政府組態基準

Microsoft Word 2019

TWGCB-04-009

(V1.0)

行政院國家資通安全會報技術服務中心

中華民國111年7月

修訂歷史紀錄表

項次	版次	修訂日期	說明
1	1.0	111/7/22	新編
2			
3			
4			
5			

目　次

表 目 次

1. 前言

政府組態基準(Government Configuration Baseline, 以下簡稱 GCB)目的在於規範資通訊終端設備(如個人電腦等)之一致性安全設定(如密碼長度、更新期限等)，以降低成為駭客入侵管道，進而引發資安事件之風險。

1.1 適用環境

本文件適用於微軟公司所發行之 Microsoft Word 2019 應用程式。

1.2 項數統計

政府組態基準針對電腦作業環境提供一致性資安防護基準與實作指引，供政府機關透過建立安全組態，提升資安防護能力。Microsoft Word 2019 組態基準共計 50 項設定項目，項目統計詳見表 1。

表1　Microsoft Word 2019 組態基準項目統計

項次	項目	項數	合計
1	Word 2019 Computer Settings	16	50
2	Word 2019 User Settings	34	

資料來源：本中心整理

1.3 文件發行

本文件最新版本公布於本中心網站之「政府組態基準」專區，網址為 https://www.nccst.nat.gov.tw/GCB。

2. Microsoft Word 2019 政府組態基準列表

表2　Microsoft Word 2019 政府組態基準列表

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
1	Word 2019 Computer Settings	TWGCB-04-009-0001	安全性設定\IE 安全性	附加元件管理	▪附加元件是在 Internet Explorer 中運行的程式，用來提供瀏覽器以外之其他功能 ▪如果啟用這項原則設定並選擇 Word 應用程式，可確保 Word 應用程式遵循 Internet Explorer 附加元件管理設定 ▪如果停用或未設定這項原則設定，若附加元件含有惡意程式，則可能危害電腦安全性	電腦設定\系統管理範本\Microsoft Office 2019(電腦)\安全性設定\IE 安全性\附加元件管理	啟用，並選取 winword.exe
2	Word 2019 Computer Settings	TWGCB-04-009-0002	安全性設定\IE 安全性	繫結到物件	▪這項原則設定決定 Internet Explorer 在開啟由 Office 2019 應用程式傳遞之 URL 時，是否對 Microsoft ActiveX 控制項進	電腦設定\系統管理範本\Microsoft Office 2019(電腦)\安全性設定	啟用，並選取 winword.exe

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					行安全檢查。預設狀況下，Internet Explorer 在 ActiveX 控制項初始化時，會執行額外的安全檢查 ▪ 如果啟用這項原則設定並選擇 Word 應用程式，Internet Explorer 安全檢查將適用於 Word 應用程式開啟之網頁所包含的 ActiveX 物件	\IE 安全性\繫結到物件	
3	Word 2019 Computer Settings	TWGCB-04-009-0003	安全性設定\IE 安全性	一致的 MIME 處理	▪ Internet Explorer 使用多用途網際網路郵件延伸標準(MIME)資料來判斷從網頁伺服器收到之檔案的檔案處理程序 ▪ 這項原則設定決定 Internet Explorer 是否要求網頁伺服器提供之所有檔案類型資訊都必須一致。例如，如果檔案之 MIME 類型是 text/plain，但是	電腦設定\系統管理範本\Microsoft Office 2019(電腦)\安全性設定\IE 安全性\一致的 MIME 處理	啟用，並選取 winword.exe

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					MIME 探查指出檔案其實是執行檔，則 Internet Explorer 會將檔案儲存在 Internet Explorer 快取中並變更其副檔名，來重新命名檔案 ▪ 如果啟用或未設定這項原則設定，Internet Explorer 將要求所有接收之檔案都有一致的 MIME 資料 ▪ 如果停用這項原則設定，Internet Explorer 將不會要求所有接收之檔案都有一致的 MIME 資料		
4	Word 2019 Computer Settings	TWGCB-04-009-0004	安全性設定\IE 安全性	停用使用者名稱及密碼	▪ 這項原則設定決定 Internet Explorer 是否開啟來自 Word 應用程式傳遞包含使用者資訊之 URL ▪ 如果啟用這項原則設定並選擇	電腦設定\系統管理範本\Microsoft Office 2019(電腦)\安全性設定\IE 安全性\停用	啟用，並選取 winword.exe

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					Word 應用程式，Internet Explorer 將阻止 Word 應用程式開啟包含使用者身分驗證資訊的任何 URL	使用者名稱及密碼	
5	Word 2019 Computer Settings	TWGCB-04-009-0005	安全性設定\IE 安全性	資訊列	▪這項原則設定決定當檔案或程式碼安裝受到限制時，是否顯示 Internet Explorer 程序的「資訊列」。預設狀況下，將會顯示 Internet Explorer 程序的「資訊列」 ▪如果啟用這項原則設定並選擇 Word 應用程式，將會顯示 Internet Explorer 程序的「資訊列」 ▪如果停用這項原則設定，將不會顯示 Internet Explorer 程序的「資訊列」 ▪如果未設定這項原則設定，將	電腦設定\系統管理範本\Microsoft Office 2019(電腦)\安全性設定\IE 安全性\資訊列	啟用，並選取 winword.exe

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					會顯示 Internet Explorer 程序的「資訊列」		
6	Word 2019 Computer Settings	TWGCB-04-009-0006	安全性設定\IE 安全性	本機電腦區域鎖定安全性	▪ Internet Explorer 根據網頁的位置(網際網路、內部網路或本機電腦區域等)，對每個開啟的網頁設定區域限制。本機電腦上的網頁擁有的安全性限制最少，且位於本機電腦區域內 ▪ 如果啟用這項原則設定並選擇 Word 應用程式，則本機電腦區域將適用於 Word 應用程式之所有本機檔案與內容 ▪ 如果停用或未設定這項原則設定，則本機電腦區域將不適用於 Word 應用程式之所有本機檔案與內容	電腦設定\系統管理範本\Microsoft Office 2019(電腦)\安全性設定\IE 安全性\本機電腦區域鎖定安全性	啟用，並選取 winword.exe
7	Word	TWGCB	安全性設定	MIME 探	▪ 這項原則設定決定 Internet	電腦設定\系統管	啟用，並選取

