CELLOPOINT
Secure Your Email

# CODLP 雲端郵件 DLP 服務等級協議（Service Level Agreement）

雲端服務使用者（CSC）: CODLP 終端用戶（甲方）

雲端服務提供者（CSP）: Cellopoint International Corporation（乙方）

## 1.1 目的與範疇

本協議旨在規範「Cellopoint 雲端郵件 DLP 服務」約定條款，包含資安控制、個資保護、資料處理與雙方責任。依據 ISO/IEC 27017:2015 與 ISO/IEC 27018:2019 所訂之最佳實務辦理。當您申請使用本服務時，即表示您已閱讀、瞭解並同意接受乙方「服務等級協議」之所有內容。

## 1.2 定義

### 1.2.1 雙方角色

個人可識別資訊（PII）: 依 ISO/IEC 29100 定義。

控制者 / 處理者：甲方為 PII 控制者，乙方為處理者。

1.2.2 雲端服務內容為寄外郵件資料外洩防護 DLP（包含郵件稽核、郵件加密）。

1.2.3 雲服務相關資訊所存放位置於日本、新加坡、或台灣，機房等級屬 5A 級數據中心。

## 1.3 服務可取得性

1.3.1 「服務可取得性」在這份協議中代表「Cellopoint 雲端郵件 DLP 服務」所提供的 SMTP (port 25) 之可建立連結性，由「Cellopoint 服務監控系統」進行衡量。

1.3.2 「Cellopoint 雲端郵件 DLP 服務」提供 99.9%的「服務可取得性」，以每個月 30 天為一個計算周期。

1.3.3 「服務中斷」代表「Cellopoint 雲端郵件 DLP 服務」無法轉送甲方之電子郵件時間超過 10 分鐘 (600 秒)。

1.3.4 當服務中斷造成「服務可取得性」低於 99.9%時，甲方可依照 1.5.1 服務補償條款申請。

1.3.5 因「計畫性維護時間」造成「服務中斷」的時間，不包含於此「服務可取得性」的計算中。

**1.4 郵件遞送、延遲時間**

**1.4.1 可追蹤 95%的郵件在收到後 5 分鐘內，其詳細 SMTP 紀錄及隔離區郵件須在「Cellopoint 雲端郵件 DLP 服務」檢視。**

**1.4.2 處理延遲時間指自收到請求至嘗試傳輸請求的時間。排除大於 1MB 的 HTTP GET/回應、DLP 分析、串流流量。**

**1.5 服務補償**

**1.5.1 「Cellopoint 雲端郵件 DLP 服務」服務補償標準**

| 每月服務中斷時間 | 補償服務天數 |
|---|---|
| <99.9%~≧99.0% | 3 天 |
| <99.0%~≧95.0% | 7 天 |
| <95.0% | 15 天 |

**1.5.2 最高補償天數，每月以不超過 15 天為限。**

**1.5.3 甲方必須提出書面申請補償，並需於服務中斷時間發生後的 7 個工作天內提出申請，否則視為放棄求償之權利。**

**1.6 技術支援**

**1.6.1 「Cellopoint 雲端郵件 DLP 服務」提供早上 9 點到 18 點(GMT+8)之電話支援。在服務時間以外，甲方只能透過電子郵件尋求支援。**

**1.6.2 技術支援回應時間**

| 優先等級 | 定義 | 回應時間 |
|---|---|---|
| 嚴重 | 服務中斷 | 2 小時 |
| 重要 | 部分服務中斷 | 4 小時 |
| 次要 | 不影響服務的一般性問題及建議 | 8 小時 |

**1.7 申請租用或終止手續**

**1.7.1 申請本服務時，甲方得透過基點資訊股份有限公司所提供之官方網站（https://www.cellopoint.com/）或專屬服務進行申請，並依乙方所要求之用戶註冊與身分驗證機制完成註冊。**

**1.7.2 甲方租用本服務時，應以乙方雲端平台（含主控台、API 管理介面或合作夥伴**

通路）所申請之服務項目與數量為準。其租用生效日以甲方於平台成功提交申請並經乙方系統確認完成之時點為起租基準。

1.7.3 甲方於租用期間申請帳號，應依照乙方所提供之雲端帳號申請表進行填寫或提供所需資訊由乙方知同仁進行協助辦理。

1.7.4 甲方如欲終止本服務，應登入乙方雲端服務平台或進行通知乙方終止申請需求。其終止生效日，以乙方系統完成「終止確認」動作之時間為準，實際租用時間及費用計算亦依乙方系統紀錄為準。

1.7.5 終止服務時，乙方應提供資料轉移方式並移除所有資料與備份，並提供清除證明紀錄。

1.7.6 乙方應提供資料匯出與刪除機制，並於終止服務後 30 日內完成。

1.8 資安與隱私責任

1.8.1 資安責任歸屬：

| RACI 矩陣 | CSP<br>雲端服務提供者 | CSC<br>雲端服務使用者 |
|---|---|---|
| 提供郵件安全掃描平台與維運 | R/A | I |
| 威脅情報與掃描規則更新 | R/A | I |
| 郵件即時掃描、攔截與隔離 | R | I |
| 雲端服務提供商安全事件通報與報告 | R | A |
| 雲端服務客戶安全事件通報與報告 | A | R |
| 客戶端安全政策設定 | C | R/A |
| 用戶帳號與權限管理 | I | R/A |
| 用戶教育與安全意識訓練 | C | R/A |
| 合規性政策設定與落實 | C | R/A |
| 監督安全事件與響應 | C | R/A |
| 定期審查與調整安全政策 | I | R/A |
| 技術支援與諮詢 | R | C |
| | | |
| 所有責任代碼意義： | | |
| R = Responsible（實際執行者） | | |
| A = Accountable（最終責任者） | | |
| C = Consulted（提供建議） | | |
| I = Informed（需知情） | | |

1.8.2 所有資料採加密儲存與傳輸，若是可行將實施存取控制與多因子驗證(MFA)。

1.8.3 個資處理：

(1) 僅依客戶授權處理資料，不得另作他用。

(2) 當發生資安事件，需於 72 小時內主動通知客戶。

**1.8.4 事件保存及日誌操作：乙方應建立重要系統的稽核事件（含雲端服務及雲端服務個人資料），以記錄使用者（包含管理者及操作者）活動、異常狀況及其它資訊安全相關事件，並保存 180 天，以協助未來的事故調查及存取控制稽核檢查。**

**1.8.5 第三方供應商管理：乙方若使用第三方技術服務，須確保其資安等同本合約規範，並依照供應商管理標準作業進行。**

## 1.9 稽核機制

**1.9.1 甲方若需進行稽核查驗（實地或遠端），應至少提前三個月告知乙方，以便於乙方提供必要協助。**

**1.9.2 若已取得第三方認證，乙方得提供第三方通過驗證之證書替代現場查驗。**

## 1.10 保密與責任

**1.10.1 雙方對合約中機敏資訊負保密責任。如違反資訊安全或導致 PII 外洩，違約方應負相關法律與賠償責任。**