自行研究計畫成果報告

智慧辦公-機房安全自動化監控管理
（以臺北區監理所機房營運為主）

研究單位：交通部公路總局臺北區監理所

研究人員：魏武盛、許芳祥、曾聰銘、陳品其、魏騰佑

交通部公路總局

中華民國 104 年 11 月

104 年度自行研究計畫成果摘要表

<table>
<tr><td colspan="3">臺北區監理所 104 年度自行研究計畫成果摘要表</td><td>填表人：臺北區監理所
填表日期：104 年 11 月</td></tr>
<tr><td>研究報告名稱</td><td colspan="3">智慧辦公-機房安全自動化監控管理</td></tr>
<tr><td>研究單位
及人員</td><td>臺北區監理所
人員:魏武盛、許芳祥、
曾聰銘、陳品其、魏騰佑</td><td>研究時間</td><td>自 104 年 1 月 1 日
至 104 年 11 月 30 日</td></tr>
<tr><td colspan="4">成果摘要</td></tr>
<tr><td colspan="4">本研究案主要是蒐集歷年來發生機房當機案例，列為未來營運時可能危及機房運作之風險因子，期能提早發現風險及早因應並施予適當控制措施，以減少故障發生機率，提升資訊系統服務水準。
目前正處於極高度資訊化時代，無論是公務機關或私人企業無不高度倚賴資通科技來維持其企業營運及其競爭力，尤其現階段行動載具及無線網路更為發達普及，也因此全天候的資訊服務(7 日 x24 小時)也被視為是基本服務水準。
本所電腦機房為資訊服務之心臟，對內提供所內同仁行政網路資源服務，對外提供民眾各項公路監理服務(如新車領牌、檢驗、考領駕照、補發稅單等等)，以往無論是在本所或外所站發生機房服務失效案例，除造成同仁辦公室電腦行政資源中斷，也會造成申辦監理業務之洽公民眾於臨櫃窗口久候，影響監理機關形象甚鉅。
由於電腦機房維運水準要求極高，不容許有片刻異常發生，稍有不慎隨即影響民眾權益並造成民怨，因此資訊人員對於機房維運工作相當重視，以往操作方式為每日上班時間由資訊同仁至機房以人工方式檢核，檢查項目為機房溫度、濕度、電力系統、網路連線狀態、磁碟容量等項目納入例行性檢查，並登載機房工作日誌。
惟人工檢查僅限於上班時間實施並未能普及例假日期間。為因應公路監理對外提供 24 小時全年無休之服務，故本所導入機房監控全自動安全管理，將機房環控項目溫溼度、電力、消防設備、漏水檢測及空調系統等外部主要設備加入即時監控及偵測機制，一旦發現有異常情形，均能全天候監測並主動發送簡訊通報相關管理人員，立即到所處理化解危機，降低資安事故發生機率。</td></tr>
</table>

目 錄

表 目 錄

圖 目 錄

第一章 緒論

第一節 研究背景與動機

2014 年 3 月 25 日自由時報報導，某監理站電腦作業系統疑因老舊，昨天中午突然大當機，業務全受影響，監理站趕緊派人搶修，但至下班前仍無法恢復運作，估計三百多人受影響。監理站表示，今天上班前可恢復運作，並向受影響民眾致歉。

有民眾反映，昨天上午前往監理站洽辦業務時，就發現電腦系統有問題，案件處理速度比往常慢了約半小時，到了上午十一點，監理站人員突然告知電腦系統當機，暫時無法受理，請民眾前往其他監理單位辦理，或是先送件，日後再補寄相關證件。

這名洽公者表示，他因工作關係常跑監理站，週一正是洽辦業務者最多的時間，他與其他人等了一個上午卻聽到這樣的消息，根本無法接受，隨後有不少人趁著中午午休時前來監理站洽公，發現白跑一趟，氣得破口大罵。

站方雖緊急搶修，但直到昨天下班時，電腦系統仍未恢復運作，估計整日下來，受影響的民眾超過三百人。該監理站人員表示，站內電腦設有三台伺服器，其中一台伺服器老舊，過去就曾故障，昨天上午疑因不堪頻繁操作而當機，造成系統混亂，影響列印輸出，雖緊急搶修，但整個上午都是時好時壞，到了近午就完全無法運作，站方雖啟動備用伺服器，但凡是與列印有關的業務，如過戶、補換行駕照等都受到影響，現場考駕照的民眾通過路考後，也無法當場取得駕照。

他說，故障的伺服器直到昨晚仍由維修人員搶修中，估計今天上班前可以修復，站方同時也會檢查其他老舊設備，並對受影響的民眾表示歉意。

以上是發生於 2014 年 3 月 25 日自由時報報導某監理站監理系統發生資訊安全事故造成對外服務中斷。吾人希望透過此次的研究蒐集近年來國內公民營單位發生資訊系統服務失效之樣態加以分析研究，施以有效控制措施以期減少發生機率。

第二節 研究目的

第三代公路監理資訊系統自 103 年 7 月 7 日進入實境測試後，公路監理系統正式啟動進入新紀元,由37個公路監理所站歷經9個月的實境測試後，於 104 年 5 月 6 日正式對外宣布第三代公路監理資訊系統正式上線啟用，由於第三代公路監理資訊系統系統架構與第二代公路監理資訊系統架構截然不同，其核心資訊設備及資料庫均集中於中華電信雲端機房，並有全年無休每日 24 小時值班人員全天候監控，以確保全國端核心系統正常維運無誤，但各所之機房監控限於經費能力就僅能於上班時間資訊同仁人工監控檢查，至於非上班時間監理所端之機房人員已下班，如何維持監測及及發生異常時及時通報機制，已達及早發現及早因應，以避免資訊系統異常影響正常服務時間的資安事故發生，即為本研究之目的。

第三節 研究流程

本研究之研究流程。首先，依據研究背景、動機、目的及蒐集近年來國內各資訊系統發生服務失效之樣態，再配合本所目前環控系統各項偵測元件之測試，以了解並確認環控各元件之有效性，藉由各項偵測元件測試及記錄，以及人員的操演，以確保將機房發生資安事故機率降至最低，倘若其他不可避免因素一旦發生時，相關人員得以順利啟動緊急應辦機制，以期能在最短期間完成修護並將資安災損降至最低。

第二章 本所機房管理維運現況

第一節本所機房設備現況及服務範圍

我國政府近年積極推動政府組織再造，資訊資源向上集中。因應此趨勢，同時規劃建立資訊集中之共享式服務，並將雲端運算、綠能 IT 等資訊技術導入政府相關資訊政策，於民國 100 年正式啟動「第四階段電子化政府計畫」。本所雖然配合政策將資訊資源向上集中，如公文系統、人事差勤系統及公路監理核心系統均已向上集中管理，惟此資訊向上集中政策並未能將本所資訊設施完全去機房化，本所機房仍需保有充足之網路服務及部分區域性主機提供本地端服務，本所機房設施任何一項設施服務失常，即會造成部分對外服務功能失效，如公路監理叫號系統故障，即會造成臨櫃等候之民眾失序，影響整體等候秩序。因此，即便目前已將資訊資源向上集中，本所機房仍須維持全天候監控，以確保監理服務品質。

第二節本所機房安全管理

103 年 7 月 7 日公路監理第 3 代資訊系統正式進入實境測試，為公路監理開創新紀元，雖然大部分核心資訊系統採主機代管方式營運，集中於中華電信東七機房，公路監理核心系統及 M3 網路係由中華電信全國維運中心 24 小時駐點人員監控，但本所仍有保有區域性資訊設施提供本地端基礎服務，本所機房核心設備如下表：

表 1 本所機房核心設備清單

	設備名稱	服務功能	重要等級
	窗口多媒體導引及叫號主機	提供民眾於本所申辦監理業務抽單功能及窗口同仁叫號等多媒體導引功能	高
	防毒及 WSUS 更新主機	終端電腦之防毒病毒碼更新及微軟作業系統弱點修補派送功能，屬於資安防護功能。	中

	M3 影像索引主機	M3 影像系統資料相當龐大，須建立資料檔索引，以利同仁查詢時迅速取得欲查詢之影像資料。	中
	影像加密處理主機	M3 影像因涉及民眾個人資料，影像存取時須經加解密處理。	中
	M3 影像儲存伺服器	儲存 M3 影像資料如車籍、駕籍登記書、稅費違規強質影像資料等等	中
	M3 影像備份伺服器	資訊人員定期執行影像資料備份	低
	M3 網路設備	提供本所同仁執行公路監理系統基本網路服務	高
	大內網網路設備	提供本所同仁執行大內網行政系統基本網路服務	高

(一)電腦機房門禁管制：

1. 電腦機房應設置自動上鎖門禁管制，解鎖權限設定為資訊室機房工作人員，進出機房須用門禁卡解鎖，且門禁系統須紀錄刷卡時間及卡號，以管制資訊室人員進出。

圖 1 機房入口門禁系統

2. 其他人員不得擅自出入，其餘同仁如因工作需要進入機房時，須經資

訊室有關主管同意，經許可後由資訊室人員陪同，並於「電腦機房進出登記表(ISMS-04-26-TPC)」登記，始得進入機房。

3. 本所或總局委外之系統管理人員於進入本所機房前應事前提出申請，委外廠商於首次進入機房前應事前提出申請，由資通安全分組組長核准後，始得進出機房。委外人員進出入機房均應填寫「電腦機房進出登記表(ISMS-04-26-TPC)」，並由資訊室人員陪同進入機房。

4. 其他機關如因作業需要進入本所機房，應先提出申請，並由資通安全分組組長核准後，由資訊室人員陪同，並於「電腦機房進出登記表(ISMS-04-26-TPC)」登記，始得進入機房。

5. 貴賓於有關主管陪同下，須由資訊室人員引領方得進入參觀。

6. 電腦主機及操作控制台除系統程式人員及值班操作人員外，非經資訊室有關主管指派或同意，不得擅自操作，如有違者將報請議處。

(二)機房環境之管理

1. 人員進入機房依據本所規定應更換機房內部拖鞋，離開機房時，應將拖鞋歸位。

2. 機房內嚴禁吸菸，亦不得攜帶飲料及食物進入機房。

3. 定期執行清潔作業以維護機房整潔，清潔工作必須以吸塵器或拖把清理，禁止提水桶進入機房工作。且機房使用之清潔工具，不得用於其他場所。

4. 機房內各種文具、報表、手冊、表單等應排列整齊，用完後歸定位，剩餘之廢棄物不得堆置於機房內。

5. 機房使用之物品如磁帶、磁碟、報表紙或手推車等應放置於規定地點並貼立標記。

6. 機房溫度應維持在 18℃至 25℃，相對濕度維持在 30%至 70%，本所資訊室指派機房輪值人員需每日於「三代公路監理系統機房工作日誌(ISMS-04-27-TPC)」記錄機房之相關環境數據。

7. 機房依據總局之要求，應設置稽核環控警告裝置，於異常發生時能以簡訊及其他方式通知機房管理人員。

8. 機房應設置監控攝影設備，24 小時監控機房之環境安全，至少包括機房門禁進出以及重要設備之監控攝影。監控攝影之錄影設備應設置防止他人未經授權存取或阻斷、中止運作之安全裝置，非必要不應置放於機房內部，以避免該設備被惡意阻斷或中止其監控功能。

圖 2 機房錄影監視系統

9. 設置符合機房專用之消防系統，並定點放置消防器材，機電維護廠商應定期檢測各項感應器。

10. 機房內應設置停電照明設備。

第三節機房環控現況

建置機房監控自動安全管理系統：

本所目前除原有之電話語音即時通報系統外，並於 101 年底另行建置機房監控自動安全管理系統，二套系統可互為備援，藉此強化機房環境監控機制，相關建置期程如下表：

表 2 機房環控建置時程

項次	建置時程	工作項目
1	101 年 07 月	總局資訊室陳主任交辦
2	101 年 7-8 月	辦理系統功能規劃及需求確認
3	101 年 08 月	簽辦機房環控系統委外建置案
		簽辦 55" 大型環境狀態顯示看板請購案
		簽辦環控系統簡訊發報門號申租案
4	101 年 09 月	系統建置
5	101 年 10 月	系統測試
6	101 年 12 月	完成驗收
7	102 年 2 月	公路監理系統核心程式運作及監測之異常告警
8	102 年 3 月	本所建置完成後由所長於 102 年 3 月監理會報提報

機房環境監控系統功能：

1. 機房溫濕度環境監控及異常即時簡訊告警

2. 機房滲漏(漏水)監控及異常即時簡訊告警

3. 市電供電監控及異常即時簡訊告警

4. UPS 電力負載監控安控系統異常即時簡訊告警

5. 機房消防設施監控及異常即時簡訊告警

6. 空調設備監控及異常即時簡訊告警

7. 智慧型空調備援系統

機房環境監控系統功能說明：

1. 機房溫度環境監控：如機房溫度超過攝氏 27 度即發送簡訊告警。
2. 機房滲漏(漏水)監控：漏水感測元件設置於機房高架地板下方，以避外牆窗戶區滲水，或是冷氣機之冷凝水滲入機房，造成電力設備或網路弱電設備異常。
3. 市電供電監控：臺電端供電異常如是電斷電時即簡訊告警，以利供電來源為市電或發電機供電，如為發電機供電已經超過相當時刻，則需要檢查發電機存油量是否足夠。
4. UPS 不斷電力負載監控：電腦的電源發生不正常中斷或是電流不穩定時，不斷電系統 UPS（Uninterruptible Power Supply）便擔負起暫時緊急供應電源的功能，使電腦不會因市電停電而被迫流失資料，或者未依正常程序關機造成系統的毀損。UPS 本身可再支援數十分鐘的電源供應緩衝時間，並使得自動電源切換開關切換至發電機端供電。因此 UPS 對於市電切換至發電機供電或是切返過程中扮演相當重要的角色。

圖 3 機房 UPS 不斷電系統

5. 機房消防設施監控：消防設施火警受信系統與機房環控系統連動，如火警受信系統偵測異常狀況即時簡訊告警。

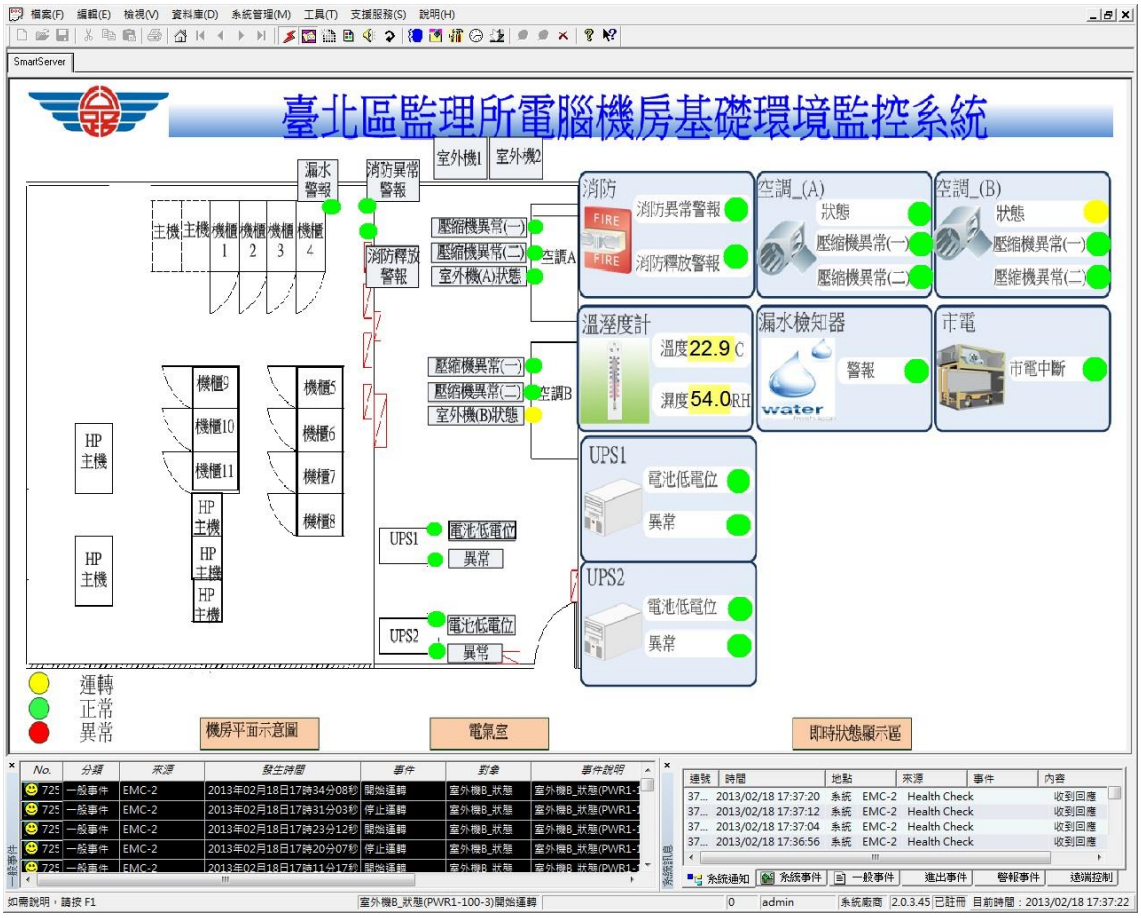
圖 4 機房消防控制面板

圖 5 機房消防系統

6. 空調設備監控：空調設備主要目的為控制機房溫度重要裝置，如機房溫度過高將損及伺服器主機，本所目前有 2 台 20KVA 落地型空調主機，以每 6 小時自動切換運轉，使機房溫度維持在 18℃至 25℃，相對濕度維持在 30%至 70%之正常工作溫濕度，任何一台空調主機異常即簡訊告警。