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	2019 Computer Settings	-04-009-0007	\IE 安全性	查安全功能	Explorer MIME 探查是否能防止單一類型的檔案提升為較危險的檔案類型 ▪ 如果啟用或未設定這項原則設定，MIME 探查永遠不會將單一類型的檔案提升為較危險的檔案類型 ▪ 如果停用這項原則設定，Internet Explorer 程序將允許 MIME 探查將單一類型的檔案提升為較危險的檔案類型	理範本\Microsoft Office 2019(電腦)\安全性設定\IE 安全性\MIME 探查安全功能	winword.exe
8	Word 2019 Computer Settings	TWGCB-04-009-0008	安全性設定\IE 安全性	瀏覽 URL	▪ 這項原則設定決定當 Word 應用程式傳送錯誤的 URL 格式時，Internet Explorer 是否嘗試載入該 URL ▪ 如果啟用這項原則設定並選擇 Word 應用程式，Internet Explorer 將封鎖由 Word 應用	電腦設定\系統管理範本\Microsoft Office 2019(電腦)\安全性設定\IE 安全性\瀏覽 URL	啟用，並選取 winword.exe

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					程式所傳送之任何格式錯誤的 URL		
9	Word 2019 Computer Settings	TWGCB-04-009-0009	安全性設定\IE 安全性	物件快取保護	▪ 這項原則設定定義使用者在相同網域內或至新網域瀏覽時，是否可以存取物件參照 ▪ 如果啟用這項原則設定，則透過 Word 應用程式存取之 Internet Explorer 程序，在相同網域內或跨網域瀏覽時將無法再存取物件參照 ▪ 如果停用或未設定這項原則設定，Internet Explorer 程序在相同網域內或跨網域瀏覽時將保留物件參照	電腦設定\系統管理範本\Microsoft Office 2019(電腦)\安全性設定\IE 安全性\物件快取保護	啟用，並選取 winword.exe
10	Word 2019 Computer	TWGCB-04-009-0010	安全性設定\IE 安全性	來自區域高度的保護	▪ Internet Explorer 對每個開啟的網頁設定限制。設定限制的標準是根據網頁的位置(網際網	電腦設定\系統管理範本\Microsoft Office 2019(電	啟用，並選取 winword.exe

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	Settings				路、內部網路或本機電腦區域等)。本機電腦上的網頁擁有的安全性限制最少，且位於本機電腦區域內，因此本機電腦安全性區域便成為惡意使用者的主要攻擊目標。如果沒有安全性內容，區域高度也會停用 JavaScript 瀏覽 ▪ 如果啟用這項原則設定，任何區域都可以透過 Internet Explorer 程序受到區域高度保護 ▪ 如果停用或未設定這項原則設定，沒有區域電腦設定會透過 Internet Explorer 程序受到區域高度保護	腦)\安全性設定\IE 安全性\來自區域高度的保護	
11	Word 2019	TWGCB-04-009-	安全性設定\IE 安全性	限制 ActiveX 安	▪ 這項原則設定決定是否封鎖 Internet Explorer 程序的	電腦設定\系統管理範本\Microsoft	啟用，並選取 winword.exe

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	Computer Settings	0011		裝	ActiveX 控制項安裝提示 ▪如果啟用這項原則設定，將會封鎖 Internet Explorer 程序的 ActiveX 控制項安裝提示，並避免 Word 應用程式更新該 ActiveX 控制項 ▪如果停用或未設定這項原則設定，將不會封鎖 Internet Explorer 程序的 ActiveX 控制項安裝提示	Office 2019(電腦)\安全性設定\IE 安全性\限制 ActiveX 安裝	
12	Word 2019 Computer Settings	TWGCB-04-009-0012	安全性設定\IE 安全性	限制檔案下載	▪這項原則設定決定是否封鎖非使用者起始之檔案下載提示 ▪如果啟用這項原則設定，將會封鎖 Internet Explorer 程序的非使用者起始之檔案下載提示 ▪如果停用這項原則設定，將會允許 Internet Explorer 程序的非	電腦設定\系統管理範本\Microsoft Office 2019(電腦)\安全性設定\IE 安全性\限制檔案下載	啟用，並選取 winword.exe

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					使用者起始之檔案下載提示		
13	Word 2019 Computer Settings	TWGCB-04-009-0013	安全性設定\IE 安全性	從 URL 儲存	▪ 這項原則設定決定 Word 應用程式傳送給 Internet Explorer 評估的 URLs，是否標示 Mark of the Web(MOTW)註解，供 Internet Explorer 判斷該 URL 是否位於安全區域 ▪ 如果啟用這項原則設定並選擇 Word 應用程式，Internet Explorer 將分析 Word 應用程式傳送的 URL，藉由 MOTW 註解判斷網頁的位置(如網際網路區域或近端內部網路區域)，並採用相對應之安全性設定來瀏覽該網頁	電腦設定\系統管理範本\Microsoft Office 2019(電腦)\安全性設定\IE 安全性\從 URL 儲存	啟用，並選取 winword.exe
14	Word 2019	TWGCB-04-009-	安全性設定\IE 安全性	已撰寫指令碼的視	▪ Internet Explorer 允許指令碼以程式開啟不同類型的視窗，調	電腦設定\系統管理範本\Microsoft	啟用，並選取 winword.exe

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	Computer Settings	0014		窗安全性限制	整其大小以及位置。視窗安全限制功能會限制快顯視窗停留在可視區域、顯示狀態列，並且無法拖曳至螢幕的可視區域外 ▪如果啟用這項原則設定，將會限制已撰寫指令碼的視窗 ▪如果停用或未設定這項原則設定，將允許未知網站： (1)建立看似來自本機作業系統的瀏覽器視窗 (2)在螢幕可視區域外建立活動視窗 (3)覆蓋父視窗，隱藏重要的系統資訊、選項或提示	Office 2019(電腦)\安全性設定\IE 安全性\已撰寫指令碼的視窗安全性限制	
15	Word 2019	TWGCB-04-009-	MS Security Guide	Block Flash	▪這項原則設定決定 Office 文件是否可啟動 Adobe Flash 元件	電腦設定\系統管理範本\MS	啟用，並選取「Block all

