1 目的：

為定義台灣保來得股份有限公司(以下簡稱本公司)的資訊安全手冊，使全體同仁能遵守資訊安全的要求以達成：

1.1 輔助使用者之各項業務順利運行，確保各項資訊媒體之安全，達成本公司資訊安全目標。

1.2 遵從國內外車用資安法規要求，提升產品開發過程中相關資安措施，增強客戶信心以提升企業品牌價值和競爭力。

2 範圍：

本公司所有正式員工、約聘員工、派遣人員等公司所聘用之人員及外來訪客、廠商等單位人員皆適用之。

3 權責單位：

本公司資訊安全管理制度及 TISAX 權責單位。

4 名詞定義：

4.1 資訊安全

即確保資訊的機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)，使資訊能安全地、正確地、適切地及可靠地運用於達成本公司經營目標之規劃、執行、管理及相關作為上

4.2 資訊安全管理制度

整體管理系統的一部分，以營運風險導向為基礎，用以規劃、建立、實施、運作、監督、查核、維護與改善資訊安全管理制度。

4.3 機密性

確保只有獲得合法授權的使用者可以存取資訊。

4.4 完整性

保障資訊與資訊處理方法的正確與完整性。

4.5 可用性

確保獲得授權的使用者於有需求時能適時存取資訊及相關資產。

5 作業內容：

5.1 資訊安全管理制度

5.1.1 概述

5.1.1.1 本公司為展現貫徹資訊安全管理的決心，確保所有資訊與資訊系統獲得適當保護，依照 ISO/IEC 27001：2022 及 TISAX 標準之要求建立、記載、實施及維護資訊安全管理制度，並持續改進系統的有效性。

5.1.1.2 資訊安全管理制度第一至四階文件是參照 ISO/IEC 27001：2022 國際資訊安全管理標準，選擇適當之控制措施，制訂「適用性聲明書」(8012-0001-0001)，條列本公司所採用之控制點及驗證範圍。

5.1.1.3 本公司「資訊安全聲明」(8012-0001-0002)、(8012-0001-0003)與資訊安全手冊作適當結合。

5.1.2 資訊安全目標

5.1.2.1 對於本公司所儲存或傳遞之資訊採取適當之保護與防範措施。

5.1.2.2 降低發生毀損、失竊、洩漏、竄改、濫用與侵權等資通安全事件時之衝擊。

5.1.2.3 持續提升各資訊服務系統所有作業之機密性、完整性與可用性。

5.1.3 目標量測方式

資訊安全管理制度目標量測方式應說明如何量測資訊安全管理制度目標之有效性，如何使用這些量測去評鑑控制措施及量測時機，產生可比較與可再製的結果，並依據「資訊安全指標管理規定」(8011-0004G)辦理。

5.1.4 運作機制

本公司依照 ISO/IEC 27001：2022 標準，採用"Plan-Do-Check-Act"（PDCA）之循環運作模式，建立與實施資訊安全管理制度(ISMS)，並維繫其有效運作與持續改進。

5.1.4.1 規劃與建立(Plan)：依據本公司整體策略與目標，藉由成立資訊安全管理組織，控制潛在之威脅及漏洞，規劃風險評鑑、設計與建置控管機制，以建立資訊安全管理制度。

