新竹市私立光復高級中學資訊機房管理辦法

112 年 07 月 25 日訂定
經 112 年 08 月 16 日主管會報修正通過
112 年 11 月 07 日陳校長校可

壹、目的

新竹市私立光復高級中學(以下簡稱本校)為健全本校資訊機房之操作及管理，維持本校資訊系統之正常運作，確保資料安全及機密維護，特訂定資訊機房管理辦法(以下簡稱本辦法)，作為本校資訊機房操作及管理之準則。

貳、通則

一、門禁管制辦法

資訊機房係屬人員管制區域，本項辦法適用於任何進出管制區域人員

（一）資訊機房管制區域應設門禁，管理人員進出，非因公務，不得進入。

（二）進出機房工作人員須向資媒組申請，並填寫人員進出記錄表。

二、安全管理辦法

（一）資訊機房等管制區域內嚴禁吸煙或飲食。

（二）資訊機房嚴禁存易燃品及未經准之電器或其他物品。

（三）資訊機房溫度合適溫度為 25℃~28℃，警示溫度為 31℃。

（四）資媒組人員應熟悉滅火器之位置及操作，遇火災預警系統發出警報時，應確認其原因，並作適當處置。

（五）資訊機房內各種器物應擺放整齊，必要時貼立標籤識別，用畢應歸還原位，廢棄物品，應儘速撤離電腦資訊機房，保持管制區域內整齊及清潔。

參、例行工作

資訊機房例行工作由資媒組指派人員負責執行。

一、注意事項

（一）注意與管制資訊機房之門禁進出及各項活動，任何異常活動時，立即進行處理，並將時間及原因登記於「新竹市私立光復高級中學資訊機房管理記錄」。

（二）監督可攜式儲存媒體確定無電腦病毒，未造成妨害系統運作因素後再放行使用。

二、每學期應辦理事項

（一）檢查防火牆事件紀錄及規則，若有異動或異常應立即更正。

（二）各主機檔案系統的重整，檢視系統例行更新是否正常運作。

（三）辦理本校資訊機房重要網段弱點掃瞄與漏洞修補工作。

（四）檢查伺服器網段的主機事件紀錄與容量。

三、每年應辦理事項

不斷電系統(UPS)、空調機保養。

肆、資料備份與復原

參見「新竹市私立光復高級中學資訊安全備份與復原作業辦法」。

伍、門禁控管

一、人員門禁對象

除本校業務有關主管、資媒組人員外，其他未經許可人員，禁止進入電腦資訊機房。

二、人員進出入管制辦法

（一）任何進出資訊機房人員應遵守本管理辦法辦理。

（二）發現資訊機房有非經核准或非執行公務之人員時，應立刻要求該人員離開。

（三）廠商維護人員若因故障檢修或維修需要而需進入資訊機房作業時，應按規定申請並填寫紀錄。

陸、物品出入管制

一、物品管制項目

包括資訊機房作業所需之各項設施、設備等有關物品。

二、物品出入管制規定

（一）所有人員均不得攜帶非作業所必須物品進出資訊機房。

（二）所有人員攜入(出)資訊機房內設備或零組件時，應登記於「新竹市私立光復高級中學資訊機房管理記錄」。

柒、設備關開機

一、辦理資訊機房設備保養如主機、網路設備、空調機、不斷電設備等可預期性停機時，應由資媒組於停機前一日，將停機事由與預計停機期間，通知相關人員。

二、資訊機房設備停機原因消失，應立即開機，恢復系統正常運作。

捌、異常狀況之應變處理

電腦系統若有異常狀況發生時，資媒組人員應依據本辦法及相關系統操作程序書進行問題排除，同時登記於「新竹市私立光復高級中學資訊機房管理記錄」。

一、電腦設備異常處理

（一）電腦設備包括電腦主機、光碟機、交換器、路由器、防火牆及其週邊設備。

（二）資訊機房電腦設備有異常狀況時，資媒組人員應運用網路管理系統或其他工具，檢查網路設備連線狀況，必要時得進入資訊機房查看設備燈號、LCD 面板及主控台訊息判斷故障情形。

（三）若故障係由線路脫落所致，資媒組人員應立即重新固定線路，恢復電腦設備正常運作。

（四）非屬前項原因所致故障，資媒組人員應立即通知維護或保護廠商前來檢修，並登記於「新竹市私立光復高級中學資訊機房管理記錄」。

（五）電腦設備異常狀況故障均應在「新竹市私立光復高級中學資訊機房管理記錄」登記故障之機型、機種、停機時間、異常訊息與處理狀況。

（六）系統軟體異常無法修復時，依「新竹市私立光復高級中學資訊安全備份與復原作業辦法」進行系統回復工作。

（七）因電腦設備故障而影響系統整體運作時，資媒組決定是否先行個別切離。其切離次序應先判斷週邊設備影響系統的嚴重程度，應從較嚴重部份開始應變，依次較輕微等部分繼續處理。