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	Computer Settings	0015		activation in Office documents	▪ 如果啟用這項原則設定，可透過下列 3 個控制選項，決定 Adobe Flash 元件是否可被啟動： (1)Block all activation：禁止啟動 Adobe Flash 元件，不論是由 Office 文件直接啟動，或由其他 Office 應用程式內建物件間接啟動 (2)Block embedding/linking, allow other activation：禁止 Adobe Flash 元件由 Office 文件直接啟動，但允許被其他 Office 應用程式內建物件啟動 (3)Allow all activation：允許 Office 文件啟動 Adobe Flash 元件，此選項為預設	Security Guide\ Block Flash activation in Office documents	activation」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					行為 ▪ 如果停用或未設定這項原則設定，則允許 Office 文件啟動 Adobe Flash 元件 ▪ 注意：若欲恢復預設行為，需將控制選項設為「Allow all activation」		
16	Word 2019 Computer Settings	TWGCB-04-009-0016	MS Security Guide	Restrict legacy JScript execution for Office	▪ 這項原則設定決定 Office 應用程式對哪些 Internet Explorer「安全性設定區域」封鎖執行舊版 JScript 程式 ▪ 如果啟用這項原則設定，並將指定之 Office 應用程式設為 69632，則該應用程式將不會在「網際網路」與「限制的網站」安全區域執行舊版 JScript 程式，且使用者不會收到通知	電腦設定\系統管理範本\MS Security Guide\Restrict legacy JScript execution for Office	啟用，並將 Word 應用程式設為「69632」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					▪ 如果停用或未設定這項原則設定，則 Office 應用程式允許執行舊版 JScript 程式		
17	Word 2019 User Settings	TWGCB-04-009-0017	全域選項\自訂	停用文件及範本延伸的 UI	▪ 這項原則設定決定 Office 2019 應用程式是否可載入文件或範本所隨附的任何自訂使用者介面(UI)程式碼。Office 2019 可讓開發人員擴充文件或範本所隨附的 UI 自訂碼 ▪ 如果啟用這項原則設定，則 Office 2019 應用程式無法載入文件與範本所隨附的任何 UI 自訂碼 ▪ 如果停用或未設定這項原則設定，則 Office 2019 應用程式會在開啟文件或範本時，載入其隨附的任何 UI 自訂碼	使用者設定\系統管理範本\Microsoft Office 2019\全域選項\自訂\停用文件及範本延伸的 UI	啟用，並選取「在 Word 中禁止」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
18	Word 2019 User Settings	TWGCB-04-009-0018	安全性設定	自動安全性	▪這項原則設定決定巨集是否能在其他應用程式以程式設計方式開啟的 Office 2019 應用程式中執行 ▪如果啟用這項原則設定，有 3 個控制選項可以選擇，可以在應用程式以程式設計方式開啟時，控制 Word 中的巨集行為： (1)根據預設停用巨集：在以程式設計方式開啟的應用程式中一律停用所有巨集 (2)已啟用巨集(預設)：巨集可以在以程式設計方式開啟的應用程式中執行。此選項會強制執行 Word 的預設設定 (3)使用應用程式巨集安全性層級：巨集功能是由「信任	使用者設定\系統管理範本\Microsoft Office 2019\安全性設定\自動安全性	啟用，並設定自動安全性層級為「使用應用程式巨集安全性層級」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					中心」內的「巨集設定」區段的設定所決定 ▪ 如果停用或未設定這項原則設定，則當以程式設計方式使用其他程式來啟動 Microsoft Word 時，任何巨集都能在以程式設計方式開啟的應用程式中執行，而不會遭到封鎖		
19	Word 2019 User Settings	TWGCB-04-009-0019	安全性設定	允許 VBA 從不受信任的內部網路位置路徑來載入 TypeLib 參照	▪ 這項原則設定決定是否允許 VBA 專案從不受信任的內部網路位置載入 TypeLib 參照 ▪ 根據預設，VBA 專案在載入 TypeLib 參照時，會優先搜尋註冊表，如果在註冊表中找不到該 TypeLib，只要專案中的參照路徑未指向不受信任的內部網路位置，則 VBA 嘗試從該路徑載入 TypeLib 參照	使用者設定\系統管理範本\Microsoft Office 2019\安全性設定\允許 VBA 從不受信任的內部網路位置路徑來載入 TypeLib 參照	停用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					▪ 如果啟用這項原則設定，VBA 專案將視內部網路路徑為本機路徑，因此，VBA 將嘗試從不在信任網站清單中的內部網路位置搜尋未登錄的參照 ▪ 如果停用或未設定這項原則設定，則 VBA 維持其預設行為，拒絕載入位於內部網路位置的 TypeLib 參照		
20	Word 2019 User Settings	TWGCB-04-009-0020	安全性設定	停用 VBA 程式庫參照上可能參照本機電腦中不安全位置的其他安全性檢查	▪ 這項原則設定決定是否限制 VBA 專案只針對註冊表及受信任區域檢查專案程式庫參照 ▪ 根據預設，VBA 專案會針對程式庫路徑執行額外檢查，以避免從可能不安全的本機位置載入參照 ▪ 如果啟用這項原則設定，VBA 專案將不對位於本機電腦不安	使用者設定\系統管理範本\Microsoft Office 2019\安全性設定\停用 VBA 程式庫參照上可能參照本機電腦中不安全位置的其他安全性檢查	停用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					全位置之程式庫參照進行安全性檢查 ▪如果停用或未設定這項原則設定，VBA 專案將對位於本機電腦不安全位置之程式庫參照進行安全性檢查		
21	Word 2019 User Settings	TWGCB-04-009-0021	隱私權\信任中心	啟用客戶經驗改進計畫	▪這項原則設定決定使用者是否參與 Microsoft Office 客戶經驗改進計畫(CEIP)，以協助改善 Microsoft Office。當使用者選擇參與客戶經驗改進計畫時，Office 2019 應用程式會自動將應用程式使用方式的相關資訊傳送給 Microsoft。此資訊會與其他 CEIP 資料結合，協助 Microsoft 解決問題並改善使用者最常使用的產品及功能。除了收集傳送資料所用的 IP 位	使用者設定\系統管理範本\Microsoft Office 2019\隱私權\信任中心\啟用客戶經驗改進計畫	停用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					址之外，此功能並不會收集使用者的姓名、地址或任何其他身分識別資訊 ▪ 如果啟用或未設定這項原則設定，使用者有機會在首次執行 Office 應用程式時選擇參與 CEIP ▪ 如果停用這項原則設定，使用者則不會參與客戶經驗改進計畫		
22	Word 2019 User Settings	TWGCB-04-009-0022	隱私權\信任中心	傳送個人資訊	▪ 這項原則設定決定使用者選擇自動傳送 Office 2019 應用程式資訊給 Microsoft 時，是否可將個人資訊傳送給 Microsoft ▪ 如果啟用或未設定這項原則設定，使用者會將個人資訊傳送給 Microsoft	使用者設定\系統管理範本\Microsoft Office 2019\隱私權\信任中心\傳送個人資訊	停用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					▪如果停用這項原則設定，使用者就無法傳送個人資訊給 Microsoft		
23	Word 2019 User Settings	TWGCB-04-009-0023	工具|選項|拼字檢查\校訂資料收集	改善校訂工具	▪這項原則設定可控制「協助改善校訂工具」功能是否會傳送使用資料給 Microsoft。「協助改善校訂工具」功能會收集校訂工具的使用資料(例如新增至自訂字典)並傳送給 Microsoft。6 個月之後，該功能會停止傳送資料給 Microsoft，並刪除來自使用者電腦的資料收集檔案 ▪如果啟用或未設定這項原則設定，則會在使用者選擇參加客戶經驗改進計畫(CEIP)時啟用此功能 ▪如果停用這項原則設定，則「協	使用者設定\系統管理範本\Microsoft Office 2019\工具|選項|拼字檢查\校訂資料收集\改善校訂工具	停用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					助改善校訂工具」功能並不會收集校訂工具的使用資訊並傳送給 Microsoft		
