

# 營業秘密管理指針

資策會科技法律研究所

2016年5月27日公開徵詢版

歡迎各界先進提供寶貴建議，請以電子郵件寄至本所創智中心  
林研究員 [franklin@iii.org.tw](mailto:franklin@iii.org.tw) 信箱。非常感謝 您的參與。

## 目錄

壹、管理架構階層圖 .....	5
貳、指針前言 .....	6
參、政策管理 .....	7
一、總則 .....	7
(一) 管理對象 .....	7
(二) 管理範圍 .....	7
(三) 管理規定 .....	7
(四) 法規遵循 .....	7
二、最高管理階層及與管理組織運作 .....	7
(一) 最高管理階層角色和態度 .....	7
(二) 統籌負責人職務 .....	8
(三) 管理組織 .....	8
(四) 稽核 .....	8
(五) 廣宣管制 .....	8
三、教育訓練 .....	9
(一) 定期周知 .....	9
(二) 非定期周知 .....	9
四、救濟 .....	9
(一) 救濟措施 .....	9
(二) 懲戒 .....	9
肆、內容管理 .....	9
一、營業秘密的處理程序 .....	9
(一) 產出 .....	9
(二) 外部取得 .....	10
(三) 管理清單 .....	10

(四) 分級/秘等.....	10
(五) 標示.....	10
二、區分管理和權限控管.....	10
(一) 營業秘密取得來源.....	10
(二) 營業秘密標的型態.....	11
三、營業秘密的使用及銷毀程序.....	12
(一) 借閱.....	12
(二) 攜出.....	13
(三) 複製、掃描等.....	13
(四) 傳遞或流通.....	14
(五) 銷毀.....	14
(六) 使用留存和預警.....	14
四、關係企業或第三方管理.....	15
(一) 共有.....	15
(二) 提供.....	15
(三) 使用控管.....	16
(四) 返還或銷毀.....	16
伍、人員管理.....	16
一、保密約定.....	16
二、從業人員.....	16
三、離職者.....	17
(一) 對離職者的告知.....	17
(二) 離職者監控與相應措施.....	17
四、關係企業或第三方及其從業人員.....	17
陸、環境及設備相關管理.....	17
一、管制區域及出入管制.....	17
二、監視.....	18

三、攜出入管制.....	18
四、網路及資訊設備的管制.....	18
(一) 網路保安.....	18
(二) 密碼.....	19

## 壹、管理架構階層圖

政策管理												
總則				最高管理階層及管理組織運作					教育訓練		救濟	
管理對象	管理範圍	管理規定	法規遵循	最高管理階層角色和態度	統籌負責人職務	管理組織	稽核	廣宣管制	定期周知	非定期周知	救濟措施	懲戒

內容管理																			
營業秘密的處理程序					區分管理和權限控管				營業秘密的使用及銷毀程序					關係企業或第三方管理					
產出			外部取得	管理清單	分級、秘等	標示	營業秘密取得來源	營業秘密標的型態	借閱	攜出		複製、掃描等	傳遞或流通	銷毀	使用留存和預警	共有	提供	使用控管	返還或銷毀
產出規範	產出申報	產出報酬					自 有	他 人	共 有	紙 本	電 子	物 品	紙本、 物品	紀錄媒體、 資訊設備		備 份	使用 紀錄	預 警	

人員管理					環境及設備相關管理				
保密約定	從業人員	離職者		關係企業或第三方及其從業人員	管制區域及出入管制	監視	攜出入管制	網路及資訊設備的管制	
		告知	監控與 相應措施					網路 保安	密碼

## 貳、指針前言

本指針是針對企業營業秘密保護的管理重點要項進行說明，以提供企業管理營業秘密時的參考。欲進行營業秘密管理的企業可依據本指針四大面向「政策」、「內容」、「人員」、「環境及設備相關」的管理重點，參考建立營業秘密管理措施或機制。

