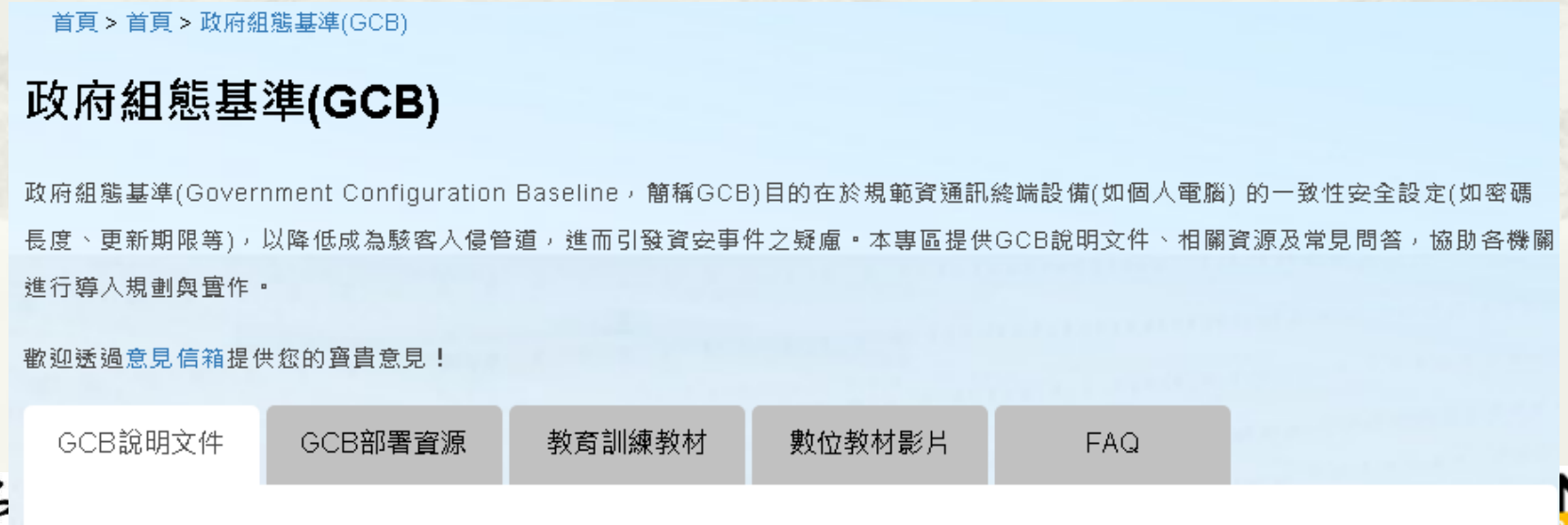
教育體系資安檢核

臺灣大學計資中心網路組
游子興
davisyou@ntu.edu.tw
02-33665008

組態設定安全檢核

政府組態基準 GCB (Government Configuration Baseline)

* 目的: 規範資通訊終端設備(如個人電腦) 的一致性安全設定(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疑慮。
* https://www.nccst.nat.gov.tw/GCB



GCB 說明文件

* 作業系統
  * Windows 7、Windows 8.1、Windows 10、Windows Server 2008 R2、Windows Server 2012 R2、Windows Server 2016、RedHat Enterprise Linux 5
* 瀏覽器
  * Internet Explorer 8、Internet Explorer 11、Google Chrome、Mozilla Firefox、Microsoft Edge
* 網通設備
  * 無線網路、Juniper Firewall、Fortinet Fortigate、Cisco Firewall
* 應用程式
  * Exchange Server 2013、Microsoft IIS 8.5

Group Policy

- Group Policy provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment.
- A set of Group Policy configurations is called a Group Policy Object (GPO).
- A version of Group Policy called Local Group Policy (LGPO or LocalGPO) allows Group Policy Object management without Active Directory on standalone computers
  - Ref. https://en.wikipedia.org/wiki/Group_Policy

Group Policy 群組原則設定

- Group Policy Objects are processed in the following order (from top to bottom)
  - Local - Any settings in the computer's local policy. Prior to Windows Vista, there was only one local group policy stored per computer. Windows Vista and later Windows versions allow individual group policies per user accounts.
  - Site - Any Group Policies associated with the Active Directory site in which the computer resides. (An Active Directory site is a logical grouping of computers, intended to facilitate management of those computers based on their physical proximity.) If multiple policies are linked to a site, they are processed in the order set by the administrator.

Group Policy 群組原則設定

* Domain - Any Group Policies associated with the Windows domain in which the computer resides. If multiple policies are linked to a domain, they are processed in the order set by the administrator.
* Organizational Unit - Group policies assigned to the Active Directory organizational unit (OU) in which the computer or user are placed. (OUs are logical units that help organizing and managing a group of users, computers or other Active Directory objects.) If multiple policies are linked to an OU, they are processed in the order set by the administrator.