24	Word 2019 User Settings	TWGCB-04-009-0024	其他	控制部落格功能	▪ 這項原則設定決定使用者是否可以從 Word 撰寫並張貼部落格文章 ▪ 如果啟用這項原則設定，則有 3 個部落格控制選項可以選擇： (1)啟用：使用者可以從 Word 撰寫並張貼部落格文章到任何可用的部落格。此為 Word 應用程式的預設設定 (2)只允許 SharePoint 部落格：使用者只能將部落格文章張貼到 SharePoint 網站 (3)停用所有部落格功能：完全	使用者設定\系統管理範本\Microsoft Office 2019\其他\控制部落格功能	啟用，並設為「停用所有部落格功能」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					停用 Word 部落格功能 ▪如果停用或未設定這項原則設定，使用者可以從 Word 撰寫並張貼部落格文章到任何可用的部落格		
25	Word 2019 User Settings	TWGCB-04-009-0025	Word 選項\儲存	預設檔案格式	▪這項原則設定決定 Word 在儲存檔案時的預設檔案格式 ▪如果啟用這項原則設定，使用者可從下列選項，設定預設的檔案格式： (1)Word 文件(*.docx)：此選項為 Word 的預設設定 (2)單一檔案網頁(*.mht) (3)網頁(*.htm; *.html) (4)已篩選的網頁(*.htm, *.html) (5)RTF 格式(*.rtf)	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\儲存\預設檔案格式	啟用，並設定另存 Word 檔案為「Word 文件(*.docx)」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值
					(6)純文字(*.txt) (7)Word 6.0/95(*.doc) (8)Word 6.0/95-中文(簡體)(*.doc) (9)Word 6.0/95-中文(繁體)(*.doc) (10)Word 6.0/95-日文(*.doc) (11)Word 6.0/95-韓文(*.doc) (12)Word 97-2002 & 6.0/95-RTF (13)Word 5.1 for Macintosh(*.mcw) (14)Word 5.0 for Macintosh(*.mcw) (15)Word 2.x for Windows(*.doc) (16)Works 4.0 for		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					Windows(*.wps) (17)WordPerfect 5.x for Windows (*.doc) (18)WordPerfect 5.1 for DOS(*.doc) (19)Word 啟用巨集的文件(*.docm) (20)Word 範本(*.dotx) (21)Word 啟用巨集的範本(*.dotm) (22)Word 97-2003 文件(*.doc) (23)Word 97-2003 範本(*.dot) (24)Word XML 文件(*.xml) (25)Strict Open XML 文件(*.docx) (26)OpenDocument 文字(*.odt)		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					▪使用者可以選擇非預設的其他檔案格式來儲存簡報或文件 ▪如果停用或未設定這項原則設定，Word 會以 Office Open XML 格式儲存新檔案，Word 檔案的副檔名則為.docx。對於執行新版 Word 的使用者，Microsoft 提供了 Microsoft Office 相容性套件，使用者們便能夠開啟與儲存 Office Open XML 檔案。如果機關有部分使用者無法安裝相容性套件，或者執行 Microsoft Office 2000 Service Pack 3 之前的舊版本 Word，這些使用者可能無法存取 Office Open XML 檔案 ▪使用者可以透過使用者介面(UI)的「檔案→選項→儲存→		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					儲存文件」索引標籤上，選取「以此格式儲存檔案」下拉選單變更設定		
26	Word 2019 User Settings	TWGCB-04-009-0026	Word 選項\檔案封鎖設定	設定預設的檔案封鎖行為	▪ 這項原則設定決定使用者是否可以開啟、檢視或編輯已被封鎖的 Word 檔案 ▪ 如果啟用這項原則設定，則有 3 個控制選項可以選擇： (1)不開啟封鎖的檔案 (2)以受保護的檢視開啟封鎖的檔案且無法編輯 (3)以受保護的檢視開啟封鎖的檔案且可以編輯 ▪ 如果停用或未設定這項原則設定，則其行為等同於「不開啟封鎖的檔案」設定，使用者將無法開啟封鎖的檔案	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\檔案封鎖設定\設定預設的檔案封鎖行為	啟用，並選取「不開啟封鎖的檔案」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					▪使用者可以透過使用者介面(UI)的「檔案→選項→信任中心→信任中心設定→檔案封鎖設定→選定檔案類型的開啟行為」核取方塊進行設定		
27	Word 2019 User Settings	TWGCB-04-009-0027	Word 選項\受保護的檢視	不要在受保護的檢視中開啟來自網際網路區域的檔案	▪這項原則設定決定是否在受保護的檢視中開啟自網際網路區域下載的檔案 ▪如果啟用這項原則設定，將不會在受保護的檢視中開啟自網際網路區域下載的檔案 ▪如果停用或未設定這項原則設定，則會在受保護的檢視中開啟自網際網路區域下載的檔案 ▪使用者可以透過使用者介面(UI)勾選「檔案→選項→信任中心→信任中心設定→受保護的檢視→針對來自於網際網路	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\受保護的檢視\不要在受保護的檢視中開啟來自網際網路區域的檔案	停用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					的檔案啟用受保護的檢視」核取方塊進行設定		
28	Word 2019 User Settings	TWGCB-04-009-0028	Word 選項\受保護的檢視	不要在受保護的檢視中開啟位在不安全位置的檔案	▪這項原則設定決定是否在受保護的檢視中開啟不安全位置上的檔案。如果未指定不安全位置，則只將「Downloaded Program Files」及「Temporary Internet Files」資料夾視為不安全位置 ▪如果啟用這項原則設定，則不會在受保護的檢視中開啟不安全位置上的檔案 ▪如果停用或未設定這項原則設定，則會在受保護的檢視中開啟不安全位置上的檔案 ▪使用者可以透過使用者介面(UI)勾選「檔案→選項→信任中心→信任中心設定→受保護	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\受保護的檢視\不要在受保護的檢視中開啟位在不安全位置的檔案	停用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					的檢視→針對位於可能不安全位置的檔案啟用受保護的檢視」核取方塊進行設定		
29	Word 2019 User Settings	TWGCB-04-009-0029	Word 選項\受保護的檢視	以受保護的檢視開啟近端內部網路 UNC 上的檔案	▪ 這項原則設定決定是否在受保護的檢視中開啟近端內部網路 UNC 檔案共用中的檔案 ▪ 如果啟用這項原則設定，若近端內部網路 UNC 檔案共用中的檔案，其 UNC 路徑位於網際網路區域內，則會在受保護的檢視中開啟 ▪ 如果停用或未設定這項原則設定，若內部網路 UNC 檔案共用中的檔案，其 UNC 路徑位於網際網路區域內，則不會在受保護的檢視中開啟	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\受保護的檢視\以受保護的檢視開啟近端內部網路 UNC 上的檔案	啟用
30	Word	TWGCB	Word 選項\	針對從	▪ 這項原則設定決定是否在受保	使用者設定\系統	停用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	2019 User Settings	-04-009-0030	受保護的檢視	Outlook 開啟的附件關閉受保護的檢視	護的檢視中開啟 Outlook 附件中的 Word 檔案 ▪ 如果啟用這項原則設定，將不會在受保護的檢視中開啟 Outlook 附件 ▪ 如果停用或未設定這項原則設定，則會在受保護的檢視中開啟 Outlook 附件 ▪ 使用者可以透過使用者介面(UI)勾選「檔案→選項→信任中心→信任中心設定→受保護的檢視→針對 Outlook 附件啟用受保護的檢視」核取方塊進行設定	管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\受保護的檢視\針對從 Outlook 開啟的附件關閉受保護的檢視	
31	Word 2019 User Settings	TWGCB-04-009-0031	Word 選項\受保護的檢視	設定檔案驗證失敗時的文件	▪ 這項原則設定可控制 Office 在文件無法通過檔案驗證時處理文件的方式	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\	啟用，並設為「在受保護檢視中開啟」或「封鎖檔

