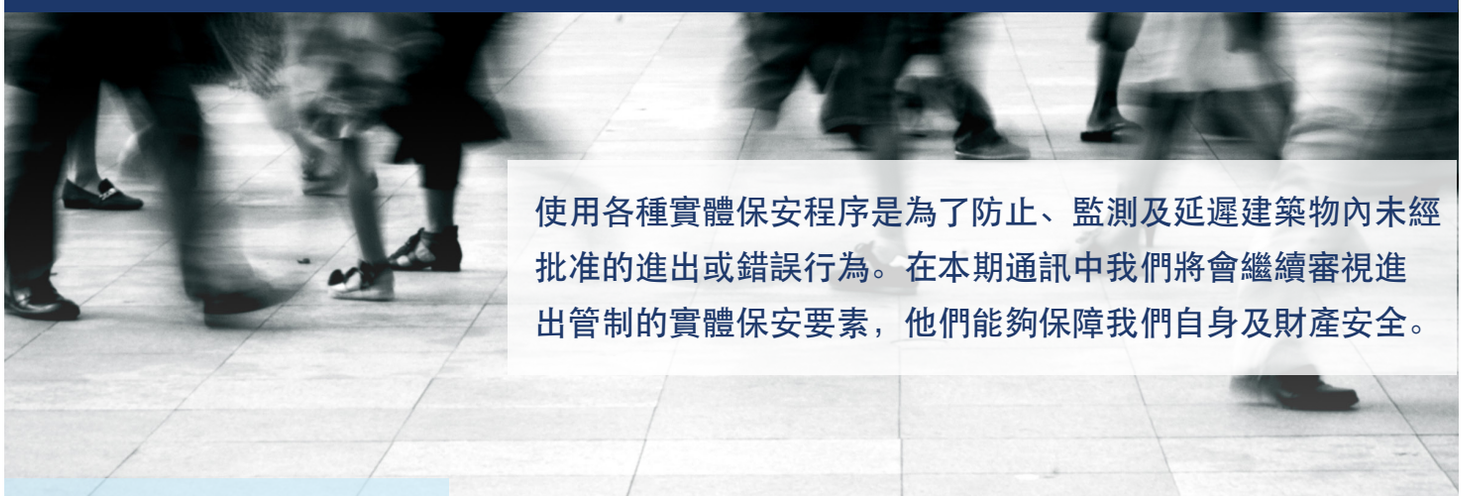
OMNIRISC
REDEFINING SECURITY

Security Newsletter

APRIL 2018 I ISSUE 8



使用各種實體保安程序是為了防止、監測及延遲建築物內未經批准的進出或錯誤行為。在本期通訊中我們將會繼續審視進出管制的實體保安要素，他們能夠保障我們自身及財產安全。

實體保安系統的各個要素包括：

- 整體及持續的威脅及危機評估
- 外部周邊及建築物保安包括門鎖及警鐘.
- 內部子空間的保安
- 員工訪客及車輛進出管制
- 電子監控
- 保安人員守衛
- 安全管理及監察服務
- 安全照明系統
- 安全事故應對
- 要員的人身安全保障
- 保安、人流管制、娛樂聚會及其他主要活動的安全

進出管制

所有建築物及設施都有數個專為行人而設的入口，以及大量為緊急逃生而設的其他出口。另外，很多建築物會提供車輛出入，這些不同的出入點會以各種方式進行保護及管理。

以下是建築物或設施的各種出入，他們都要經過仔細考量，因為每一種都需要不同的安全管理措施。

- 員工出入
- 訪客進出
- 員工車輛進出
- 訪客車輛出入以及
- 運輸車輛訪問

一般來說，為了應對以上各種出入而運用的保安管理措施可以分為封閉式和開放式。封閉式的進出管理系統會把所有建築物或設施的出入控制在其物理範圍內，而開放式的進出管理系統會允許建築物或設施的初步訪問，隨後會由內部空間持有人進行內部管制。