GCB 作業系統

Windows 10

GCB 作業系統
Windows 10

* 政府組態基準GCB_Microsoft Windows 10 說明文件(V1.2).docx

表1　Windows 10 組態基準項目統計

項次	項目	項數	合計
1	Windows10 Account Settings	9	345
2	Windows10 Computer Settings	291	
3	Windows10 User Settings	12	
4	Windows10 Firewall Settings	33	

GCB 作業系統
Windows 10

* Windows10 Account Settings

2	Windows 10 Account Settings	TWGCB-01-005-0002	帳戶原則\密碼原則	密碼最長使用期限	▪ 此項原則設定決定系統要求使用者變更密碼之前，密碼可以使用的期限(天數)。使用者可以設定密碼在 1 至 999 天之後到期；或將天數設為 0，表示密碼永遠不會到期。如果「密碼最長使用期限」介於 1 到 999 天之間，則「密碼最短使用期限」不得超過「密碼最長使用期限」的天數。如果「密碼最長使用期限」設定為 0，則「密碼最短使用期限」可以是介於 0 到 998 天之間的任何數值 ▪ 注意：根據使用者的環境而定，安全性的最佳作法是讓密碼每 30 至 90 天到期。如此一來，攻擊者破解使用者密碼及存取使用者的網路資源的時間便很有限	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\密碼最長使用期限	90 天以下	CCE-ID：CCE-43535-4

GCB 作業系統 Windows 10

3	Windows 10 Account Settings	TWGCB-01-005-0003	帳戶原則\密碼原則	最小密碼長度	▪此項原則設定決定使用者帳戶的密碼可包含的最少字元數。可以設定介於 1 到 14 個字元之間的值 ▪將字元數設為 0，則表示不需要密碼	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\最小密碼長度	8 個字元以上	CCE-ID：CCE-41679-2
4	Windows 10 Account Settings	TWGCB-01-005-0004	帳戶原則\密碼原則	密碼必須符合複雜性需求	▪此項原則設定決定密碼是否必須符合複雜性需求 ▪如果啟用了此原則，則密碼必須符合下列最小需求： -不包含使用者的帳戶名稱全名中，超過兩個以上的連續字元 -長度至少為 6 個字元 -包含下列四種字元中的三種： (1)英文大寫字元(A 到 Z) (2)英文小寫字元(a 到 z) (3)10 進位數字(0 到 9) (4)非英文字母字元(例如：!、$、	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\密碼必須符合複雜性需求	啟用	CCE-ID：CCE-42872-2

GCB 作業系統
Windows 10

5	Windows 10 Account Settings	TWGCB-01-005-0005	帳戶原則\密碼原則	強制執行密碼歷程記錄	▪ 此項原則設定決定重複使用舊密碼前，必須與使用者帳戶相關的唯一新密碼數目。此值必須介於 0 與 24 個密碼之間 ▪ 此項原則可讓系統管理員藉由確定不再繼續重複使用舊密碼，以增加安全性	電腦設定\Windows 設定\安全性設定\帳戶原則\密碼原則\強制執行密碼歷程記錄	3 以上記憶的密碼	CCE-ID：CCE-42136-2

GCB 作業系統 Windows 10

* Windows10 Computer Settings

112	Windows 10 Computer Settings	TWGCB-01-005-0112	安全性選項\互動式登入	互動式登入：電腦未使用時間限制	Windows 會監控登入工作階段的未使用時間，而且會在未使用時間超過未使用時間限制時執行螢幕保護裝置並鎖定該工作階段	電腦設定\Windows 設定\安全性設定\本機原則\安全性選項\互動式登入：電腦未使用時間限制	900 秒	CCE-ID：CCE-43844-0

GCB 作業系統 Windows 10

* Windows10 User Settings

項次	GPO	TWG CB-ID	類別	原則設定名稱	說明	GPO 設定路徑	GCB 設定值	備註
306	Windows 10 User Settings	TWG CB-01-005-0306	個人化	啟用螢幕保護裝置	▪此項原則設定決定是否啟用桌面螢幕保護裝置 ▪如果啟用此項原則設定，只要下列兩項條件成立，螢幕保護裝置就會執行： (1)已透過「螢幕保護裝置執行檔名稱」設定或用戶端電腦上的「控制台」，在用戶端上指定有效的螢幕保護裝置 (2)已透過設定或「控制台」將螢幕保護裝置逾時設定為非零的值 ▪如果停用此項原則設定，螢幕保護裝置不會執行。此外，此項設定會停用「個人化」或「顯示」控制台中的「螢幕保護裝置」對	使用者設定\系統管理範本\控制台\個人化\啟用螢幕保護裝置	啟用	CCE-ID：CCE-42836-7

GCB 作業系統 Windows 10

					段。因此，使用者無法變更螢幕保護裝置選項 ▪ 如果未設定此項原則設定，此項設定對系統沒有作用			
307	Windows 10 User Settings	TWGCB-01-005-0307	個人化	以密碼保護螢幕保護裝置	▪ 此項原則設定決定是否要以密碼保護電腦上使用的螢幕保護裝置 ▪ 如果啟用此項原則設定，所有螢幕保護裝置都會受到密碼保護 ▪ 如果停用此項原則設定，則無法在任何螢幕保護裝置上設定密碼保護。此設定也會停用「個人化」或「顯示」控制台的「螢幕保護裝置」對話方塊中的「受密碼保護」核取方塊，以防止使用者變更密碼保護設定	使用者設定\系統管理範本\控制台\個人化\以密碼保護螢幕保護裝置	啟用	CCE-ID：CCE-43863-0

