中國聯塑集團控股有限公司

（於開曼群島註冊成立的有限公司）

（股份代號：2128）

（「本公司」）

信息安全與隱私保護政策（「本政策」）

1. 目的

中國聯塑集團控股有限公司(「本公司」)高度重視信息安全與隱私保護工作，嚴格遵守《中華人民共和國網絡安全法》《中華人民共和國數據安全法》《中華人民共和國個人信息保護法》等及其他適用國家的相關法律法規，參考 ISO/IEC 27001 推進信息安全管理體系建設，落實信息及數據安全保護措施。本公司制定本政策旨在規範信息處理行為、保障信息安全、維護相關方合法權益。

2. 適用範圍

本政策適用於本公司及旗下分子公司、控股企業的所有人員、所有業務與運營活動，並涵蓋信息收集、存儲、處理、傳輸、使用及銷毀的全流程。本公司要求與本公司有業務往來的供應商、經銷商、合作夥伴和其他利益相關方積極遵守本政策，共同構建安全可靠的信息環境。

3. 責任部門

信息管理中心為信息安全與隱私保護的主要責任部門，負責統籌協調信息安全與隱私保護工作，包括政策制定、修訂、執行監督、培訓宣傳以及隱私問題的接收、調查與處理等。各部門負責人為本部門信息安全與隱私保護的第一責任人，確保本部門人員嚴格遵守相關規定，協同保障本公司信息系統的信息安全。

4. 政策內容

4.1 風險管理

本公司不斷推進信息安全管理體系完善、升級，將信息安全管理政策與相關工作的實施整合融入本公司的風險與合規管理環節，本公司定期對信息安全與隱私保護風險進行識別、評估和分析，針對可能存在的風險點制定相應的防控措施和應急預案。信息管理中心通過安全威脅情報平台、行業安全網站、第三方安全機構合作等方式，監控和收集各類信息安全威脅情報，並對所收集的威脅情報實施評估與分析。對於評估判定為高風險威脅及時制定內部應對措施，通過企業郵箱、內部系統發布預警，指導各部門人員做好安全防範。

4.2 信息安全管理體系

信息管理中心按照「計劃、執行、檢查、改進」的循環來建立和運行信息安全管理體系。每年都會由內審部門牽頭，對本公司的信息安全管理工作進行系統性的內部審核。通過分析各種安全檢查結果，關注行業內的安全動態和最新威脅情報並持續地完善安全管理體系。

4.3 內外部審計

通過內審部的定期信息安全內部審核，核查各部門政策落實情況；同時定期邀請具備資質的第三方機構開展外部審計，重點審查數據合規性與隱私保護情況。審計發現問題需限期整改，整改結果納入部門考核，確保政策有效執行。

4.4 信息與數據安全

為確保信息及數據的保密性、完整性、可用性，本公司強化信息傳輸全流程安全管控，通過部署加密技術、存取控制、數據備份、備份數據恢復等手段，防止信息及數據被篡改、泄露或破壞。

4.5 員工個人責任與培訓

本公司明確全體員工在信息安全與隱私保護中的個人責任，每位員工均有義務保護本公司信息資產與客戶數據，嚴格遵守安全操作規程。本公司通過定期培訓，提升員工的信息安全與

保密意識，確保理解並履行與崗位對應的信息安全職責。

4.6 安全事件與漏洞報告流程

本公司建立並維護清晰、便捷的安全事件、漏洞或可疑活動上報渠道，確保所有員工能夠及時報告潛在的安全風險。員工在發現任何信息安全事件、系統漏洞或涉及信息與隱私安全的可疑活動時，應迅速上報至信息管理中心，接報後第一時間進行評估確認，並啟動相應的響應處理流程。通過建立和執行報告流程，能有效地應對安全威脅，將安全風險降至最低。

4.7 隱私信息收集與使用管理

本公司收集客戶個人信息時，明確告知收集範圍與用途，並獲得客戶同意。按照法律的規定在合理必要期限內存儲客戶個人信息，採取各種符合行業標準的安全措施來防範客戶個人信息泄露。並積極建立數據分類分級制度、數據安全管理規範、數據安全開發規範來管理規範個人信息的存儲和使用，確保收集的個人信息與本公司提供的服務相關。

4.8 合作夥伴管理

本公司要求合作夥伴 (包括供應商等) 積極配合信息安全與隱私保護相關制度與要求。在與重點合作夥伴確立合作之前，本公司積極開展信息安全相關盡職調查，確保不存在重大風險。同時，要求合作夥伴簽署保密協議，明確雙方保密責任和義務。本公司對供應商實施全流程信息安全管理，明確供應商在信息資產存取的安全責任與操作規範；規範授權流程，定期審查授權合理性，動態調整授權範圍等措施，避免因授權不當導致敏感信息泄露，確保本公司信息資產的安全性與保密性。

4.9 第三方披露政策

本公司承諾將相關數據分享、轉移或提供給第三方時，嚴格遵守國家、註冊成立地與上市地的相關法律法規和隱私保護準則，以確保數據轉移活動符合法律規定並尊重數據主體的權利。數據轉移的目的和範圍不能超出收集時所聲明內容，涉及敏感及機密性的數據須採用安全傳輸通道或加密後傳輸。數據輸出者必須獲得接收者的明確承諾。如涉及數據的跨境傳輸，需遵從當地法律法規的要求。

4.10 業務連續性管理

本公司圍繞信息安全保障需求，在業務影響分析和風險分析中，依據多方面因素識別支撐信息安全的關鍵系統，並定期對信息系統進行安全風險評估，對安全風險相關影響及可能性進行實際分析；每年開展突發事件信息安全風險防範措施及應急響應工作的全面評估審計，將信息安全保障納入全面風險管理體系，以保證信息安全管理工作的連續性，有效性和合規性。

5. 監察與修訂

本政策的有效執行由董事會負責監察，董事會授權可持續發展委員會進行日常監督與定期檢討，以確保本政策在應對新興網絡威脅和滿足法律法規要求方面的持續適宜性、充分性和有效性。當內外部條件發生重大變化時，委員會將及時向董事會提出修訂建議，經董事會審批後實施。

6. 信息披露

本政策全文，以及與信息安全與隱私保護有關的主要方案和行動，將通過公告、培訓等方式傳達至所有為本公司工作的人員，並在本公司官方網站予以披露，供公眾查閱。

7. 附則

本政策由本公司董事會負責解釋，自董事會審議通過之日起生效，修訂時亦同。