圖 6 機房空調主機

圖 7 機房環控監控螢幕



7. 智慧型空調備援系統

為補強 2 台 20KVA 落地型空調主機，每 6 小時定時自動切換運轉機制之不足，如遇單一空調主機運轉未達 6 小時切換點即發生硬體故障無預警停機，導致機房溫度異常，透過「智慧型空調備援系統」及時偵測機房溫度，如遇機房溫度超過設定之臨界值（27℃），除環控系統即時發出簡訊通知管理人員外，「智慧型空調備援系統」同時強制啟動另一備援空調主機，瞬間降溫以為因應，藉以維持機房正常工作溫濕度，並爭取維修時間，標準設定程序如下：

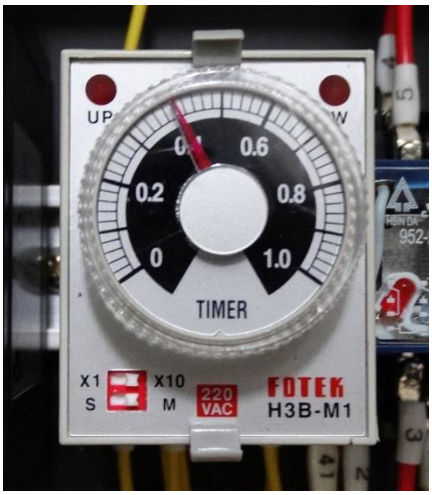
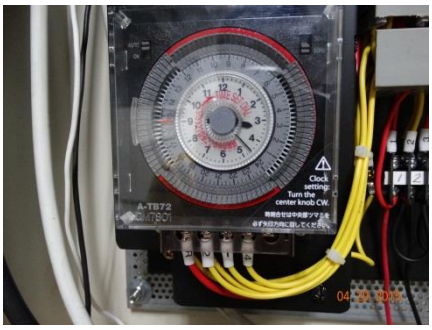
(1)警報溫度設定:

1. 溫度警報設定: 長按 SET 鍵 for 3 sec	
2. 按 SET 鍵 2 次跳到「AL1」畫面	
3. 警報溫度調升鍵	
4. 警報溫度調降鍵	
5. 溫度設定好後，連續按 Press SET 鍵回復至 右圖狀態即完成。	

(2)環境溫度校正流程:

1. **環境溫度校正:** 長按  鍵 for 3 sec	
2. 按 SET 鍵數次跳到右圖畫面	
3. 警報溫度調升鍵	
4. 警報溫度調降鍵	
5. 溫度設定好後，連續按 Press SET 鍵回復至右圖狀態即完成。	

(3)空調主機切換時延遲時間設定及調整標準程序：

Delay timer:設定單位(0.1 為 1 分鐘) 右圖示為延遲 4 分鐘。	
冷氣 A、B 機交互運轉時間設為 轉 6hr 休 6 hr	
冷氣 A、B 機自動運轉狀態時，旋鈕開關務必 至於中間位置(右圖畫面)。	

第三章 研究方法與資料分析

表 3 本年度重大資訊系統當機統計

發生時間	新聞標題	影響層面	發生主因
東森新聞 104.01.05	江蕙演唱會售票系統頻寬增到 200M 不夠用！ 35 萬人搶票 網頁今又當	民眾使用網路訂票失敗，所以改由提早到現場排隊買票	系統服務能量不足
東森新聞 104.01.27	全球最大的社交網站「臉書」，突然發生全球大當機，	用戶無法登入，時間長達 50 分鐘 。	內部工程師出錯引發系統故障
TVBS 104.02.25	台彩當機刮刮樂難兌獎-	伺服器硬碟損壞，造成全台 5500 家投注站,連線出現異常，部分投注站刮刮樂無法兌獎，當機持續一個小時。	核心設備硬碟故障
東森新聞 104.03.15	Ubike 當機 失效數據超載惹禍	YouBike 微笑單車系統前天出包，塞車 7.5 小時，大批民眾無法順利借車與註冊，抱怨聲不斷，緊急搶修後恢復正常，經一整晚徹查當機原因。	核心系統當機許多民眾借車失敗，產生「失效數據」累積在網路雲端達上，造成正常交易無法進入，失效交易未清理。
TVBS 104.08.17	台鐵票務系統,發生全台大當機	台鐵票務系統當機，全台網路、臨櫃都沒辦法買票劃位，連先訂好的票也無法取票，各車站售票口都大排長龍。	現網路供電設備因為過熱自燃
自由時報 104.09.09	貽笑國際！移民署電腦當機修不好 旅遊業跳腳	移民署作業電腦系統當機未修復，造成中、港、澳地區短期入臺旅客入台證無法順利申請，對臺灣觀光產業鏈產生實質傷害，連帶影響到航空業者、觀光旅遊業者、旅遊觀光景點經營、旅館飯店業者、遊覽車業者等。	核心系統當機

由於第 3 代公路監理資訊系統已將大部分核心系統向上統一集中管理，但本所仍有保有區域性資訊設施提供本地端基礎服，因此未來本所機房維護重點仍在於維持網路通訊、電力系統、機房溫度、異常告警等面向加以管理，以維持其監控功能的有效性，本研究案最主要係透過對本所機房 6 大監控點機房溫度、漏水監控、市電監控、UPS 不斷電系統、消防設備、空調設備等監控點，每個月執行模擬觸發過程並收集統計資料，以分析目前各項監測元件，是否有能力於異常發生時確實發送告警訊息通知資訊人員。

第一節 機房各式偵測元件測試及記錄

(1) 機房溫度感測元件測試：本測試以每月(104.01~104.10)使用吹風機加熱溫度感測元件到達攝氏 27 度以上，並記錄告警簡訊是否正常發送至預設人員。

表 4 每月機房溫度感測元件測試紀錄表

月份	1	2	3	4	5	6	7	8	9	10
觸發溫度(℃)	27. 1	27.0	27.2	27.0	27.1	27.1	28.2	27.0	27.2	27.1
是否發送簡訊	是	是	是	是	是	是	是	是	是	是

經每月測試機房環控溫度約在 27.0 ℃~27.2 ℃範圍即會正常觸發並發送告警簡訊，故本項測試正確無誤。

(2) 漏水監控感測元件測試：本項裝置係為防止外牆因雨勢過大窗戶區滲水，或是空調設備冷氣機之冷凝水滲入機房網路區或電力區，本測試以每月(104.01~104.10)以微量水滴實際測試感測元件，並記錄告警簡訊是否正常發送，測試完必須將感測區水滴擦拭乾淨。

表 5 每月漏水感測元件測試紀錄表

月份	1	2	3	4	5	6	7	8	9	10
是否發送簡訊	是	是	是	是	是	是	是	是	是	是

經每月測試漏水監控感測元件均能正常觸發並發送告警簡訊，故本項測試正確無誤。

(3) 市電監控、UPS 不斷電系統：本項測試須將臺電端斷電，其斷電切換操作應具備專業技術人員方可執行，故本所委由電力維護廠商每月定期操作臺電端斷電切換，觀察 UPS 不斷電系統及發電機供電是否正常，並記錄告警簡訊是否正常發送。

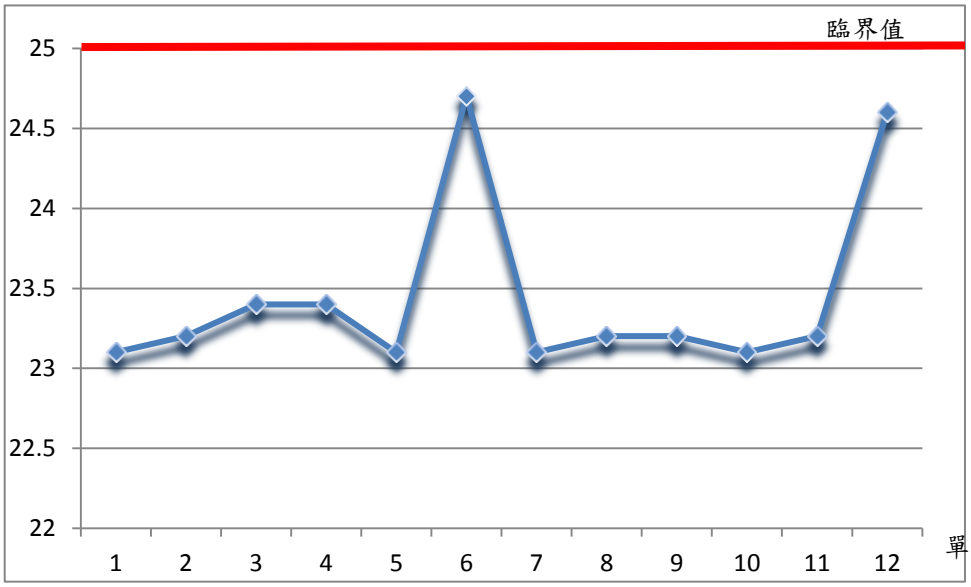
表 6 每月台電端市電斷電測試紀錄表

月份	1	2	3	4	5	6	7	8	9	10
UPS 運作	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常
發電機運作	正常	正常	正常	正常	正常	正常	正常	正常	正常	正常
是否發送簡訊	是	是	是	是	是	是	是	是	是	是

(4) 空調設備系統：本所資訊機房空調設備係由 2 台空調主機互相切換運行，主機 A 運轉時則主機 B 停機，主機 B 運轉時則主機 A 停機，每間隔 6 小時相互切換，本次觀察在 2 台空調主機切換運行溫度有上升趨勢，即原先機房溫度大約維持在 23℃~23.5℃之間，但是每逢主機 A 切換至主機 B 或是主機 B 切換至主機 A 運轉時，機房監測溫度即會上升至 24.5℃以上，溫度變化記錄情形如下表

單位:℃

圖 8 機房每小時溫度記錄圖(無延遲)



(5) 經詢問冷氣維護廠商說明為何會有此種現象，經技術人員說明大型空調主機基於供電自我保護，一般而言供電後大約 3~4 分鐘壓縮機才會正式運轉，冷氣機開機前 4 分鐘並不會運轉提供冷氣，因此 2 機切換(如 A 機啟動，B 機關機)期間將有 4 分鐘是沒有冷房效果，此現象如發生在平均室溫 20℃以下的寒冬季節，對於機房溫控短暫停滯 5 分鐘可能影響不大。但是處於室溫 34℃以上的炎熱夏天環境，機房溫度極可能超高而產生風險，因此這種現象必須妥善處理。

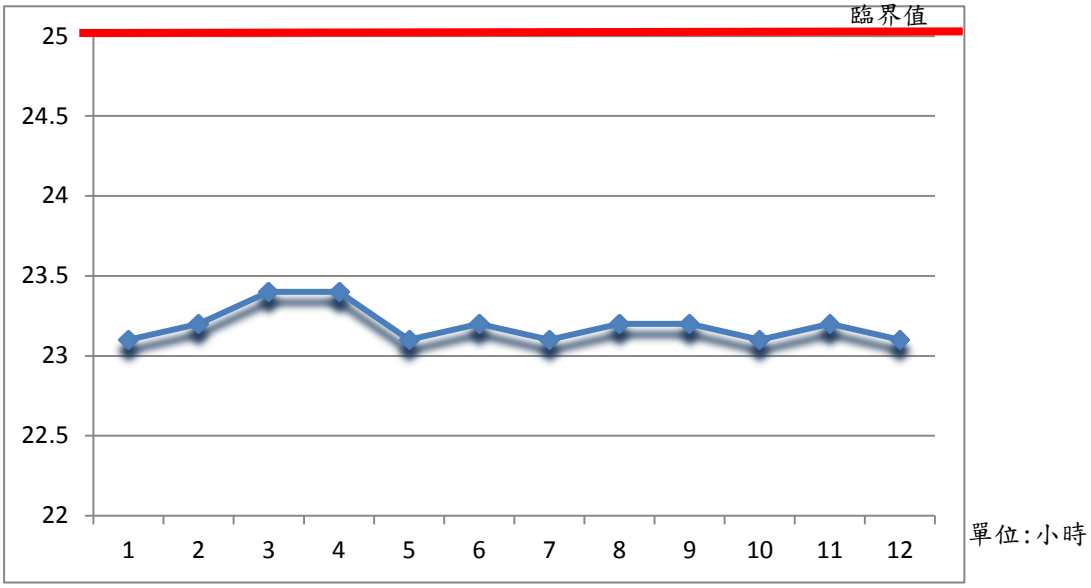
第二節 改善措施

(1) 為解決空調主機切換初期約 4 分鐘是沒有供應冷氣，此時機房存在有冷房效果之風險，也就是機房溫度可能過高超過臨界值 25℃，因此研議如何改善，經評估以最經濟的方式來解決此問題，即加裝延遲裝置來延緩切換時關機時間，例如主機 B 切換至主機 A(其動作為如 A 機供電啟動，B 機斷電關機)，增加延遲裝置之動作為(A 機供電啟動，B 機延遲 5 分鐘再斷電關機)，如此作法即可將 A 機供電啟動時自我保

護期間的空窗期，由 B 機延遲關機來持續提供冷房效果，經測試後即得下圖

單位:℃

圖 9 機房每小時溫度記錄圖(加延遲)



(2) 上節空調主機經加裝延遲控制開關即可克服供電自我保護期間，空調設備待機時間，另外為建立空調 A、B 2 台主機互為備援機制，其目的是為避免空調任何 1 台故障失效，造成整冷氣供應失效。本所曾於 104 年 4 月 18 日星期六晚上 20:25 時分，因空調 A 主機電路板故障，於 B 機運轉 6 小時候切換至 A 機，因 A 機故障且 B 機又停止運轉，造成機房溫度過高而發送簡訊通知資訊人員前來處理，雖未造成資訊服務中斷及任何災損，但也造成資訊同仁面對機房營運之壓力，為建立空調 A、B 2 台主機互為備援機制，避免因為其中一台空調主機故障導致無法正常運作時發生機房溫度過高情形，利用可程式控制器(PLC)及溫度感測元件，如機房溫度偵測超過 27℃時，此時則強制啟動 A、B 2 台主機，即可維持機房冷氣正常供應。