GCB 作業系統
Windows 10

					者可以選擇是否要在每個螢幕保護裝置上設定密碼保護 ▪ 若要確保電腦受到密碼保護，必須啟用「啟用螢幕保護裝置」設定，並透過「螢幕保護裝置逾時」設定指定逾時 ▪ 注意：若要移除「螢幕保護裝置」對話方塊，請使用「防止變更螢幕保護裝置」設定			
308	Windows 10 User Settings	TWGCB-01-005-0308	個人化	螢幕保護裝置逾時	▪ 此項原則設定決定螢幕保護裝置必須在使用者閒置時間經過多久之後才啟動 ▪ 如果已設定，這個閒置時間可以設定在最少 1 秒到最多 86,400 秒(或 24 小時)之間。如果設為零，螢幕保護裝置將不會啟動 ▪ 在下列任一狀況下，此項設定沒	使用者設定\系統管理範本\控制台\個人化\螢幕保護裝置逾時	啟用，900 秒	CCE-ID：CCE-43159-3

GCB 作業系統
Windows 10

					有作用： (1)設定已停用或未設定 (2)等候時間設為零 (3)「啟用螢幕保護裝置」設定已停用 (4)「螢幕保護裝置執行檔名稱」設定和用戶端電腦的「個人化」或「顯示」控制台中的「螢幕保護裝置」對話方塊都沒有在用戶端上指定有效的現有螢幕保護裝置程式 ▪ 如果未設定，則會使用透過「個人化」或「顯示」控制台中的「螢幕保護裝置」對話方塊在用戶端上設定的等候時間。預設值是 15 分鐘			

GCB 導入方法

群組原則匯入程式

作業系統GPO檔 下載

* https://www.nccst.nat.gov.tw/GCBDownloadDetail?lang=zh&seq=1079

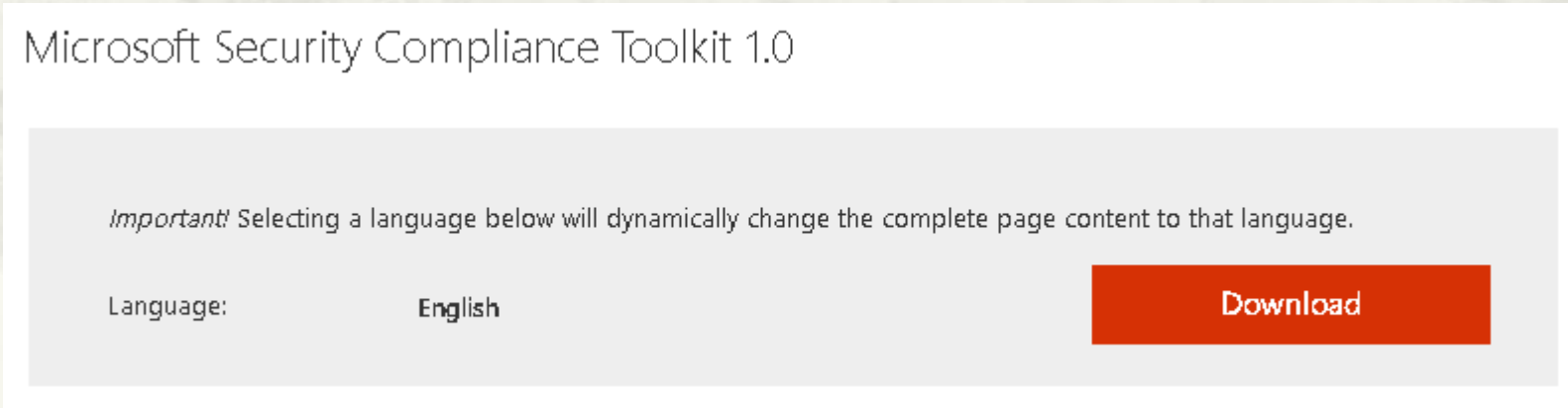
> 首頁 > 政府組態基準(GCB)

GCB下載

主題	作業系統GPO
內容	1. GCB-Windows7-gpos.zip 2018/3/26 2. GCB-Windows8.1-gpos.zip 2018/1/29 3. GCB-Windows10-gpos.zip 2019/12/24 4. GCB-WindowsServer2008R2SP1-gpos.zip 2018/1/29 5. GCB-WindowsServer2012R2-gpos.zip 2019/12/24 6. GCB-WindowsServer2016-gpos.zip 2019/9/27