5.1.4.2 實施與運作(Do)：依據評估規劃之結果，建立或修正應有之管控機制。

5.1.4.3 監督與稽核(Check)：監督資訊安全管理制度各項作業之落實執行，並評估及稽核其有效性。

5.1.4.4 維護與改進(Act)：根據監督稽核之結果與建議，執行矯正措施，改善並執行應有之控管機制，以持續維護資訊安全管理制度之運作。

5.2 管理責任

5.2.1 應建立資訊安全管理組織，負責推動、協調及督導下列資訊安全管理事項：

5.2.1.1 資訊安全政策之核定、宣導及督導。

5.2.1.2 資訊安全責任之分配及協調。

5.2.1.3 宣導符合各項資訊安全目標、資訊安全政策及法律規範下之責任，以及持續改進之需求。

5.2.1.4 充分提供資源以建立、實作、運作、監視、審查、維持與改進資訊安全管理制度。

5.2.1.5 決定接受風險與可接受風險等級的準則。

5.2.1.6 資訊安全稽核計劃制定、資訊風險評估及不定期之資訊安全測試。

5.2.1.7 施行資訊安全管理制度之管理審查。

5.2.1.8 鑑別資訊安全管理制度之內外部利害關係人，考量其對本公司之資訊安全需求與期望，並決定內外部所需之溝通。

5.2.1.9 資訊安全事件之檢討及監督，考量可能影響資訊安全管理制度之內外部議題。

5.2.1.10每年實施資訊安全相關教育訓練與宣導，評估所提供資訊安全教育訓練之有效性。

5.2.1.11其他資訊安全事項之核定。

5.2.2 管理審查

本公司管理審查作業由資訊安全管理委員會執行，管理階層應每年執行 1 次管理審查以持續確保資訊安全管理制度運作之適切、充足與有效，審查範圍包括資訊安全管理制度改進方案與變更需求之評估，審查結果應予詳實記錄並妥善保存。

5.2.3 資訊安全指標

本公司應建立資訊安全指標評估資訊安全的績效及資訊安全管理制度之有效性，資訊安全指標應至少包含量測之項目、方式、時間、頻率及負責人員等資訊，以確保資訊安全指標量測之有效性。資訊安全指標應與本公司資訊安全政策作適當結合。

5.2.4 資訊安全內部稽核

管理階層應確保定期或不定期進行安全評估或稽核作業，以檢討控管目標、措施與程序是否合乎相關標準、法令規章或資訊安全需求，並依預期規劃有效執行與維持，以持續增進資訊安全管理制度的有效性。

5.2.5 資訊安全管理制度之改善

5.2.5.1 持續改善

本公司應透過內外部稽核結果、資訊安全事件分析、矯正措施及管理審查等機制，持續增進資訊安全管理系統之有效性。

5.2.5.2 矯正措施

本公司應採取適當的控管措施，以減少資訊安全管理制度建置與運作過程中所發現之不符合事項，並防止再度發生。矯正措施之作業程序如下：

5.2.5.2.1 識別各項不符合事項。

5.2.5.2.2 判定各項不符合之原因。

5.2.5.2.3 評估所需採取之矯正措施，以確保各項不符合事項不再重複發生。

5.2.5.2.4 決定及實作所需之矯正措施。

5.2.5.2.5 記錄及審查所採取之矯正措施的有效性。

5.2.6 文件管理系統

5.2.6.1 文件管制

本公司資訊安全管理制度相關文件之管制方式，第一至四階資訊安全文件之管制、核發與變更均應依據本公司文件管制相關作業程序之規定辦理。

5.2.6.2 紀錄管制

本公司資訊安全管理制度運作所產生之任何文件、表單及紀錄，應指定相關紀錄保存人員妥善保管，訂定保存期限與核閱權限，以利追蹤資訊安全管理制度之執行狀況，維護系統有效運作。

5.2.7 資訊安全政策指導與覆核

本公司資訊安全政策每年至少評估內容 1 次，檢討覆核與修訂，以符合內外部利害關係團體的需求與期望，確保資訊安全實務作業之有效性。

5.2.8 實施規範與法令之遵循

所有人員均須遵循此資訊安全政策，違反者須依本公司相關規定予以處分，如涉有相關刑責或法律責任者，如營業秘密法、著作權法、個人資料保護法等，將衡酌情節追訴其法律責任。

一、 相關作業辦法

作 業 辦 法 代 號	作 業 辦 法 名 稱
8011-0001G	資訊安全管理制度實施管理規定
8011-0002G	資訊安全文件與紀錄管理規定
8011-0004G	資訊安全指標管理規定
8011-0015G	資訊安全查核作業管理規定

二、 表單索引

表 單 代 號	表 單 名 稱
8012-0001-0001	適用性聲明書
8012-0001-0002	資訊安全聲明_廠內
8012-0001-0003	資訊安全聲明_廠外

文 件 變 更 記 錄		
版 本	變更日期	變更內容
第 1 版	2023/2/23	資訊安全管理制度導入建置
第 2 版	2023/11/20	TISAX 稽核調整目的敘述