第四章 結論與建議

第一節 結論

機房設施是各項資訊作業的基礎環境，隨著網際網路的發展，資訊安全的環境成為確保資訊作業正常運作之必要條件。

為統籌管理本所資訊網路、資訊安全及資訊資源等基礎建設及強化整體市政資訊運作平台。於101年7月將原分屬網路、資訊安全及電腦設備維護等不同之監控系統，委由具有整合技術能力之專業資訊廠商進行統籌規劃，並導入即時監控告警概念，整合資訊網路、資訊安全、機房、資訊設備及資訊系統等管理作業，以高角度的視野進行機房基礎環境整合監控建設，合理化的資源配置，並加強維運管理的橫向連繫，提供安全、可靠且高效能的機房資訊基礎環境，重新統籌規劃及部署機房空間配置，因應資訊化業務發展需求，使有限資源做最有效利用，為維持資訊設備用電之安全，有必要對各迴路之用電狀況加以監控，將各迴路之用電狀況控制在安全範圍之內，及門禁、監視、溫濕度、電力及空調設備運轉監控整體擴充，並符合ISO 27001安全規範之相關原則。藉以達成本所資訊業務推動的績效，提升為民服務良好品質的目標。

第二節 建議

由於行動化、雲端物聯、巨量資料(Big Data)等各種新興智慧型科技逐漸成熟進入市場應用，而作為資訊時代企業營運核心的電腦機房(Data Center)，也發展出一套新的維運管理方向！

新科技不僅重新詮釋現代企業的各種營運服務，也重新改變資訊機房維運管理模式。此外，在國內能源政策未明朗的情況下，作為公司營運耗能大戶的企業機房，該如何實踐綠色節能的願景目標，也考驗著各相關管理者的工作能力！

新技術與新應用趨勢下，一個卓越的企業機房管理者必須思考：那些需要調整、那些卻不能改變？該如何應付公司越來越龐大的E化要求，同時卻又要兼顧減少機房能耗及維運費用？當前公司機房的維運與效能，是

否符合ROI(投資回報率Return On Investment，ROI)的要求？相關設備投資，是否能做到最優化標準？

政府機關及組織的電腦機房委外共構是目前政府施政的策略之一，但其前題必先滿足政府行政組織之再造的架構及符合經濟成本效益的狀況下，才能真正的達到政府資源的充分運用與政府資源共享的目的，而不致於流為形式，而重複及浪費地投入資源。

機房委外共構具有以下之優點：

一、整體維運成本及經費較少。

二、可以節省機房之搬遷費用。

三、電腦機房的設備可以就近方便管理。

四、人員進出管控較為便利及徹底，對資訊安全之疑慮較少。

五、系統及網路的架構不必更動，異動的複雜度較低且容易掌控。

六、現有之空間可以完全充分利用，加值性較佳。

七、可充分利用 IDC 業者所提供之基礎設施，可無需考量因業務擴充而必新增基礎設施。

又如未來因應政府行政組織調整之要求的考量因素下；因目前政府正大力推動政府組織再造的計畫,未來很可能會與其他機關合併或組織調整，經 由此一活動可能造成多個機房必須合併或共構，不論合併或共構均有機房設置位置的問題，當發生此一狀況時，首先必須評估每一機構的機房大小,是否其空間可以 容納所有設備,如果可以的話便可以擴充其基礎設施，以維持未來的營運正常無慮。

當所有之合併調整機關的機房均無法容納全部時，按照現有資源分享的前提下，不建議另建一機房，可採取委外共構的模式來進行。其共構服務之挑選可以參照前面章節所述之選擇提供機房共構之業者的服務內容及要求，根據文中所述挑選合適之業者來為本所機房共構提供服務。

交通部公路總局臺北區監理所

資通安全管理規範

文件編號：ISMS-03-01-TPC

文件版本：V1.1

中華民國104年10月26日

版本更新歷史

[redacted]

1.0	104/09/01	文件管理分組	初版	
1.1	104/10/21	文件管理分組	1. 增訂第伍章、風險評鑑與管理。 2. 增訂第柒章第一節之(一)第1項：資訊室人員進出機房管制。 3. 增列第肆章第二節之(四)資訊資產價值：定義高風險資訊資產。	

目 次

壹、資通安全政策

一、目的

交通部公路總局臺北區監理所(以下簡稱本所)制定本資通安全政策，管理本所各項資通安全措施之標準。透過本資通安全政策之制定，明確宣示高階主管支持資通安全之決心，並使相關人員有所依循。

二、依據

依據公路總局資訊安全管理制度全組織管理規範，訂定本所資訊安全管理政策。

三、目標

本所資通安全政策為「**資訊保護、全體動員，資通安全、人人有責**」，以期建立一個機密性、完整性與可用性的資通安全環境，並達成以下目標。

(一)「資訊保護、全體動員」目標

1.落實資訊保護政策，確實遵守資訊存取與實體環境安全管理作業程序。

2.尊重智慧財產權，禁止安裝未經授權之電腦軟體，並對可攜式設備之使用嚴加管控。

3.全體共同攜手動員，確保資訊妥適安全，防止任何外力危害。

(二)「資通安全、人人有責」目標

1.落實資通安全政策，加強資通安全教育宣導。

2.建立資通安全量測指標，評估資通安全運作成效，落實營運持續與管理改善。

3.嚴格遵守網路與通訊管理作業程序規定，防止各類惡意程式與電腦病毒入侵。

4.人人遵守資訊存取控制管理作業程序規定，避免資通安全人為疏失。

四、資通安全之定義

維護本所資訊通訊資料的機密性、完整性及可用性。

五、資通安全之涵蓋範圍

資通安全之管理範圍共分十二大管理領域：

(一)資通安全政策

(二)資通安全組織及權責

(三)資通安全文件管理

(四)資訊資產之分類與管理

(五)人力資源安全管理暨資通安全教育訓練

(六)實體及環境安全管理

(七)網路安全與網站資料管理

(八)系統存取控制

(九)新科技與便民設備管理

(十)櫃檯作業與文檔管理

(十一)營運持續運作之管理

(十二)內部稽核作業

六、適用性

本資通安全政策所規範之事項，其適用之對象為本所各科、課、室等區域。 人員涵蓋範圍包括區域內所有正式編制人員及駐警隊或保全人員、約僱、臨時或因業務需要僱用之非編制內人員、資訊業務委外服

務駐點廠商等，皆有責任遵循及執行本資通安全政策。

七、成立資通安全工作小組

本所為推動辦理資通安全相關工作，爰成立資通安全工作小組(以下稱工作小組)，負責規劃、推動、協調及執行資通安全管理事項，並回報總局資通安全管理成效。

八、召開本所資通安全管理審查會議

本所依總局規範時間及方式，每年召開資通安全管理審查會議，包括宣達資通安全政策、資通安全規範、核定工作計畫及處理資安事件，並審查資通安全稽核之結果與矯正預防措施。另視需要得不定期召開資通安全管理相關會議，以強化推動資通安全管理事項。管理審查會議及資通安全管理會議之會議紀錄函報總局以利進行全組織之資通安全管理作業。

九、資通安全程序制定

本所依據總局全組織管理規定及相關辦法，制定及執行本所資通安全作業程序，作為控管本所資通安全之執行依據。

十、資通安全政策之評估

本所於每年管理審查會議中依據總局全組織管理規定，進行獨立及客觀評估，並考量本所須遵循之法令規定、資訊技術環境及業務之最新需求及本所權責範圍內之資通訊安全管理需求，提出對於本所及全組織資通安全政策之修訂建議，併同資通安全管理審查結果提供總局作為年度政策修訂之參考。

十一、資通安全政策及規定之宣達

(一)於總局修訂頒行全組織資通安全政策後，本所將透過公告程序，進行所內傳達與溝通，責成所屬人員瞭解總局全組織資通安全政策之相關規定及責任，俾益其遵循及達成總局規範之資通安全政

策。

(二)員工如違反本政策相關規定，應依本所規範之紀律程序處理。

貳、資通安全組織及權責

一、依據

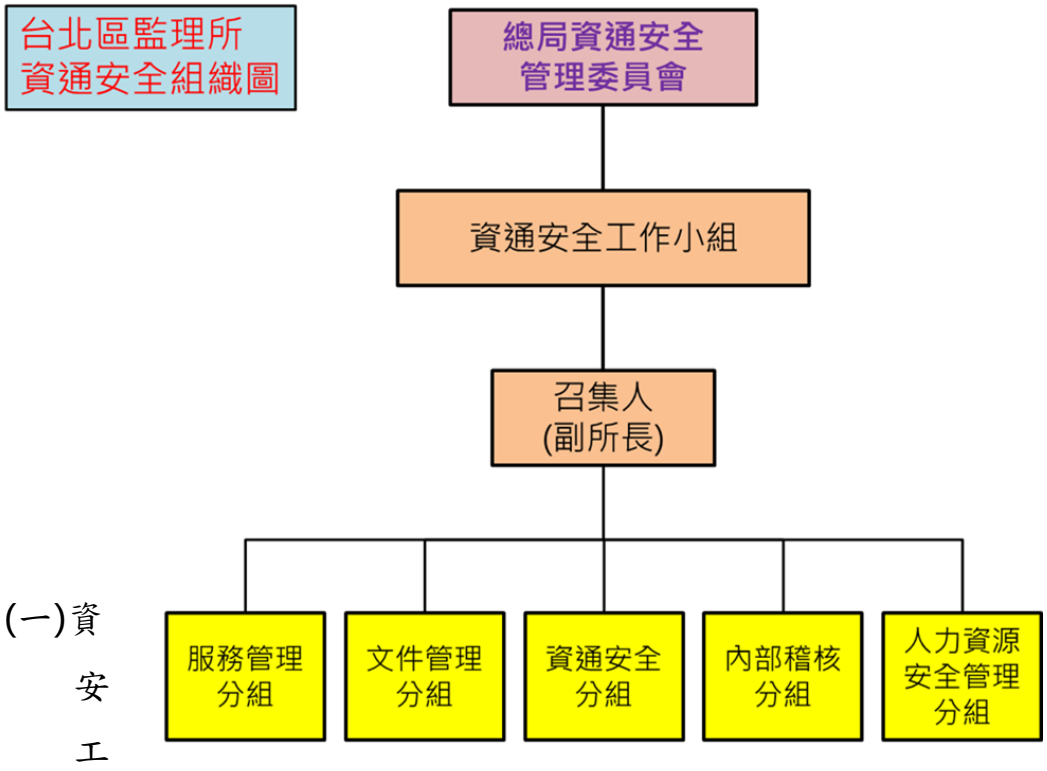
依據總局全組織管理之組織規定，本所設立「資通安全工作小組」(以下簡稱工作小組)。

二、管理組織

本工作小組負責處理本所資通安全管理、推動相關事務及遵循事項，包括資通安全管理、危機處理等相關事宜，並配合總局建立之資通安全通報體系及應變機制進行對於資通安全管理之通報，以達成本所於總局資通安全管理之管理分工。

三、組織架構

依據總局對於資通安全作業之管理需求，本所組成以下管理組織工作小組:



(一)資通安全工作小組：由副所長擔任召集人(本所之資通安全長)，各單位主管為

小組成員。

(二)內部稽核分組：由政風室擔任幕僚單位，並由政風室主任擔任內部稽核分組組長，協同資訊室進行內部稽核。

(三)人力資源安全管理分組：由人事室擔任幕僚單位，並由人事室主任擔任人力資源安全管理分組組長。

(四)服務管理分組：由各業務單位推派一員擔任，並由各業務單位主管輪流擔任分組組長。

(五)文件管理分組：由資訊室擔任幕僚單位，並由資訊室主任擔任文件管理分組組長。

(六)資通安全分組：由資訊室擔任幕僚單位，並由資訊室主任擔任資通安全管理分組組長。

四、工作職掌

(一)資通安全工作小組：

1.召開與主持管理審查會議及資通安全相關管理會議。

2.執行工作小組公告事項。

3.資通安全事務之推動與監督。

4.資通安全事件之通報、檢討與改善。

5.啟動資通安全事故應變程序。

6.資通安全工作分配、協調與督導。

(二)內部稽核分組：

1.依據總局之規範執行本所資通安全之稽核。

2.稽核結果與改善追蹤於管理審查會議提報。

(三)人力資源安全管理分組：

1.規劃與執行本所資通安全管理之人力資源。

2.規劃與執行本所資通安全教育訓練暨推廣作業。

3.制定、量測與執行資通安全教育訓練之績效指標評估。

(四)文件管理分組：

1.本所資通安全文件之制定、修訂、發行與廢止。

2.執行本所之文件管制作業(含文件存放、文件標示、文件存取及借/調閱、文件傳遞、保存期限及銷毀)。

3.依據總局文件管制規定，回報本所文件制定之執行狀況及報備相關文件之制定、修訂、發行與廢止狀況。

(五)服務管理分組：

1.規劃與制定本所監理作業區及櫃台作業管理辦法。

2.監督及推廣本所作業區安全管理規定。

3.執行作業區及櫃檯作業之文件管制作業。

(六)資通安全分組：

1.負責本所實體及環境安全管理。

2.負責本所內機房及資訊設備之實體及運營安全。

3.網路安全及系統存取控制。

4.依總局規劃及統籌執行本所資訊資產盤點及風險評鑑作業。

5.依據風險評鑑需求制定本所之風險處理計畫。

6.監督及追蹤本所風險處理計畫之執行。

7.規劃與執行資通安全事件處理。

8.規劃與執行本所營運持續管理及演練。

參、資通安全文件管理

一、依據

依據總局「資通安全管理系統文件與紀錄管控作業程序書」，由文件管理分組執行本所資通安全文件管理。

二、範圍

本所資通安全管理作業內之內部、外部文件與記錄管理作業。

三、作業程序

(一)文件制訂、修訂、發行及廢止

1.資通安全管理系統之第一階、第二階文件由總局頒布施行，文件管理分組負責發行及通知事項。

2.第三階及第四階文件由本所相關單位制訂，文件管理分組執行本所制定文件之文件管控事項，並陳報總局之資通安全文件管理小組。

3.各單位制定、修訂、廢止、銷毀本所第三階、第四階文件應填寫「文件制訂/修訂/廢止/銷毀申請單(ISMS-04-01-TPC)」，並向文件管理分組提出申請。

4.文件檢討時機：

(1) 相關標準變更或法令修改，現行規範不盡適用

(2) 業務新增或業務變更時，現行規範不盡適用。

(3) 經評估或稽核後發現文件需修訂。

(二)文件編碼

本所之文件編碼依據總局「資通安全管理系統文件與紀錄管控作業程序書」訂定之。

(三)文件審查及核准

1.本所四階表單文件之制定、修訂、廢止及銷毀由該文件之管理課室進行審查、核定後送交文件管理分組進行文件之制定、修訂、廢止、銷毀及發行。

2.本資通安全管理規範，應由相關課室制定，陳報工作小組召集人核定。

(四)文件發行、廢止及紀錄銷毀

1.本所三、四階文件依規定經核准後，交由文件管理分組統一發行與公布。

2.三階文件需廢止時，應填寫「文件制訂/修訂/廢止/銷毀申請單(ISMS-04-01-TPC)」，陳報工作小組核定後，交由文件管理分組進行廢止作業，並保留必要管理紀錄。

3.文件紀錄銷毀：

(1)廢止之程序文件由文件管理分組依規定進行文件之廢止，並預防相關人員使用廢止之文件。

(2)依據文件保存規定過期之紀錄 (指第四階文件有實質紀錄內容者)，由本所相關課室人員確認其屬性 (紙本 及/或 電子檔案格式)後填寫「文件制訂/修訂/廢止/銷毀申請單(ISMS-04-01-TPC)」，核准後由文件管理分組依據本所銷毀文件之方式進行銷毀動作，文件管理分組應確保其文件銷毀之安全性及有效性，並保留相關處理紀錄。