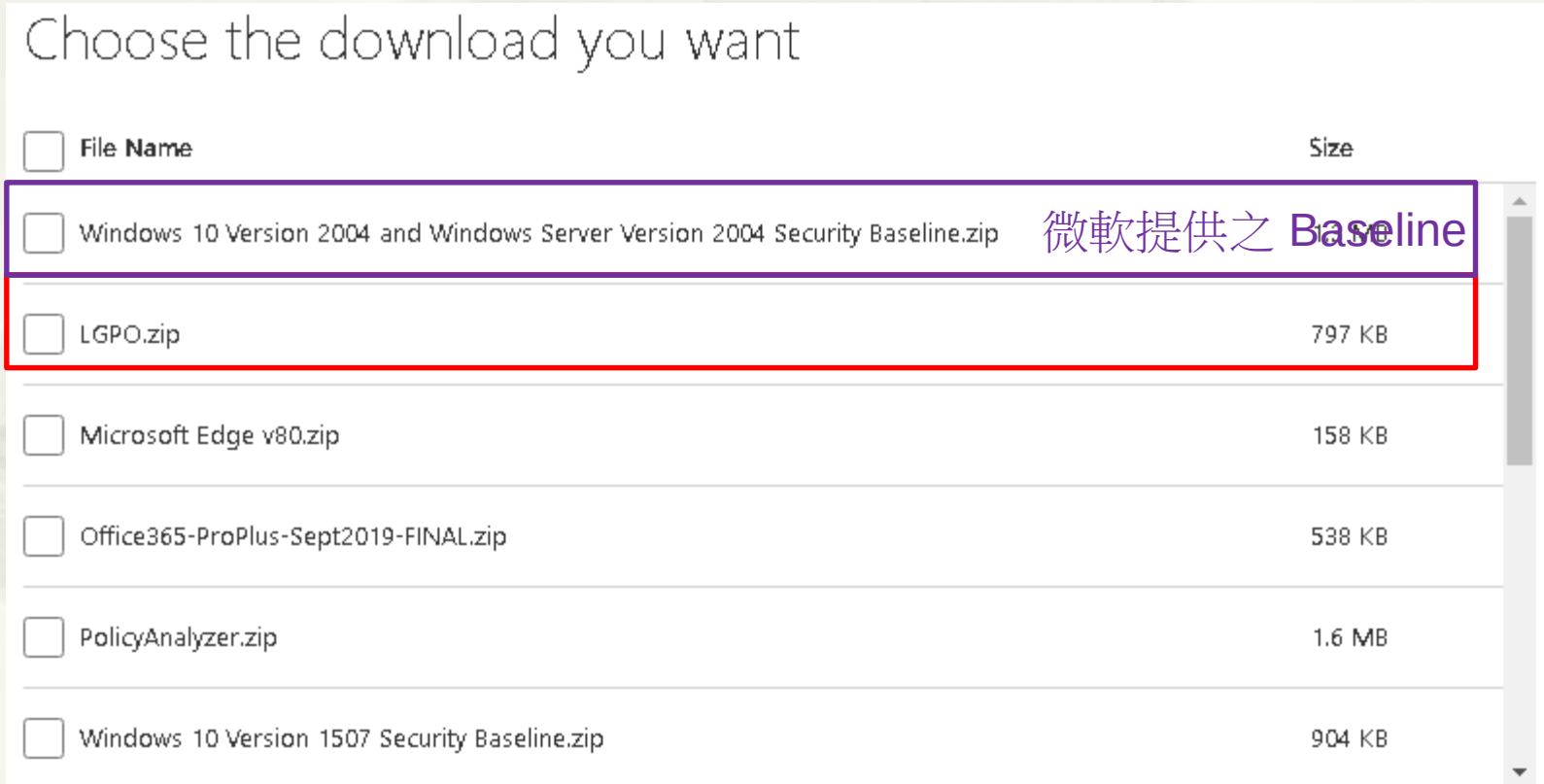
群組原則匯入程式

* LGPO v2.2
* Microsoft Security Compliance Toolkit 1.0
* https://www.microsoft.com/en-us/download/details.aspx?id=55319



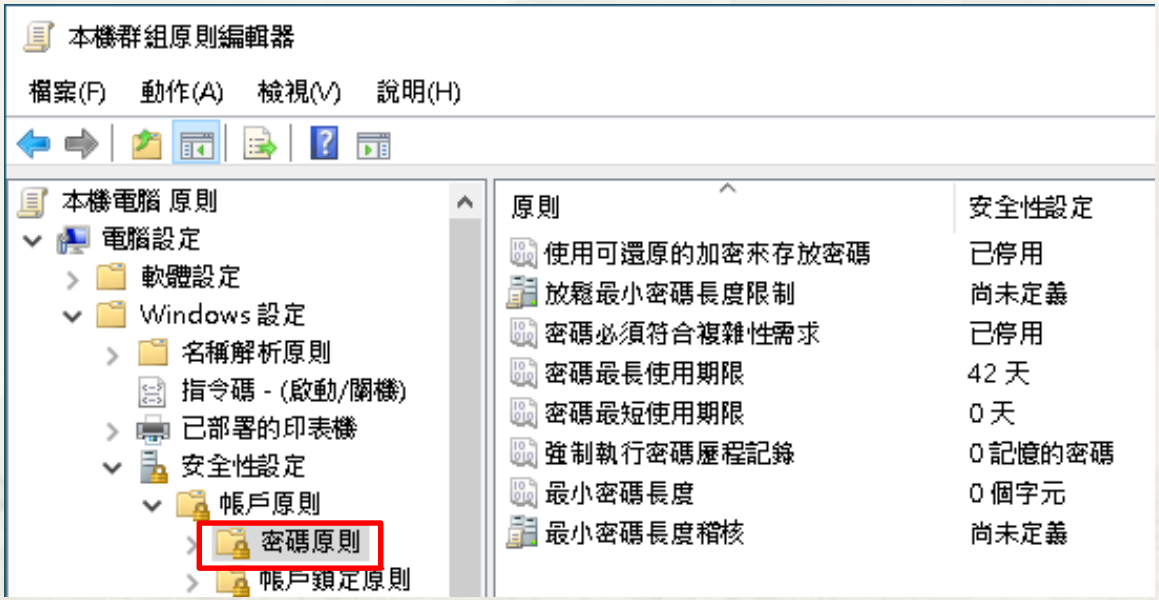
群組原則匯入程式

* 下載


Choose the download you want
File Name
Size
Windows 10 Version 2004 and Windows Server Version 2004 Security Baseline.zip
1.4 MB
微軟提供之 Baseline
LGPO.zip
797 KB
Microsoft Edge v80.zip
158 KB
Office365-ProPlus-Sept2019-FINAL.zip
538 KB
PolicyAnalyzer.zip
1.6 MB
Windows 10 Version 1507 Security Baseline.zip
904 KB