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
				行為	▪如果啟用這項原則設定，即可針對無法通過驗證的檔案設定下列選項： (1)封鎖檔案：使用者無法開啟檔案 (2)在受保護檢視中開啟檔案並禁止編輯：使用者無法編輯檔案 (3)在受保護檢視中開啟檔案並允許編輯：使用者可以編輯檔案 ▪如果停用這項原則設定，Office將採用「在受保護檢視中開啟檔案並禁止編輯」行為 ▪如果未設定這項原則設定，Office 將採用「在受保護檢視中開啟檔案並允許編輯」行為	安全性\信任中心\受保護的檢視\設定檔案驗證失敗時的文件行為	案」，且不核取允許編輯

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
32	Word 2019 User Settings	TWGCB-04-009-0032	Word 選項\信任位置	允許網路上的信任位置	▪這項原則設定決定是否可使用網路上的信任位置 ▪如果啟用這項原則設定，使用者就可以在「信任中心」的「信任位置」區段中點選「新增位置」按鈕，以便在網路共用上指定信任位置，或在其未直接控制的其他遠端位置中指定信任位置。允許內容、程式碼和增益集以最低限度的安全性由信任位置載入，且不會提示使用者以取得同意 ▪如果停用這項原則設定，則選取的應用程式將忽略「信任中心」的「信任位置」區段所列出的任何網路位置 ▪如果同時經由群組原則部署信任位置，則應該確認其中是否	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\信任位置\允許網路上的信任位置	停用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值
					有任何遠端位置。如果有任何遠端位置，而且機關不允許經由此原則設定的遠端位置，則會在用戶端電腦上忽略那些指向遠端位置的原則機碼 ▪停用這項原則設定時，並不會從「信任位置」清單刪除任何網路位置，但將對那些將網路位置新增至「信任位置」清單的使用者造成運作中斷。使用者也將無法新增網路位置至「信任中心」的「信任位置」清單。正如同「允許我的網路上信任的位置(不建議使用)」核取方塊所述，並不建議啟用這項原則設定 ▪如果未啟用這項原則設定，使用者將可以視需要於使用者介		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					面(UI)勾選「檔案→選項→信任中心→信任中心設定→信任位置→允許我的網路上信任的位置(不建議使用)」核取方塊，並點選「新增位置」按鈕指定信任位置		
33	Word 2019 User Settings	TWGCB-04-009-0033	Word 選項\信任位置	停用所有信任位置	▪ 這項原則設定可讓管理員停用指定應用程式中所有的信任位置。信任中心所指定的信任位置是用來定義假設為安全的檔案位置。內容、程式碼和增益集可以在最低限度的安全性下從信任位置載入，而不要求使用者具備權限。如果從信任位置開啟危險的檔案，該檔案將不受標準安全性措施的規範，因而可能會損害使用者的電腦或資料	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\信任位置\停用所有信任位置	啟用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					▪如果啟用這項原則設定，則會略過指定應用程式中所有的信任位置(信任中心所指定的位置)，包括 Office 2019 在安裝期間所建立的任何信任位置、使用「群組原則」為使用者部署的信任位置，或是使用者自行新增的信任位置。當使用者從信任位置開啟檔案時，系統會再次提示使用者 ▪如果停用或未設定這項原則設定，則系統會假設指定應用程式中所有的信任位置(信任中心所指定的位置)都是安全的		
34	Word 2019 User Settings	TWGCB-04-009-0034	Word 選項\信任中心	停用未簽署應用程式增益集的信任列	▪這項原則設定決定當載入未簽署的應用程式增益集時，是否讓指定的 Office 應用程式通知使用者，還是無訊息停用此類	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\	啟用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
				通知，並封鎖它們	增益集而不通知。只有在啟用「應用程式增益集必須經過信任的發行者簽署」原則設定(以防止使用者變更此原則設定)的情況下，才能設定這項原則 ▪ 如果啟用這項原則設定，應用程式將自動停用未簽署的增益集，並且不會通知使用者 ▪ 如果停用這項原則設定，則當應用程式的設定要求所有增益集必須經過信任的發行者簽署時，將會停用應用程式載入的任何未簽署的增益集，且應用程式將在使用中視窗頂端顯示信任列。信任列包含一則訊息，通知使用者關於未簽署的增益集 ▪ 如果未設定這項原則設定，就	安全性\信任中心\停用未簽署應用程式增益集的信任列通知，並封鎖它們	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					會套用停用行為，另外使用者可在「信任中心」的「增益集」類別中，針對應用程式自行設定此需求 ▪ 使用者可以透過使用者介面(UI)勾選「檔案→選項→信任中心→信任中心設定→增益集→增益集(COM、VSTO 及其他)→停用所有應用程式增益集(可能會影響功能)」核取方塊進行設定		
35	Word 2019 User Settings	TWGCB-04-009-0035	Word 選項\信任中心	應用程式增益集必須經過信任的發行者簽署	▪ 這項原則設定決定此應用程式的增益集是否必須經由信任的發行者數位簽署 ▪ 如果啟用這項原則設定，則該應用程式在載入每個增益集前，會先檢查其數位簽章。如果增益集沒有數位簽章，或簽	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\應用程式增益集必須經過信任的	啟用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					章並非來自信任的發行者，則該應用程式會停用增益集並通知使用者。如果要求所有的增益集都必須經過信任的發行者簽署，即必須將這些憑證新增至「受信任的發行者」清單 ▪ Office 2019 將信任發行者的憑證儲存在 Internet Explorer 信任發行者存放區中。在舊版 Microsoft Office 中，信任發行者的憑證資訊(尤其是憑證指紋)是儲存在一個特別的 Office 信任發行者存放區。Office 2019 仍可從 Office 信任發行者存放區讀取信任的發行者憑證資訊，但不會將資訊寫入這個存放區。因此，如果使用者在舊版 Office 上建立了信任發行	發行者簽署	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					者清單，然後升級到 Office 2019，系統仍可辨識使用者的信任發行者清單。不過新增至清單的任何信任發行者憑證，都將儲存在 Internet Explorer 信任發行者存放區中 ▪ 如果停用或未設定這項原則設定，該應用程式就不會在開啟應用程式增益集前檢查其數位簽章。如果載入危險的增益集，就可能會危害使用者的電腦或資料安全性 ▪ 使用者可以透過使用者介面(UI)勾選「檔案→選項→信任中心→信任中心設定→增益集→增益集(COM、VSTO 及其他)→要求應用程式增益集由受信任的發行者簽署」核取方		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					塊進行設定		
36	Word 2019 User Settings	TWGCB-04-009-0036	Word 選項\信任中心	信任存取 Visual Basic 專案	▪這項原則設定決定自動化用戶端(例如 Microsoft Visual Studio 2005 Tools for Microsoft Office (VSTO))是否能夠使用指定的應用程式存取 Visual Basic for Applications 專案系統。即使 VSTO 專案不使用 Visual Basic for Applications，但專案仍需要存取 Excel、PowerPoint 及 Word 的 Visual Basic for Applications 專案系統。Visual Basic 及 C#專案的設計階段支援控制項皆依賴 Word 和 Excel 中的 Visual Basic for Applications 專案系統 ▪如果啟用這項原則設定，則	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\信任存取 Visual Basic 專案	停用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值
					VSTO 與其他自動化用戶端就可以在指定的應用程式中存取 Visual Basic for Applications 專案系統。使用者將無法透過使用者介面(UI)變更「信任存取 VBA 專案物件模型」設定 ▪ 如果停用這項原則設定，VSTO 將無法利用程式設計存取 VBA 專案。此外，會清除「信任存取 VBA 專案物件模型」核取方塊，且使用者無法進行變更。(注意：停用此原則設定會禁止 VSTO 專案與選取的應用程式中的 VBA 專案系統進行正常互動) ▪ 如果未設定這項原則設定，自動化用戶端就無法利用程式設計存取 VBA 專案。使用者可藉		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					由選取「信任存取 VBA 專案物件模型」來啟用此設定。然而，這樣做會允許使用者所開啟之任何文件中的巨集能夠存取核心 Visual Basic 物件、方法及屬性，這代表可能會有安全性方面的危險 ▪ 使用者可以透過使用者介面(UI)「檔案→選項→信任中心→信任中心設定→巨集設定→開發人員巨集設定→信任存取 VBA 專案物件模型」進行設定		
37	Word 2019 User Settings	TWGCB-04-009-0037	Word 選項\信任中心	VBA 巨集通知設定	▪ 這項原則設定決定指定的應用程式在 Visual Basic for Applications(VBA)巨集出現時警告使用者的方式 ▪ 如果啟用這項原則設定，有 4 個選項可以選擇，以決定指定	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\VBA 巨集通知	啟用，並設為「全部停用(事先通知)」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					的應用程式如何向使用者發出巨集相關警告： (1)全部停用(事先通知)：無論巨集是否經過簽署，應用程式都會針對所有巨集顯示信任列。此選項會強制套用 Office 中的預設設定 (2)除了經數位簽章的巨集外，停用所有巨集：應用程式會針對經過數位簽署的巨集顯示信任列，允許使用者啟用巨集或保持停用。任何未經簽署的巨集將一律停用，而且使用者不會收到通知 (3)全部停用(不事先通知)：無論巨集是否經過簽署，應用程式一律停用所有巨集，而	設定	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					且使用者不會收到通知 (4)啟用所有巨集(不建議使用)：巨集無論是否經過簽署，一律啟用。此選項可能會允許危險程式碼執行但又未偵測到，因而大幅降低安全性 ▪ 如果停用這項原則設定，其行為將等同於「全部停用(事先通知)」選項 ▪ 如果未設定這項原則設定，則使用者在指定的應用程式中開啟內含 VBA 巨集的檔案時，應用程式會開啟檔案並停用巨集，然後顯示信任列，警告使用者有巨集且已經停用。使用者可以視需要檢查和編輯檔案，但無法使用任何已停用的		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					功能，直到使用者點選信任列上的「啟用內容」啟用功能為止。如果使用者點選「啟用內容」，文件就會新增為信任的文件 ▪ 使用者可以透過使用者介面(UI)點選「檔案→選項→信任中心→信任中心設定→巨集設定→巨集設定」單選按鈕進行設定 ▪ 重要事項：如果選取「除了經數位簽章的巨集外，停用所有巨集」，使用者將無法開啟未簽署的 Access 資料庫 ▪ 請注意，Microsoft Office 會將受信任發行者的憑證儲存在 Internet Explorer 信任的發行者存放區。舊版 Microsoft Office		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					則是將受信任發行者的憑證資訊(尤其是憑證指紋)儲存在特別的 Office 信任的發行者存放區。Microsoft Office 仍可讀取 Office 信任的發行者存放區中的受信任發行者憑證資訊，但不會將資訊寫入此存放區。因此，如果使用者在舊版 Microsoft Office 中建立受信任發行者的清單，之後升級到新版 Office，系統仍可辨識該受信任發行者的清單。但是，使用者之後新增至該清單的任何受信任發行者憑證，都將儲存到 Internet Explorer 信任的發行者存放區		
38	Word 2019 User	TWGCB-04-009-	Word 選項\安全性	顯示隱藏標記	▪ 這項原則設定決定是否將機敏資訊保留在 Word 2019 的文件	使用者設定\系統管理範本	啟用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	Settings	0038			中 ▪ 如果啟用這項原則設定，會在開啟與儲存文件時顯示隱藏標記，讓使用者可以看到該標記，避免提供予非受信任之人員	\Microsoft Word 2019\Word 選項\安全性\顯示隱藏標記	
39	Word 2019 User Settings	TWGCB-04-009-0039	Word 選項\信任中心	掃描 Word Open XML 文件中的加密巨集	▪ 這項原則設定決定是否需要先使用防毒軟體掃描，再開啟 Open XML 文件中的加密巨集 ▪ 如果啟用這項原則設定，則可選擇的選項如下： (1)掃描加密巨集(預設)：除非已安裝防毒軟體，否則會停用加密巨集。當使用者嘗試開啟內含巨集的加密活頁簿時，防毒軟體就會掃描加密巨集	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\掃描 Word Open XML 文件中的加密巨集	啟用，並設為「掃描加密巨集(預設)」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					(2)若有防毒軟體便掃描：如果已安裝防毒軟體，則會先掃描加密的巨集才允許載入。如果沒有防毒軟體，則允許加密巨集載入 (3)不掃描即載入巨集：不檢查是否有防毒軟體，並且允許在加密檔案中載入巨集 ▪如果停用或未設定這項原則設定，則行為等同於「掃描加密巨集(預設)」選項		
40	Word 2019 User Settings	TWGCB-04-009-0040	Word 選項\信任中心	封鎖在 Office 檔案中執行來自網際網路的巨集	▪這項原則設定決定是否在 Office 檔案中封鎖執行來自網際網路的巨集 ▪如果啟用這項原則設定，則 Office 檔案封鎖執行來自網際網路的巨集。即使已透過使用者介面(UI)選取「檔案→選項	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\封鎖在 Office 檔案中執行來自網	啟用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					→信任中心→信任中心設定→巨集設定→啟用所有巨集(不建議使用;會執行有潛在危險的程式碼)」，仍將封鎖執行巨集，使用者會收到已封鎖執行巨集的通知，而無法點選信任列上的「啟用內容」按鈕啟用功能。此外，如果 Office 檔案已儲存至信任的位置，或是使用者先前已選擇信任，將允許執行巨集 ▪ 如果停用或未設定這項原則設定，則使用「信任中心」內「巨集設定」區段的設定決定是否在 Office 檔案中執行來自網際網路的巨集	際網路的巨集	
41	Word 2019 User	TWGCB-04-009-	Word 選項\信任中心	動態資料交換	▪ 這項原則設定決定是否允許 Word 應用程式使用動態資料	使用者設定\系統管理範本	停用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	Settings	0041			交換(Dynamic Data Exchange, DDE)功能 ▪如果啟用這項原則設定，則允許 Word 應用程式取得其他 Windows 應用程式中的資料，選項如下： (1)有限的動態資料交換：允許 Word 應用程式對執行中的應用程式進行 DDE 要求，但不允許可啟動程式的 DDE 要求 (2)允許動態資料交換：允許任何 DDE 要求 ▪如果停用或未設定這項原則設定，則不允許 DDE 功能	\Microsoft Word 2019\Word 選項\安全性\信任中心\動態資料交換	
42	Word 2019 User	TWGCB-04-009-	Word 選項\安全性	關閉檔案驗證	▪這項原則設定決定是否關閉檔案驗證功能	使用者設定\系統管理範本	停用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
	Settings	0042			▪如果啟用這項原則設定，將會關閉檔案驗證功能 ▪如果停用或未設定這項原則設定，將會開啟檔案驗證。開啟 Office 二進位文件(97-2003)之前，會先檢查這些文件是否符合檔案格式結構，再開啟這些文件	\Microsoft Word 2019\Word 選項\安全性\關閉檔案驗證	
43	Word 2019 User Settings	TWGCB-04-009-0043	Word 選項\安全性	檔案中若包含追蹤修訂或註解,則在列印、儲存或傳送之前警告	▪在文件中追蹤插入的修改或註解可能含有機敏資訊 ▪這項原則設定決定檔案中若包含追蹤修訂或註解，是否在列印、儲存或傳送之前警告使用者 ▪如果啟用這項原則設定，則使用者每次嘗試使用包含追蹤修訂或註釋的檔案時(如透過電子郵件發送檔案、列印檔案或	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\檔案中若包含追蹤修訂或註解，則在列印、儲存或傳送之前警告	啟用

