Access Control System

I. POLICY:

It is the policy of East Penn Manufacturing to identify locations where access control and video monitoring measures will enhance security and then implement those devices along with employee education regarding their purpose and use.

II. PURPOSE:

To make employees and visitors more secure in the workplace, as well as protect property and assets.

III. PROCEDURES:

Description of System:

a. At select locations electronic locks and cameras are installed on employee only exterior doors. Commonly known as "card reader" access control locks, these can be opened easily by our employees by means of their company issued "proximity" identification card. Access control locks may also be installed at some interior doors in offices and manufacturing facilities.

b. There are also monitoring cameras at each building entrance equipped with a card reader, so that authorized security officers can see and record who is entering and leaving the building; helping to make sure only authorized persons enter our facility.

c. The doors will be equipped with sensors that can lock and unlock the doors, either by predetermined time periods or by using your company I.D. cards.

d. There are devices – I. D. Card Readers - placed at the all entrances used by employees that will unlock doors when the employee holds up their I.D. card, which has a bar code imbedded in it similar to those on credit cards and driver's licenses.

e. There is a small light on the card reader that glows RED when the door is locked and GREEN when it is unlocked. When you present your I.D. card to the card reader, the light changes from red to green and you can open the door.

f. Not only will this unlock the door, but it will record which employee accessed the door and the date and time the door was opened.

g. These doors will be kept locked at all times, thus cutting down on the chance that a visitor or unwanted person will be able to get into the building without authorization.

h. Generally, the main public access door(s) will be placed in an "open mode" during normal business hours unless a receptionist is not present or there is some other reason for it to be in locked mode.

i. The doors can also be programmed to lock or unlock at certain times of the day, such as automatically locking at 5 PM.

j. The system is beneficial since it stays locked or automatically locks, and is not subject to someone forgetting to lock up or having to worry about an ex-employee retaining a key.

k. It's also good to know who is coming into the building, and we'll be able to provide a printout of who could be inside in case of emergency.

l. Access control card readers that are located inside a building, such as for office suites, may not be accompanied by a camera.

m. If you forget your card, the guards will have an access card to open the doors after properly identifying you.

To Operate:

a. Hold your I.D. card up to the reader so the bar code faces the reader. (Point out bar code on I.D. card, demonstrate how to hold up to reader). You don't have to touch it to the reader or be really close, just in proximity.

b. The reader will turn from a red light indicator to a green light, and you can now pull the door open.

c. You don't need the I.D. card to exit the building, as the doors will open when you push the panic bar or turn a handle.

IV. STATUS CHANGE MANAGEMENT REPONSIBILTY

In accordance with current practices, the Personnel Department will notify the Security Director when a proximity ID card holder is terminated, transferred, or has any change in status affecting his or her access to facilities.

V. EMPLOYEE RESPONSIBILTY:

a. Employees will use their ID access card to enter only those facilities and sections of facilities for which they've been duly authorized. Employees will not attempt to unlock doors which they are not authorized to open.

b. Employees must retain their ID access card on or about their person and must not lend it to others.

c. ID cards will not be duplicated without authorization by the Security Director.

d. Lost cards must be immediately reported to your supervisor, who will in turn notify security.

e. Employees will not allow unauthorized people or non-employees to enter a building using the employee's access card or by holding open a door for them.

f. Never allow unknown persons to enter a building after you have used your ID card to open it. Direct the person to enter thru the main entrance designated for visitors, vendors, consultants, and other clients and customers.

g. Do not prop open doors or leave them unattended.

VI. SECURITY SERVICE RESPONSIBILITY

a. The Security Director will be responsible for the overall administration and operation of the access control system

b. The Personnel Department under the direction of the Security Director will coordinate the issuance of proximity ID cards, level of access, and termination of access with the Information Technology Department.

c. Designated security officers on duty will have the ability to monitor the access system and cameras in real time, as well as search recordings as needed for security concerns.

d. Security officers will be issued proximity ID cards to access the buildings and portions of buildings they need access to in order to perform their duties.

e. On-duty security officers will immediately investigate all alarms, unauthorized entries, and suspicious circumstances indicated by the access control system.

f. Security officers will document and report all such incidents, unusual actions, and system malfunctions to the Security Director as soon as practical.

g. Security officers will not use the access control system, including cameras, for any purpose other than to monitor security. Under no circumstances will the privacy of persons be compromised when not connected to the need to monitor and maintain security. Any officer who witnesses or is aware of misuse of the system must report it to the Security Director immediately.

h. Security officers are not authorized to permit viewing of images or data to anyone unless approved the Security Director. Security officers will not print out still photos unless needed for an emergency by the police or with the authorization of those listed in section VIII.

VII. CONTRACTOR and VENDOR ACCESS

Approved contractors and vendors who need access to card reader controlled buildings or portions of a building may be issued proximity ID cards with approval by the Security Director. These will be limited to those who regularly deliver services to East Penn Manufacturing, and may be valid and active only for a specified period of time.

VIII. VIEWING and RETENTION

Only those persons authorized by the Security Director, a member of executive management, the Vice President of Personnel or the Director of Personnel may access the card reader data and camera images and data.

Camera footage will be retained for 30 days unless bookmarked. Card access data shall be retained for a one year period. At the conclusions of the retention period, the data will be either overridden or destroyed.

Remember, any type of security is effective only if used correctly.

Record of Revisions

REVISION #	REVISION DATE	DESCRIPTION