資通安全管理政策聲明

INFORMATION SECURITY MANAGEMENT POLICY STATEMENT

保綠資源股份有限公司、其子公司及及關聯企業（以下稱本公司）資通安全管理政策及聲明如下：

一、 資通安全管理政策：

本公司為強化資通安全管理、確保資訊的機密性、完整性與可用性、資訊設備（包括電腦硬體、軟體、周邊）與網路系統之可靠性以及同仁對資訊安全之認知，並確保上述事項所需之資源免受任何因素之不當使用、洩漏、竄改、破壞或任何不利之行為與企圖，且在符合機密管理原則下，將正確的資訊適時的送達，特頒布本政策。

二、 權責：

依下列分項原則，配賦適當之人員其權責：

(一) 本政策、計畫及技術規範之研議、建置及評估等事項。

(二) 資料及資通系統之安全需求研議、使用管理及保護等事項。

(三) 資訊機密維護及安全稽核等事項。

The information security management (ISM) policy and statement of the Polygreen Resources Co., Ltd, its subsidiaries and associates (the Company) are as follows:

I. ISM Policy:

Strengthening the management of information security, by ensuring the integrity, confidentiality, availability, and reliability of IT infrastructure. Including but not limited to workstations, networking, and information security awareness among employees. Necessary precaution shall be implemented to ensure sensitive information are protected from improper usage, leakage, tampering and tampering in accordance with standard confidentiality management. The policy shall be promulgated in a timely manner.

II. Duty and Responsibility:

Relevant personnel shall be assigned proper authority and responsibilities in accordance with the following subpoint.

(I) Generating and reviewing of relevant policy and plan.

(II) Management of information security usage and data protection.

(III) Information security review and audit.

三、 範圍：

(一) 人員管理及資通安全教育訓練。

(二) 電腦系統安全管理。

(三) 網路安全管理。

(四) 系統存取控制管理。

(五) 系統發展及維護安全管理。

(六) 資訊資產安全管理。

(七) 實體及環境安全管理。

(八) 業務永續運作計畫之規劃與管理。

(九) 持續改善及績效管理。

四、 作業說明：

(一) 人員管理及資通安全教育訓練：

1. 對資通相關職務及工作，應進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。

2. 針對管理、業務及資訊等不同工作類別之需求，定期辦理資通安全教育訓練及宣導，建立員工資通安全認知，提升資通安全水準。

III. Scope:

(I) Personnel administration and information security training.

(II) Computer system security management.

(III) Cybersecurity management.

(IV) System access control management.

(V) System development and maintenance security management.

(VI) Information assets security management.

(VII) Physical and environmental security management.

(VIII) Planning and management of business continuity plan.

(IX) Continuous improvement and performance management.

IV. Description of Operations

(I) Personnel administration and information security training:

1. Security review shall be conducted for any information security position to access the suitability of personnel prior to employment.

2. Training shall be conducted to raise awareness among employees in fields related to information security in accordance with the criteria set.

3. 權責主管應負責督導所屬員工之資通作業安全，防範不法及不當行為。

資安目標：定期教育訓練。

(二) 電腦系統安全管理：

1. 辦理業務委外作業，應於事前研擬資訊安全需求，明訂廠商之資通安全責任及保密規定，並列入契約，要求廠商遵守及定期考核。

2. 複製及使用軟體依相關法規或契約規定，並建立軟體使用管理制度。

3. 為確保系統正常運作，應採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體。

4. 對各種系統變更作業，應建立控管制度，並建立紀錄，以備查考。

(三) 網路安全管理：

1. 開放外界連線作業之資通系統，應視資料及系統之重要性及價值，採用資料加密、身分鑑別、電子簽章、防火牆及安全漏洞偵測等不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。

3. Authorized personnel shall be responsible for the safety of the information security operations and its employees.

Information security objectives: Regular training and education.

(II) Computer system security management:

1. Contractual responsibilities shall be clearly defined prior to any outsourcing operations.

2. Usage and distribution of software shall be in managed accordance with relevant laws and regulatory.

3. Preventive and precautionary measures shall be implemented to ensure normal information security operation.

4. Operational changes shall be controlled and recorded for future reference.

(III) Cybersecurity management:

1. All information security and features accessible from external network shall be encrypted and restricted to authorized personnel.