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					儲存檔案)，都會看到警告		
44	Word 2019 User Settings	TWGCB-04-009-0044	Word 選項\檔案封鎖設定	Word 2 與舊版二進位文件和範本	▪這項原則設定決定使用者是否能以 Word 2 與舊版二進位格式，來開啟、檢視、編輯或儲存 Word 檔案 ▪如果啟用這項原則設定，則可以指定使用者是否可以開啟、檢視、編輯或儲存檔案。可選擇的選項如下： (1)不要封鎖：不封鎖此檔案類型 (2)封鎖開啟/儲存，使用開啟原則：將同時封鎖此檔案類型的開啟及儲存。檔案會根據在「預設的檔案封鎖行為」機碼所設定的原則設定而開啟	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\檔案封鎖設定\Word 2 與舊版二進位文件和範本	啟用，並設定檔案封鎖設定為「封鎖開啟/儲存，使用開啟原則」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					(3)封鎖：將同時封鎖此檔案類型的開啟及儲存，且檔案一律不會開啟 (4)在受保護的檢視中開啟：將同時封鎖此檔案類型的開啟及儲存，且不會啟用編輯此檔案類型的選項 (5)允許在受保護的檢視中編輯和開啟：將同時封鎖此檔案類型的開啟及儲存，但會啟用編輯的選項 ▪如果停用或未設定這項原則設定，則會封鎖 Word 2 與舊版二進位檔案類型		
45	Word 2019 User Settings	TWGCB-04-009-0045	Word 選項\檔案封鎖設定	Word 6.0 二進位文件和範本	▪這項原則設定決定使用者是否能以 Word 6.0 二進位格式，來開啟、檢視、編輯或儲存 Word	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\	啟用，並設定檔案封鎖設定為「封鎖開啟/儲存，使