顯示群組原則設定-單機 (Win 10 初始預設值)

* gpedit.msc

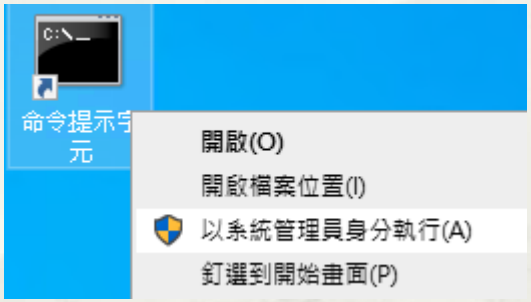


變更密碼測試
(Win 10 初始預設值)

* 允許密碼長度: 四個字元

群組原則匯入程式

* 開啟命令提示字元(系統管理者身份)



* 備份目前組態
  * LGPO /b C:\GCB\backup

```
C:\GCB>LGPO /b C:\GCB\20200827
LGPO.exe v2.2 - Local Group Policy Object utility

Creating LGPO backup in "C:\GCB\20200827\{D1CE1C9E-2FFC-42E0-B2F8-87B5C17FC0EB}"
```

備份目前組態

- C:\GCB\backup\{EF1BEBB1-034D-4281-A07A-CBFDED7918AC}\DomainSysvol\GPO\
  - \Machine\registry.pol – 無內容
  - \User\ registry.pol – 無內容

- C:\GCB\backup \{EF1BEBB1-034D-4281-A07A-CBFDED7918AC}\DomainSysvol\GPO\Machine\microsoft \windows nt\
  - \Audit\audit.csv
  - \SecEdit\GptTmpl.inf

匯入 GCB 組態設定檔

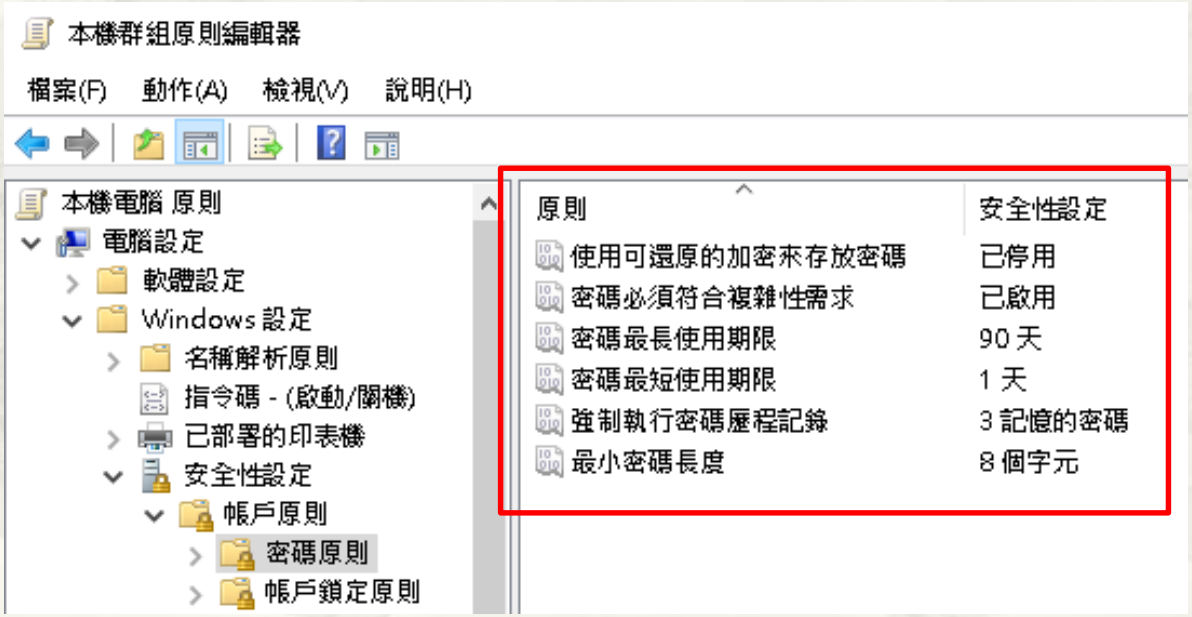
- 全部導入
  - LGPO /g .\GCB-Windows10-gpos
- 部分導入， Only AccountSettings
  - LGPO /g .\GCB-Windows10-gpos\Windows10AccountSettings
- 重開機 或 gpupdate /force

```
C:\LGPO>LGPO /g C:\GCB-Windows10-gpos
LGPO.exe v2.2 - Local Group Policy Object utility

Apply security template: C:\GCB-Windows10-gpos\Windows10AccountSettings\{BB605EAD-FFC0-4763-AD67-F9B2125C54DA}\DomainSysvol\GPO\Ma
chine\microsoft\windows nt\SecEdit\GptTmpl.inf
Created directory for audit policy
Copied C:\GCB-Windows10-gpos\Windows10ComputerSettings\Windows10AuditSettings\{06BE0013-44C8-445E-BDBB-7876F3AA1BC7}\DomainSysvol\
GPO\Machine\microsoft\windows nt\Audit\audit.csv
to C:\Windows\system32\GroupPolicy\Machine\Microsoft\Windows NT\Audit\audit.csv
Clearing existing audit policy
Apply Audit policy from C:\GCB-Windows10-gpos\Windows10ComputerSettings\Windows10AuditSettings\{06BE0013-44C8-445E-BDBB-7876F3AA1B
C7}\DomainSysvol\GPO\Machine\microsoft\windows nt\Audit\audit.csv
Apply security template: C:\GCB-Windows10-gpos\Windows10ComputerSettings\Windows10AuditSettings\{06BE0013-44C8-445E-BDBB-7876F3AA1
BC7}\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf
Apply security template: C:\GCB-Windows10-gpos\Windows10ComputerSettings\Windows10ComputerSettings(Other)\{E12EA9E0-D8AB-4EB8-818A
-E521D26A470F}\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf
Import Machine settings from registry.pol: C:\GCB-Windows10-gpos\Windows10ComputerSettings\Windows10ComputerSettings(Other)\{E12EA
9E0-D8AB-4EB8-818A-E521D26A470F}\DomainSysvol\GPO\Machine\registry.pol
Apply security template: C:\GCB-Windows10-gpos\Windows10FirewallSettings\{370D17DB-6E02-46A0-816F-9BF347BB6713}\DomainSysvol\GPO\M
achine\Microsoft\Windows NT\SecEdit\GptTmpl.inf
Import Machine settings from registry.pol: C:\GCB-Windows10-gpos\Windows10FirewallSettings\{370D17DB-6E02-46A0-816F-9BF347BB6713}\
DomainSysvol\GPO\Machine\registry.pol
Import User settings from registry.pol: C:\GCB-Windows10-gpos\Windows10UserSettings\{591F3C24-5250-4F47-A19F-55B3C78E147D}\DomainS
ysvol\GPO\User\registry.pol
```