在此，將本指針中所使用的用語定義如下：

1. 「營業秘密」，指符合我國營業秘密法第 2 條規定者。
2. 「營業秘密統籌負責人」，指統籌規劃、決策、推動營業秘密保護管理者，屬企業中營業秘密最高權限管理者，於企業中具獨立地位。
3. 「營業秘密管理執行人」，指由在營業秘密統籌負責人授權指定就特定範圍(例：樓層、部門、專案等)執行營業秘密管理者。
4. 「管制區域」，指在企業或其辦事處、分公司中，存放有企業營業秘密而受管制的資料室、實驗室、樓層等空間。
5. 「營業秘密管理清單」，指對企業自有、與第三方共有或從外部取得的營業秘密進行盤點、並記錄所製成的表單。
6. 「借閱紀錄表」，指記錄企業內部借調、閱覽營業秘密相關歷程紀錄的表單。
7. 「流通紀錄表」，指記錄營業秘密對外提供、攜出企業外相關歷程紀錄的表單。
8. 「紀錄媒體」，指將資訊以數位或類比方式儲存的媒體，如硬碟、隨身碟、記憶卡、光碟、磁帶等。
9. 「資訊設備」，指可處理資訊、訊號、影像、聲音，並與其他資訊裝置交換資訊的設備，如電腦、伺服器、智慧型手機等。
10. 「Log」，指為一種電腦使用紀錄，記錄有行為操作者的 ID、操作日期、操作內容等。
11. 「關係企業」，指符合我國公司法第 369-1 條定義者。
12. 「分公司」，指符合我國公司法第 3 條第 2 項定義者。

## 參、政策管理

### 一、總則

#### (一) 管理對象

在企業中，有關營業秘密的管理對象，應包含企業的董事、監事、職員、派遣/派駐人員、顧問、經理人、工讀生、實習生等(以下統稱「從業人員」)，以及與企業簽訂契約或根據誠實信用原則有遵守保密義務的關係企業及第三方。

#### (二) 管理範圍

企業應將下列內容納入營業秘密管理範圍：

1. 營業秘密本身。
2. 營業秘密實體化後的有體物。
3. 營業秘密的生產設備或裝置。
4. 營業秘密管制區域。
5. 其他與企業營業秘密相關的資訊。

#### (三) 管理規定

企業應訂定營業秘密管理規定及相關配套程序，於明確營業秘密管理範圍及對象下，進行營業秘密的內容、人員、環境及相關設備等管理。

企業應向從業人員公告周知前述營業秘密管理規定及相關配套程序，並隨時使從業人員瞭解營業秘密管理規定及相關配套程序的執行現況及更新。

#### (四) 法規遵循

除營業秘密法外，企業亦應遵循相關法規訂定營業秘密管理相關政策及規定，例如勞動基準法、個人資料保護法、刑法、民法、智慧財產相關法律等。

## 二、最高管理階層及與管理組織運作

### (一) 最高管理階層角色和態度

企業的最高管理階層應明確對營業秘密管理目標，參與營業秘密管理規定的制訂，並宣導推動。

在會議、教育訓練等場合，最高管理階層應定期強調營業秘密的重要性、管理目標，並確認營業秘密管理的實施狀況，展現出積極的態度。

最高管理階層應定期檢視營業秘密管理落實狀況(包含日常檢視、內部定期稽核或第三方驗證結果與改善措施)，並配合調整營業秘密的管理目標或管理規定。

## (二) 統籌負責人職務

營業秘密統籌負責人的職務如下：

1. 擬定及調整企業或各部門的營業秘密相關計畫。
2. 統籌、規劃、推行營業秘密管理的相關配套程序或措施，並追蹤成效。如規劃或推行營業秘密教育訓練、定期盤點稽核檢視營業秘密管理落實情形。
3. 覆核、監督營業秘密管理執行人的執行狀況及內容。如覆核或監督列管營業秘密的紀錄與分類、營業秘密使用權限的相關事項、營業秘密的盤點等。
4. 其他與營業秘密管理相關的必要事項。

營業秘密統籌負責人須遵守誠信原則，確實執行營業秘密的保護、管理等相關職務。

## (三) 管理組織

企業整體或各部門須指定營業秘密統籌負責人，負責企業的營業秘密管理。營業秘密統籌負責人得視需求就營業秘密管理的執行項目，授權營業秘密管理執行人於其監督下協助其執行。

## (四) 稽核

企業應定期檢驗營業秘密管理的執行現況，並採取矯正因應及後續預防措施。

前述定期檢驗包含日常檢視、內部稽核，有必要時得經由第三方驗證稽核。

## (五) 廣宣管制

企業的官方發行資料(宣傳品/小冊子/出版物/網站公告/參展物等)、論文發表資料，於對外公開前，應由營業秘密統籌負責人確認該資料是否含有營業秘密，並以書面通知可否對外公開的核決結果。