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					檔案 ▪ 如果啟用這項原則設定，則可以指定使用者是否可以開啟、檢視、編輯或儲存檔案。可選擇的選項如下： (1)不要封鎖：不封鎖此檔案類型 (2)封鎖開啟/儲存，使用開啟原則：將同時封鎖此檔案類型的開啟及儲存。檔案會根據在「預設的檔案封鎖行為」機碼所設定的原則設定而開啟 (3)封鎖：將同時封鎖此檔案類型的開啟及儲存，且檔案一律不會開啟 (4)在受保護的檢視中開啟：將同時封鎖此檔案類型的開	安全性\信任中心\檔案封鎖設定\Word 6.0 二進位文件和範本	用開啟原則」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					啟及儲存，且不會啟用編輯此檔案類型的選項 (5)允許在受保護的檢視中編輯和開啟：將同時封鎖此檔案類型的開啟及儲存，但會啟用編輯的選項 ▪如果停用或未設定這項原則設定，則會封鎖 Word 6.0 二進位檔案類型		
46	Word 2019 User Settings	TWGCB-04-009-0046	Word 選項\檔案封鎖設定	Word 95 二進位文件和範本	▪這項原則設定決定使用者是否能以 Word 95 二進位格式，來開啟、檢視、編輯或儲存 Word 檔案 ▪如果啟用這項原則設定，則可以指定使用者是否可以開啟、檢視、編輯或儲存檔案。可選擇的選項如下：	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\檔案封鎖設定\Word 95 二進位文件和範本	啟用，並設定檔案封鎖設定為「封鎖開啟/儲存，使用開啟原則」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值
					(1)不要封鎖：不封鎖此檔案類型 (2)封鎖開啟/儲存,使用開啟原則：將同時封鎖此檔案類型的開啟及儲存。檔案會根據在「預設的檔案封鎖行為」機碼所設定的原則設定而開啟 (3)封鎖：將同時封鎖此檔案類型的開啟及儲存，且檔案一律不會開啟 (4)在受保護的檢視中開啟：將同時封鎖此檔案類型的開啟及儲存，且不會啟用編輯此檔案類型的選項 (5)允許在受保護的檢視中編輯和開啟：將同時封鎖此檔案類型的開啟及儲存，但會		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					啟用編輯的選項 ▪如果停用或未設定這項原則設定，則會封鎖 Word 95 二進位檔案類型		
47	Word 2019 User Settings	TWGCB-04-009-0047	Word 選項\檔案封鎖設定	Word 97 二進位文件和範本	▪這項原則設定決定使用者是否能以 Word 97 二進位格式，來開啟、檢視、編輯或儲存 Word 檔案 ▪如果啟用這項原則設定，則可以指定使用者是否可以開啟、檢視、編輯或儲存檔案。可選擇的選項如下： (1)不要封鎖：不封鎖此檔案類型 (2)封鎖開啟/儲存，使用開啟原則：將同時封鎖此檔案類型的開啟及儲存。檔案會根據	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\檔案封鎖設定\Word 97 二進位文件和範本	啟用，並設定檔案封鎖設定為「封鎖開啟/儲存，使用開啟原則」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值
					在「預設的檔案封鎖行為」機碼所設定的原則設定而開啟 (3)封鎖：將同時封鎖此檔案類型的開啟及儲存，且檔案一律不會開啟 (4)在受保護的檢視中開啟：將同時封鎖此檔案類型的開啟及儲存，且不會啟用編輯此檔案類型的選項 (5)允許在受保護的檢視中編輯和開啟：將同時封鎖此檔案類型的開啟及儲存，但會啟用編輯的選項 ▪如果停用或未設定這項原則設定，則不會封鎖 Word 97 二進位檔案類型		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
48	Word 2019 User Settings	TWGCB-04-009-0048	Word 選項\檔案封鎖設定	Word XP 二進位文件和範本	▪這項原則設定決定使用者是否能以 Word XP 二進位格式，來開啟、檢視、編輯或儲存 Word 檔案 ▪如果啟用這項原則設定，則可以指定使用者是否可以開啟、檢視、編輯或儲存檔案。可選擇的選項如下： (1)不要封鎖：不封鎖此檔案類型 (2)封鎖開啟/儲存，使用開啟原則：將同時封鎖此檔案類型的開啟及儲存。檔案會根據在「預設的檔案封鎖行為」機碼所設定的原則設定而開啟 (3)封鎖：將同時封鎖此檔案類型的開啟及儲存，且檔案一	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\檔案封鎖設定\Word XP 二進位文件和範本	啟用，並設定檔案封鎖設定為「封鎖開啟/儲存，使用開啟原則」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					律不會開啟 (4)在受保護的檢視中開啟：將同時封鎖此檔案類型的開啟及儲存，且不會啟用編輯此檔案類型的選項 (5)允許在受保護的檢視中編輯和開啟：將同時封鎖此檔案類型的開啟及儲存，但會啟用編輯的選項 ▪如果停用或未設定這項原則設定，則不會封鎖 Word XP 二進位檔案類型		
49	Word 2019 User Settings	TWGCB-04-009-0049	Word 選項\檔案封鎖設定	Word 2000 二進位文件和範本	▪這項原則設定決定使用者是否能以 Word 2000 二進位格式，來開啟、檢視、編輯或儲存 Word 檔案 ▪如果啟用這項原則設定，則可	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\檔案封鎖設定	啟用，並設定檔案封鎖設定為「封鎖開啟/儲存，使用開啟原則」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值
					以指定使用者是否可以開啟、檢視、編輯或儲存檔案。可選擇的選項如下： (1)不要封鎖：不封鎖此檔案類型 (2)封鎖開啟/儲存，使用開啟原則：將同時封鎖此檔案類型的開啟及儲存。檔案會根據在「預設的檔案封鎖行為」機碼所設定的原則設定而開啟 (3)封鎖：將同時封鎖此檔案類型的開啟及儲存，且檔案一律不會開啟 (4)在受保護的檢視中開啟：將同時封鎖此檔案類型的開啟及儲存，且不會啟用編輯此檔案類型的選項	\Word 2000 二進位文件和範本	

