ISMS驗證作業通知

致 我們尊敬的客戶、親愛的合作夥伴:

首先感謝您長期對法標國際認證股份有限公司的信任與支持。因應國際 ISO/IEC 27006-1:2024 轉版要求，本公司在取得新版認證後，將依新標準執行初次驗證與重新驗證（複評）。本通知旨在讓您了解新版對驗證規劃的影響，以及在申請與準備作業上需要注意的事項。簡易說明如下：

一、更新稽核時間計算要求

在驗證範圍內組織管理下，所有班別(shift)的總工作人數，是決定稽核時間的起始點。以及組織管制的工作人員包括所有在驗證範圍內必須依 ISMS 要求工作的全體員工(不論是否為組織編制人力)。在此要求下，驗證範圍之人數將為廣義之計入實施風險管控，例如包括驗證範圍內使用資訊系統行使職務之各部門員工或無存取權限之現場工作人員等。

二、提供減少人數的合理作法

提供減少人數的合理作法，因此驗證客戶將需提供人數較高從事特定相同活動的相關資訊，包括：

-從事的活動或過程；

-從事該活動的人數。

例如以下群組：

1. 為履行職責之需，對資訊具有唯讀存取權限的員工。
2. 對於 ISMS 範圍涵蓋的組織資訊處理設施，不具存取權限的員工。
3. 對於 ISMS 範圍涵蓋的公司資訊處理設施，具有可具體證明之限制存取權限的員工。
4. 從事活動有嚴格限制以防止資訊外洩的員工，例如：制訂禁止將個人物品及裝置帶入工作區域的措施。

各群組之人數將可考量以平方根方式進行工作人數減少之處理。

三、多場區與遠端稽核安排同步更新

更新遠端稽核、多場區及擴增範圍的相關要求。例如，標準新增「遠端稽核」適用規範，並明確說明多場區與擴增範圍時應如何計算稽核時間。

四、關於轉版的時程安排如下

驗證機構對所有客戶採行 ISO/IEC 27006-1:2024 不得晚於 2026 年 3 月 31 日。對於在認證轉版日期之前獲得驗證的客戶，驗證機構在獲得 ISO/IEC 27006-1:2024 認可後可使用 ISO/IEC 27006:2015 或 ISO/IEC 27006-1:2024 進行追查稽核。

如您對轉版內容、驗證範圍或人員計算方式有任何疑問，歡迎隨時與我們聯繫。法標國際將協助您平順銜接新版要求，並持續提供最專業的服務。

順頌

時祺

總經理 General Manager

凌孝光 Jeff Ling