### 三、教育訓練

#### (一) 定期周知

企業應定期辦理教育訓練，使從業人員瞭解營業秘密相關法規、企業的營業秘密管理規定與相關配套程序以及營業秘密外洩的因應處理程序等內容。

#### (二) 非定期周知

要求從業人員繳交營業秘密保護聲明書、簽訂保密約定或競業禁止等約定時，企業應同時周知企業營業秘密管理規定。

### 四、救濟

#### (一) 救濟措施

發現營業秘密受侵害或有受侵害的疑慮時，企業應立即蒐集、保全相關證據，並依據相關法令規定採取必要救濟措施。

#### (二) 懲戒

企業應對違反企業營業秘密管理規定的從業人員，訂定懲戒規則。

### 肆、內容管理

#### 一、營業秘密的處理程序

企業須針對營業秘密的產出、取得、管理清單、分級、標示等事項，規範處理程序。

#### (一) 產出

##### 【產出規範】

從業人員應就營業秘密的產出過程進行記錄，以確保可證明由從業人員所產出。

有關營業秘密的產出僅能於企業許可的紙本或紀錄媒體上作業，不得於私人電腦、手機、隨身碟、企業無法直接控管的網路資訊設備(如公有雲端)等進行產出。若於業務上有特殊需求、或會議等臨時性使用狀況時，依企業內的營業秘密管理規定的程序處理。

企業有與關係企業或第三方共同產出營業秘密時，企業應以書面約定該營業秘密權利歸屬。

##### 【產出申報】

從業人員在職中產出營業秘密時(包含自有、與顧問、派遣勞動者等其他從業人員共有)，須向相關部門主管及營業秘密統籌負責人申報，營業秘密統籌負責人應將此記錄於營業秘密管理清單中。

與關係企業或第三方共同產出與公司業務相關的營業秘密時，從業人員也必須根據前述規定申報。

### 【產出報酬】

對於產出營業秘密的從業人員，企業得根據該營業秘密價值給予合理報酬。

### (二) 外部取得

從業人員從外部取得營業秘密時，須向營業秘密統籌負責人申報，營業秘密統籌負責人應將此記錄於營業秘密管理清單中，並與企業所擁有的營業秘密區分管理。

### (三) 管理清單

企業應就其營業秘密的產出，建立營業秘密管理清單，並據此進行營業秘密管理。

前述清單中應至少包含營業秘密管理編號、保管處、營業秘密等級、使用權限、保密期限、複製、銷毀等事項。

### (四) 分級/秘等

營業秘密統籌負責人須針對營業秘密管理規定中所規範的評估標準，將企業所保有的營業秘密進行分級，並且依分級實施相應的營業秘密管理。

前述評估標準，可依照營業秘密的經濟價值、外洩風險等因素來制定。

### (五) 標示

企業應確保登錄於營業秘密管理清單上的營業秘密，其標示方式足以讓從業人員認知其為營業秘密。

## 二、區分管理和權限控管

### (一) 營業秘密取得來源

#### 【自有】

企業須將營業秘密與其他資訊作區分管理，以使從業人員認知管理內容為營業秘密。

## 【他人】

企業須將其營業秘密與從企業外部如關係企業、客戶、供應商、承包商、連鎖加盟店等所取得的營業秘密作區分管理，以使從業人員認知管理內容分別為企業自有、他人的營業秘密。

## 【共有】

企業與外部如關係企業、客戶、供應商、承包商、連鎖加盟店等共有營業秘密的情況下，應將營業秘密作區分管理，以使從業人員認知管理內容為企業與外部共有的營業秘密。

## (二) 營業秘密標的型態

### 【紙本】

營業秘密紙本，應依照營業秘密分級進行標示，標示方式可為標籤、戳章等。

前述已進行標示或不適合標示的營業秘密紙本，皆須保管於可上鎖的資料櫃或設有門禁管制的區域中。

企業應依照營業秘密紙本的營業秘密分級設定不同使用權限，並實施相應程度的保管措施。若有權限者職務變更、專案異動等變化情形時，企業應立即更改其使用權限，包含鑰匙交接、換鎖等。

