KAELITH SECURITY GUIDE

雙重驗證 2FA

高權限帳號的基本控管

說明 2FA 導入順序、備援碼管理、帳號分級、離職交接與日常維護檢查方式。

分類	閱讀時間	適用對象	版本日期
帳號防護	8–10 分鐘	主機管理者、DNS 管理者、信箱管理者、網站後台管理者	2026-06-19

文件摘要

說明 2FA 導入順序、備援碼管理、帳號分級、離職交接與日常維護檢查方式。

使用範圍與維護原則

雙重驗證能降低密碼外洩後的接管風險。對主機、DNS、網域註冊商、信箱與網站後台來說，2FA 應被視為基本控管，而不是選用功能。

導入時不能只按下啟用按鈕，還要同時處理備援碼、帳號分級、離職交接、登入通知與定期盤點。

風險等級

高

建議檢查頻率

每季檢查一次；若有主機、DNS、信箱或人員異動，應額外盤點。

02 / 導入順序

先保護能改變網站命運的帳號。

最先啟用 2FA 的通常是 cPanel、DNS 管理、網域註冊商、主要信箱、網站後台、雲端儲存與付款相關帳號。

這些帳號一旦被接管，可能造成網站內容被改、DNS 被導向、信件被轉寄、帳號被重設或付款資料被變更。

項目	說明
第一優先	主機控制台、DNS、網域註冊商、主要信箱
第二優先	網站後台、雲端儲存、付款與發票平台
第三優先	社群帳號、協作工具、次要通知信箱

03 / 驗證方式

驗證器、Passkey 或安全金鑰優先於簡訊。

建議優先使用驗證器 App、硬體安全金鑰或平台原生 Passkey。簡訊驗證雖然比沒有 2FA 好，但容易受到門號轉移、簡訊攔截與社交工程影響。

高權限帳號不應只依賴簡訊驗證；若平台只支援簡訊，應搭配強密碼、登入通知與可疑活動檢查。

備援碼

啟用後立即離線保存，限制可接觸人員。

復原流程

避免用單一訊息或口頭確認直接恢復權限。

04 / 日常維護

帳號分級與定期盤點比一次性設定更重要。

維護階段應區分擁有者、管理員、內容更新者與一般使用者，並定期移除不再使用的帳號。共享帳號應盡量避免，否則很難追查實際操作來源。

若有主機搬移、DNS 變更、人員異動或異常登入通知，應立即重新盤點高權限帳號與 2FA 狀態。

1. 每季盤點高權限帳號與 2FA 啟用狀態。
2. 確認備援碼保存位置與接觸人員。
3. 移除離職、停用或不再需要的帳號。
4. 檢查登入通知、異常登入紀錄與工作階段撤銷能力。

維護檢核

維護檢查清單

以下項目可用於定期維護、權限盤點或事件回應前的初步確認。

- cPanel、DNS、網域註冊商與主要信箱是否已啟用 2FA。
- 是否避免以簡訊作為唯一高權限驗證方式。
- 備援碼是否離線保存，且只有必要人員可接觸。
- 是否定期移除離職、停用或不再需要的帳號。
- 是否保留登入通知、異常登入紀錄與工作階段撤銷能力。
- 是否每季盤點一次高權限帳號與 2FA 狀態。

本文件由 Kaelith 數位開發整理，供網站維護、帳號安全與日常風險控管參考。實際處理仍應依主機商、DNS 供應商、信箱服務與系統權限條件調整。