四維航業股份有限公司
個人資料保護及管理政策

第一條　制定目的及依據

本公司為落實對於個人資料之保護及管理，確保本公司對個人資料之蒐集、處理及利用皆符合「個人資料保護法」（下稱「個資法」）、「個人資料保護法施行細則」、「船舶運送業個人資料檔案安全維護計畫及處理辦法」等相關法規之要求，特制定本「個人資料保護及管理政策」（以下簡稱「本政策」）以作為本公司之個人資料保護最高指導方針。

第二條　適用範圍

本公司內所有員工，以及客戶、供應商、外部顧問等協力廠商所屬人員，皆為本政策所涵蓋之對象。

第三條　名詞定義

一、 個人資料（下簡稱「個資」）：指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。個資之定義及範圍如日後因應主管機關或法規變動配合修訂時，以修訂後之定義及範圍為準。

二、 特種個資：指有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個資。

三、 當事人：指個資之本人。

四、 其餘用詞定義參見個資法第二條之規定。

第四條　個人資料之管理

一、 對於個資之蒐集、處理及利用，應尊重當事人之權益，依法令相關規定及誠實信用原則為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯。

二、 本公司所蒐集、利用、處理之個資包括但不限於員工個資、客戶或客戶員工個資、供應廠商或其員工個資等；蒐集、利用、處理之個資種類以一般性個資為主，非營運或法規所必要，本公司不蒐集特種個資。

三、 為尊重當事人對其個資之法定權利，如需執行國際傳輸，本公司並承諾以高度機密性處理個資，並應在合法、適當、充分保護之狀況

下實施。

四、 如有委託第三方蒐集、處理與利用個資時，應適當監督受委託者，並確認其採取之個資管理規範及制度，符合法令與本政策之規定。

五、 本公司應明定當事人行使個資法第三條所定權利之相關事項，包括當事人行使權利之方式、所需支付之費用及本公司對當事人請求之審查方式等。

六、 本公司設置個資保護管理小組作為專責管理單位，由公司治理主管擔任召集人，成員由行政管理部、業務部及資訊室等各部門人員組成，負責建立和維護各項個資處理程序之管理機制，並定期向董事會報告執行情形。

第五條　個人資料之安全維護

一、 本公司對於所蒐集、處理或利用之個資，將採取適當之安全維護及管理措施，以防止個資被竊取、竄改、損毀、滅失或洩漏。為確保個資之安全與正確，並應定期檢視資料檔案系統之安全維護。

二、 為維護所保存個資之安全，本公司應依執行業務之必要，設定相關人員接觸個資之權限及控管其接觸情形，並應與所屬人員約定保密義務。

第六條　個人資料之紀錄保存及持續改善機制

一、 對於依法所定之個資管理制度及安全維護及保護措施之實際施行情況，管理單位應留存紀錄資料或相關證據。

二、 本公司為持續改善個資安全維護，管理單位或人員應檢視、修訂個資保護事項，並定期提出相關評估報告。

第七條　業務終止後個人資料處理辦法

為防止個資被竊取、竄改、毀損、滅失或洩漏，管理單位應依法明定及辦理業務終止後個資處理事項。

第八條　通報機制

為因應個資之竊取、竄改、毀損、滅失或洩漏等安全事故（下簡稱「個資事故」），應訂定相關緊急應變處理程序、通報及預防機制，包括個資事故發生後應採取之各類措施、個資事故發生後應受通報之對象、通報方式、通報事項、回應機制及個資事故發生後，其影響之評估、矯正預防措施之研議機制及後續處分。

第九條　個資保護管理小組

一、 管理單位應制定個資管理制度風險評估，要求各部門定期確認個資管理程序是否依照法規或本公司相關政策及規範執行，並對管理制度執行風險評估與改善，以確保本公司個資保護管理相關作業符合相關法令規範等要求。

二、 管理單位除應依本政策建立管理制度，並應就個資管理保護，積極擬定個資準則、相關辦法、文件同意書等並進行推展；於個資法規有變動時，並應及時制定及修正管理程序作業並執行。

第十條　教育訓練及罰則

一、 為確保本公司對個資之管理皆符合現行法律規定，本公司將定期針對所有人員進行個資保護及管理之訓練，並留存相關紀錄。

二、 本公司對於任何人員如有違反個資保護之情事，將依內部人事管理規章、員工獎懲規範進行相關懲處，並視情節輕重依法送辦。

第十一條　申訴與舉報

如有發生可能導致本人權益受損的個資事故或情況，以及發現可能有違反本政策之情事時，本公司之員工、外部單位或自然人，皆可透過管理單位設置之個資保護電子郵件信箱進行申訴或舉報，本公司將嚴格保護舉報人之相關資訊，以維護舉報人之權益。

第十二條　施行

本政策經董事會通過後生效施行，修正時亦同。

本政策於114年12月23日訂定
第一次修訂於115年3月10日

SHIH WEI NAVIGATION CO., LTD.

Personal Data Protection and Management Policy

Article 1 Purpose and Legal Basis

In order to implement the protection and management of personal data and to ensure that the collection, processing, and use of personal data by the Company comply with the requirements of the "Personal Data Protection Act" (hereinafter referred to as the "PDPA"), the "Enforcement Rules of the Personal Data Protection Act", the "Regulations of Governing Personal Data File Security Maintenance Plan and Processing Method for the Vessel Carrier", and other applicable laws and regulations, the Company hereby establishes this "Personal Data Protection and Management Policy" (hereinafter referred to as the "Policy") as the highest guiding principle for personal data protection within the Company.

Article 2 Scope of Application

This Policy applies to all employees of the Company, as well as personnel of customers, suppliers, external consultants, and other third-party partners.

