EVERY8D | SECURITY WHITE PAPER

EVERY8D 企業簡訊平台

資安白皮書

企業通訊服務的安全架構、資料保護與營運韌性

Security Architecture, Data Protection & Operational Resilience

2026 Edition

提供企業、金融機構、政府單位與大型組織進行供應商安全評估與系統導入審查時參考。

文件定位　本白皮書聚焦 EVERY8D 現行安全設計、資料治理與營運韌性，不以個別事件作為敘事主軸。實際功能、保存政策與技術設定仍依服務方案、契約與客戶介接方式而異。

互動資通股份有限公司

EVERY8D Enterprise Messaging Service

文件說明與目錄

Document Scope & Contents

適用範圍

EVERY8D 為企業簡訊與 OTP 等通訊情境提供平台服務與系統介接能力。本白皮書從資安治理、平台架構、身分存取、資料生命週期、API、安全監控、端點與弱點管理、備援及第三方風險等面向，說明平台現行的安全管理原則，作為客戶在採購、導入、稽核或供應商管理時的參考。

重要聲明　本文件屬安全設計與管理原則之說明，不取代雙方契約、SLA、個資處理約定或特定稽核報告。涉及認證、測試報告、RTO / RPO、客製化保存期限等項目，應以正式提供之最新版文件或合約為準。

章節目錄

10	備援與營運持續	備份、復原、BCP / DR
11	供應鏈與第三方管理	電信、雲端與供應商風險
12	合規與企業客戶保障	個資、問卷、稽核與佐證

1. 白皮書摘要

Executive Summary

企業簡訊承載的往往不是一般訊息，而是登入驗證、交易通知、服務提醒、緊急通報與大量客戶溝通。對企業而言，通訊平台的安全，不只關乎「能不能發出去」，也同時關乎帳號是否被妥善管理、資料是否只在必要期間存在、系統是否能被持續監控，以及在異常情境下能否維持可控的服務。

EVERY8D 的安全設計以「最小暴露、最小權限、資料最小化、持續監控、可追溯、可復原」為核心原則。安全控制不集中於單一設備或單一技術，而是分布於治理制度、網路與主機、應用與 API、身分權限、資料處理、日誌監控與備援復原等不同層次，形成多層防護。

六項核心安全原則

原則	EVERY8D 的落實方向
最小暴露	降低不必要的服務、埠號、管理介面與資料暴露範圍。
最小權限	帳號與系統權限依角色與工作需求配置，避免過度授權。
資料最小化	只處理服務所必要的資料，並依用途設定保存與刪除政策。
持續監控	以日誌、端點與異常行為偵測建立可追蹤的監控能力。
安全預設	新功能、介接與變更在設計階段即納入存取、資料與稽核需求。
營運韌性	透過備份、復原程序、異地或雲端備援與演練降低中斷衝擊。

給採購與資訊單位的閱讀方式　若您正在進行供應商資安評估，可先閱讀第 4、5、7、8、10 章，再搭配附錄「企業客戶資安評估快速索引」對照內部問卷。

2. 資安治理架構

Security Governance

EVERY8D 將資訊安全視為營運管理的一部分，而非單一技術部門的工作。治理範圍涵蓋制度與責任、資產與風險、權限與變更、弱點與修補、資料治理、供應商管理、備援及異常應變，並要求相關作業留下可追溯紀錄。

治理架構的四個層次

政策與責任	由管理制度定義資安責任、管理原則與核決邊界，使安全要求能被納入日常營運。
風險與資產	持續盤點重要系統、資料、帳號與第三方依賴，依重要性與風險決定控制強度。
執行與稽核	透過權限管理、變更程序、弱點修補、日誌查核與例行檢核，使制度可被執行與驗證。
持續改善	依監控結果、風險評估、客戶要求、法規與技術環境變化調整控制措施。

管理重點

- 高權限帳號與重大系統變更採較高強度的核准與留痕要求。
- 重要系統與資料依用途、敏感度及營運影響程度進行分類管理。
- 弱點、端點告警與安全事件由指定角色追蹤，並建立處理與回報程序。
- 第三方服務、電信介接與雲端資源納入供應鏈風險與權限邊界管理。
- 對外提供的資安佐證與客戶問卷，由技術、管理與必要的法務 / 合規角色共同確認。