二、環境設施異常處理

（一）電力設施異常處理要點：

1. 資訊機房內設備電力過載、不足或無故中斷時，應立即聯繫相關人員處理。
2. 若係不斷電系統(UPS)電池故障，應改以旁路(bypass)方式供電繼續作業；如為單一 UPS 故障，應迅速執行關機程序，關閉僅連結該部 UPS 之電腦主機設備，並立即通知維護或保固廠商前來檢修。
3. 若發生電力過載或突波致使火災或爆炸意外時，應立即切斷該迴路斷路器，以防止意外發生。

（二）空調設施異常處理要點：

應儘快找出原因，並請總務處聯絡廠商解決。

三、災害、脅迫與入侵系統異常處理

（一）駭客網路入侵事件處理

1. 立即阻絕入侵者任何存取動作，防止災害繼續擴大。
2. 隔絕受入侵主機之網路連線，並視需要停機。
3. 保留受入侵主機的所有資料，以做為後續調查之用。
4. 檢查防火牆及系統紀錄，研判入侵管道及方式，並作安全漏洞修補。
5. 將完整的系統備份資料存回重要的主機上，並測試其功能，直至完全回復止，最後再將重要主機重新上線。
6. 填寫「新竹市私立光復高級中學資訊機房管理記錄」紀錄事件處理經過。

（二）駭客阻絕與攻擊事件處理

1. 如駭客惡意攻擊本校網路系統或服務主機，阻絕本校對外提供之資訊服務及對外網路連結，且已造成本校對外之服務中斷，應迅速截斷本校路由器對外之網路連結，並保留防火及所有受攻擊主機之紀錄，資媒組應迅速通告本校所有教職員生暫時中斷本校對外之網路服務。
2. 資媒組聯繫 TANet 新竹區網中心及校園骨幹路提供業者機房服務人員，請其協助追查入侵駭客之來源並截斷其攻擊路徑，且保留相關資訊作為法律追訴的證據。
3. 確認完成駭客阻絕攻擊事件之處理後，檢視路由器、防火牆及遭受阻絕攻擊之系統正常無虞，重新將網路連結。
4. 填寫「新竹市私立光復高級中學資訊機房管理記錄」紀錄事件處理經過。

（三）發現後門、暗門或病毒、木馬程式事件處理

1. 檢視防火牆及入侵偵測系統之稽核紀錄，清查造成網路癱瘓之來源，確認是外部

攻擊或內部主機遭受病毒或木馬程式入侵引發內部攻擊事件，並確認所有遭受破壞或入侵的網段區域及系統範圍。

2. 全面整理各網段的 IP 資料，並對整個網路進行病毒/木馬程式掃描，確認該後門、暗門或病毒、木馬程式之影響。

(1) 如判斷僅為單一主機事件，則迅速排除該主機之後門、暗門或病毒、木馬程式。

(2) 如判斷已擴散至本校多部主機，且有持續擴散之趨勢時，應迅速截斷本校相關網路設備之連結，避免事件繼續擴散，並保留防火牆及所有受攻擊主機之紀錄，保留相關資訊作為法律追訴的證據，資媒組應迅速通告本校所有教職員生暫時中斷日常資訊處理作業。

3. 必要時依「新竹市私立光復高級中學備份與復原作業辦法」復原受損之系統。

4. 確認所有受後門、暗門或病毒、欄馬程式攻擊的系統均已恢復正常後，重新將網路連結。

5. 填寫「新竹市私立光復高級中學資訊機房管理記錄」紀錄事件處理經過。

四、重大災難事件處理

(一) 部份設施損毀，但仍可於原址回復提供服務

1. 如判斷資訊機房僅輕微受損，不影響電腦系統運作及人員安全時，則資訊機房線持繼續運作，並聯繫廠商到達現場進行維修處理。

2. 依照各設備/設施損害程度，由資媒組諮詢維護廠商，研擬解決暨回復方案。如果硬體設備毀損不堪使用，聯繫廠商維修或訂購新貨。

3. 應注意資訊機房地板是否損毀，電線電纜是否被浸泡或潮濕，如有需要應立即通知廠商修復。

4. 當系統與機房內之備份同時損時，應由異地備份設備進行回復作業。

5. 必要時可請 TANet 新竹區網中心或資通安全顧問廠商的支援。

(二) 若為嚴重災害，無法於原址回復提供服務

1. 資媒組一方面儘快確認辦公室設備的損壞情形，尤其是主機房內的各類資訊設備，另一方面聯繫洽詢可用的異地作業環境，及各項設備等級及可用度，如空調、電力及通訊線路等。

2. 規劃臨時網路架構與通訊方式，安排廠商將原辦公地點可用的設備搬移至新的辦公地點，並連絡廠商安置所有設備至臨時辦公地點。

3. 將個別系統逐項測試回復，軟、硬體毀損者依相關之回復程序進行系統回復。

玖、參考及相關文件

一、行政院及所屬各機關資訊安全管理要點。

二、新竹市私立光復高級中學資訊機房管理記錄。

三、新竹市私立光復高級中學資訊安全備份與復原作業辦法。

拾、本辦法提報行政主管會議審核，陳請校長核可後施行，修訂時亦同。