2. 與外界網路連接之網點，應以防火牆及其他必要安全設施，控管外界與內部網路之資料傳輸與資源存取。

3. 利用網際網路及全球資訊網公布及流通資訊，應實施資料安全等級評估，機密性、敏感性及未經當事人同意之個人隱私資料及文件，不得上網公布。

4. 訂定電子郵件使用規定，機密性資料及文件不得以電子郵件或其他電子方式傳送。

資安目標：核心網路訂定 MTPD (最大容許中斷時間)。

(四) 系統存取控制管理：

1. 系統存取政策及各單位人員之存取權限應予明確規定，並以書面、電子或其他方式告知員工及使用者相關權限及責任。

2. 離（休、停）職人員，應立即取消各項資安資源之所有權限，並列入離（休、停）職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。

3. 為加強作業系統之安全管理，應建立系統使用者註冊管理制度，並落實使用者通行密碼管理，使用者通行密

2. Usage of firewall and relevant security features shall be implemented to ensure safety of any data transmitted.

3. Prior to any publication of information onto the web, security assessment shall be conducted to ensure confidential, sensitive, and personal information and documents are not published without consent from relevant parties.

4. Regulations on proper handling of confidential information and documents to ensure no unauthorized electronic transmission of mentioned documents.

Information security objectives: Network MTPD (Maximum Tolerable Period of Disruption)

(IX) System access control management:

1. System access rights shall be clearly defined, controlled and any changes notified.

2. User access rights shall be terminated immediately upon user resignation or termination. Any transfer of user authority shall be done in a timely manner.

3. A directory of users shall be implemented to manage all user access and ensure system security.

碼應定期更新。

4. 對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，並建立人員名冊，課其相關安全保密責任。

5. 為維護資通安全，應建立資通安全稽核制度，定期或不定期進行資通安全稽核作業。

(五) 系統發展及維護安全管理：

1. 自行開發或委外發展系統，應在系統生命周期之初始階段，即將資訊安全需求納入考量；系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。

2. 對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，且使用完畢後應立即取消其使用權限。

3. 委託廠商建置及維護重要之軟硬體措施，應在本公司相關人員監督及陪同下始得為之。

(六) 資訊資產安全管理：

1. 建立與資訊及資通系統有關的資產清冊，訂定資訊資產的項目、品名、使用者等資訊，以利管理。

4. Any remote access by vendors for system maintenance shall be strictly controlled.

5. Information security audit shall be conducted on a regular or irregular basis to maintain system security.

(V) System development and maintenance security management:

1. Information security requirement shall be taken into consideration prior to any acquisition of new or changes of existing software. Enhancements of existing information security systems shall be controlled by authorized personnel.

2. Access to information security systems by suppliers for maintenance work shall be limited and controlled, and access revoked upon completion of tasks.

3. Any enhancement of existing information security systems shall be carried out under the supervision of authorized personnel.

(VI) Information assets security management:

1. Establishing a directory of assets and inventories related to information security, with relevant information to facilitate

2. 依據國家機密保護、電腦處理個人資料保護及政府資訊公開等相關法規，建立資通安全等級之分類標準，以及相對應的保護措施。

3. 已列入安全等級分類的資訊及系統之輸出資料，應標示適當的安全等級以利使用者遵循。

(七) 實體及環境安全管理：

就設備安置、周邊環境及人員進出管制等，訂定實體及環境安全管理措施。

資安目標：核心網路訂定 RTO (資料復原時間點目標) 及 RPO (復原時間目標)。

(八) 業務永續運作計畫之規劃與管理：

1. 訂定業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。

2. 為維持業務正常運作，建立資通安全事件緊急處理機制，在發生資通安全事件時，應依規定之處理程序，立即向資訊單位或人員通報，採取反應措施，如有必要聯

asset management.

2. Establishing a classification standard for information security levels and corresponding protection measures in accordance with relevant laws and regulations, to protect sensitive or personal data.

3. Information security data shall be clearly classified and marked base on security level to facilitate user compliance.

(VII) Physical and environmental security management:

Establishing safety management measures for equipment placement and access.

