

REAL ESTATE WEEKLY

Construction & DESIGN

SECTION B

Wednesday, July 23, 2008

Designing an effective identification credential system

By PAUL BENNE, SENIOR ASSOCIATE/SECURITY DISCIPLINE LEADER, SYSKA HENNESSY GROUP

Identification credentials (ID's) are used everywhere, hanging from people's belts, on lanyards around necks, and in wallets.

Their most common use has been identifying people, but with the demand for increased security and with the many supplemental technologies available today – e.g., access control, time and attendance, computer access, purchasing programs, etc. – ID Cards are becoming a multi-functional necessity.

ID cards are now commonly used to enable access to buildings and other restricted areas by means of interfacing with electronic access control systems.

This practice, intended to increase security is unfortunately, in many cases, leaving businesses exposed to unnecessary risk.

Using ID cards as the primary means to identify and authorize access to a facility would be the equivalent of putting a home address on house keys, or a PIN number on the ATM card. If lost, the card can easily be used by someone with less than desirable intentions.

The following are some recommendations for designing a credentialing and access control card program that is both functional and secure:

Access Control Card Tips

ID cards and access control cards should be kept separate.

If an ID card must be used as an access control card, it should be used in conjunction with a biometric device (i.e. fingerprint scanner, hand geometry, etc.) on the exterior of the building and internal high security areas.

Access control cards should contain limited information such as name, photo, and a non-descript identifier (i.e.: color codes, numbers, or symbols to indicate an authorized point of entry, authorized destination, or authorized entry time). Access control cards should never contain the company name, logo, building name, address or other identifying indicia.

Access control systems should be programmed to "Use-it-or-loose-it". This feature allows an access card to be automatically deactivated if not used within a predetermined number of days.

Every time the card is used the day count is reset. Card holders should be trained to display their access card to front desk personnel in addition to presenting the card to the access control device.

ID Card Tips:

• ID cards should identify the card holder by photo, name, rank, title, and work location(s).

• ID cards should be designed to offer single glance identification markers; such as color photo back drops that can identify card holder types, or numeric or symbolic indicia that identifies areas of authorized presents.

Company policy should support the wearing and display of ID Cards from all employees and visitors.

• ID cards should be reissued every 12-18 months with an updated photo, and card holder information.

• ID cards should have a unique numerical or alpha-numerical identifier.

• ID cards should never contain personal information such as Social Security Numbers.

By following the above recommendations and regularly evaluating the credentialing and access control program, an organization can ensure that it does not open itself up to unnecessary risk. ■

"ID cards and access control cards should be kept separate. If an ID card must be used as an access control card, it should be used in conjunction with a biometric device."