顯示群組原則設定-單機 (導入 GCB 設定檔)

* gpedit.msc
  * 需關閉再重新開啟才會更新



變更密碼測試
(已導入 GCB 設定檔)

* 不允許密碼長度: 四個字元

完整導入 GCB
可能遭遇問題

* 政府組態基準(GCB)-FAQ-作業系統專區
  * https://www.nccst.nat.gov.tw/GCBOS

4.如何解決Windows市集App(如:相片、計算機)無法使用的問題？

政府組態基準(GCB)之設定值原則上不宜隨意更動，但如因公務執行需求，必須調整TWGCB-01-005-0285與TWGCB-01-005-0284設定值，方法如下：

將「"電腦設定"=>"系統管理範本"=>"Windows元件"=>"Windows市集"=>"安全性選項"=>"停用Windows市集中的所有應用程式"」設為啟用，以及將「"電腦設定"=>"系統管理範本"=>"Windows元件"=>"市集"=>"關閉市集應用程式"」設為停用即可。

5.如何解決Miracast投影功能無法使用的問題？

政府組態基準(GCB)之設定值原則上不宜隨意更動，但如因公務執行需求，必須調整TWGCB-01-005-0285與TWGCB-01-005-00284設定值，方法如下：

將「"電腦設定"=>"系統管理範本"=>"Windows元件"=>"Windows市集"=>"安全性選項"=>"停用Windows市集中的所有應用程式"」設為啟用，以及將「"電腦設定"=>"系統管理範本"=>"Windows元件"=>"市集"=>"關閉市集應用程式"」設為停用即可。

完整導入 GCB
可能遭遇問題

- 11.套用政府組態基準(GCB)後，本機防火牆規則不會生效，怎麼辦呢？
- 12.微軟持續發布新版Microsoft Windows 10管理範本，是否需進行更新，以更精準的管控Windows 10作業系統呢？
- 13.套用政府組態基準(GCB)後，連線WiFi時顯示無網際網路，怎麼辦呢？
- 14.套用政府組態基準(GCB)後，購買的字型無法使用，怎麼辦呢？

* 不允許遠端桌面連線

GCB 導入方法(部分)