### 【電子】

有關營業秘密電子檔案的標示、保管和使用權限，企業應進行下列管理：

1. 儲存有營業秘密的紀錄媒體、資料夾及營業秘密電子檔案等，應依照營業秘密分級進行標示，標示方式可為標籤、戳章、浮水印、檔名或資料夾加註秘字等。
2. 前述紀錄媒體若不適合標示者，須保管於上鎖的資料櫃或設有門禁管制的區域。
3. 企業應依照紀錄媒體、電子檔案的營業秘密分級設定不同使用權限，並實施相應程度的保管措施。
4. 企業設定使用權限後，若有權限者職務變更、專案異動等變化情形時，應立即

更改其使用權限。

5. 針對營業秘密電子檔案、存有該電子檔案的資料夾或電腦等資訊設備及其儲存空間的使用權限，企業應設定所須的帳號與密碼。

有關前述帳號與密碼的設定，企業應進行下列管理：

1. 確實落實一使用者一帳號密碼的原則。
2. 於企業內的營業秘密管理規定中，訂定有關使用者帳號註冊與刪除的規定。
3. 以至少三個月一次的頻率變更密碼，密碼的設定須避免單純、容易猜測的字串。
4. 螢幕保護程式須設定密碼，且離席時須開啟螢幕保護程式。
5. 定期刪除不使用的帳號(包含離職者、調職者)。

此外，企業得視需求，針對營業秘密電子檔案、存有該電子檔案的資料夾或電腦等資訊設備的使用權限，實施使用者的認證(如使用 USB Key 或 IC 卡、生體認證等)。

而在可存取營業秘密的場所中，嚴禁使用私人的紀錄媒體或資訊設備。

### 【物品】

具有營業秘密內容但不適合標示的物品(如製造機械、模具、高機能微生物、新產品的試作品等)，企業應明定使用權限並製作該等物品的營業秘密清單進行管理。

## 三、營業秘密的使用及銷毀程序

### (一) 借閱

企業針對營業秘密的借閱，應進行下列管理：

1. 僅有具使用權限者，才可閱覽企業的營業秘密。
2. 無營業秘密使用權限者，應申請取得營業秘密統籌負責人許可，並且由營業秘密統籌負責人至少將申請者、申請時間、申請的營業秘密、申請事由、借閱期間、許可簽章等基本事項記錄於借閱紀錄表。
3. 企業應依照前述借閱紀錄表所載事項，追蹤管理借閱的營業秘密。

## (二) 攜出

### 【紙本、物品】

企業針對外攜營業秘密的紙本或物品時，應進行下列管理：

1. 向營業秘密統籌負責人申請並取得許可，並且由營業秘密統籌負責人至少將申請者、申請時間、申請的營業秘密、申請事由、揭露對象、攜出期間、許可簽章等基本事項記錄於流通紀錄表。
2. 攜出營業秘密紙本或物品者應妥善保管，使用完畢後應立即依企業營業秘密管理規定執行返還程序。
3. 外攜營業秘密的紙本或物品時，應以密封、特殊文件夾等方式進行保護。

### 【紀錄媒體、資訊設備】

企業針對外攜存有營業秘密的紀錄媒體或可登入存有營業秘密系統的資訊設備，應進行下列管理：

1. 向營業秘密統籌負責人申請並取得許可，並且由營業秘密統籌負責人至少將申請者、申請時間、申請的營業秘密、申請事由、揭露對象、攜出期間、許可簽章等基本事項記錄於流通紀錄表中。
2. 針對攜出紀錄媒體或資訊設備者，企業應實施使用者的認證(如設定帳號與密碼、使用 USB Key 或 IC 卡、生體認證、檔案加密等)。
3. 攜出紀錄媒體或資訊設備者應妥善保管，使用完畢後應立即依企業營業秘密管理規定，執行返還紀錄媒體、資訊設備或銷毀營業秘密電子檔案的程序。