封閉式的進出管理系統

例子一

一個封閉式的進出管理系統，例如：綜合辦公大樓內可能包括：博彩企業、金融服務公司及尋求高端保安服務的公司

這幢大樓會確保各個外圍控制點運作正常而員工出入受到管制，授權的訪客能夠被引導、管理及妥善地護送。在適當情況下，授權車輛能被允許停泊而車輛使用者需通過全面的進出管制檢查，以及只有獲得許可的運輸車輛才能夠進入建築物或設施。

在使用封閉式系統的情況下，以下各種出入均需要不同的安全管理程序。

員工出入：授權的員工經常(但不總)是通過獨立的員工通道進入建築物。這種出入一般會由駐守保安員操控，並使用一系列的身份認證方法，有時通過使用一定數量的物理障礙能加強管制。[請參見以下例子]

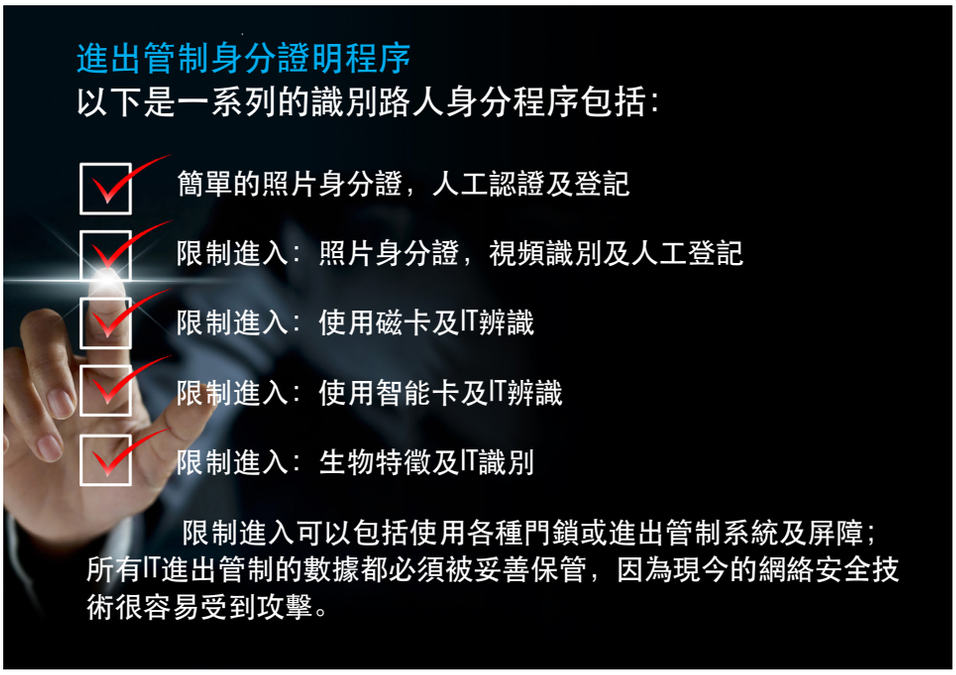
訪客出入：許可的訪客應在某一個地點被引導、檢查及管理，例如主要入口。一旦確認身份，訪客應會獲得明確的身份標識，且被引導到他們想去的地方，如有必要他們需被護送至該區域並移交給相關負責人。

員工車輛進出：假如員工的私人車輛獲得進出大樓的許可，到達外圍時應通過智能卡出入管制系統的檢查，其後車輛使用者就能就能繼續進入一般的員工進出程序。

訪客車輛進出：同樣地，授權的訪客車輛應受到管制，而使用者則被引導至一般的訪客出入口。

運輸車輛訪問：在允許進入前，所有運輸車輛都應預先獲得授權，接收部門應檢查他們的貨物；所有車輛在離開前必須通過安全檢查。

OMNIRISC SECURITY SERVICE (MACAO) LTD. 26 Avenida De Marciano Baptista, Chong Fok Comercial Centre, 12/H, Macau
Office: +853 28558964 Email: info@omnirisc.com
www.omnirisc.com



