CNA CHECKSUM EM
1=CLEAR  2=IGNORE
```

- Press [1-Clear] will continue the reset process.
- Press [2-Ignore] will stop the process to where it was interrupted. Consequently, most of the unit configuration will be reset to default settings, whereas some cards may remain in the unit.

Quick Reference Programming Table

1.ENROLL					
	1.ACCESS CARD	*PROGRAM CARDS*	*1.S_ADD*		
		VIEW CARDS	*2.S_DEL*		
			3.B_ADD		
			4.B_DEL		
	2.AUX. CARD	*PROGRAM CARDS*	*1.S_ADD*		
		VIEW CARDS	*2.S_DEL*		
2.PASSWD					
	1.MASTER				
	2.MAIN				
	3.AUX.CR				
	4.GUARD				
3.TIMER					
	1.STRIKE				
	2.ALARM				
	3.DURESS				
	4.AJAR				
4.SYSTEM					
	1.ALARM	*1.TAMPER*			
		2.FORCE			
		3.D_AJAR	1.DOOR TIMER		
			2.ALARM RELAY		
		4.P_ERR			
	2.CHECK	*1.CHECK CARD NO*			
		2.RECORD CHECK			
	3.MODE	*1.ACCESS MODE*			
		2.DOOR_INPUT	1.EXIT BUTTON		
			2.DOOR		
	4.OTHER	*1.TONE*			
		2.DURESS			
		3.MORE	1.GUARD	1.GUARD FUNCTION	
		4. LANGUAGE		2. STRIKE ACTIVE	1. ENABLE
					2. DISABLE
			2.AUX. CARD		
			3.A_DEL		
			4.RESET		

Programming Worksheet

Installation Information

Site Name:

Address:

Contact Name:

Tel./Fax/E-mail: / /

Installation Date:

Numbers in brackets [X] indicate the number sequence to key in to access a particular function of the system once the master password has been entered to access the programming mode.

To **enter programming mode**, enter your 6-digit master password: i.e.: [111111] followed by the [#] key.

System Passwords

Passwords	Default	New
Master [2]-[1]	[111111]	I__I__I__I__I__I__I
Main [2]-[2]	[1234]	I__I__I__I__I
Auxiliary [2]-[3]	[1234567]	I__I__I__I__I__I__I__I
Guard [2]-[4]	[123]	I__I__I__I

Access Mode

[4]-[3]-[1]

❐ Mode “0” - Card only (DEFAULT)
❐ Mode “1” - Card and PIN
❐ Mode “2” - Card **OR** main password

Timers

Timers	Default	New
Strike relay [3]-[1]	10 seconds	I__I__I__I
Alarm relay [3]-[2]	10 seconds	I__I__I__I
Door ajar [3]-[4]	20 seconds	I__I__I__I
Duress [3]-[3]	10 seconds	I__I__I__I

NOTE: *Allowed from 1 to 255 seconds.*

System Functions

NOTE: *For more information, see “IoPass Factory Defaults” (page 13).*

Functions	YES	NO
Tamper alarm [4]-[1]-[1]	❐	❐
Door forced open [4]-[1]-[2]	❐	❐
Door ajar [4]-[1]-[3]	❐	❐
Alarm relay activated on door ajar [4]-[1]-[3]-[2]	❐	❐
Tone/beeper [4]-[4]-[1]	❐	❐
PIN error [4]-[1]-[4]	❐	❐
Card auto-deletion on PIN error [4]-[4]-[3]-[3]	❐	❐
Duress function [4]-[4]-[2]	❐	❐
Guard function [4]-[4]-[3]-[1] **Arming**: Strike enable: Yes ❐ No ❐	❐	❐
Auxiliary function [4]-[4]-[3]-[2]	❐	❐

Door contact type [4]-[3]-[2]-[2]
NO ❐ NC ❐

Exit button contact type [4]-[3]-[2]-[1]
NO ❐ NC ❐

Card Information Record Sheet

NOTE: *Make copies of this sheet to record cardholder information.*

Cardholder Name	Card Number	Auxiliary Card	PIN (if used)
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	
	:	□	

Using the IoPass™ System

How to Enter the Secured Area

By default, the LED (indicator) is red, and the LCD of the IoPass unit displays:

`READY FOR CARD`

You may have been given an access card, PIN or main password for the secured area. Depending on how the system is configured, the procedure remains the same:

1. Present your card at the reader OR enter the 4-digit main password followed by the [#] key;
2. The system will either grant you access (see step 4) or prompt you to enter your PIN:

   `PASSWORD:`
3. Using the keypad, enter your 4-digit PIN followed by the [#] key. If you key in an incorrect password, the system will display “Invalid Password”. In this case, start from step 1.