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值
					(5)允許在受保護的檢視中編輯和開啟：將同時封鎖此檔案類型的開啟及儲存，但會啟用編輯的選項 ▪如果停用或未設定這項原則設定，則不會封鎖 Word 2000 二進位檔案類型		
50	Word 2019 User Settings	TWGCB-04-009-0050	Word 選項\檔案封鎖設定	Word 2003 二進位文件和範本	▪這項原則設定決定使用者是否能以 Word 2003 二進位格式，來開啟、檢視、編輯或儲存 Word 檔案 ▪如果啟用這項原則設定，則可以指定使用者是否可以開啟、檢視、編輯或儲存檔案。可選擇的選項如下： (1)不要封鎖：不封鎖此檔案類型	使用者設定\系統管理範本\Microsoft Word 2019\Word 選項\安全性\信任中心\檔案封鎖設定\Word 2003 二進位文件和範本	啟用，並設定檔案封鎖設定為「封鎖開啟/儲存，使用開啟原則」

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值
					(2)封鎖開啟/儲存,使用開啟原則：將同時封鎖此檔案類型的開啟及儲存。檔案會根據在「預設的檔案封鎖行為」機碼所設定的原則設定而開啟 (3)封鎖：將同時封鎖此檔案類型的開啟及儲存，且檔案一律不會開啟 (4)在受保護的檢視中開啟：將同時封鎖此檔案類型的開啟及儲存，且不會啟用編輯此檔案類型的選項 (5)允許在受保護的檢視中編輯和開啟：將同時封鎖此檔案類型的開啟及儲存，但會啟用編輯的選項 ▪如果停用或未設定這項原則設		

項次	GPO	TWGCB-ID	類別	原則設定名稱	說明	GPO設定路徑	GCB設定值
					定，則不會封鎖 Word 2003 二進位檔案類型		

資料來源：本中心整理

3. 參考文獻

[1]Microsoft Corporation, Microsoft 365 Apps for Enterprise 2104 FINAL Security Baseline.

https://www.microsoft.com/en-us/download/details.aspx?id=55319

[2]Defense Information Systems Agency (DISA), Microsoft Office 365 ProPlus STIG Version: 2 Release: 3.

https://public.cyber.mil/stigs/downloads/