安迅士 與網路安全

所有網路裝置都可能受到威脅，包括網路攝影機在內。網路攝影機是整體系統的一部分，而網路則是當中的骨幹所在。無論是系統整體或個別裝置，所有環節都有漏洞，而這一整套系統需要受到保護。

您的強大防護是最脆弱的一環。

Axis 裝置能夠針對不同的安全級別進行設定。Axis**安全強化指南**現已在我們的網站上推出！

貴組織的 IT 和網路政策須與適當的風險分析相互結合，才能提供更高層級的防護來對抗網路威脅。網路型裝置可提供額外的價值與情報。透過攜手合作，我們能降低曝露於危險的範圍與風險，讓您的系統更加安全。雖然無法阻止攻擊，但是 Axis 的安全風險政策 (Vulnerability Policy) (已在網站上推出) 當中說明了 Axis 能夠為合作夥伴和終端使用者提供什麼樣的服務。

Axis 的網路安全任務：

> 提高對資安產業的認知
> 提供領先思維
> 依據營運與需求，幫助相關者達到理想的攝影機/影像系統防護層級

www.axis.com/support/product-security

AXIS COMMUNICATIONS

安迅士 的 10 大網路安全建議

1. 進行風險分析找出潛在威脅，以及了解系統遭受攻擊時可能蒙受的損失/費用。

2. 增進有關系統防護與可能威脅的知識。與零售商、系統整合商、專家顧問、產品供應商密切合作。網際網路就是絕佳的資源。

3. 保護網路安全。如果網路防護措施遭到破壞，機密資料遭到窺探以及個別伺服器和網路裝置遭到攻擊的風險就會增加。

4. 使用強大獨特的密碼，並且定期變更。

5. 切勿倚賴網路裝置的出廠預設設定
   > 變更預設密碼。
   > 啟用並設定裝置保護服務。
   > 將不使用的服務停用。

6. 盡可能採用加密的連線，包括區域網路在內。

7. 為減少曝露危險範圍，除非是系統/解決方案所需，否則影像用戶端不得直接存取攝影機。用戶端只能透過 VMS (影像管理系統) 或媒體 Proxy 存取影像。

8. 定期查看存取記錄中是否有企圖進行未經授權存取的情形。

9. 定期監控裝置。在適當且支援的情況下，啟用系統通知。

10. 使用最新韌體，因為當中可能包含安全性修補程式。

www.axis.com/support/product-security

AXIS COMMUNICATIONS