(五)文件管制

1.文件存放：文件管理分組應對本所之資通安全管理文件編製文

件清冊，且陳報總局資通安全文件管理小組，並依公務機關之機密等級及文件層級依序分類歸檔或由檔管人員依據檔管規定進行管制，且應不定時檢查文件內容之可讀性，避免文件因自然條件或物理、化學特性喪失其內容。

2.文件標示

(1) 文件之機密等級應於文件封面及內頁的頁首或頁尾做明確標示，機密等級為「公開」之文件可選擇不做機密等級之標示。文件於歸檔時文件管理分組應對文件或紀錄之機密等級進行檢視。

(2) 系統輸出機密等級為「機密」之報表時，如未自動標示為機密者，應由報表輸出者做額外的明顯註記(如加戳記)。

3.文件存取及借/調閱

(1) 機密性文件應依使用者職權賦予適當之文件存取權限，並由文件管理分組控管。

(2) 資通安全之文件借/調閱，由文件管理小組依據該文件之機密等級進行管制，機密分級之文件須由本所工作小組核准後始得借/調閱。且須於指定之場所內查閱，非經許可複製之文件，不得以任何形式私自複製。

4.文件傳遞：「機密」等級文件於遞送過程應加封套密封，由專人或交授權之快遞公司遞送。

5.保存期限及銷毀

(1) 各階文件修訂時，其相關之四階文件應同步進行更新。文件管理分組應保留各版次，以供回溯追蹤文件之異動過程。

(2) 與資通安全相關之第四階文件紀錄至少應保留三年，相關

文件之保存期限，得依業務需求而訂定。

(3) 本所保留之「機密」等級文件或紀錄，如無繼續保留之需要時，應填寫「文件制訂/修訂/廢止/銷毀申請單(ISMS-04-01-TPC)」並註明銷毀原因，應經本所工作小組核准後，由文件管理分組進行銷毀並留下管理紀錄。

肆、資訊資產之分類與管理

一、資訊資產分類

本所資訊資產依其性質不同，分為五大類，其說明如下表：

資產類別	說明
資訊紀錄 DA	紙本文件、資料庫 (電子檔案形式)及儲存於硬碟、光碟等儲存媒介內之資料
實體設備 HW	電腦硬體、伺服器主機、網路設備、機房環境管理設備等
系統及軟體 SW	套裝軟體、程式碼、編程(compiled)之後的應用系統、資料庫套裝軟體等
服務 SV	服務類型資產，例如資訊連線專線、委外之安全服務等
人員 PE	包含本所全體資通安全作業相關之同仁

二、資訊資產分級與價值

本所針對資訊資產對組織之價值、敏感性及重要性等特性，進行資產之機密性、完整性及可用性分級，各項資訊資產價值之計算以此 3 種分級數值之總合訂定。

(一) 機密性等級評估表

機密等級	資產類別	評估標準	價值
公開	資訊紀錄	無機密性且可公開之文件與電磁紀錄。	1
	實體設備	不具機密性特質之實體。	
	系統及軟體	無機密性且可公開使用之資訊系統或軟體。	
	服務	無機密性且不影響其他資產機密特質之服務。	
	人員	無涉及機密性資訊處理之人員。	
內部使用	資訊紀錄	無機密性要求且僅限本所內部使用之文件與電磁紀錄。	2
	實體設備	無機密性且僅限本所內部使用之實體。	
	系統及軟體	無機密性且僅限【本所內部人員或授權使用之人員】所使用之系統及軟體。	
	服務	無機密性且僅限本所內部使用之服務。	
	人員	本所員工其工作職掌不涉及機密資訊之處理者。	
機密	資訊紀錄	本所或法律所規範的機密文件及電磁紀錄，僅供【本所授權使用之人員】存取。	3
	實體設備	存放本所機密文件及電磁紀錄之實體資產，僅供【本	

機密等級	資產類別	評估標準	價值
		所授權使用之人員】存取。	
	系統及軟體	具機密性且僅限【本所授權使用之人員】存取之系統及軟體。	
	服務	具機密性且僅限【本所授權使用之人員】所使用之服務。	
	人員	工作內容涉及機密資訊處理之本所員工。	

註：各項不同等級之機密資訊資產合併使用或處理時，以其中最高之等級為機密等級。

(二) 完整性等級評估表

完整等級	資產類別	評估標準	價值
微或無	資訊紀錄	文件或電磁紀錄不正確或不完整時，對本所營運不會造成任何影響。	1
	實體設備	實體環境或設備發生損壞或故障時，對本所營運不會造成任何影響。	
	系統及軟體	不當使用系統或軟體時，不會造成任何影響或其影響是僅出現異常訊息，可另於其他時間檢測。	
	服務	所使用之服務發生中斷時，對本所營運不會造成任何影響。	
	人員	人員所負責之作業，因操作錯誤造成的資訊不完整，對本所營運不會造成任何影響。	
低	資訊紀錄	文件或電磁紀錄不正確或不完整時可被立即更正，並讓本所持續正常營運。	2
	實體設備	實體環境或設備發生損壞或故障時有備援設備能立即更換，並讓本所持續營運。	
	系統及軟體	因不當使用，造成系統或軟體運作異常，但可由使用者自行立即排除，或由資訊人員協助立即排除，並讓本所持續營運。	
	服務	所使用之服務發生中斷時，但有備援機制可立即置換，並讓本所持續營運。	
	人員	人員所負責之作業，因操作錯誤造成的資訊不完整，可被立即更正，並讓本所持續正常營運。	
中	資訊紀錄	文件或電磁紀錄不正確或不完整且無法被立即更正，可以人工作業或其他方式代替執行，雖已造成人員執行上的困擾，但本所仍可持續營運。	3
	實體設備	實體環境或設備發生損壞或故障時無法立即更換，可以人工作業或其他方式代替執行，雖已造成人員執行上的困擾，但本所仍可持續營運。	
	系統及軟體	因不當使用，造成系統或軟體運作異常且無法立即排除，可以人工作業或其他方式代替執行，雖已造成人員執行上的困擾，但本所仍可持續營運。	
	服務	所使用之服務發生中斷且無法立即置換，可以人工作業或其他方式代替執行，雖已造成人員執行上的	

完整等級	資產類別	評估標準	價值
		困擾，但本所仍可持續營運。	
	人員	人員所負責之作業，因操作錯誤造成的資訊不完整且無法被立即更正，可以人工作業或其他方式代替執行，雖已造成人員執行上的困擾，但本所仍可持續營運。	
高	資訊紀錄	文件及電磁紀錄具有完整性要求，當完整性被破壞時，除無法被立即更正，且無替代執行方案，將使本所營運停頓。	4
	實體設備	實體環境或設備發生損壞或故障時，除無法被立即更換，且無替代執行方案，將使本所營運停頓。	
	系統及軟體	因不當使用，造成系統或軟體運作異常時，除問題無法被立即排除，且無替代執行方案，將使本所營運停頓。	
	服務	所使用之服務發生中斷時，除無法被立即置換，且無替代執行方案，將使本所營運停頓。	
	人員	人員所負責之作業，因操作錯誤造成的資訊不完整，除無法被立即更正，且無替代執行方案，將使本所營運停頓。	

(三) 可用性等級評估表

可用等級	資產類別	評估標準	價值
微或無	資訊紀錄	可容忍文件及電磁紀錄 72 小時以上無法存取。	1
	實體設備	可容忍實體環境或設備 72 小時以上無法使用。	
	系統及軟體	可容忍系統或軟體 72 小時以上無法使用。	
	服務	可容忍服務 72 小時以上無法使用。	
	人員	可容忍人員缺席 72 小時以上。	
低	資訊紀錄	可容忍文件及電磁紀錄 8 小時以上 72 小時以下無法存取。	2
	實體設備	可容忍實體環境或設備失效 8 小時以上 72 小時以下。	
	系統及軟體	可容忍系統或軟體失效 8 小時以上 72 小時以下。	
	服務	可容忍服務失效 8 小時以上 72 小時以下。	
	人員	可容忍人員缺席 8 小時以上 72 小時以下。	
中	資訊紀錄	可容忍文件及電磁紀錄 4 小時以上 8 小時以下無法存取。	3
	實體設備	可容忍實體環境或設備失效 4 小時以上 8 小時以下。	
	系統及軟體	可容忍系統或軟體失效 4 小時以上 8 小時以下。	
	服務	可容忍服務失效 4 小時以上 8 小時以下。	
	人員	可容忍人員缺席 4 小時以上 8 小時以下。	
高	資訊紀錄	可容忍文件及電磁紀錄 4 小時以下無法存取。	4
	實體設備	可容忍實體環境或設備失效 4 小時以下。	
	系統及軟體	可容忍系統或軟體失效 4 小時以下。	

可用等級	資產類別	評估標準	價值
	服務	可容忍服務失效 4 小時以下。	
	人員	可容忍人員缺席 4 小時以下。	

(四) 資訊資產價值

1.本所針對資訊資產對組織之價值、敏感性及重要性等特性，進行資產之機密性、完整性及可用性分級，各項資訊資產價值之計算以此 3 種分級數值之總合訂定。

2.高風險資訊資產為資訊資產價值大於等於 7 以上者，7 以下為中低風險資訊資產，高風險資訊資產於任何異動時須填列「資產異動申請單(ISMS-04-03-TPC)」且須經資通安全分組組長核准，並於異動後即時更新「資訊資產清單(ISMS-04-02-TPC)」。

三、資訊資產管理

(一)資訊資產新增管理

1.廠商交付資訊資產時，需詳列細目，並由使用單位逐項點收。

2.新增資訊資產於安裝完工後，應由指定專人為資訊資產保管人並更新於本所之「資訊資產清單(ISMS-04-02-TPC)」。

3.非經本所資通安全分組確認，個人電腦不得隨意進行軟體安裝。

(二)資訊資產異動管理

1.資訊資產異動時，任何涉儲存有資訊紀錄或系統與軟體之資訊資產，應先予作適當處理(例如含有機敏性資料之軟硬體應予卸除)，以避免資料外洩。

2.高風險資訊資產異動時，由資訊資產保管人填寫「資產異動申請單(ISMS-04-03-TPC)」，並經資通安全分組組長核准，異動完成後應通知更新「資訊資產清單(ISMS-04-02-TPC)」。

3.中低風險資訊資產異動時，於年度資訊資產盤點時清查並更新「資訊資產清單(ISMS-04-02-TPC)」。

(三)資訊資產之送修

1.資訊資產送修若涉儲存有資訊紀錄或系統與軟體時，應將含有機敏性資料之軟硬體先予卸除，以避免資料外洩。

2.資訊資產送修之承辦人，必須負責追蹤送修情況。

3.高風險資訊資產送修應時，須填寫「資產異動申請單(ISMS-04-03-TPC)」，並經資通安全分組組長核准。

(四)資訊資產之安全維護

1.儲存機密等級文件的儲存媒體應由保管人員妥善保管(例如加鎖)，存放設備如有損壞應立即修復。

2.儲存機密等級之媒體，於遞送過程應有保護裝置，以防止遞送過程中受損，電磁紀錄檔需經加密或設定檔案開啟密碼之處理，以防儲存媒體遺失時敏感資訊外洩，且該儲存機密等級之媒體應交由本所專人或交授權之快遞公司遞送。

3.儲存機密等級之媒體，改儲存非機密等級之資訊或待銷毀時，應先將原儲存之資訊完整格式化(Format)，才可以儲存其他資訊；光碟一律將反光層完全抹除，或全碎銷毀。

(五)資訊資產之保養維護

1.資訊資產有關實體設備，應依照廠商說明書指示操作使用，若有簽訂保養或保固維護合約，應依合約規定進行定期保養及檢查等維護作業，並保留相關紀錄，以確保其正確運作。

2.設備使用人發現設備故障或疑似故障情形時，應通知主管，若為高風險資訊資產須填寫「資產異動申請單(ISMS-04-03-TPC)」後報修，如牽涉資訊安全事件時應依總局頒布之「資通安全事件通報作業標準書」規範辦理。

(六)資訊資產報廢

1.資訊資產不堪使用時(紙本文件除外)，若涉儲存有資訊紀錄或系統與軟體時，應將含有機敏性資料之儲存裝置消磁破壞並留有消磁紀錄，以避免資料外洩。

2.若為高風險資訊資產須填寫「資產異動申請單(ISMS-04-03-TPC)」，將原有資訊資產作適當處理，確認重要相關資料已刪除，並通知資通安全分組更新「資訊資產清單(ISMS-04-02-TPC)」。

3.中低風險資訊資產異動，於年度資訊資產盤點時清查並更新「資訊資產清單(ISMS-04-02-TPC)」。

(七)資訊資產盤點

每年盤點一次，由資通安全分組發起，並由各課室配合盤點作業，盤點結果送資通安全分組複核，並更新「資訊資產清單(ISMS-04-02-TPC)」以確保資訊資產之完整性。

(八)合法版權軟體抽查

資通安全分組應於每年內部稽核前抽查使用者安裝之軟體，若發現有自行安裝非法軟體，由資通安全分組負責移除非法軟體。

伍、風險評鑑與管理

一、目的

為鑑別本所所掌理資通業務之資訊資產風險，透過以系統化方法建立風險評鑑之過程標準，依據評鑑結果找出潛在的高風險事項並對其採取對策 (如: 降低、避免、轉移風險、接受)等方式，以降低本所可能遭受的損害風險，使本所業務能順利運作及推展。

二、權責

(一)資通安全工作小組召集人

負責核定可接受風險值及風險改善計畫。

(二)風險擁有者 (Risk Owner)

擬定風險改善計畫

(三)資通安全分組

1.確定風險評鑑之結果。

2.提出可接受風險值之建議。

3.審閱並確認風險改善計畫。

4.監督及追蹤風險改善計畫之執行。

(四)定義

(五)資訊資產價值

依據本管理規範第肆章「資訊資產之分類與管理」規定之作業方式評定本所各項資訊資產之價值。

(六)衝擊性 (Impact, Consequences)

當資訊安全事件發生時，對本所之資訊資產或業務營運造成損失或影響之嚴重程度。

衝擊性評估標準/等級對應表如下所示：

衝擊性	衝擊評估標準	數值
無或微	➢ 資訊安全事件發生時，對資產並不會造成損失或僅造成極小的損失。 ➢ 對於業務執行沒有影響。 ➢ 可以立即完成復原。 ➢ 若持續發生且次數頻繁，對業務執行可能帶來潛在風險。 ➢ 非核心業務資料遭洩漏。 ➢ 發現業務資料或機敏資訊可能發生洩漏但未發生。 ➢ 非核心業務系統或資料遭竄改。 ➢ 發現業務系統或資料可能遭受非授權竄改但未發生。 ➢ 非核心業務運作遭影響或短暫停頓。 ➢ 發現業務運作可能遭受影響或潛在危險，但系統仍可正常運作。	1
低	➢ 資訊安全事件發生時，對資產會造成輕微的損失。 ➢ 對於整體營運或業務執行影響不大。 ➢ 造成的損害可能僅影響單一業務或系統。 ➢ 損失僅影響個人或少數幾人。 ➢ 可以由內部人員進行復原。 ➢ 修復或進行復原的措施可以在很短時間(1 小時)內完成。 ➢ 非屬機密級或敏感之核心業務資料遭洩漏。 ➢ 核心業務系統或資料遭輕微竄改。 ➢ 核心業務運作遭影響或系統效率降低，於可容忍中斷時間內回復正常運作。	2
中	➢ 資產機密等級誤判或機密性維護機制失能時，對資產本身或相關資產造成間接或輕微的影響。 ➢ 資訊安全事件發生時，對資產會造成較大的損失。 ➢ 對於本所數項業務營運或執行造成停頓。 ➢ 造成的損害可能影響多種業務、數個系統、多個部門或合作夥伴。 ➢ 復原的措施必須由專業人員才能進行。	3