治理原則　安全控制的目標不是增加流程，而是讓「誰可以做什麼、資料在哪裡、系統發生什麼、

異常時如何處理」都有清楚且可追溯的答案。

3. 平台安全架構

Security Architecture

EVERY8D 採多層防護與分區隔離的安全思維，將對外服務、應用處理、管理操作、資料存取、監控與備份等功能置於不同的安全邊界。此設計可降低單一帳號、單一主機或單一區域異常時，風險向其他核心資產擴散的機會。

分層防護概念

入口與邊界	對外服務僅開放必要介面，搭配網路存取控制、流量與異常監控，降低非必要暴露。
應用服務	簡訊送出、排程、帳號、API 與管理功能依服務角色切分，減少不必要的相互存取。
資料層	核心資料與系統服務採權限限制與存取邊界，避免一般操作帳號直接接觸底層資料。
管理層	管理性操作與一般使用者操作區隔，高權限存取採更嚴格驗證、權限與稽核要求。
監控與備援	安全日誌、端點偵測、備份與復原機制形成獨立的監測與韌性層。

安全架構設計原則

設計原則	說明
分區與隔離	不同功能與信任等級間建立存取邊界，僅允許業務必要的連線。
最小服務面	關閉不必要服務與管理入口，降低可被探測與利用的攻

	擊面。
管理面分離	管理操作與一般服務流量分開治理，降低管理權限被濫用的風險。
可監控性	重要登入、權限、系統與應用活動保留記錄，以支援異常調查與稽核。

4. 身分與存取管理

Identity & Access Management

在企業通訊平台中，最重要的安全邊界之一是「身分」。EVERY8D 以帳號生命週期、最小權限、角色分工、高權限治理與多因素驗證等方式降低帳號被濫用的風險，並將管理性操作納入稽核與追蹤。

帳號與權限控制

控制面向	管理原則
帳號建立與異動	依角色與業務需要建立帳號；人員異動或職務變更時同步調整權限。
角色與最小權限	權限依工作職責分配，避免使用共用或過度授權帳號執行日常作業。
多因素驗證	對管理性帳號與高風險存取採較高強度的驗證策略，包含 MFA 等機制；適用範圍依角色與政策設定。
高權限帳號	高權限操作與一般操作分離，降低長期使用高權限帳號的必要性。
定期檢視	重要帳號與權限定期盤點，確認權限仍符合現行職責與實際需要。
操作留痕	重要登入、權限異動與管理操作保留必要紀錄，以支援稽核與追蹤。

客戶端的共同責任

Shared Responsibility　客戶應妥善保管管理者帳號、API Key 與介接憑證，避免多人共用；可行時採來源限制、強密碼與定期輪替，並在同仁離職、委外關係結束或系統汰換時立即撤銷不再需要的權限。

5. 資料安全與生命週期

Data Protection & Lifecycle

EVERY8D 對資料採「必要、最小、可控、可追蹤」的處理原則。安全不是只看資料是否加密，而是從資料進入平台開始，即考量用途、存取對象、保存時間、呈現方式、匯出與刪除，降低資料在生命週期中被不當使用或長期累積的風險。

資料生命週期

階段	安全重點
1. 進入平台	確認服務用途與必要欄位；API 與管理介面採安全傳輸與身分驗證。
2. 處理與發送	訊息依服務流程處理，系統與人員僅取得完成任務所需的權限。
3. 顯示與查詢	敏感識別資訊於適當介面採遮罩或受限顯示，降低不必要曝露。
4. 保存	依資料類型、服務用途、契約與管理政策設定保存期間，避免無目的長期保存。
5. 到期刪除	到期資料依系統政策或管理程序進行刪除 / 清除，降低歷史資料累積。
6. 稽核與追蹤	重要查詢、管理與權限活動保留必要記錄，支援稽核與異常調查。

資料保護方法

- 傳輸階段：對支援的介接通道採 TLS 等安全傳輸機制。
- 顯示階段：對具識別性的欄位依使用情境採遮罩或限制查詢。
- 存取階段：以角色、系統服務帳號與權限邊界降低直接接觸底層資料的必要性。
- 保存階段：依資料用途採期限管理，不以「無限期保留」作為預設。

