

資安白皮書

睿鼎數位股份有限公司

目錄

目錄 1

一．前言 2

二．資料傳輸 2

三．資料保護 2

四．內控稽核 3

五．系統可用性 3

六．系統監控管理 4

七．系統實體安全 4

八．結論 5

一．前言

為了能與用戶提供更好的服務體驗，品牌公司多半需要與第三方公司進行服務系統整合來達成目標。除了業務上的需要外，這些整合多半會帶來許多額外需要考量的資訊安全議題，如系統的穩定性、安全性與資料保護措施等等。

睿鼎數位作為 O2O 服務提供商的領導品牌，了解我們的客戶對於資訊安全上的重視與需要。因此我們在資料傳輸、資料保護、內控稽核、系統可用性、系統監控管理、系統實體安全的層面上採取了許多必要的安全措施。本文件將會針對這些層面來說明我們如何提供這些保障。

二．資料傳輸

在網際網路間傳輸資料時，其保密性與完整性是最重要的。在兩者有被保障的情況下，資料才不會於傳輸中遭到截取、窺竊而洩漏資料，甚至是被篡改內容。睿鼎數位的系統，在公開傳輸資料時，都會使用 TLS（Transport Layer Security）協定，並支援最新的 TLS 版本，來保障透過 HTTP 來傳輸資料時的安全性。

我們所使用的 TLS 的憑證，是經由國際組織認證的憑證頒發機構（Certificate Authority）所發行的有效憑證，而非使用私有憑證。除此之外也會定期更新，確保我們的系統隨時都能與客戶系統和消費者使用的瀏覽器間正常地加密傳輸。

三．資料保護

在資料進入系統後，我們會使用數道措施來保護這些資料，來減少資料外洩、遺失等可能的風險。我們使用了資料庫透明資料加密（Transparent Data Encryption）技術，讓資料在進入資料庫後，就隨時保持著被加密的狀態；只有在正常授權的存取方式，才能夠還原出資料的內容。

為了保護客戶的資料不會在設備異常的情況下遺失，我們還會定期自動地進行對資料庫與主機進行備份。備份時我們遵循著業界常用的 3-2-1 備份原則，使用不同的儲存媒體與地點來存放備份資料，並加上存取限制讓非授權的人員無法取得備份檔案。同時，這些備份也有使用透明資料加密技術保護，因此在資料庫外的資料也有被加密，同樣需要通過驗證後才可被還原。

四．內控稽核

我們的開發與維運工程師，都需要經過教育訓練與數次檢閱通過認可後，才可以正式地參與和客戶有關的開發與維運工作。

開發工程師，不僅需要依規範進行程式更新管理，並且需要完成測試流程、自動檢測與程式碼審查後，才可以將程式更新，為了是減少程式問題造成系統與資料錯誤的風險。除了存取程式碼之外，開發人員均使用測試資料進行開發，無法任意存取客戶的資料。唯有在業務上需要時（例如排除系統問題），才能與授權的資深維運工程師一同確認線上的資料狀態。

維運工程師，在進行系統維護時，都需要至少兩位工程師同時進行：一位執行作業，另一位復核檢查。這些維運工作，工程師都需要事先熟讀並演練過作業流程，並在執行時留下過程紀錄與執行指令，來做為事後檢查的依據。我們的系統也只有授權的工程師才可以存取；這些人員不但需要經過多重驗證才可以使用，存取時系統也會自動留下紀錄作為日後稽核使用。

五．系統可用性

為了避免造成客戶日常作業影響，系統的可用性是我們很重視的一環。我們採取了數個措施來維持系統的穩定度，目的就是讓設備在發生異常狀況時也能繼續正常服務。首先，我們的服務使用了負載平衡器，讓每個系統隨時都有二台以上的主機在線上服務，一旦主機出現異常，就會自動將有問題的主機下線，避免影響系統整體穩定度。負載平衡器本身也

有自動備援，避免系統單點故障導致服務中斷的狀況。資料庫除了日常的資料備份外，隨時也有複寫的備援機在，會在主系統發生問題時，自動接替，來減少對系統整體的衝擊。

這些系統設備不僅都有備援，而且還同時存放於不同的實體機房內，讓我們的系統即使在單一機房出現障礙時，仍有正常服務，不會影響客戶作業。

除了維持系統穩定外，我們也能依照客戶需要擴充系統的承載量，讓客戶可以放心地使用我們的服務。

六．系統監控管理

我們監控了系統許多的指標，務求是全時全面地能得知系統的即時狀況。這些指標包含如請求執行時間與數量、系統錯誤率、流量、儲存空間等等與服務運行有關的重要資訊。這些資訊都會被收集進監控的系統內，由維運工程師負責管理，讓我們能隨時發現系統異常。當監控系統發現異常發生時，也自動會透過簡訊、Email 等數種管道同時發送告警給多位負責人員，讓我們可以得知異常發生後馬上進行處理。

我們的系統都有防火牆保護，並以最小權限原則使用白名單的方式只開放必要的連線通過。同時，為避免系統上的資安弱點造成損害，我們定期更新主機系統軟體元件，來防範可能的弱點。我們也會定期的對系統主機進行弱點掃描，來掌握程式與主機的狀況，即時修正可能的漏洞，避免資訊資料外洩，還會針對任何外部的可疑攻擊行為進行監測與阻擋，務求早期防範。

七．系統實體安全

我們的系統都建置於符合業界標準的資料中心機房內進行管理。在資料中心的監管下，除了硬體應該具備的溫濕度控管、雙迴路電源與備援、避震、防火等條件外，還有嚴格的人員出入管理政策。

所有需要接觸硬體的人員，都需要事先申請並提供事由原因，經過審核同意後才可進入。嚴謹的登記與門禁管制，就算是授權人員進出機房也都需要經過驗證，進入的人員也無法接觸沒有申請的硬體機房。這些機房也都有監視攝影與安全人員來保護可能的非法入侵。

這些資料中心機房同時也都有通過數個資安管理 ISO 認證，如 27001、27017 的資安管理認證與 9001 的品質管理認證。此外，我們選用的數個實體機房，彼此之間均相隔數十公里且依賴著不同的電源與網路來源，務求就是服務的穩定性。

八．結論

維護系統穩定並保護客戶資料，是我們在資安議題上最主要的考量。我們投資在這些措施上，目的就是讓我們可以提供一個讓客戶放心使用的系統服務。睿鼎數位將會持續投資在這些項目上，不斷地改善加強資安措施，來讓我們的客戶可以更專注於商業需求與創新上。