衝擊性	衝擊評估標準	數值
	➢ 復原可能要數個小時到一天才能完成。 ➢ 可能造成人員遭遇危險或受到傷害。 ➢ 機密級或敏感公務資料遭洩漏。 ➢ 核心業務系統或資料遭嚴重竄改。 ➢ 核心業務運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。	
高	➢ 資產機密等級誤判或機密性維護機制失能時，對資產本身或相關資產造成直接且嚴重的影響。 ➢ 資訊安全事件發生時，對資產會造成嚴重的損失。 ➢ 對於本所多項業務營運或執行造成停頓。 ➢ 造成的損害可能影響全所或利益相關者。 ➢ 復原的措施僅能由外部特定專業人員才能進行或修復人員不易取得。 ➢ 復原無法於一天內完成。 ➢ 可能造成人員傷亡。 ➢ 機密資料遭洩漏。 ➢ 本所重要資訊基礎建設系統或資料遭竄改。 ➢ 本所重要資訊基礎建設運作遭影響或系統停頓，無法於可容忍中斷時間內回復正常運作。	4

(七)資訊安全事件發生機率 (Likelihoods)

係指因已存在之脆弱點未妥善處理,導致觸發威脅或因不可抗力之因素致使威脅發生，進而引起資訊安全事件發生之可能性。

可能性對應表如下所示：

可能性	評估標準	數值

可能性	評估標準	數值
無或微	➢ 無發生可能或不適用之情形。 ➢ 對於可預期之資訊安全威脅缺乏動機或能力不足以利用脆弱點造成資安事件。 ➢ 資訊安全事件因控制措施執行得當，有效降低脆弱點被利用，幾乎不可能發生。 ➢ 一年發生之次數約一次或不發生，或屬於天災無法預估其發生機率。	1
低	➢ 很少發生。 ➢ 對於可預期之資訊安全威脅具有動機但能力不足以利用脆弱點造成資安事件。 ➢ 資訊安全事件因控制措施執行得當，有效降低脆弱點被利用，致使威脅發生之可能性極低。 ➢ 一季發生之次數約一次，或一年一次以上 四次以下。	2
中	➢ 偶爾發生。 ➢ 對於可預期之資訊安全威脅具有動機且有能力利用脆弱點造成資安事件。 ➢ 已採行部份資訊安全措施，脆弱點仍未被有效降低或減少，致使威脅發生之機率略高。 ➢ 一個月發生之次數約一次，或一年四次以上十二次以下。	3
高	➢ 經常發生。 ➢ 對於可預期之資訊安全威脅具有動機且有能力利用脆弱點造成資安事件。 ➢ 未實行資訊安全措施或安全措施無效，脆弱點仍未被有效降低或減少，致使威脅發生機率偏高。 ➢ 一週發生次數一次以上，或一個月發生數次。	4

(八)可接受風險值

資訊資產之最低風險容忍度。

(九)剩餘風險 (Residual Risk)

在採用相關控制措施後尚存在之風險，由風險擁有者確認核准。如無法接受者，需另提改善方式或由風險擁有者核准。

三、作業程序

(一)資訊資產評鑑

依據識別出本所業務中之關鍵業務所產出之資訊資產之結果，列入後續風險評鑑使用。

(二)風險評鑑

1.風險分析

由資通安全分組協助各風險擁有者針對可能面臨之資訊安全事件風險進行分析，同時參考衝擊與可能性並填寫營運衝擊分析表第三部分。

2.風險評估 (綜合風險評估)

依據所建立的關鍵營運項目以及相對應資訊資產清單之關鍵營運流程價值，由資通安全分組協助各風險擁有者計算各項資訊資產之綜合風險值，其公式如下：

綜合風險值=關鍵營運流程價值 * 衝擊性(數值) * 事件發生機率(數值)將上述計算結果完成「營運衝擊分析表」。

(1) 確認風險評估結果

「營運衝擊分析表(ISMS-04-12-TPC)」由本所資通安全分組確認。

(2) 風險管理

A. 決定可接受風險值

由本所資通安全分組依據「營運衝擊分析表」，並就以下準則，提出資訊資產可接受風險值之建議，並陳報本所資通安全工作小組召集人核定。

◆ 綜合風險值統計結果≦880，且(無衝擊性或可能性≦2 者)，無須進行任何管理措施規劃。

◆非上述者必須進行風險處理及管理措施規劃。

B. 選擇控制措施

◆針對各項資訊資產，若其綜合風險值大於可接受風險值，風險擁有者得參考 ISO 27001 標準，選擇適當控制措施，提出「風險改善計畫表」之建議。

◆資通安全分組應就前開「風險改善計畫表」予以評估，提出可行之風險改善建議，由風險擁有者確認核准，並陳報本所資通安全工作小組召集人。

C. 風險改善狀況的執行與監控

各單位應落實執行風險改善計畫，由資通安全分組予以監督並追蹤控管其實施狀況及成效。

(三)複核

1.檢討風險評鑑方法

資通安全分組得定期（每兩年）或不定期檢討本風險評鑑方法之有效性與適用性，包括可接受風險值、威脅及弱點評估表之項目，依本所資通環境與作業之安全需求作適當調整。

2.定期或不定期辦理風險評鑑

(1) 每年至少應執行 1 次風險評鑑。

(2) 當系統有重大異動或作業環境改變時應執行風險評鑑。

(3) 當有新增關鍵服務時，應執行風險評鑑。

陸、人力資源安全管理暨資通安全教育訓練

一、人員進用之評估

(一)進用之人員安全評估由用人單位、政風室與人事室負責，如其工作職責須使用處理敏感性、機密性等資訊者應經適當的安全評估程序。

(二)人員進用之安全評估參考項目如下：

1.個人性格。

2.申請者之經歷。

3.學術及專業能力與資格。

~~4.~~人員身分之確認。

二、人員安全管理與訓練

(一)本所新進人員於報到時，需依照人事室規定填寫「就職報告單(ISMS-04-20-TPC)」，並簽署「保密切結書(ISMS-04-21-TPC)」。「保密切結書(ISMS-04-21-TPC)」涵蓋期間包括從業期間與離職後，均有保密之責任，任何因未遵守本管理程序導致之資通安全意外事件將依相關規定懲處。

(二)本所資訊業務委外服務駐點之廠商人員，於接觸本所資料前必須完成簽署保密切結書(ISMS-04-21-TPC)，切結遵守本資通安全管理規範。

(三)本所編制內人員及約僱、臨時之非編制內人員到職時，須依照人事室規定填寫「就職報告單(ISMS-04-20-TPC)」並附「大內網系統帳號申請暨變更聯繫單(ISMS-04-22-TPC)」、「電子公文系統帳號申請表(ISMS-04-23-TPC)」，由資訊室核准開立帳號後，始能使用權責業務系統。

(四)本所編制內人員及約僱、臨時之非編制內人員離職或調任其他機關時，須依照人事室規定填寫「離職手續單(ISMS-04-24-TPC)」並附「大內網系統帳號申請暨變更聯繫單(ISMS-04-22-TPC)」、「電子公文系統帳號申請表(ISMS-04-23-TPC)」，由資訊室撤銷帳號核章後，以完成離職程序。

(五)使用者職務異動時，須依總局之規定保留其帳號，並將權限全部清除後，重新申請該帳號之權限，經資訊室核可後，始完成職務異動程序。

(六)本所新進人員應由業務單位實施適當的系統操作訓練。

(七)人事室每年度應對員工施以個人資料保護法等相關法令之宣導、訓練或講習，提升其法治觀念。

三、使用者資通安全教育訓練

(一)資通安全責任分級規定訓練需求

本所具政府機關（構）資通安全責任等級分級作業規定為 B 級機關，

1.每年資安人員(資訊人員)至少 1 人次須接受 12 小時以上資安專業課程訓練或資安職能訓練。

2.每年一般使用者與主管至少須接受 3 小時資安教育訓練(一般主管、資訊人員/資安人員、一般使用者)

(二)資通安全教育訓練

資通安全教育訓練由人力資源安全管理分組統籌並委由資通安全分組定期或不定期負責推行，訓練內容應考慮以下各項：

1.資通安全分組每年應規劃資訊安全訓練課程，填報「年度資通安全教育訓練計畫表(ISMS-04-06-TPC)」，若有重大資安議題發生時，應適時評估增加必要之訓練課程。

2.應定期或不定期對本所編制內人員及約僱、臨時之非編制內人員進行資通安全教育及訓練，促使所有人員瞭解資通安全的重要性，各種可能的安全風險，以提高所有人員資通安全意識，促其遵守資通安全相關規定。

3.本所員工應不定期參加外單位辦理之專業資通安全課程，以提升資通安全知識及警覺意識。

4.應以人員角色及職能為基礎，針對不同層級的人員，進行適當的資通安全教育及訓練；資通安全教育及訓練的內容應包括：資通安全管理規範、資通安全法令規定，以及如何正確使用資訊科技設施之訓練等。

5.辦理資通安全訓練時，資通安全分組得視需要規劃學習評量(如隨堂測試或問卷)，以評估訓練之成效。

6.本所辦理之各項資通安全教育訓練，得視實際需要要求委外廠商人員參加，若有特殊資通安全議題需要，得對委外廠商人員單獨辦理。

7.辦理資通安全訓練時，資通安全分組人員應備妥「資通安全教育訓練簽到表(ISMS-04-31-TPC)」，並編號控管。

8.人力資源安全管理分組每年須彙整該年度之教育時數，確保人員訓練之時數符合資通安全責任分級之規定及總局對於資通安全教育之訓練時數，將整體之訓練時數及成效，提管理審查會議，並回報總局。

(三)對員工進行資通安全及資訊系統使用之教育及訓練之政策，除適用所屬員工外，對機關外部的使用者亦適用。

柒、實體及環境安全管理

一、電腦機房之管制

(一)電腦機房門禁管制：

1.電腦機房應設置自動上鎖門禁管制，解鎖權限設定為資訊室機房工作人員，進出機房須用門禁卡解鎖，且門禁系統須紀錄刷卡時間及卡號，以管制資訊室人員進出。

2.其他人員不得擅自出入，其餘同仁如因工作需要進入機房時，須經資訊室有關主管同意，經許可後由資訊室人員陪同，並於「電腦機房進出登記表(ISMS-04-26-TPC)」登記，始得進入機房。

3.本所或總局委外之系統管理人員於進入本所機房前應事前提出申請，委外廠商於首次進入機房前應事前提出申請，由資通安全分組組長核准後，始得進出機房。委外人員進出入機房均應填寫「電腦機房進出登記表(ISMS-04-26-TPC)」，並由資訊室人員陪同進入機房。

4.其他機關如因作業需要進入本所機房，應先提出申請，並由資通安全分組組長核准後，由資訊室人員陪同，並於「電腦機房進出登記表(ISMS-04-26-TPC)」登記，始得進入機房。

5.貴賓於有關主管陪同下，須由資訊室人員引領方得進入參觀。

6.電腦主機及操作控制台除系統程式人員及值班操作人員外，非經資訊室有關主管指派或同意，不得擅自操作，如有違者將報請議處。

(二)機房環境之管理

1.人員進入機房依據本所規定應更換機房內部拖鞋,離開機房時，應將拖鞋歸位。

2.機房內嚴禁吸菸，亦不得攜帶飲料及食物進入機房。

3.定期執行清潔作業以維護機房整潔，清潔工作必須以吸塵器或拖把清理,禁止提水桶進入機房工作。且機房使用之清潔工具，不得用於其他場所。

4.機房內各種文具、報表、手冊、表單等應排列整齊，用完後歸定位，剩餘之廢棄物不得堆置於機房內。

5.機房使用之物品如磁帶、磁碟、報表紙或手推車等應放置於規定地點並貼立標記。

6.機房溫度應維持在18℃至25℃,相對濕度維持在30%至70%，本所資訊室指派機房輪值人員需每日於「三代公路監理系統機房工作日誌(ISMS-04-27-TPC)」記錄機房之相關環境數據。

7.機房依據總局之要求，應設置稽核環控警告裝置，於異常發生時能以簡訊及其他方式通知機房管理人員。

8.機房應設置監控攝影設備，24 小時監控機房之環境安全，至少包括機房門禁進出以及重要設備之監控攝影。監控攝影之錄影設備應設置防止他人未經授權存取或阻斷、中止運作之安全裝置，非必要不應置放於機房內部，以避免該設備被惡意阻斷或中止其監控功能。

9.設置符合機房專用之消防系統，並定點放置消防器材，機電維護廠商應定期檢測各項感應器。

10.機房內應設置停電照明設備。

二、機房環境安全之維護

(一)機房輪值作業規定：機房輪值規定由資訊室依實際需要自行訂定。

(二)輪值人員職責：

1.注意各終端通信線路及作業狀況，並與各單位保持密切連繫。

2.監視主控台螢幕訊號，依指示操作，無法處理時，應立即向有關主管反應，予以適當處置。

3.隨時注意機房之溫度、濕度及防火措施之狀況。

4.維護機房、配電室、電腦與週邊設備之環境清潔。

5.應定期實施防治鼠害及其他蟲害等措施，以保護電纜、電線及機器設備。

6.每天應檢查電腦有關機器設備之使用狀況並記錄於「三代公路監理系統機房工作日誌(ISMS-04-27-TPC)」。

7.廠商進行定期維護，應作成維護紀錄，每月整理陳報主管核閱。

8.電腦系統操作，除系統程式人員及值班操作人員外，應禁止其他人員操作。

9.機房各項作業及狀況處理應詳實記錄於「三代公路監理系統機房工作日誌(ISMS-04-27-TPC)」，並定時陳核。

三、機房設備及檔案之存取控制

(一)非經本所許可不得攜帶電腦設備進入機房，廠商或人員需要攜帶電腦設備進入機房作業，應事前取得資通安全分組之核可後始得辦理。

(二)機房應設置保護機制(如門禁管制)以避免人員任意使用非權責業務之伺服器或設備，人員進入機房作業時應注意不得操作非權責業務相關之系統或設備。

(三)伺服器使用完畢後必須即刻登出或鎖定系統，以避免遭受不當或

未授權之使用。所有機房伺服器設備，應設置自動登出或螢幕保護之控管措施。

(四)電腦磁片、隨身碟及光碟等可攜式媒體進入機房前，須經機房輪值人員掃毒確認安全合格後，方可攜入機房。

(五)除需對系統必要之直接檢修或維護，其餘維修均應移至電腦機房外進行，重要主機維護作業，如由外部人員進行，應由機房輪值人員全程陪同。

(六)機房設備如需移出機房，應由機房輪值人員於移出前經資訊室主管核可後始得辦理，機房設備如存放敏感資訊者，應於移出前由資通安全分組人員將設備之資料清除或移除後始得放行。

四、緊急狀況處理措施

任何狀況造成服務中斷時，應依總局之「公路監理系統服務中斷通報作業要點」辦理。

五、安全維護

(一)主機系統：資訊室應本於權責訂定相關作業規定，並督導操作人員定期執行、演練。

(二)空調及供電系統：

1.電腦機房應有獨立的空調系統，並應定期維護檢測。

2.機房輪值人員應於系統維護後，於「三代公路監理系統機房工作日誌(ISMS-04-27-TPC)」進行記錄，並留存廠商維運資料

3.供電設備應有切斷所有電腦設備電源的裝置，其裝設位置應能便利操作人員緊急狀況時處理。

(三)消防系統：

1.消防系統應有自動偵測及警報之功能。

2.消防系統應採用滅火效果佳、不燃性、不導電、不污損等之滅火系統。

3.資訊室人員均應接受良好的消防訓練，熟悉各項消防器材設備的使用及火災時應採取的行動。

(四)防盜系統：

1.防盜偵測系統應能在保護範圍內感應而觸發警報。

2.警報器於非正常工作時間內，應自動進入警戒狀況；如須臨時加班作業，應由資訊室主動協調駐警隊或保全人員配合辦理。

(五)維護：機房所有設備應定期維護保養。

捌、網路安全與網站資料管理

一、網路及系統安全管理規定

本所依據資通安全責任分級為 B 級單位，依規定應對於系統及主機進行:

(一)每年至少辦理 1 次網站安全弱點檢測

(二)每 2 年至少辦理 1 次系統滲透測試

(三)每 2 年至少辦理 1 次安全性檢測

二、網路安全管理規定

(一)網路安全規劃與管理

1.網路安全規劃

(1) 第三代公路監理系統(M3)、大內網設備及人員設備均須依總局之規範，全面使用防毒軟體，即時更新病毒碼，且須定期對電腦系統及資料儲存媒體進行病毒掃描。

(2) 定期執行各項系統漏洞修補程式。

(3) 定期檢討及執行網路安全控管事項。

2.網路服務之管理

(1) 設置網路系統管理人員負責網路管理。

(2) 如網路系統偵測出使用者為非合法授權時，系統管理人員應立即撤銷其使用者帳號；離（休）職人員應依機關資通安全規定及程序，取消其存取系統之權利。

(3) 網路系統管理人員除相關法令或機關規定外，不得閱覽使用者之私人檔案；但如發現可疑的網路安全情事，網路系統管理人員得依授權規定檢查檔案。

(4) 網路系統管理人員未經使用者同意，不得增加、刪除及修

改私人檔案。如有特殊緊急狀況，須刪除私人檔案，應事先知會檔案擁有者。

(5) 本所同仁如有發現任何網路安全事件，應即時向資通安全分組反應，由網路系統管理人員處理，並向資通安全分組組長報告；如果事情無法獨立處理，需迅速連絡相關廠商或通報總局。

(6) 網路系統管理人員不得新增、刪除、修改 LOG 資料檔案，以避免違反資通安全事件發生時，造成追蹤查詢的困擾。

3.網路使用者之管理

(1) 員工使用網路資源，需恪遵授權的權限。

(2) 員工應主動了解本所網路安全相關規定，並確實瞭解其應負的責任。

(3) 員工不得將自己的登入身份識別與網路通行碼交付他人使用。

(4) 員工不得以任何方法竊取他人的登入身份識別與網路通行碼。

(5) 員工不得以任何儀器設備或軟體工具竊取網路之資訊。

(6) 員工不得在機關設備建置色情文字、圖片、影像、聲音等不法或不當的資訊，亦不得在網路散播。

(7) 員工不得發送騷擾他人電子郵件，亦不得發送匿名信，或偽造他人名義發送電子郵件。

(8) 員工不得以任何手段蓄意干擾或妨害網路系統的正常運作。

(9) 非本所員工需經授權後才得使用網路及電腦資源，並須遵

守員工使用網路之一切規定。

(10) 儲存機密性及敏感性資料之主機或伺服器，應防制非法使用者假冒合法使用者身分登入主機，進行偷竊、破壞等情事。

4.軟體使用與控制

(1) 員工不得經由網際網路下載非授權軟體使用，若需要下載授權軟體，亦應注意預防電腦病毒感染。

(2) 員工不得使用來路不明之軟體，亦不得測試來路不明之軟體，以免引入「木馬」。

(3) 員工於網路下載軟體使用，應進行掃描病毒，以確定下載軟體安全。

(4) 員工應全面使用防毒軟體並即時更新病毒碼。

(5) 員工應隨時注意有關病毒最新資訊公告。

5.網路資訊之管理

(1) 對外開放的資訊系統所提供之資料內容，由各業務單位決定其適當性，並協調電腦系統管理人員作安全權限之設定。

(2) 機密性及敏感性的資料或文件，不得存放在對外開放的資訊系統中。

(3) 對外開放的資訊系統，如存放民眾申請或註冊的私人資料檔案，應加密處理，並妥善保管。

(二)電子郵件之安全管理

1.禁止以遠程終端機模擬形式開啟電子郵件。

2.禁止開啟自動轉信功能，防止有心人士利用郵件伺服器做非法信件的轉寄。

3.對於不明寄件者寄來之郵件勿任意開啟，避免被植入木馬或病毒。

(三)網站之安全管理

1.網路設備備援

(1) 網路設備均應使用不斷電設備之電源，以防止不正常斷電影響業務正常運作。

(2) 應規劃二條專線，作為網際網路之相互備援，以負載平衡模式運作，使網際網路服務不中斷。

2.網路入侵之處理

如發現網站遭入侵，處理事項如下：

(1) 非必要不應關閉該主機，以確保相關入侵證據不被破壞。

(2) 非必要不應登入該主機，以避免重要權限帳號遭側錄。

(3) 關閉防火牆通道及本機網路連線或以線路插拔方式移除相關連線。

(4) 以安全之方式備份被入侵主機當時之系統，作為日後檢驗之用。

(5) 檢視被入侵之程度，決定善後之方式。

(6) 全面檢討網路安全措施，以防禦類似入侵與攻擊。

三、網站資料管理規定

(一)網站網頁資料維護分工原則

1.網頁檢視：本所各課室網頁資料應指派專人管理，每月定期或

不定期檢視網頁資料及表格內容，資料新增或異動時應依照作業程序辦理,並隨時保持最新資料,以免提供過期或錯誤資訊。

2.資料提供：由各課室專人負責資料之蒐集、更新及彙整，並於網頁製作完成後進行必要之檢視與校對。

3.網頁製作：由資訊室負責靜態網頁製作；暫態網頁資料更新(如各課室最新消息公告),由各課室網頁專人藉由系統後臺管理，負責所屬課室相關頁面更新。

(二)靜態網頁資料上/下網之作業程序

1.檢視網站資料

(1) 各課室網頁檢視人員，每月至少檢視相關業務之網站資料一次，並填寫「網站內容更新檢視單(ISMS-04-28-TPC)」陳報課室主管簽核，簽核後存於各課室，於業務檢查時進行查核。

(2) 各課室承辦人因作業程序變更或網站資料有疑慮時，應立即檢視相關業務網站資料。

2.靜態網頁內容更新：靜態網頁更新由資料提供單位負責將更新資料（含書面資料及電子檔）彙整，並填寫「電腦業務聯繫單(ISMS-04-29-TPC)」，提供網頁製作單位更新網頁內容；另欲刪除資料，辦理下網作業時亦同。

3.靜態網頁製作：更新靜態網頁由資訊室負責。

4.資料校對：網頁內容由資料提供單位線上檢視或列印校對。

5.靜態網頁上／下網：由資訊室負責靜態網頁製作上/下網。

6.本程序中各單位提供之電子檔,若為文字或表格資料應以 Word 或 Excel 檔案相容格式提供，並於摘要資訊加註服務分類，其

他視網頁展現需求協同資訊室訂定。

7.資料提供單位之承辦人核對無誤後，將「電腦業務聯繫單(ISMS-04-29-TPC)」陳報資訊室主管簽核，並存於資訊室。

(三)暫態網頁資料上/下網之作業程序：

1.檢視網站資料：同靜態網頁檢視流程。

2.暫態網頁內容更新：由各課室網頁專人藉由系統後臺管理，負責所屬課室相關頁面更新。

3.暫態網頁製作：由各課室專人藉由系統後臺製作。

(四)為鼓勵各課室網頁檢視人員及承辦人積極主動檢視及更新網頁內容，確保本所網頁保持最新之資料狀態，凡執行網頁內容更新績效良好者，得依相關程序予以敘獎。

玖、系統存取控制

一、資訊系統存取控制規定

(一)有關 M3 及大內網相關系統,目前已完成單一簽入(SSO)管控方式，人員對於該系統之存取管控，由 SSO 之技術機制進行管制。其他非 SSO 管制之相關系統或非由總局以 AD server 進行管制之系統應依據本存取控制程序進行管制。

(二)應將業務系統之存取控制需求，明確告知系統服務提供者，以利其執行及維持有效的存取控制機制。

(三)業務應用系統擁有者，應訂定系統存取控制政策，並明定使用單位及使用人員的系統存取權利。

(四)資訊系統存取控制規定研擬，應考量事項如下：

1.個別業務應用系統安全需求。

2.資訊傳佈及資料應用之名義及授權規定。

3.相關法規或契約對資料保護及資料存取規定。

二、使用者存取管理

(一)使用者註冊管理

1.各資訊系統使用單位,須向資訊室提出系統使用人員註冊申請，交由各系統負責人審核處理。

2.各資訊系統負責人於受理業務使用人員註冊申請時，須考慮下列事項：

(1) 公路監理電腦使用權限,由各業務使用單位課室主管核定，經資訊室主管確認後，進行權限建立或異動作業。

(2) 權限的取得應切合業務需要，且符合資通安全政策及規

定。

(3) 系統使用者尚未取得正式授權前，資訊服務提供者不得對其提供系統存取服務。

3.使用者帳號管理人員應做事項：

(1) 應建立及維持系統使用者註冊資料紀錄，以備日後查考。

(2) 使用者離（休）職時，應儘速註銷其系統存取權利。

(3) 使用者調整職務時，應依總局之規定保留其帳號並調整其系統存取權限。

(4) 應定期檢查及取消閒置不用的識別碼及帳號。

(5) 閒置不用的識別碼，不應重新配賦給其他的使用者。

(二)系統存取特別權限管理

1.帳號管理人員應針對使用者業務性質，賦予不同存取權限，並分開造冊管理。

2.對於擁有特別存取權限的使用者，帳號管理人員應隨時瞭解記錄其對系統使用情形。

3.帳號管理人員如有必要賦予使用者系統存取特別權限，應依下列的授權程序管理：

(1) 應確認系統存取特別權限事項，例如作業系統、資料庫管理系統、以及須賦予系統存取特別權限的人員名單。

(2) 應依執行業務需求，視個案逐項考量賦予使用者系統存取特別權限；系統存取特別權限配賦，應以執行業務及職務所必要者為限。

(3) 應建立申請系統存取特別權限授權程序，並只能在完成正

式授權程序後，才能配賦給使用者；另外，應將系統存取特別權限之申請及授權資料建檔，以備日後查核。

(三)使用者通行碼管理

1.使用者若遺忘通行碼，須依新申請使用者程序，申請清除通行碼。

2.應以書面約定要求使用者善盡保護個人通行碼之責任；如屬於群組軟體使用者，應確保工作群組的通行碼，僅限群組成員使用。

3.系統如經評估須建立更高等級的安全機制，可利用電子簽章等安全等級更高的存取控制技術。

(四)系統存取權限之清查、檢討、評估

1.為有效控管資料及系統存取,帳號管理人員應定期清查、檢討、評估使用者存取權限。

2.系統帳號及存取權限清查、檢討、評估，每年應於內部稽核前完成，內部稽核人員應進行帳號存取權限之管理稽核。

3.系統存取特別權限之清查、檢討、評估，應每六個月執行一次。

4.應每六個月檢討系統存取特別權限核發情形，防止有人未經正式的授權程序取得特別權限。

三、系統存取之責任

(一)使用者通行碼管理

1.使用者帳號採單一帳號原則，已整併使用 SSO 相關系統，每一人員進入本所，由資訊人員協助申請大內網帳號，並於 M3 相關系統權限申請介面依權責開立 M3 帳號及權限。

2.使用者通行碼之配賦、管理要點如下：

(1) 以嚴謹的程序核發通行碼，明確規定使用者應負的責任。

(2) 個人應負責保護通行碼，維持通行碼的機密性。

(3) 應避免將通行碼記錄在書面上，或張貼在個人電腦或終端機螢幕或其他容易洩漏之場所。

(4) 當有跡象足以顯示系統及使用者通行碼可能遭破解時，應立即更改通行碼。

(5) 使用者通行碼的長度最少八位且需以大小寫字母、數字及符號混合組成。

(6) 應儘量避免以下列事項作為通行碼：

- 年、月、日等時間資訊。
- 個人姓名、出生日、身分證字號或汽機車牌照號碼。
- 機關、單位名稱或簡稱、識別代碼或是其他相關事項。
- 電話號碼。
- 使用者識別碼、使用者姓名、群體使用者之識別碼或是其他系統識別碼。
- 重複出現兩個字以上的識別字碼。
- 以全部數字或是全部字母組成通行碼。
- 英文或是其他外文字典的字。
- 電腦上使用者的名字。
- 電腦主機名稱、作業系統名稱。
- 地方名稱。
- 專有名詞。
- 任何人的名字。

(7) 應每三個月更新一次通行碼，並應儘量避免重複或循環使用舊的通行碼。

(二)暫時不使用或無人看管設備之安全管理

1.當作業結束時應完全登出電腦系統，不宜只關閉電腦系統或是端末機。

2.當個人離開辦公位置或個人電腦、終端機不使用時，重要資訊不得閒置於桌面上，應保持螢幕淨空或使用鍵盤鎖或其他控管措施保護個人電腦及端末機的安全。

四、網路存取之安全控制

(一)網路服務之限制

1.本所之網路依據大內網及 M3 網路技術管制方式進行管控。

2.其他網路使用，本所網路系統管理者須確實了解網路使用申請者的需求，具以建置新的網路使用者帳號及通行碼，並賦予正確的網路使用權限。

3.本所網路使用者應在授權範圍內存取網路系統服務事項。

(二)強制性的通道

1.對使用本所網路系統的使用者端末機或電腦之連接線路，應適當加以控制（例如:建立強制性的通道、連接於本所內部網段、非軍事區網段、或外部網段等），以減少未經授權存取系統或電腦設施之風險。

2.建立強制性的通道應考量的安全措施如下：

(1) 指定專線及電話號碼。

(2) 自動將通訊埠連上特定的應用系統及安全通道。

(3) 限制使用者只能選擇特定的路線。

(4) 防止無限制的網路漫遊。

五、電腦系統之存取控制

(一)登入程序

除 M3 及大內網相關網段依據技術管控機制登入，於其他網段登入本所任何電腦系統，均須作身分鑑別，其查驗程序如下：

1.只有在完成所有的登入資料輸入後，系統才開始查驗登入資訊的正確性。

2.應限制系統登入不成功時可以再嘗試的次數，原則上以三次為原則，系統並應：

(1) 記錄系統登入不成功的事件。

(2) 在使用者嘗試登入系統失敗後，應強迫必須間隔 15 分鐘之後才能再次登入。

(3) 應中斷資料連結作業。

3.系統登入被拒絕後，應立即中斷登入程序。

4.應限制系統登入程序的最長及最短時間，如果超出時間限制，系統應自動中斷登入。

(1)於成功登入系統後，亦應設定最高「閒置時間」，若使用者於閒置時間內，未有繼續使用電腦的情形，應予自動鎖定(如螢幕保護機制，且需以通行碼解開)。

(二)使用者身分辨識

1.本所應對使用者核發使用者識別碼，以明責任歸屬；使用者識別碼不應顯示任何足以辨識使用者特別權限的訊息，例如：顯示其為管理者或監督者。

2.只有在例外的情況下，可為整體效益，經權責主管人員之同意，核發群組內人員共享同一使用者識別碼。但應採取額外的安全

控制措施，明確程序使用者的責任。

(三)端末機作業時間限制

1.安置在高風險地區，且不經常使用的端末機，或是對高風險的系統提供服務，須限定其作業時間，以防止未經授權的人員存取系統。

2.須設定系統的作業時間限制，包括間隔一定時間後自動清除螢幕上的資訊，以及依據事前訂定的時間限制，結束應用系統及網路通信。

(四)連線作業時間控制

1.有高風險的應用系統，應限制使用者的連線作業時間。

2.對處理機密及敏感性系統的端末機，應限定連線作業及網址連線時間，以減少未經授權存取系統的機會。

3.限定連線作業時間的措施如下：

(1) 只允許在設定的時間內與系統連線。

(2) 如無特別延長作業時間的需求，應限制只能在正常的上班時間內進行連線作業。

(3) 應限制連線的網址。

六、應用系統存取控制

(一)資訊存取限制

1.應用軟體開發時，應依資訊存取規定，配賦應用系統的使用者（包括應用系統支援人員）與業務需求相稱的資料存取及應用系統使用權限。必要時需詳列組織架構，工作職掌，作業負責單位及作業負責人員之項目及其使用系統權限。其中包含使用