## (三) 複製、掃描等

營業秘密不得以複製、印刷、掃描、拍攝或列印等方式產出副本/複本，若於業務上有特殊需求或會議使用需要等特定、臨時性使用狀況時，應依企業營業秘密管理規定的程序處理。

營業秘密副本/複本視同營業秘密正本進行管理，但前述因特定、臨時性使用狀況所產生的營業秘密副本/複本，須於使用狀況結束時立即回收與銷毀，並將銷毀事項記錄於營

業秘密管理清單中。

#### (四) 傳遞或流通

企業傳遞紙本營業秘密時，應以密封、特殊文件夾等方式進行保護。

企業透過數位通訊傳遞/流通營業秘密電子檔案時，應實施通訊資料加密的保護措施，必要時另應針對含有重要營業秘密的電子檔案設置密碼。

企業針對電子郵件等數位通訊傳遞、資訊設備或儲存空間的流通使用，應設定發送容量限制、上傳/下載容量限制。

#### (五) 銷毀

企業應訂定營業秘密銷毀流程，並將銷毀事項記錄於營業秘密管理清單中。

企業應禁止將應銷毀的營業秘密紙本回收，將其空白背面再利用。

有關營業秘密紙本或物品的銷毀，應以無法回復的破壞性方式銷毀，如碎紙機、火銷、水銷等。

有關營業秘密電子檔案、紀錄媒體的銷毀，應以無法回復的方式確實銷毀，如安裝且執行檔案刪除軟體等。

#### (六) 使用留存和預警

##### 【備份】

針對企業電子郵件、營業秘密電子檔案或與其相關的系統應定期實施備份，備份資料的保存處應不同於正本資料的保存處。

備份的資料視同營業秘密進行管理。

##### 【使用紀錄】

企業應針對從業人員使用營業秘密的行為，訂定 log 紀錄及保管程序。

營業秘密統籌負責人應指定負責管理 log 紀錄的人員，並要求其定期記錄 log 並保管之。

前述 log 的紀錄內容，應至少包含行為者的 ID、操作日期、操作內容。

##### 【預警】



當發生有下列情況時，負責管理 log 紀錄的人員應將該狀況立即通知營業秘密統籌負責人：

1. 使用存有營業秘密的紀錄媒體、資訊設備、資料庫等的次數突然大幅增加。
2. 無業務上的需要卻使用存有營業秘密的紀錄媒體、資訊設備、資料庫等。
3. 向外部傳輸大量資料的情況。
4. 其他任何違反企業營業秘密管理規定的情況。

#### 四、關係企業或第三方管理

##### (一) 共有

與關係企業或第三方(如客戶、供應商、承包商、連鎖加盟店等)共有營業秘密的情況下，除參酌本指針肆、「內容管理」中的一、「營業秘密的處理程序」裡有關(一)「產出」與(三)「管理清單」的內容，建立營業秘密管理清單，據此進行營業秘密管理外，應以書面約定共有的營業秘密權利歸屬、要求關係企業或第三方進行營業秘密保護管理，並參酌本指針伍、「人員管理」中的四、「關係企業或第三方及其從業人員」進行人員管理，要求簽訂保密相關書面，以及提供營業秘密共有證明。

##### (二) 提供

企業針對營業秘密的對外提供，應進行下列管理：

1. 從業人員因共同開發、技術合作、委託業務、產品代工等互動過程而對外提供企業內部營業秘密時，應申請取得營業秘密統籌負責人許可，並且由營業秘密統籌負責人至少將申請者、申請時間、申請的營業秘密、申請事由、第三方組織或單位的名稱、第三方收受人姓名、返還或銷毀的日期、許可簽章等基本事項記錄於流通紀錄表中。
2. 企業應依照前述流通紀錄表所載事項，追蹤管理對外提供的營業秘密。
3. 企業應以書面約定關係企業或第三方應就收受的營業秘密進行保護管理，並參酌本指針伍、「人員管理」中的四、「關係企業或第三方及其從業人員」進行人員管理，要求簽訂保密相關書面，以及提供營業秘密收受證明。

### (三) 使用控管

無論與關係企業或第三方共有或提供其營業秘密的情形，企業除應依上述要求書面約定對方進行營業秘密管理外，亦應明定營業秘密使用範圍。

### (四) 返還或銷毀

企業就與關係企業或第三方共有或提供關係企業或第三方的營業秘密，應明定返還或銷毀事由及流程，並定期追蹤控管。

## 伍、人員管理

### 一、保密約定

企業對從業人員、離職者、關係企業或第三方及其從業人員簽訂有關營業秘密的保密約定時，至少須明確界定營業秘密的範圍、保密義務的內容以及保密期間。

### 二、從業人員

企業對從業人員，須明示就業上有關營業秘密的相關規定，並針對下列情形分別簽訂相關書面：

1. 聘僱時，企業應與從業人員簽訂保密約定。於就職一段期間後，企業應再檢視保密約定內容，調整或具體營業秘密保密範圍及義務，避免保密約定過於模糊籠統。
2. 針對從業人員在參與特殊專案或營運計畫等有另行接觸新的、特殊的營業秘密或具體接觸營業秘密的情況下，企業應要求從業人員另簽訂相關的保密約定或營業秘密保護聲明書。
3. 若從業人員職位涉及研發或與經營重要事項，得另約定競業禁止，但須注意合理性與必要性，例如限制期間、職務及區域的限制範圍等，以符合聘僱當地相關法規。此外，企業應依員工的條件及在公司的發展，定期檢視競業禁止約定內容，適時調整約定範圍或重新訂定競業禁止約定。
4. 企業須完備從業人員違反營業秘密遵守事項時的懲戒程序。