4. The LCD displays:

   `ACCESS GRANTED`

   The door will unlock and the LED (indicator) will turn green.

NOTE: *Do not give your PIN to anybody.*

How to Arm/Disarm the Connected System

Arming

1. Enter the guard code followed by the [#] key. The unit will prompt:

   `CARD PLEASE`
2. Present a card to the reader (any card programmed in the unit and associated with a PIN will do). You will have 20 seconds, after that the LCD will display a “Time-Out” message and return to the normal greeting screen. Once you have presented the card, the relay will be triggered (and remains activated until disarmed) and the LCD will display:

   `ARMED`
3. You will also notice that the LED (on the unit itself) will be blinking RED to indicate the armed status.

Disarming

Follow these steps to disarm the system:

NOTE: *The LCD should display “Armed”.*

1. Enter guard code [123] followed by the [#] key;
2. The LCD will prompt for a card:

   `CARD PLEASE`
3. Present a card to the reader (any card programmed in the unit and associated with a PIN will do). You will have 20 seconds, after that the LCD will display a “Time-Out” message and return to the normal greeting screen;
4. The relay will be triggered and the system will disarm. Depending on how the system is set up, the strike may activate or deactivate.
5. The LCD will return to the normal greeting display and the red LED will not flash.

When the door unlocks, access is granted instantly. When the door remains locked, you must present your card at the reader to be granted access.

How to Stop a Tamper Alarm

Follow this procedure to STOP the tamper alarm if it has been activated.

1. When the tamper alarm has been activated, the alarm relay will be triggered (usually an annunciator) and the LCD will display:

   ```
   READY FOR CARD
    TAMPER ALARM (blink)
   ```
2. This “Tamper Alarm” message is displayed (and blinking) and will remain on the LCD until an “access granted” operation is processed by the unit;
3. Present your card and enter your PIN (depending on the system set up) followed by the [#] key. Access will be granted and the message will disappear.

How to Stop a Force Entry Alarm

Follow this procedure to STOP the force entry alarm if it has been activated.

1. When the force entry has been activated, the alarm relay will be triggered (usually an annunciator) and the LCD will display:

   ```
   READY FOR CARD
    FORCE ENTRY
   ```
2. This “Force Entry” message is displayed (and blinking) and will remain on the LCD until an “access granted” operation is processed by the unit;
3. Present your card and enter your PIN (depending on the system set up) followed by the [#] key. Access will be granted and the message will disappear.

How to Use the Door Ajar Function

Depending if the door ajar function is configured to trigger the alarm relay, follow this procedure to STOP the warning device.

1. When the door is left opened, the alarm relay will be triggered OR the unit’s piezo will sound. The LCD will display:

```
READY FOR CARD
 DOOR OPEN
```

2. The “Door Open” message is displayed (and blinking) and will remain on the LCD until the door is closed properly.

How to use the Duress Function

Once the function is enabled in the system, follow this procedure to use the duress function:

1. Present your card at the reader (skip this step if you are using mode 2);
2. Key in your PIN or the main password (if mode 2) immediately followed by the digit [9].

   Example:

   `55559` followed by [#]
3. The door will open normally (access granted) and the relay will activate for the pre-set period of time.

KANTECH | access control and integrated systems

Kantech Systems

Tel: +1(978) 731-6252 • **Toll Free:** US & Canada: 1 888 222-1560 • **Fax:** +1(978) 731-7759

Web Site: www.Kantech.com

E-mail: techlink@tycoint.com

Printed in USA • DN1445-0303