Article 3 Definitions

1. Personal Data (hereinafter referred to as "Personal Data"):
   Refers to a natural person's name, date of birth, national identification number, passport number, physical characteristics, fingerprints, marital status, family information, education, occupation, medical records, medical treatment, genetic information, sexual life, health examination records, criminal records, contact information, financial status, social activities, and any other information that may directly or indirectly identify a specific individual.
   The definition and scope of Personal Data shall be subject to amendment in accordance with changes made by competent authorities or relevant laws and regulations.

2. Sensitive Personal Data:
   Refers to Personal Data relating to medical records, medical treatment, genetic information, sexual life, health examination records, and criminal records.

3. Data Subject:
   Refers to the individual to whom the Personal Data pertains.

4. Other terms shall be defined in accordance with Article 2 of the PDPA.

Article 4 Management of Personal Data

1. The collection, processing, and use of Personal Data shall respect the rights and interests of the Data Subject, comply with applicable laws and regulations, and be conducted in good faith. Such activities shall not exceed the necessary scope of specific purposes and shall have a legitimate and reasonable connection with the purpose of collection.

2. The Personal Data collected, processed, and used by the Company includes, but is not limited to, employee Personal Data, Personal Data of customers or their employees, and Personal Data of suppliers or their employees. In principle, the Company mainly collects general Personal Data and shall not collect Sensitive Personal Data unless required for business operations or by law.

3. To respect the statutory rights of Data Subjects, if international transmission of Personal Data is required, the Company shall handle such Personal Data with a high level of confidentiality and ensure that such transmission is conducted under lawful, appropriate, and adequately protected conditions.

4. Where the Company entrusts a third party with the collection, processing, or use of Personal Data, the Company shall properly supervise the entrusted party and confirm that its personal data management systems and measures comply with applicable laws and this Policy.

5. The Company shall clearly define matters related to the exercise of rights by Data Subjects as set forth in Article 3 of the PDPA, including the methods for exercising such rights, any fees payable, and the Company's review procedures for requests made by Data Subjects.

6. The Company shall establish a Personal Data Protection Management Task Force as the designated management unit. The Corporate Governance Officer serves as the convener, and members consist of personnel from various departments, including the Administration Department, Business Department, and Information Technology Office. The Task Force is responsible for establishing and maintaining management mechanisms for various personal data processing procedures and regularly reporting the implementation status to the Board of Directors.

   The Company has established a Personal Data Protection Management Task Force as the dedicated management unit. The Corporate Governance Officer serves as the convener, and members consist of personnel from various departments, including the Administration Department, Business Department, and Information Technology Office. The Task Force is responsible for establishing and maintaining management mechanisms for various personal data processing procedures and regularly reporting the implementation status to the Board of Directors.

Article 5 Security Maintenance of Personal Data

1. The Company shall adopt appropriate security maintenance and management measures for Personal Data collected, processed, or used to prevent theft, alteration, damage, destruction, loss, or leakage. To ensure the security and accuracy of Personal Data, the Company shall regularly review the security maintenance of its data file systems.
2. To safeguard the security of retained Personal Data, the Company shall, based on business needs, define access authorization for relevant personnel and control access to Personal Data, and shall require personnel to assume confidentiality obligations.

Article 6 Record Retention and Continuous Improvement Mechanism

1. The management unit shall retain records or relevant evidence regarding the actual implementation of legally required personal data management systems and security maintenance and protection measures.
2. To continuously improve personal data security maintenance, the management unit or personnel shall review and revise personal data protection matters and periodically submit relevant assessment reports.

Article 7 Handling of Personal Data after Business Termination

To prevent theft, alteration, damage, destruction, loss, or leakage of Personal Data, the management unit shall define and handle matters related to Personal Data after business termination in accordance with applicable laws.

Article 8 Notification Mechanism

To address security incidents involving theft, alteration, damage, destruction, loss, or leakage of Personal Data (hereinafter referred to as “Personal Data Incidents”), the Company shall establish emergency response procedures, notification, and prevention mechanisms. These shall include measures to be taken after an incident occurs, parties to be notified, notification methods and contents, response mechanisms, assessment of impacts, formulation of corrective and preventive measures, and subsequent disciplinary actions.

Article 9 Personal Data Protection Management Task Force

1. The management unit shall conduct risk assessments of the personal data management system and require each department to periodically confirm whether personal data management procedures are implemented in accordance with laws, regulations, and Company policies. The management unit shall also assess and improve risks related to system implementation to ensure compliance with applicable legal requirements.
2. In addition to establishing management systems in accordance with this Policy, the

management unit shall proactively formulate and promote personal data protection guidelines, related measures, documentation, and consent forms. Where personal data laws or regulations are amended, the management unit shall promptly formulate, revise, and implement relevant management procedures.

Article 10 Education, Training, and Penalties

1. To ensure compliance with current laws and regulations regarding personal data management, the Company shall periodically provide personal data protection and management training to all personnel and retain relevant records.
2. Any personnel who violate personal data protection requirements shall be subject to disciplinary actions in accordance with internal personnel management rules and employee reward and punishment regulations, and may be referred to competent authorities in accordance with the law depending on the severity of the violation.

Article 11 Grievance and Whistleblowing

Where a Personal Data Incident or situation that may harm the rights and interests of an individual occurs, or where any potential violation of this Policy is discovered, employees, external entities, or natural persons may submit grievances or reports through the personal data protection email mailbox established by the management unit. The Company shall strictly protect the information of whistleblowers to safeguard their rights and interests.

Article 12 Implementation

This Policy shall come into effect upon approval by the Board of Directors. The same shall apply to any amendments hereto.

This Policy was established on December 23, 2025.
The first amendment was made on March 10, 2026.