資訊安全政策及管理方針

Information Security Policy and Management Guidelines

乙方與其人員(包括但不限於乙方之受僱人、使用人、代理人、受任人及其他參與相關人員，以下合稱乙方人員)應共同遵守甲方資訊安全政策及管理方針

The second party and its personnel (including but not limited to employees, users, agents, delegates, and other related personnel of the second party, hereinafter referred to as the second party personnel) shall jointly comply with the first party's information security policy and management guidelines.

壹. 目的 Purpose：

為確保集團(本公司及子公司)營運及服務提供流程中之資訊機密性、完整性及可用性，並符合相關法規之要求，以降低公司面臨之內外部資訊安全風險

To ensure the confidentiality, integrity, and availability of information in the Corporation(including the Company and its subsidiaries) operation and service delivery processes, and to comply with relevant legal requirements, thereby reducing the internal and external information security risks that the company faces.

貳. 定義 Definitions：

一、機密性：確保只有經授權的人才可以存取資訊。

Confidentiality: Ensuring that only authorized personnel can access information.

二、完整性：確保資訊與處理方法的正確性與完整性。

Integrity: Ensuring the accuracy and completeness of information and processing methods.

三、可用性：確保經授權的使用者在需要時可以取得資訊及相關服務。

Availability: Ensuring that authorized users can access information and related services when needed.

參. 管理目標 Management Objectives：

一、確保集團業務相關資訊之機密性，保障本集團機密與隱私。To ensure the confidentiality of information related to the Corporation operations and to protect the Corporation confidential and private information.

二、確保集團業務相關資訊之正確及完整，提高行政效能與品質。To ensure the accuracy and completeness of information related to the Corporation operations and to improve administrative efficiency and quality.

三、確保集團業務相關資訊資產之可用性，提供資訊服務之所需。To ensure the availability of information assets related to the Corporation operations and to provide the necessary information services.

肆. 管理指標 Management Indicators：

集團將依業務性質，從機密性、完整性、可用性及法令遵循面考量，制訂管理指標，利用量化指標之管理落實本政策。The Corporation will develop management indicators based on the nature of its business, with considerations for confidentiality, integrity, availability, and compliance with laws and regulations, and use quantitative indicators to implement this policy.

伍. 管理責任 Management Responsibilities：

一、為推動與執行資訊安全管理制度，應成立資訊安全小組。To promote and implement the information security management system, an information security team should be established.

二、資訊安全小組召集人應定期召開管理審查會議，討論本政策是否符合現行需求。The convener of the information security team should convene regular management review meetings to discuss whether this policy meets current requirements.

三、集團高階主管應積極參與資訊安全管理活動，提供對資訊安全之支持及承諾。Top managers of the Corporation should actively participate in information security management activities and provide support and commitment to information security.

四、集團應舉辦資訊安全訓練課程，以提升員工資訊安全認知。The Corporation should hold information security training courses to enhance employees' awareness of information security.

五、集團員工、約聘（雇）人員及廠商都有責任遵循本政策，並持續改善資訊安全管理活動。Corporation employees, contractors, and contractors are responsible for complying with this policy and continuously improving information security management activities.

六、集團員工、約聘（雇）人員及廠商若未遵守本政策或發生任何違反本政策之行為，都應該被訴諸適當之懲罰程序或法律行動。If Corporation employees, contractors, and contractors fail to comply with this policy or engage in any behavior that violates this policy, appropriate punitive procedures or legal actions should be taken.

陸. 政策評估 Policy Evaluation：

本程序每年應依組織、業務、法令或環境等因素之變動予以適時調整，經管理代表核准後公告實施。This procedure should be adjusted on a timely basis each year based on changes in the organization, business, laws and regulations, or the environment, and be announced after approval by management representatives.

柒. 委外廠商識別及相關作業管制 Outsourcing Contractor Identification and Related Operational Control：

一、集團應識別委外廠商並留存相關紀錄，包含其提供之資訊服務。The Corporation should identify outsourcing contractors and keep relevant records, including the information services they provide.