資料最小化　「能少收就少收、能少留就少留、非必要就不讓更多人看見」是企業通訊服務降低資料風險最直接也最有效的原則之一。

6. 簡訊資料安全

SMS Data Security

企業簡訊會產生不同性質的資料，若將所有資料都視為同一類型，容易造成保存與權限政策失焦。

EVERY8D 依訊息方向、用途與系統功能區分資料型態，並以服務必要性決定其處理方式。

常見資料類型

資料類型	說明	安全治理重點
MT（Mobile Terminated）	企業由平台送往使用者手機的訊息。	重點在訊息內容、收件門號、查詢權限與保存期限。
MO（Mobile Originated）	手機使用者主動回覆至企業指定接收端的訊息。	回覆內容具有不可預測性，應特別重視用途、最小化與保存政策。
OTP / 驗證碼	用於登入、交易或身分驗證的一次性訊息。	應避免不必要長期保留，並確保訊息流程、帳號與 API 存取安全。
DLR（Delivery Receipt）	電信網路回傳的投遞狀態或結果。	屬傳送狀態資訊，與使用者主動回覆的 MO 性質不同。
傳送中繼資料	如時間、狀態、服務識別與必要的路由資訊。	僅保留營運、對帳、客服或稽核所必要的範圍。

簡訊內容的安全原則

- 避免將完整密碼、完整金融敏感資訊或不必要的個資直接放入簡訊內容。
- OTP 類訊息應搭配有效期限、驗證次數與後端風險控制，而非只依賴簡訊本身。
- MO 回覆內容由收件者主動產生，企業在設計雙向互動流程時應明確限制用途與後續保存。
- DLR 用於傳送結果追蹤，不應與使用者主動輸入的回覆內容混為同一資料類型。

新客導入建議　若服務包含雙向簡訊、OTP 或大量通知，建議在導入階段即共同確認資料欄位、

保存期間、查詢角色與 API 權限，以避免上線後再補做資料治理。

7. API 與應用安全

API & Application Security

API 是企業系統與 EVERY8D 之間最重要的自動化介面，也是必須被妥善治理的信任邊界。安全設計的重點不只在加密連線，也包含憑證生命週期、來源限制、呼叫行為、權限範圍與錯誤處理。

API 安全控制

面向	控制方向
安全傳輸	對支援的介接方式使用 TLS 等安全傳輸，降低傳輸途中被攔截或竄改的風險。
憑證與金鑰	API Key / 介接憑證應妥善保管，避免直接寫入公開程式碼或多人共用。
來源與權限	依方案與介接情境，可採來源限制、帳號權限與功能範圍控管，降低非預期呼叫。
呼叫行為	對大量、異常或不合理的呼叫行為建立監控、限制或告警機制。
錯誤處理	回應內容避免揭露不必要的內部資訊；重要錯誤與異常活動納入記錄與追蹤。
開發變更	新功能或重大變更在設計與上線前納入權限、資料、日誌與回復需求評估。

客戶系統介接建議

- 不同環境（開發 / 測試 / 正式）避免共用同一組正式憑證。
- 設定憑證輪替與撤銷流程，避免永久有效的金鑰被長期使用。
- 伺服器端呼叫優先於將敏感憑證置於前端或行動應用程式。
- 建立發送量、錯誤率與異常時段的監控，以利及早辨識帳號或金鑰異常。

8. 日誌、監控與威脅偵測

Logging, Monitoring & Threat Detection

沒有記錄，就難以判斷系統發生了什麼；只有記錄而沒有監控，也無法及時發現異常。EVERY8D 將日誌與監控視為安全營運的核心能力，對重要登入、系統、應用、權限與端點活動建立必要的記錄與告警機制。

監控範圍

監控類別	關注行為
身分與登入	異常登入、高權限使用、帳號狀態與權限異動。
系統與主機	服務狀態、資源異常、端點安全告警與可疑行為。
應用與 API	異常錯誤、呼叫量變化、非預期來源或大量操作。
資料與管理操作	重要查詢、匯出、設定變更與管理性操作。
網路與邊界	異常連線、掃描、阻擋事件與非預期流量。

從「紀錄」到「處置」

Collect	收集重要系統、應用、帳號、端點與網路的必要日誌。
Correlate	依時間、來源、帳號與事件類型進行關聯，找出單一設備看不見的異常。
Alert	依嚴重度與可疑程度觸發告警，交由指定角色判讀。
Respond	針對高風險活動啟動阻擋、隔離、權限處置、調查與紀錄。