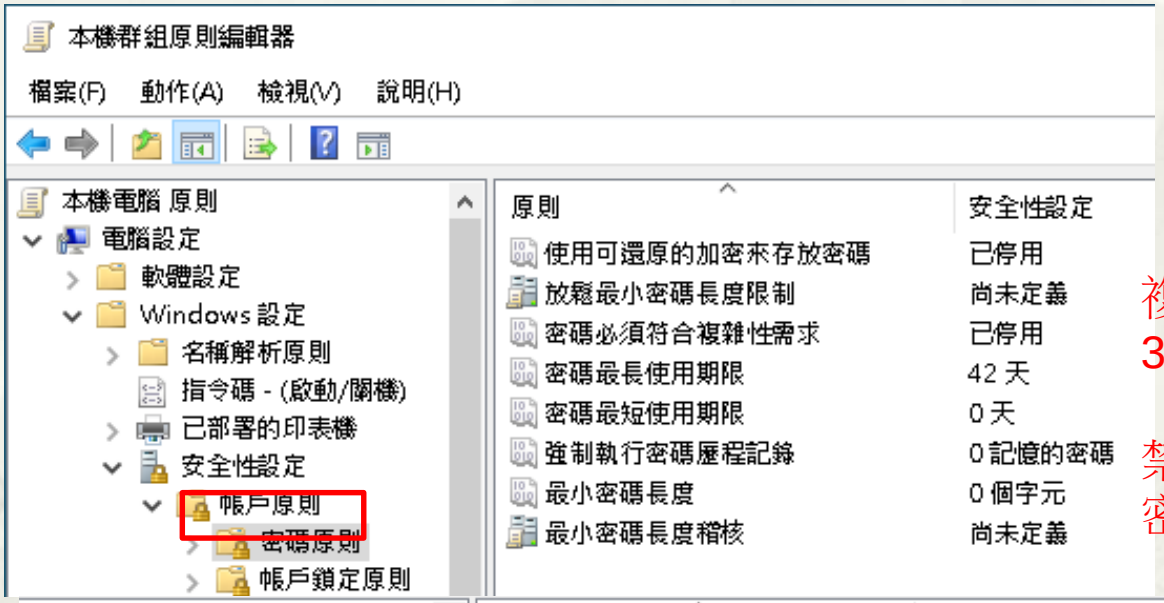
手動設定

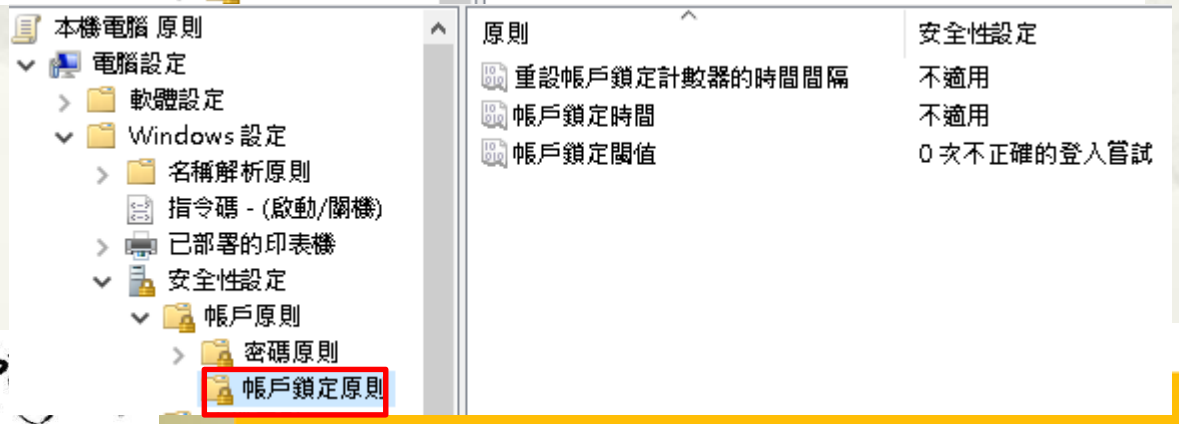
計資中心ISO27001資訊安全準則
個人電腦及密碼設置規定

* 電腦應設定螢幕保護程式及密碼保護，並將螢幕保護程式啟動時間設定為15分鐘。
* 電腦應安裝防毒軟體並即時更新病毒碼。
* 應保護通行密碼，維持通行密碼的機密性；一般電腦6個月內變更一次密碼，重要主機密碼3個月內變更一次密碼，並禁止重複使用相同的密碼。
* 通行密碼的長度最少應有8位長度，且應符合中心密碼設置原則。