二、安全需求選擇及評估 Security Requirements Selection and Assessment

1. 集團欲委託委外廠商時，應由專案負責人協同資訊部相關人員共同對委外廠商進行資格評估並留下記錄。集團於規劃委外服務時應考量成本、人力、管理、安全、相關系統之機密性、完整性及可用性及服務水準等方面，且可視委外性質增加評估項目，規範於合約、建議書或需求規格書等文件中。When the Corporation wishes to contract with an outsourcing contractor, the project leader and relevant personnel of the information department should jointly conduct a qualification assessment of the outsourcing contractor and keep records. When planning outsourcing services, the Corporation should consider cost, manpower, management, security, confidentiality, integrity and availability of related systems, service level, and other aspects, and increase evaluation items depending on the nature of outsourcing, which should be regulated in the contract, proposal, or demand specification documents.
2. 於委外作業前，須進行專案風險評估時，應視實際評估結果選列為合約條款要求事項。Before outsourcing operations, a project risk assessment should be conducted, and the items should be selected as contract clauses if necessary based on the actual assessment results.
3. 集團應針對委外廠商對集團資訊資產及支持資產之存取與影響納入風險評估。The Corporation should include the access and impact to the Corporation information assets and support assets by the outsourcing contractor in the risk assessment.

三、委外作業辦理時，應與委外廠商簽訂合約，包括下列內容 When performing outsourcing operations, a contract should be signed with the outsourcing contractor, including the following：

1. 合約期限 Contract period

明訂合約有效期間或自動展期之條款，包含軟硬體之維護方法及保固期限。Clearly specify the effective period of the contract or automatic renewal clause, including software and hardware maintenance methods and warranty periods.

2. 服務範圍 Service Scope

   詳細記載所承包之作業範圍，包含委外作業之項目、規格、時程、控管方式、驗收方式、保固維護／技術支援等項目。Detailed description of the contracted scope of operations, including items, specifications, schedule, control methods, acceptance methods, warranty maintenance, technical support, and other items related to outsourcing operations.

3. 服務水準 Service Levels

   根據委外廠商提供服務之項目，訂定集團可接受之最低服務水準及要求受託廠商確保能履行並維持相關資訊安全要求。Based on the outsourcing contractor's service items, establish the minimum service level that the Corporation can accept and require the contracting contractor to comply with and maintain relevant information security requirements.

4. 法令遵循 Compliance with laws and regulations

   委外服務合約除包含集團所提出之安全需求外，尚應說明應遵循之法律要求（如：個人資料保護法等）並清楚界定集團與委外廠商之權責義務。In addition to the security requirements proposed by the Corporation, the outsourcing service contract should also describe the legal requirements to be followed (such as the Personal Data Protection Act), and clearly define the rights and obligations of the Corporation and the outsourcing contractor.

(1) 委外廠商處理個人資料應遵守個資保護相關法令及集團所訂定個資相關規定及主管機關頒布之法令及行政規章主管機關之規定，不得將職務上所接觸之資料交付或告知他人。The outsourcing contractor shall handle personal information in compliance with relevant legal regulations on personal information and the related regulations on personal information established by the Corporation and the competent authority issuing administrative regulations and shall not disclose or inform others.

(2) 使用合法軟體尊重智慧財產權。Lawful software should be used to respect intellectual property rights.

(3) 其他轉包廠商及相關參與者的責任義務。委外廠商應保證與委外作業有關的各方（包括分包商）都應遵守集團之資訊安全要求及法令規定。Responsibilities of other subcontractors and related participants. The outsourcing contractor should ensure that all parties related to the outsourcing operations (including subcontractors) comply with both the information security requirements of the Corporation and the legal regulations.

5. 委外服務承包廠商作業之審查 The audit of outsourcing service contractor operations

進行委外作業時，集團擁有自行或聘請其他獨立單位或人員對委外廠商進行詢問、監督與稽核之權利。When conducting outsourcing operations, the Corporation has the right to monitor, supervise, and audit the outsourcing contractor either by itself or by engaging other independent units or personnel.