系統功能、使用資料檔案、及使用資料內容。並訂定使用該應用系統時機及處所。

2.資訊存取的控制措施如下：

(1) 應用軟體系統設計應以選單方式，控制使用者僅能使用系統的部分功能。

(2) 應用軟體開發應適當的編輯作業手冊，例如使用者操作手冊，需依不同分類之使用者製作不同操作程序操作手冊，以期限制使用者僅能獲知或取得授權範圍內的資料及系統存取資訊。

(3) 控制使用者存取系統的能力（例如限定使用者僅能執行唯讀、寫入、刪除或執行等功能），並於各系統文件中載明不當使用、超範圍使用或錯誤使用須負責任。

(4) 處理敏感性資訊的應用系統，系統輸出的資料，應僅限於與使用目的有關者，且只能輸出到指定的端末機及位址。必要時需控制連網時間、地點及離線時間、地點。

(二)系統公用程式安全管理

1.應嚴格限制及控制電腦公用程式使用。

2.電腦公用程式之安控措施如下：

(1) 設定使用者通行碼以保護系統公用程式。

(2) 將系統公用程式與應用系統分離。

(3) 將有權使用系統公用程式的人數限制到最小的數目。

(4) 應建立臨時使用公用程式的授權制度。

(5) 應限制系統公用程式可用性，例如變更公用程式的使用時

間授權規定。

(6) 應記錄系統公用程式的使用情形，以備日後查核。

(7) 應訂定系統公用程式的授權規定，並以書面或其他電子方式為之。

(8) 應移除非必要的公用程式及系統軟體。

(三)原始程式資源存取控制

1.對應用系統原始程式資料之存取，應建立嚴格的安全控制機制。

2.原始程式資源之存取控制，應考量下列事項：

(1) 應用程式原始碼資料庫，應與作業系統的檔案分開存放。

(2) 每一項應用程式原始碼，應指定一位管理人員。委外製作之系統不得直接授權廠商管理。

(3) 不應核發無限制存取應用程式原始碼之權限。

(4) 開發中或是維護中的應用程式，應與實務作業程式原始碼資料庫區隔。

(5) 應用程式原始碼資料庫更新，以及核發應用程式原始碼供程式設計人員使用，應由原始碼資料庫管理人員執行。

(6) 程式目錄清單應放置在安全的環境中。

(7) 應建立存取程式原始碼資料庫的稽核軌跡。系統管理人員須定期或不定期稽核，並將稽查報告陳報相關業務主管。

(8) 舊版的原始程式應妥慎典藏保管，詳細記錄使用的明確時間，並應保存所有的支援應用程式軟體、作業控制、資料定義及操作程序等資訊。

(9) 應用程式原始碼資料庫維護及複製，應依嚴格的變更控制程序進行。

(四)機密及敏感性系統之獨立作業

1.對機密及敏感性的系統，應考量建置獨立的或是專屬的電腦作業環境。

2.建置獨立的或是專屬的電腦作業環境，應考量的事項如下：

(1) 應由系統擁有者決定應用系統是否屬於機密或敏感性，並以書面記錄之。

(2) 機密及敏感性的應用系統，須在分享式的電腦環境中執行時，應界定其他須共享資源的系統項目，並經系統擁有者的同意。

七、系統存取及應用之監督

(一)事件記錄

1.系統管理人員應保留其系統記錄檔(system log)至少三個月，以為日後稽核調查及監督之用。

2.系統稽核軌跡應包括下列事項：

(1) 使用者識別碼。

(2) 登入及登出系統之日期及時間。

(3) 記錄端末機的識別資料或其位址。

3.若作業平台本身所提供之系統記錄檔的資料不足以作為稽核之用，須另行開發或購置進階之管理工具。

(二)系統使用之監督

1.各電腦系統之監督程序如下：

(1) 各應用系統負責人應將其所轄檔案之重要性，告知相關電腦系統管理人員，並討論各檔案存取權限。

(2) 各電腦系統管理人員依前項之結果，定期監控系統檔案之存取記錄（log）檔。

2.系統使用監督應考量事項如下：

(1) 系統存取失敗情形。

(2) 檢查系統登入的模式，確定使用者識別碼是否有不正常使用或是被重新使用的情形。

(3) 查核系統存取特別權限的帳號使用情形及配置情形。

(4) 追蹤特定的系統交易處理事項。

(5) 敏感性資源的使用情形。

(三)電腦作業時間校正

電腦系統負責人應定期校正電腦系統作業時間，以維持系統稽核紀錄的正確性及可信度，俾作為法律上或是紀律處理上的重要依據。

八、機關外部人員存取資訊之安全管理

(一)外部連線作業之風險評估

1.如開放外界與其連線作業，應評估可能的安全風險；如因業務需要，須與外界連線作業時，應先進行風險分析，決定採行應特別強化的資通安全項目。

2.存取資訊系統之風險分析，應充分考量下列事項：

(1) 第三者需要存取的資訊類型及資訊的價值等。

(2) 第三者採行的資通安全措施及安全保護水準。

(3) 第三者之存取對本機關資訊架構可能產生的安全風險及影響。

(4) 第三者如使用 USB 等行動硬碟存取本所之業務資訊，該行動硬碟須以獨立之個人電腦進行掃毒後始可為之。

3.第三者欲存取本所資訊者，需簽訂資安協議，並確定執行適當的安全措施，且應遵守本所網路連線相關規定。

4.開放外界連線系統存取時，不得直接存取本所內部網路之任何電腦資源，若有必要應採透過電腦設備上之特殊程式，間接存取內部網路電腦系統資源。

5.各系統維護廠商不得以遠端登入的方式遂行系統維護之作業。

(二)第三者存取之安全契約

1.第三者欲存取本所資訊設施，應於實施前，簽訂正式的契約或協定，俟契約或協定生效後始能提供存取服務。

2.契約或協定內容應規定第三者須遵守之資通安全規定、標準及必要的連線條件。

3.與第三者簽訂安全契約參考條款如下：

(1) 第三者應遵守的一般性資通安全規定。

(2) 第三者可以使用的系統存取方法，以及使用者識別碼及通行碼的管理規定。

(3) 每一項資訊系統的使用作業說明。

(4) 應要求第三者建立及維持具系統存取權限的名單。

(5) 資訊系統開放連線使用的期程及時間。

(6) 簽約單位應負的安全保密責任。

(7) 保護資訊資產的作業程序。

(8) 第三者應負的法律責任，例如個人資料保護法相關規定。

(9) 監督及撤銷使用者系統存取權限之權利及相關規定。

(10) 硬體、軟體建置及系統維護的責任。

(11) 稽核第三者是否履行契約責任的權利。

(12) 智慧財產權及資訊公開的限制。

(13) 契約終止時，可確保機關資訊及資產安全回收或銷毀措施。

(14) 必要的實體保護措施。

(15) 對使用者進行操作程序及安全教育訓練之相關規定。

(16) 防止電腦病毒散佈之措施。

(17) 使用者存取系統之授權規定及程序。

(18) 通報及處理資通安全事件之作業程序。

(19) 其他下包廠商及相關參與者的責任關係。

壹拾、新科技與便民設備管理

一、傳真或影印設備管理：

(一)本所人員於點收傳真或影印設備時，應確認該設備是否內含硬碟等儲存元件。

(二)內含硬碟等儲存元件之傳真或影印設備交付時，本所點收人員應請廠商提供清除內含硬碟等儲存元件資料之操作步驟。

(三)內含硬碟等儲存元件之傳真或影印設備送修或報廢時，應先清除設備內之儲存資料，並於「資產異動申請單(ISMS-04-03-TPC)」內註明已清除後再行送修或報廢。

二、便民使用之輸出入設備管理：

(一)便民設備之設立(如 Kiosk)，應避免於公眾場所使用，如因場地因素只能於公眾場所設置，應規劃民眾動線及等候區。

(二)舉凡所有能連進所內網路(如 M3 或大內網)之便民設備，應避免有線網路接頭暴露於外部之公眾區域。

(三)如便民設備僅能設立於公眾場所，必須設置監控或網路無可另行外接之防護措施。

(四)公眾區域列印設備之使用，應設立設備故障回報窗口，以免個資安全議題之發生。

(五)iTaiwan、監理服務網等便民之網路服務應採獨立之網路線路運行，禁止與所內之 M3 或大內網網段相通。

壹拾壹、櫃檯作業與文檔管理

一、目的

為使本所民眾服務人員之櫃台作業與紙本文件歸檔、銷毀作業，能符合資通安全管理之要求，特制定本管理辦法。

二、範圍

(一)本所櫃檯服務及管理人員。

(二)本所檔案管理人員。

三、權責

服務管理分組：制定本櫃檯作業與文檔管理辦法，督導櫃檯作業與管理人員、文件檔案/資料管理人員，避免資通安全人為疏失。

四、作業規範

(一)櫃檯作業區

1.櫃檯作業應以實體櫃檯隔離之方式與民眾區隔。

2.與民眾之晤談應於櫃檯作業區外或於會客區域內進行。

(二)櫃檯服務及管理人員

1.使用電腦作業時，應符合本所網路安全管理規定。

2.除業務之需求，不應將作業中之電腦畫面交由民眾觀看並嚴禁將電腦交由民眾自行使用。

3.電腦當機時得重新再次開機，如依舊無法正常作業，應通知資訊室人員處理。

4.掃描後之紙本文件應妥善保存，並於每日下班前交於文件檔案/資料管理人員進行歸檔作業。如作業當日因故無法進行歸檔作

業，應將文件置於儲物櫃內並上鎖。

5.業務服務中斷時，應依總局頒布之「公路監理系統服務中斷通報作業要點」處理。

6.暫時離座時應登出作業之系統，並將螢幕進入保護模式，有關民眾之個資紙本文件資料應適當隱藏(例如以覆蓋方式)後始可離開。

7.長時間離座時應登出作業之系統後關機，並將桌面淨空。

(三)紙本文件歸檔儲存區

1.紙本文件載體上應紀錄歸檔日期、保存期限或可銷毀日期。

2.紙本文件進出歸檔儲存區均應填寫「儲存保管銷毀清冊(ISMS-04-30-TPC)」。

3.除於歸檔儲存區執行作業之人員外，其餘人員進出歸檔儲存區均應填寫「資料室進出登記表(ISMS-04-25-TPC)」。

(四)紙本文件檔案管理人員

1.紙本文件歸檔時，應由紙本文件檔案/資料管理人員填寫「儲存保管銷毀清冊(ISMS-04-30-TPC)」，並詳實紀錄歸檔日期及紙本文件類別。

2.紙本文件檔案/資料管理人員應每年至少一次檢核保存期限或可銷毀日期。

(五)銷毀作業

1.紙本文件銷毀前，檔案/資料管理人員應填寫「儲存保管銷毀清冊(ISMS-04-30-TPC)」，並紀錄銷毀日期及紙本文件類別。

2.紙本文件檔案/資料管理人員應隨同銷毀作業廠商進行銷毀作

業，並取得銷毀作業廠商之相關銷毀作業文件。

壹拾貳、營運持續運作之管理

一、依據

依據總局全組織管理之組織規定，擬定本所營運持續運作管理規定。

二、範圍

(一)本所所屬人員、設備及各應用系統資訊。

(二)關鍵性業務為提供便捷完善之公路監理服務，並配合環境變遷、相關法令更新、組織經營障礙及人員之變更而更新。

(三)加強各項專長在職訓練，並落實職務代理人制度，以保持各項業務之持續推動。

三、緊急應變

(一)資料備份、存放與回復

1.公路監理系統、公文系統：由總局進行資料備份、存放與回復。

2.個人電腦重要資料：由同仁定期自行進行備份。

3.其他應用系統：由各系統負責人定期進行備份。

(二)天然災害應變

1.火災應變：

(1) 本所機房裝置配有消防系統，遇火災發生時視火災急迫狀況，得先行解除警報，以免消防逕自噴灑，破壞相關設備；遇大火已漫延無法撲滅時，則再依手動方式啟動消防噴灑撲滅之，有關消防設備之使用應舉辦相關教育訓練，操作人員均應能熟悉操作。

(2) 火災發生時應立刻關閉電源開關，設法移除燃燒物或使用滅火器撲滅火苗；滅火器之使用，除非情況之絕對需要，

儘量以避免對電腦設備直接噴灑為原則。

(3) 易燃物品及相關設備、媒體應即時移離，並向長官報告請求支援。

2.震災應變：

(1) 遇有強烈地震發生，應依震災逃生法則尋求掩避，如狀況稍有紓解時即進行緊急關機，逃離現場至安全地帶。

(2) 地震發生後，機房輪值人員應立即檢視機房各項設備，對於電源線路應小心查察，並將檢查狀況登錄於「三代公路監理系統機房工作日誌(ISMS-04-27-TPC)」，有異狀時即刻排除或報請有關人員修護。

3.其他災變：應先視發生狀況採取適當應變措施，並逐級陳報。

(三)人為破壞應變

1.人員闖入：

(1) 機房設有門禁管制，如遇有陌生人員意圖進入機房，應即刻予以查問其來意，引導至正確場所。

(2) 如有來意不善人員闖入，則應立即通報主管轉請駐警隊或保全人員派員前來處理。

2.網路入侵

(1) 伺服器主機重要資料應即時備份，如發現有駭客侵入，應立即報告資訊室主管並將該主機先行隔離，隨即展開執行檢查與回復作業；事後應即時檢討改進並將處理情況依規定逐級陳報。

(2) 應運用相關網路監控軟體不定期監控本所網路使用概況，遇有疑似駭客入侵時，應運用有關軟體予以監控、追踪、

查察，必要時得以予以斷訊，並將入侵情形依資通安全通報流程向總局陳報並採取應變措施。

3.病毒風暴

(1) 如有因病毒事件造成網路風暴，應立即運用本所之防毒軟體進行解除病毒處理，設法排除網路障礙恢復正常。

(2) 如無法自行排除應緊急與合約廠商連繫尋求支援。

(3) 並依資通安全通報流程通報。

(四)災變破壞之應變與復原

1.如有上開災變發生，短期間資訊設備當機或資料漏失無法回覆正常，各業務系統負責人員應洽各業務單位相關作業人員，改採人工方式辦理，並將人工表單資料妥善保存，供設備修護完畢後補正資料之需。

2.操作單位應儘速進行故障排除，或請相關維護廠商即刻修護，必要時依維護合約規定,督促維護廠商調度相關資訊設備資源,或取回原先備份資料進行回儲作業，以回復至當機前之狀況。

3.回復時間視資料或設備毀損情況而定，概分下列幾種情況：

(1) 資料檔案輕微損害：作部分資料回復，約只需 5 分鐘至 30 分鐘左右。

(2) 資料檔案嚴重毀損：作全部資料回復，約需 1 至 2 小時左右。

(3) 機器硬體設備受損:視損害情形,約 30 分鐘至 8 小時左右。

4.設備與資料恢復正常後應盡快通知相關作業人員，檢查並補正漏失資料以便繼續作業，以免影響為民服務之績效。

(五)一般當機及服務中斷之應變

1.一般當機及服務中斷時，依下列情況處理之：

(1) 公路監理系統設備當機或中斷服務：

依總局頒布之「公路監理資訊系統服務中斷通報作業要點」辦理。

(2) INTERNET 服務中斷：

- 查明 INTERNET 中斷處並設法排除問題。
- 如屬網際網路中斷，應積極聯繫促其儘速修護。
- 與使用單位連繫，告知當機情況並預告修復時刻。
- 將處理結果登錄於「三代公路監理系統機房工作日誌(ISMS-40-27)」。

2.公文系統、M3 或其他應用系統設備當機或中斷服務：

(1) 則由相關系統負責人負責排除，如屬硬體問題應儘速要求維護廠商修護，必要時依維護合約要求維護廠商，調度相關資訊設備資源；如屬應用系統問題則需會同業務權責單位處理之。