帳戶原則

* gpedit.msc

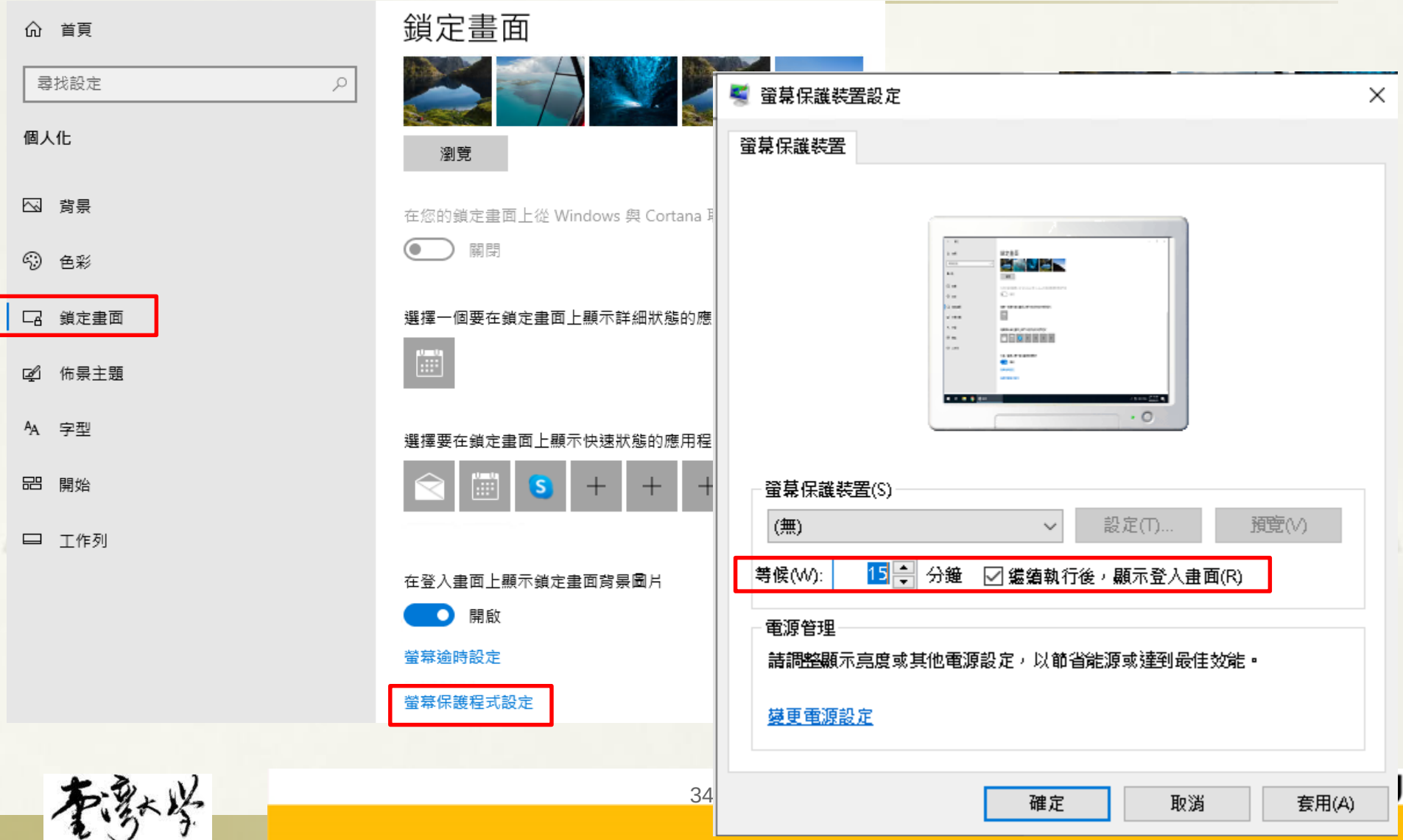




複雜密碼設置原則
3個月內變更一次密碼

禁止重複使用相同的密碼
密碼的長度最少應有8位長度

螢幕保護程式及密碼保護設定



GCB 導入方法(部分)

群組原則匯入程式

帳戶原則

* LGPO /g .\GCB-Windows10-gpos\Windows10AccountSettings

```
C:\GCB>LGPO /g .\GCB-Windows10-gpos\Windows10AccountSettings
LGPO.exe v2.2 - Local Group Policy Object utility

Apply security template: .\GCB-Windows10-gpos\Windows10AccountSettings\{BB605EAD-FFC0-4763-AD67-F9B2125C54DA}
\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\GptTmpl.inf
```

GCB 導入方法(部分)

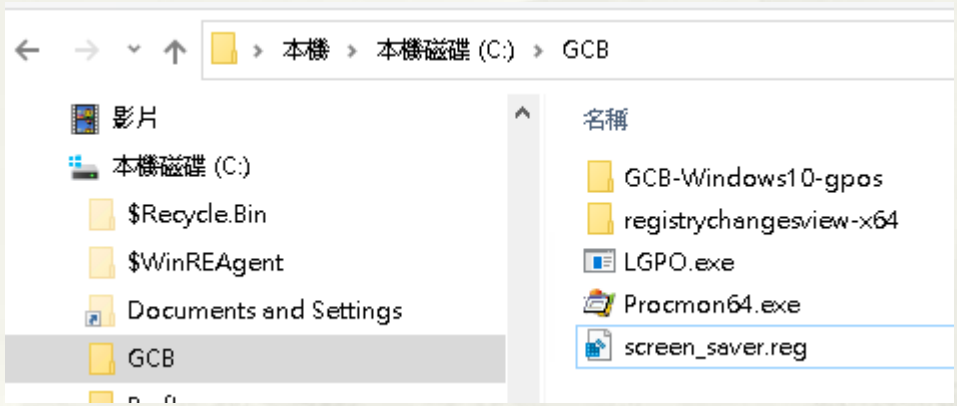
- GptTmpl.inf

```
[Unicode]
Unicode=yes
[System Access]
MinimumPasswordAge = 1
MaximumPasswordAge = 90
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 3
LockoutBadCount = 5
ResetLockoutCount = 15
LockoutDuration = 15
ClearTextPassword = 0
[Version]
signature="$CHICAGO$"
Revision=1
[Registry Values]
```

3個月內變更一次密碼
密碼的長度最少應有8位長度
複雜密碼設置原則
禁止重複使用相同的密碼

螢幕保護程式及密碼保護設定

* screen_saver.reg



簡報完畢
謝謝