6. 應要求委外廠商對於資訊安全事件，須配合通報暨處理。The outsourcing contractor should be required to cooperate in reporting and handling information security incidents.

四、於適用之情況下，與客戶之合約將提供予委外廠商使其瞭解特殊要求。

When applicable, the contract with the customer should be provided to the outsourcing contractor for better understanding of special requirements.

五、集團若因成本、時效、委外服務之特性、委外廠商之侷限性等因素之考量，而致本程序所規範之安全需求無法完全適用時，應敘明理由並經資訊部主管同意。The reason should be explained if the security requirements specified in this procedure cannot be fully applied due to cost, time, the nature of outsourcing services, the limitations of outsourcing contractors, or other factors, and should be agreed by the supervisor of the information department.

六、委外作業辦理時，若委外廠商服務涉及傳遞敏感資訊，應要求委外廠商簽訂保密協議，包括下列內容 If the outsourcing service involves conveying sensitive information, the outsourcing contractor should be required to sign a NDA, including the following：

1. 所涉及之個人/組織 The individuals/organizations involved.
2. 同意書有效期限(若適用) The validity of the agreement (if applicable)
3. 義務方之責任 Responsibilities of the parties involved.
4. 處理超出合約範圍的敏感資訊之規範 Regulations on handling sensitive information beyond the scope of the contract.
5. 集團應確保傳遞須保護資訊之委外廠商人員皆知悉保密協議之要求及流程，並於傳遞機敏資訊前已簽訂有效之保密協議。The Corporation should ensure that outsourcing contractor personnel who need to protect information that needs to be distributed are aware of the requirements and process of the NDA and have signed a valid NDA before transmitting sensitive information.

捌. 外部服務管理 External Service Management：

一、應定期審查確認僅使用經核准之外部服務。Regular audits should be conducted to confirm that only approved external services are being used.

二、使用之外部服務其安全措施應與相關資訊資產之機密性﹑完整性及可用性等級相符。The security measures of the external services used should match the confidentiality, integrity, and availability levels of the related information assets.

三、委外關係終止或解除時，屬集團之資訊資產應返還，及儲存於委外廠商資訊設備之機敏資料應刪除。When outsourcing relationships are terminated or revoked, the information assets belonging to the Corporation should be returned, and sensitive data stored on the outsourcing contractor's information devices should be deleted.

玖. 委外廠商監督及審查 Outsourcing Contractor Supervision and Review：

一、如管理階層認為有進行監控或審查之必要時，應知會資訊安全小組或相關權責部門，安排定期或不定期依合約及保密協議，對委外廠商進行之品質審核並留下相關記錄，視不符合情節之嚴重性依據原契約所規定之罰則行使之。審核之紀錄文件由資訊安全小組或相關權責部門存查。

When management considers it necessary to monitor or review outsourcing contractors, the information security team or related authority should be notified to arrange for regular or non-regular quality audits of the outsourcing contractors according to the contract and NDA, and relevant records should be kept. Depending on the severity of the non-compliance, the Corporation should enforce the penalty stipulated in the original agreement. The records of the audit should be stored and checked by the information security team or related authority.

二、應要求委外廠商依契約及附件要求，提供必要資料（如：證書、證明）或產出內容以作為評量標準。本集團相關權責部門應審查相關文件以衡量是否符合服務水準之要求。The outsourcing contractor should be required, in accordance with the contract and NDA, to provide necessary data (such as certificates, certification) or output content as evaluation criteria. The relevant department of the Corporation should review the relevant documents to measure whether they comply with the service level requirements.

三、專案負責人應定期審查保密協議之有效性，若有期間限制之保密協議簽訂情事，應定期監督及於時效將屆時由專案負責人與委外廠商協調延長期限。The validity of the NDA should be reviewed periodically by the project leader. If sensitive information needs to be protected, the project leader and the outsourcing contractor should coordinate to extend the validity period before the deadline. The project leader should periodically review the effectiveness of the NDA.