可追溯性　白皮書中的「可追溯」並不代表無限制蒐集所有操作資料，而是對安全與稽核真正需要的活動保留適當紀錄，並搭配保存與權限政策。

9. 弱點與端點安全

Vulnerability & Endpoint Security

企業平台的安全狀態會隨著作業系統、套件、應用程式與攻擊技術持續變化，因此資安不能只依靠一次性的建置。EVERY8D 透過弱點盤點、修補、端點偵測與防護、組態管理及變更控制，降低已知弱點與惡意程式帶來的風險。

持續性安全管理

控制項	管理方向
弱點掃描	定期或依風險執行系統與服務弱點檢視，追蹤高風險項目的處理狀態。
修補管理	依漏洞嚴重度、系統重要性與營運影響安排修補或緩解措施。
端點防護	重要主機與管理端點採防毒 / EDR 等偵測與防護機制，提升可疑活動能見度。
組態管理	降低預設帳號、不必要服務、過度開放權限與非必要管理入口。
變更控制	重大系統與安全設定變更保留核准、執行與回復資訊，降低變更本身造成的風險。
驗證與追蹤	修補或調整後進行必要驗證，並持續觀察是否仍有相同或衍生風險。

風險排序原則

弱點不只看 CVSS 或單一分數，也應綜合考量是否對外暴露、是否已有可利用方式、系統是否承載關鍵服務、可否被其他控制措施緩解，以及修補是否會影響營運。以風險排序取代「看到漏洞就同等處理」，才能兼顧安全與服務穩定。

10. 備援與營運持續

Backup, BCP & Disaster Recovery

對企業通訊服務而言，「安全」也包含可用性與復原能力。EVERY8D 將重要系統、設定與資料納入備份與復原管理，並以異地或雲端備援、復原程序與演練思維降低單點故障、設備異常或其他重大中斷對服務的影響。

營運韌性的四個環節

Backup	依系統重要性與資料特性建立備份策略，避免備份與正式環境完全依賴同一故障域。
Protect	備份本身同樣受到權限、存取與保存管理，降低備份遭誤刪或未授權存取的風險。
Recover	建立系統與資料復原程序，明確區分基礎設施、應用、資料與對外服務的恢復順序。
Exercise	透過演練、驗證或實際復原測試持續確認備份「可用」，而不是只有備份檔「存在」。

BCP / DR 管理重點

項目	說明
服務優先順序	依服務影響程度決定核心功能與依賴系統的恢復順序。
復原目標	RTO / RPO 等目標依服務方案、風險與契約需求定義，非所有系統採相同數值。
異地 / 雲端備援	降低單一機房或單一儲存環境故障對備份與復原能力的影響。
通訊與決策	異常期間建立內部決策、客戶溝通、技術處理與紀錄責任。

重要觀念　備份不是「把資料多存一份」而已；真正的營運韌性來自可隔離、可驗證、可還原、可按優先順序恢復。

11. 供應鏈與第三方管理

Third-Party & Supply Chain Security

企業簡訊服務牽涉電信網路、雲端或備援資源、軟體與資安服務等第三方。EVERY8D 將第三方視為整體安全邊界的一部分，從必要性、權限、資料範圍、服務依賴與終止管理等面向降低供應鏈風險。

第三方風險管理重點

面向	管理原則
必要性與範圍	第三方僅取得履行服務所必要的系統、資料與權限。
身分與權限	外部維護、顧問或供應商帳號應可識別、可撤銷，並避免永久保留不再使用的權限。
資料與保密	涉及客戶資料或敏感資訊時，依契約、保密與個資要求限制使用與揭露範圍。
服務依賴	評估電信、網路、雲端、備援與關鍵軟體的依賴程度及替代 / 復原策略。
安全佐證	依風險與需求取得或檢視適當的安全說明、測試結果、合約條款或第三方佐證。
終止管理	合作終止時回收帳號、憑證、遠端連線與不再必要的資料或存取權。

供應鏈的共同安全

第三方本身具有大型品牌、電信商或雲端服務商身分，不代表供應鏈風險自然消失；安全仍取決於實際介接方式、權限邊界、資料流向與責任分工。EVERY8D 因此以「服務必要性與最小授權」作為第三方管理的基本原則。

12. 合規與企業客戶保障

Compliance & Customer Assurance

大型企業、金融機構與政府單位在導入外部通訊服務時，通常會從個資、資安治理、存取控制、弱點管理、日誌、備援與委外管理等面向進行審查。EVERY8D 的白皮書與資安佐證，目的在讓客戶可以把平台安全能力對應到既有的供應商風險與稽核框架。