開放式進出管制系統

例子二

開放式系統例如賭場，其中包括：
綜合式度假村
賭博區
現金存放區
會展中心
餐飲店
零售商店
珠寶商店
以及
體育設施

以上大部份區域都使用開放式進出管制系統，允許大眾出入以及減少顯眼的安全監管，但某些包括賭博區及現金存放區，則需要更小心謹慎地運作。

在開放式系統中，個別的商舖一般會根據自身的威脅及風險進行保安工作。例如在賭場裡，珠寶商店與餐飲店的安全需求大不相同。即使賭場保安負責保護整個設施，珠寶店仍會需要增加額外的安全保障。

緊急逃生出口

所有設施或建築物為了對抗火災和疏散，都設有一些額外的緊急逃生出口，他們通常都是關閉及鎖上的，一般不會進出。(雖然某些機構會使用他們作為入口)

一些員工可能會為了方便行動而開啟緊急出口大門，這樣會破壞進出管制計劃，應該要通過定期保安巡邏以及設置開門感應器和警鐘來阻止。

緊急逃生大門應該向外開啟並設有推杆(緊急手把)鎖以便離開，至於使用代碼、數字組合、刷卡或者觸碰式卡鎖的安全門應能用推杆解除鎖定。

應該定期檢查逃生路線及門鎖機制以確保路線暢通無阻以及太平門能正確有效地使用。

內部威脅

有效地使用一個設計周詳、管理有方的進出管制系統，能夠確保機構的外部威脅在不能避免的情況下得以減低。但若內部威脅來自於獲得授權的進入者呢？我們必須考慮這樣的情況。

為了防止內部人員任何不道德或犯罪行為，機構必須建立多層或同心圓式的實體保安。例如應用額外的進出管制以保証只有授權及必要人士才能進入特定區域。以上所提到的進出管制系統只是一個起步，之後需要重複或多次調配這些行動以保障脆弱的設施、器材及數據。

有效的保安訓練

即是機構在最佳狀態下運用高度完善的保安系統，人類亦可以成為最脆弱的部分；懶惰、犯錯或不誠實的員工都可以在瞬間破壞一個進出管制系統。

為了應對這個狀況，機構必須定立有效的安全政策，使所有員工都清楚並接納其中細節，他們必須經過專業訓練並嚴格遵守政策，保安部門必須積極主動地尋找及解決任何進出管制安全的漏洞。

進出管制審計

所有運用進出管制程序的機構必須定期檢查及審計以保證持續合規性。

違反出入管制的行為包括：

- 把鑰匙或通行卡借給第三方
- 未經批准轉交鑰匙或通行卡
- 未經授權複製鑰匙或通行卡信息
- 未能報告丟失鑰匙或通行卡
- 打開安全門
- 允許未經授權人士進入建築物
- 允許未經許可車輛進入建築物
- 未能報告損壞的門鎖
- 暴露IT密碼
- 錯誤使用IT密碼
- 下載過量數據
- 保安人員未能妥善管理進出管制系統

員工應報告任何違規行為，以便安全人員及時發現並解決。

安全部門的定期審計，以及由獨立機構偶爾就所有進出管制的做法和程序的個別審計，都能確保進出管理程序能有效合適地持續使用。

在接下來的數期安利通訊中我們會繼續審視實體保安以及安全審計的其他方面例如電子監控、人手保安、安全控制及管理。

關於作者

James Langton, 安利保安服務(澳門)有限公司的顧問，在保安和執法行動方面擁有超過40年的經驗。

OMNIRISC
REDEFINING SECURITY

Office: +853 28558964 Email: info@omnirisc.com
www.omnirisc.com