從業人員除了因業務執行而使用的營業秘密外，亦不得試圖使用與自身業務無關的其



他任何資訊。

### 三、離職者

#### (一) 對離職者的告知

從業人員離職時，企業應與其進行面談，提醒其注意相關智慧財產、保密義務或競業禁止的約定，並再以書面通知其前述相關事項。

離職時，從業人員須繳回自己所保有的所有營業秘密，並提交營業秘密保護聲明書。在沒有營業秘密統籌負責人的許可下，不得公開、使用營業秘密。

#### (二) 離職者監控與相應措施

企業須掌握從業人員的離職徵兆及離職者的離職後動向，並針對擬離職者追蹤管理其經手的一切資訊至離職後一定期間。

如企業已知擬離職的從業人員或離職者將任職於企業的競爭對手，並從事相同或類似的研發工作，企業於必要時應通知其新任職的企業組織，說明該從業人員與企業已簽定的保密約定、競業禁止約定及相關智財權歸屬等事項，避免該組織侵害到企業的營業秘密。

### 四、關係企業或第三方及其從業人員

進行交易或簽訂契約時，若與關係企業或第三方共有或必要向其揭露營業秘密的情形下，應於雙方協商階段、交易洽談或契約修正階段、最終簽約階段等各個主要協議過程中，要求關係企業或第三方及其相關從業人員簽訂保密約定或營業秘密保護聲明書，以及提供共有或收受證明等方式，確保營業秘密的保密管理。

### 陸、環境及設備相關管理

#### 一、管制區域及出入管制

企業對保管、處理重要資訊的空間，應進行下列管理：

1. 明定管制區域，與一般區域明確劃分，並於管制區域入口處張貼「未經授權者禁止進入」、於醒目處張貼「禁止攝影」等警語標示。
2. 於前述管制區域中，依照營業秘密等級高低實施不同程度的管制措施。如屬較

低秘等者，實施上鎖、門禁管制、專人看管等管理對策，並輔以定期換鎖、更換密碼等措施，防止不法入侵管制區域；較高秘等者，以導入認證系統(如設定帳號與密碼、使用 USB Key 或 IC 卡、生體認證等方式)、或配置保全人員的方式管理。

3. 限制可進入管制區域的從業人員，並記錄進出人員、時間等事項。
4. 針對外來人士(包含關係企業或第三方及其從業人員)出入企業，訂定出入管制程序，如專人引導到位於一般區域的貴賓接待處或會議室的外賓引導程序，以避免關係企業或第三方及其從業人員外來人士任意進出管制區域甚至接觸營業秘密。必要時得要求外來人士其繳交營業秘密保護聲明書。

## 二、監視

於管制區域及相關重要設施中裝設監視設備。

## 三、攜出入管制

企業應針對含有營業秘密的紀錄媒體、資訊設備及模具、試作品等物品進行攜出公司外及回收的管制程序，並如實遵守。

企業應對於有照相、錄影、錄音功能的相機、手機、隨身碟、電腦等紀錄媒體或資訊設備實施管制，必要時得全面禁止攜入。

## 四、網路及資訊設備的管制

### (一) 網路保安

針對網路安全措施，企業應進行下列管理：

1. 針對連線到網路上的特定網站進行管制。
2. 導入防毒軟體與防火牆等，並定期針對各伺服器、電腦等實施掃毒作業。
3. 禁止或限制安裝未經企業許可的軟體，並進行網站或電子郵件軟體的安全設定。
4. 從業人員只能使用受企業認可的電子信箱。

5. 企業應將含有營業秘密的資訊設備與外部通訊網路區隔，必要時可將該資訊設備配置在無法與網路(內網或外網)連接的封閉狀態下。

## (二) 密碼

企業內的電腦及企業作業系統登入密碼以至少三個月一次的頻率變更。

以定期周知的方式，教育從業人員須定期變更密碼及密碼設定注意事項。