(2) 請系統負責人與使用單位連繫，告知當機情況並預告修復時刻。

(3) 將當機狀況與處理結果登錄於「三代公路監理系統機房工作日誌(ISMS-04-27-TPC)」。

3.上開當機或中斷服務，權責單位應儘速確認當機損害及原因，判斷修護時間，設法進行故障排除，如中斷時間將超過 30 分鐘以上應即刻依資通安全通報流程通報，並告知各使用單位。

四、狀況通報

依「交通部公路總局臺北區監理所資通安全事件緊急應變計畫暨作業

處理程序」辦理

(一)本所機房主機之操作，如有安全異常事件除由值班操作員及時處理並向上反映外，應依規定登錄於「三代公路監理系統機房工作日誌(ISMS-04-27-TPC)」，並依資通安全通報流程通報。

(二)各應用系統異常存取或發生影響資通安全之事件，如有嚴重危害或具有時間急迫性時，由各系統負責人立即向上級反映，並依資通安全通報流程通報；如有駭客入侵、病毒風暴或嚴重影響資通安全事件發生時應向國家資通安全應變中心進行通報。

(三)通報類別：

1.任何狀況：

隨時報告各單位主管及資訊室

2.天然災害、危險品或人員闖入：

應先通知政風室、人事室、駐警隊或保全人員、秘書室、資訊室，如有資訊重大災害應向國家資通安全應變中心通報

3.網路入侵或病毒風暴：

應先向總局資訊室、政風室通報，再進行國家資通安全應變中心通報

4.當機或服務中斷：

依總局頒布之「公路監理資訊系統服務中斷通報作業要點」辦理。

五、演練

本管理辦法規定事項，應定期檢視相關程序，依不同程序實施各項演練，並檢討演練結果作為改善參考。

六、考核

所有人員均應依本管理辦法規定辦理，以確保資通安全工作，違反本管理辦法規定者，依情節予以適當處分，若協助組織服務機能提升或減輕相關災害所造成之減損者將予以獎勵。

壹拾參、內部稽核作業

一、依據

依據總局「資通安全內部稽核作業程序書」，本所擬定內部稽核作業。

二、權責

(一)內部稽核分組組長

負責擬定資通安全內部稽核計畫、監督稽核作業實施成效，並執行工作小組召集人交辦之不定期資通安全內部稽核任務。

(二)內部稽核分組成員（內部稽核員）

由資訊室與政風室遴選經適當訓練之人員擔任，負責資通安全內部稽核之執行、矯正預防措施之跟催，並參與外部稽核作業。

(三)權責獨立

為求稽核之公正性與獨立性，應給予內部稽核員充分權責，於稽核時可不受任何外力之干擾，不稽核本身業務，並保持客觀、公正心態。

(四)人員資格

1.受過內、外部資通安全管理系統(ISMS)條文或稽核相關課程之專業訓練。

2.曾有資通安全內部稽核相關經驗。

三、作業內容

(一)稽核方式

1.定期

每年至少實施一次資通安全內部稽核。

2.不定期

資通安全有異常情況或受威脅時，視需要實施內部稽核。

(二)稽核計畫

1.內部稽核分組組長應訂定「年度資通安全內部稽核計畫表(ISMS-04-08-TPC)」。

2.稽核項目選定原則（可複選）

(1) 資通安全受到威脅之項目。

(2) 資通安全中不易管制之項目。

(3) 前次稽核發現之缺點。

(4) 資通安全管理系統文件（必須稽核項目）。

(5) 資通安全管理系統控制目標與措施（必須稽核項目）。

(三)稽核工作指派

內部稽核員應依內部稽核分組組長之分派，執行資通安全內部稽核之工作。

(四)工作文件準備

1.內部稽核分組組長分派內部稽核員稽核時執行的項目與單位、排定稽核時程，以「資通安全內部稽核通知單(ISMS-04-08-TPC)」通知受稽核單位。

2.內部稽核員負責編定所需稽核單位之「資通安全內部稽核查檢表(ISMS-04-09-TPC)」。

3.受稽核單位主管接獲「資通安全內部稽核通知單(ISMS-04-08-TPC)」後，應備妥相關文件與紀錄，並安排各受檢項目之對應人員接受稽核。

(五)稽核實施

1.依照 ISO 27001:2013 標準由內部稽核員主導，且在受稽核單位有關人員配合下實施內部稽核。

2.稽核分三階段實施，依序為稽前會議、稽核、稽後會議。

(1) 稽前會議（Opening Meeting）由內部稽核分組組長主持。

- 說明稽核目的及範圍。
- 提供稽核方法與程序參考。
- 確認內部稽核分組所需的資源已備齊。
- 確認結束會議以及任何中間會議的日期、時間。
- 澄清內部稽核計畫中不清楚之細節。

(2) 稽核由內部稽核員主導。

- 內部稽核員依指派之稽核項目與單位，將稽核過程所發現之事實，依下表稽核標準，記載於「資通安全內部稽核查檢表(ISMS-04-09-TPC)」。
- 稽核標準

評　分	標　準　說　明
不符合	未滿足要求，稽核之項目沒有建立或沒有完全運作，判為「完全無法接受」。
改　善	受稽核項目已經能滿足稽核要求，但是仍有可以改善之空間，判為「可改善事項」。
觀　察	有某部份稽核項目因特別因素（如年度、地點之限制）無法在本次稽核中取得具體佐證資料，證明該項目已被執行，判為「觀察」。
符　合	滿足所有的要求，稽核項目完全被發展、執行，資料完整，判為「符合」。

- 稽核時，如發現不符合事項，應依照總局頒布之「資安缺失矯正預防措施管理作業程序書」之規定開立「矯正預防措施單(ISMS-04-11-TPC)」並由受稽核單位認簽。

(3) 稽後會議（Closing Meeting）由內部稽核分組組長主持。

由內部稽核員針對稽核之過程與發現之缺失、觀察事項與改善建議提出報告，並將所開立之「矯正預防措施單(ISMS-04-11-TPC)」陳交內部稽核分組組長。

3.稽核報告

(1) 內部稽核員所開立之「矯正預防措施單(ISMS-04-11-TPC)」，須由內部稽核員與受稽核單位雙方認簽。

(2) 「資通安全內部稽核查檢表(ISMS-04-09-TPC)」經認簽後複印一式二份，由內部稽核分組與受稽核單位分持，作為執行矯正作業與後續效果確認與跟催之依據。

(3) 稽核完成後，受稽核單位收到「矯正預防措施單(ISMS-04-11-TPC)」應於 2 週內，提出改善措施。

(4) 受稽核單位之缺失於預定改善期限內改善完成後，應通知內部稽核分組，執行矯正行動之追蹤確認。

(5) 內部稽核分組組長將所有稽核時所開立之「矯正預防措施單(ISMS-04-11-TPC)」彙總成「資通安全內部稽核總報告(ISMS-04-10-TPC)」，提報管理審查會議中討論改進。

(6) 稽核完成後所有之當次稽核資料，由內部稽核分組與受稽核單位分別保存。

(7) 每次稽核實施後，內部稽核分組組長對所發現之不符合事項，應知會資通安全分組，檢視是否有重新風險評鑑之需求。

表單列表

表單名稱	文件編號
文件制訂/修訂/廢止/銷毀申請單	ISMS-04-01-TPC
資訊資產清單	ISMS-04-02-TPC
資產異動申請單	ISMS-04-03-TPC
年度資通安全教育訓練計畫表	ISMS-04-06-TPC
資通安全內部稽核通知單	ISMS-04-07-TPC
資通安全內部稽核計畫表	ISMS-04-08-TPC
資通安全內部稽核查檢表	ISMS-04-09-TPC
資通安全內部稽核總報告	ISMS-04-10-TPC
矯正預防措施單	ISMS-04-11-TPC
營運衝擊分析表	ISMS-04-12-TPC
就職報告單表格	ISMS-04-20-TPC
保密切結書	ISMS-04-21-TPC
大內網系統帳號申請暨變更聯繫單	ISMS-04-22-TPC
電子公文系統帳號申請表	ISMS-04-23-TPC
離職報告單	ISMS-04-24-TPC
資料室進出登記表	ISMS-04-25-TPC
電腦機房進出登記表	ISMS-04-26-TPC
三代公路監理系統機房工作日誌	ISMS-04-27-TPC
網站內容更新檢視單	ISMS-04-28-TPC
電腦異動聯繫單	ISMS-04-29-TPC
資料室儲存保管銷毀清冊	ISMS-04-30-TPC
資通安全教育訓練簽到表	ISMS-04-31-TPC

一、抽號碼機故障：

（一）號碼單改由服務台人員以人工作業發放，並連繫相關人員(或維護廠商)修護。

（二）由服務台人員使用人工編號，並於空白號碼單上寫上編號號碼，替代現有抽取式號碼單使用。

（三）由引導人員依順序引導至櫃台處等候。

（四）於服務台明顯位置處豎立「因抽號碼機故障，改由人工作業，造成不便之處，敬請見諒」。

二、汽機車新領（或重領）牌照作業：

（一）審核相關證件、車主證明文件、強制汽車責任保險證及各項書表。

（二）經審察核格後，於相關證件、書表上加蓋核銷章戳、新編牌照號碼等。

（三）核算牌照稅、汽燃費需繳納金額並挈開繳納單據。

（四）以人工挈開規費收據。(各單位自行以流水號登記列管,並於電腦恢復後補鍵入資料,以利核帳)

（五）於牌照登記書車主聯於左上角加蓋『本登記書自發照日起一週內暫代行照使用』章戳及日期戳。

（六）對於繳、註、吊銷牌照重領之案件，應告知車主（或申辦者）是否有積欠使用牌照稅、汽車燃料使用費、違規或動產擔保交易法、違反使用牌照稅法、違反強制險、禁止異動案件無法查核，請填寫切結書。

（七）請車主(或申辦者)填寫回郵信封及電話號碼(由窗口供應)俟系統修復後補登資料，並列印行車執照以通信方式寄還車主。

三、汽機車各項異動作業：

（一）於受理窗口處豎立告示牌「因電腦系統故障,改以人工作業,造成不便及久候之處，敬請見諒」。

（二）告知車主(或申辦者)是否有積欠使用牌照稅、汽車燃料使用費、違規或動產擔保交易法、違反使用牌照稅法、違反強制險、禁止異動案件無法查核，請填寫切結書。

（三）審核證件書表，合格者將行車執照影印乙份存查，並請車主(或申辦者)填寫回郵信封（由窗口供應）及連絡電話號碼。

（四）對於需更換行照者，先於異動書表單加蓋『因電腦故障，以本登記書一週內暫代行車執照使用』再收取行車執照規費。

（五）俟電腦系統恢復後，再行將資料補鍵入電腦、印行車執照書表等寄還車主。

四、車輛檢驗線系統故障：

(一)於車輛檢驗線受理窗口豎立告示牌「電腦系統故障，改以人工機械檢驗，造成不便及久候，敬請見諒」。

(二)請告知車主(或申辦者)因電腦故障無法查核是否欠汽車燃料使用費及違章記錄，改至稅費課窗口查詢。

(三)於自動電腦檢驗記錄表上加蓋「停電改以目測檢驗」章戳，填寫車號、車別、出廠年月、日期、檢驗別，並以人工開立規費收據。(各單位自行以流水號登錄列管，並於電腦恢復後補鍵資料以利核帳)，同時掣開檢驗費收據。

(四)廢、排氣測試器、側滑器、腳、手煞車測試器、儀器等，所測試數值請車主(或申辦者)確認後，將其測試值登錄於記錄表內，並核計合格與否。

(五)目測項目，依規定項目檢驗並登錄於記錄表內，並告知車主動或駕駛人)不合格項目。

(六)由後段檢驗員總評簽證或登錄下次檢驗日期，需換發行照者加蓋『需換發行照』章戳。

(七)俟電腦恢復後再以整批鍵檔方式鍵入備查。

五、考領駕駛執照核發作業：

(一)於核發駕駛執照窗口前豎立告示牌「因電腦系統故障，改以人工作業，造成不便與久候，敬請見諒」。

(二)查核考驗成績記錄表及各項書表後符合核發規定後收件。

(三)收取相片乙張及規費並以人工掣開收據聯，並請填寫回郵信封（由窗口供應）及連絡電話號碼。

(四)於駕駛人登記書影本上加蓋「自發照日一週內暫代駕駛執照使用」及日期戳章供駕駛汽車之許可憑證使用。

(五)俟電腦系統恢復正常後鍵入駕駛人資料印製駕駛執照並登載於規費系統以通信寄發。

六、汽、機車駕駛人各項異動作業：

(一) 於駕駛人各項異動受理窗口前豎立告示牌「因電腦系統故障，改以人工作業，造成不便與久候，敬請見諒」。

(二) 審核書表及各項證件符合後，依規定收件。

(三) 影印身分證明、駕駛執照後正本發還駕駛人。

(四) 收取相片乙張及規費，以人工掣開收據，並請駕駛人(或申辦者)填寫回郵信封(由窗口供應）及連絡電話號碼，如有違規或禁止異動之情形再另行連繫。

(五) 於汽、機車駕駛人各項異動登記書上加蓋「本登記書影本自核發起一週內暫代駕駛執照使用」及日期戳章。

（六） 定期換發駕駛執照者於原駕駛執照上加蓋「本駕駛執照有效期間順延一週內」及日期戳章發還駕駛人。

（七）俟電腦系統恢復正常後依異動登記書表項目印製駕駛執照並登載於規費系統以通信寄發駕駛人。

七、路考駕照筆試電腦系統故障：

（一）於筆試場前豎立告示牌「筆試電腦系統故障，改以人工閱卷，造成不便與久候，敬請見諒」。

（二）依報考清冊點名進場依指定座位入座。

（三）以備份之筆試試題號碼由應考人選派代表一人抽籤，決定本場使用筆試試卷。

（四）以人工方式閱卷。

（五）登計成績於報名表及清冊中並公佈成績。

（六）不及格者檢還證件並告知應考人下次可報考日期，及格者引導至報名窗口安排路試時間。

八、申領學習駕證：

（一） 以人工書寫核發及掣開收據。

（二） 俟電腦系統恢復正常後鍵入並登載於規費系統列管。

九、違規裁決作業:

（一）受理違規民眾電話查詢違規案件時，先行登記相關資料，俟電腦回復後，再行電話答覆。

（二）向車主或申辦者委婉解釋因電腦故障無法查詢，請告知牌照號碼，到案日期、連絡電話、違規行為並登錄表件，依單展延。

（三）俟電腦系統回復後主動以電話答詢。

（四）備置違規案件查詢登記簿登錄。

十、違規案件裁罰並受理繳納罰款:

（一）於受理窗口處豎立告示牌「因電腦系統故障，改以人工作業，造成不便與久候，敬請見諒」。

（二）車主(或申辦者)辦理違規未扣件者，依人工作業裁罰，如有扣件者，依人工作業裁罰後，扣件當場發還。並告知違反道路交通管理事件統一裁罰標準及處理細則第 39 條之規定，如有積案日後仍需繳清，並請填寫「切結書」。

（三）以人工掣開收據(如有扣件者，加蓋扣件發還章戳)。

（四）俟電腦系統回復後，依受理案件逐一銷號並登載於規費系統結案。

（五）車主(或申辦者)到案後，因故未解繳結案者，於違規單通知聯加蓋延期章戳及職名

章並登記。

（六）未持違規單到案者，填發到案證明單及准延日期(適用對象：限通知單未逾應到案日期者)並登記。

十一、違規吊扣處分案件:

（一）受理吊註銷駕駛執照或汽車牌照者，請車主(或申辦者)填妥吊扣各項表格及暫代保管駕照同意書。

（二）經審核後先予收件辦理並請車主(或申辦者)填寫回郵信封（由窗口供應）及連絡電話號碼。

（三）俟電腦系統回復後鍵入吊扣起迄日期執行吊扣資料。

（四）將執行單以通信郵寄。