客戶可要求的安全資訊

類型	可提供或配合方向
資安問卷	依合理範圍回覆企業供應商資安評估、個資或委外管理問卷。
架構與控制說明	提供本白皮書、資料流與必要的控制機制說明，協助資訊 / 資安單位判讀。
資料治理說明	依服務類型說明資料欄位、用途、保存、查詢與刪除等原則。
測試與佐證	涉及弱點掃描、第三方檢視或其他報告時，依保密義務、適用範圍與版本提供必要資訊。
合約與責任	安全與資料處理責任以正式合約、SLA、個資約定及雙方確認的服務範圍為準。

法規與標準的使用方式

EVERY8D 的安全管理持續參考企業常用的資訊安全與個資治理要求，並依服務特性與適用法規落實必要控制。若客戶要求特定認證、特定控制框架或產業規範，應在採購 / 導入階段共同確認適用範圍，而非僅以單一標章取代實際的架構與控制審查。

不過度宣稱　本白皮書刻意不以未經正式文件驗證的認證、單一百分比或固定 RTO / RPO 作為宣傳內容。對企業客戶而言，可被驗證的控制與清楚的責任邊界，比過度簡化的安全口號更重要。

附錄 A 企業客戶資安評估快速索引

Security Assessment Quick Reference

下表可作為資訊、資安、採購與稽核單位進行初步供應商審查時的快速索引。若需更深入的技術佐證，可依實際服務方案與保密條件另行提供。

常見稽核項目	EVERY8D 對應機制	參考章節
身分驗證	帳號治理、管理性存取、多因素驗證策略	4
最小權限	角色權限、職責分離、高權限治理	4
資料傳輸	TLS 等安全傳輸與 API 身分驗證	5、7
資料保存	生命週期、用途管理與到期刪除	5、6
資料遮罩	依介面與角色限制敏感欄位顯示	5
API 安全	金鑰、來源 / 權限、呼叫監控與錯誤處理	7
日誌管理	重要登入、系統、應用、管理與網路活動記錄	8
威脅偵測	集中監控、端點告警、異常關聯與處置	8、9
弱點管理	弱掃、修補、組態與風險排序	9
惡意程式防護	防毒 / EDR 與端點安全監控	9
備份與復原	備份保護、異地 / 雲端備援與復原驗證	10
營運持續	BCP / DR、服務優先順序與復原程序	10
第三方管理	最小授權、資料範圍、終止與服務依賴管理	11
個資與合規	資料治理、問卷、合約與適用法規確認	12
異常應變	監控、升級、處置、溝通與紀錄程序	2、8、10

建議採購流程　新客戶可將本白皮書作為第一層安全審查文件；若進入正式採購，再依內部風險等級提出進階問卷、架構訪談、合約條款或必要的第三方佐證要求。

結語｜以可被驗證的安全能力，支撐企業通訊

Security as an Operating Capability

EVERY8D 的資安目標，不是用單一產品或單一標章宣稱「絕對安全」，而是透過清楚的治理、分層架構、身分權限、資料最小化、持續監控、弱點管理與營運韌性，持續降低企業通訊服務的實際風險。

對企業客戶而言，一個成熟的通訊平台應能回答三個問題：資料如何被處理與刪除？誰能接觸系統與資料？當系統或環境發生異常時，平台如何偵測、處置與恢復？本白皮書所建立的架構，就是以這三個問題為核心，讓安全能力能被理解、被檢視，也能持續改進。

名詞說明

名詞	說明
MT	Mobile Terminated，企業由平台送往手機使用者的訊息。
MO	Mobile Originated，手機使用者主動回覆至企業端的訊息。
DLR	Delivery Receipt，電信網路回傳的訊息投遞狀態或結果。
OTP	One-Time Password / 一次性驗證碼，用於登入、交易或身分驗證。
MFA	Multi-Factor Authentication，多因素驗證。
EDR	Endpoint Detection and Response，端點偵測與回應。
BCP	Business Continuity Planning，營運持續計畫。
DR	Disaster Recovery，災難復原。
RTO / RPO	復原時間目標 / 復原點目標，依服務與契約需求定義。

文件版本

版本：2026 Edition | 適用：EVERY8D 企業簡訊平台新客戶資安說明 | 文件性質：對外安全白皮書第一版

聯繫與後續　若客戶需進一步進行資安問卷、系統介接安全審查、資料保存政策確認或供應商風險評估，可由 EVERY8D 專案與技術窗口依實際服務範圍提供進一步說明。