# 達和環保服務股份有限公司

## 資訊矯正與預防處理單

填表日期：113 年 8 月 26 日

| 提出單位 | 達和總公司 | 提出人員 | 駱正達 | 提出日期 | 113.8.8 |
|---|---|---|---|---|---|
| 處理單位 | 永康廠 | 處理人員 | 陳君華 | 填寫日期 | |

| 事件分類： | 事件來源： |
|---|---|
| □建議 □觀察 □次要缺失 □主要缺失<br>（內部稽核所發現之問題、缺失與事件項目不需填寫本欄位） | ☑內部稽核 □外部稽核 □資訊安全事件<br>□自行提出 □其他_____ |

| | |
|---|---|
| 問題或缺失說明 | 查核同仁電腦，在 windows update 的介面上，顯示「檢查日期:今日」及「您現在為最新狀態」，但細查更新記錄卻發現只更新到 2023 年 12 月。 |
| 原因分析 | 電腦於 windows update service 管理下，由組織統一政策規劃進行更新項目派送。但是因為 Wsus 主機上的異常，造成 Client 端的電腦沒有接受到更新指令，認為電腦的更新已經是最新的狀況。<br><br>本次異常實屬總公司防火牆的設定，未將 Wsus 主機變更後的 IP，更新到防火牆可允許造訪的白名單中，造成外部電腦並沒有成功連接到 wsus 主機。 |
| 矯正與預防措施評估 | 暫時性對策：（控制缺失的擴大或消除單一事件的影響）<br>總處解除設定錯誤後，請廠端確認所有的電腦是否都已經恢復更新檢查狀態，並確認已經更新到近期的版本。<br><br>預訂完成日期：113 年 12 月 31 日 |

| 追蹤人： | 追蹤日期： | 確認結果：陳君華 |
|---|---|---|

永久性對策：（消除缺失或潛在風險的根本原因，防止類似事件發生）

12/26 日隨機採樣三台檢視更新記錄，確實每個月都有更新記錄。

# 達和環保服務股份有限公司

## 資訊矯正與預防處理單




預訂完成日期：113年 12月 3日

| 追蹤人：[illegible] | 追蹤日期：113.12.26 | 確認結果：陳君華 |
|---|---|---|

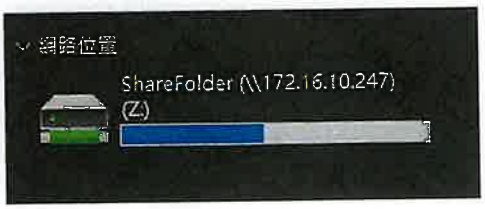
近期Windows update更新已完成。

表單編號：4-43-1501-01

# 達和環保服務股份有限公司

## 資訊矯正與預防處理單

填表日期： 113 年 8 月 26 日

<table>
<tr><td>提出單位</td><td>達和總公司</td><td>提出人員</td><td>駱正達</td><td>提出日期</td><td>113.8.8</td></tr>
<tr><td>處理單位</td><td>永康廠</td><td>處理人員</td><td>陳君華</td><td>填寫日期</td><td></td></tr>
<tr><td colspan="3">事件分類：<br>☐建議 ☐觀察 ☐次要缺失 ☐主要缺失<br>（內部稽核所發現之問題、缺失與事件項目不需填寫本欄位）</td><td colspan="3">事件來源：<br>☑內部稽核 ☐外部稽核 ☐資訊安全事件<br>☐自行提出 ☐其他＿＿＿＿＿＿＿＿</td></tr>
<tr><td>問題或缺失說明</td><td colspan="5">內部網段無區分一般使用者及伺服器設備網段</td></tr>
<tr><td>原因分析</td><td colspan="5">伺服器與使用者設備處於同一網段中，若使用者的電腦發生資安事件，同網段內的伺服器有可能很輕易地就遭受攻擊。<br>也無法將遭受攻擊或是可疑活動，限制於某一區域，降低影響層面</td></tr>
<tr><td>矯正與預防措施評估</td><td colspan="5">暫時性對策：（控制缺失的擴大或消除單一事件的影響）<br>無<br><br>預訂完成日期： 年 月 日<br>追蹤人： 追蹤日期： 確認結果：<br><br>永久性對策：（消除缺失或潛在風險的根本原因，防止類似事件發生）<br>於防火牆或是 swich Hub 上規劃 vlan 切割網段，將伺服器與使用者端的網段進行分割。<br>已於永康 NAS 上的 IP 由 192.168.10.X 修正為 172.16.10.X<br>並將所有電腦網路磁碟 IP 做全面修正。<br>12/26 日再次確認備份及使用正常。<br>  <br><br>預訂完成日期：113年12月31日<br>追蹤人： 追蹤日期：113.12.26 確認結果：<br>已完成區段劃</td></tr>
</table>

表單編號：4-43-1501-01

# 達和環保服務股份有限公司

## 資訊矯正與預防處理單

填表日期： 113 年 8 月 26 日

| | | | | | |
|---|---|---|---|---|---|
| 提出單位 | 達和總公司 | 提出人員 | 駱正達 | 提出日期 | 113.8.8 |
| 處理單位 | 永康廠 | 處理人員 | 陳君華 | 填寫日期 | 113.8.28 |

| | |
|---|---|
| 事件分類：<br>□建議 □觀察 □次要缺失 □主要缺失<br>（內部稽核所發現之問題、缺失與事件項目不需填寫本欄位） | 事件來源：<br>☑內部稽核 □外部稽核 □資訊安全事件<br>□自行提出 □其他＿＿＿＿＿＿ |

| | |
|---|---|
| 問題或缺失說明 | 管理者與操作者日誌僅保存在 NAS 內，原始資料可能損毀或是被刪除 |
| 原因分析 | 日誌保留在原系統內部，可能因為設備損壞無法讀取、遭受資安事件而被清除，導致無法追朔查找問題原因。 |
| 矯正與預防措施評估 | 暫時性對策：（控制缺失的擴大或消除單一事件的影響）<br>NAS 日誌，手動匯出並備份儲存到其他的儲存裝置<br><br>預訂完成日期：113年9月30日 |

| 追蹤人： | 追蹤日期： | 確認結果： |
|---|---|---|

永久性對策：（消除缺失或潛在風險的根本原因，防止類似事件發生）
利用 NAS 系統中的封存日誌或是日誌傳送功能，設定系統自動傳輸到安全的儲存區存放。

已於TahoYK-NAS1將日誌傳輸到另一台日誌專用NAS Server上(DS420YK)備份，如右圖所示。

預訂完成日期：113年12月31日

| 追蹤人：駱正達 | 追蹤日期：113.12.4 | 確認結果：陳君華 |
|---|---|---|

已設定備份日誌於另一主機上。

表單編號：4-43-1501-01