Information security objectives: Maintaining a RPO (Recovery Time Objectives) and RPO (Recovery Point Objectives) for core network.

(VIII) Planning and management of business continuity plan (BCP):

1. Assessing the impact of impact of various man-made or natural disasters on business operations and formulating an emergency recovery plan to ensure business continuity with regular drills to enhance recovery plans.

2. To maintain normal business operation, an incident reporting mechanism is established to ensure timely incident reporting and respond in accordance to prescribed

繫檢警單位協助偵查。

3. 依相關法規，訂定及區分資料安全等級，並依不同安全等級，採取適當及充足之資通安全措施。

資安目標：核心系統訂定 RTO (資料復原時間點目標) 及 RPO (復原時間目標)。

(九) 持續改善及績效管理：

1. 每年至少一次透過本政策於管理審查時進行持續檢討改進檢討與措施擬定、執行、追蹤。

2. 資通安全目標的定期統計、審核並在管理月報會議中討論改善目標。

五、 資通安全管理聲明：

(一) 資通安全是確保本公司永續經營的必要元素之一。

(二) 本公司資訊部負責督導資通安全管理制度之運作，提供必要之資源，鑑識資通安全管理制度之內外部議題與利害相關團體對本公司資通安全之需求與期望。

handling procedures.

3. In accordance with relevant laws and regulations, appropriate information security measures shall be taken when handling data based on data sensitivity.

Information security objectives: Maintaining a RPO (Recovery Time Objectives) and RPO (Recovery Point Objectives) for core network.

(IX) Continuous improvement and performance management:

1. Existing policies shall be reviewed annually for continuous improvement.

2. Regular review and discussion of information security objectives shall be held during the monthly management meeting.

V. ISM Statement:

(I) Information security is a core element to ensuring a sustainable operation.

(II) The information technology department shall be responsible for the monitoring and management of the company's information security system. Providing necessary support to identify potential issues and meeting the needs and expectation of the organization.

(三) 本公司管理階層宣示支持資通安全之決心，將持續改善資通安全體質，降低資通安全事故可能帶來之衝擊，以保障所有利害關係人之權益。

(四) 本公司全體同仁、與本公司有業務往來之廠商及其員工或臨時雇員等，應確實遵循本政策及相關資通安全規範，以維護本公司所有業務之資通安全與永續經營。

(五) 所有資通系統之開發、修改及維護，皆須符合相關資通安全之規範並遵循本政策之規定。

(六) 所有人員對於有發生安全事件、安全弱點及違反本政策與規範之虞者，應隨時保持警戒，並依程序進行通報。

(七) 本公司遵循內外部相關法令規定，建立對應之管控程序，定期執行資通安全查核作業，以確保資通安全管理制度之持續有效運作。

(八) 如有違反本政策及相關安全規定者，將視情節輕重追究其法律責任。

六、 發布實施：

本政策聲明經報總經理核准後施行，並以書面、電子或其他方式通知本公司所有同仁和委外廠商，並通過選定的媒體提供給

(III) Management shall see to it that sufficient support is provided for its information security structure to ensure continuous improvement and minimizing security incidents to protect the interest of its stakeholders.

(IV) Employees shall comply with all relevant information security regulation to ensure sustained business operation.

(V) Development, modification, and maintenance of any information security systems shall comply with relevant regulations and comply with the provision of the policy.

(VI) All personnel shall always remain vigilance for any security incidents and or violations. Report shall be made in accordance with the procedure.

(VII) The company shall comply with relevant laws and regulations, establishing corresponding procedures and perform regular information security audit to ensure continuous and effective operation of its information security management system.

(VIII) Any violation of the information security policy shall be investigated, and further action taken based on severity.

VI. Promulgation and Implementation:

This policy statement, and any amendments hereto, shall enter into force following submission to and approval by the general manager,

利害關係人，包括公眾，修正時亦同。

and notify all colleagues and outsourced contractors of the Company in writing, electronically, or via other means, and make available to interested parties include public through selected media.

簽章 Signature	:		簽章 Signature		
姓名 Name	:	侯明強 How Beng Keong	姓名 Name	:	李雲山 Lee Yin Sun
職稱 Designation	:	資安主管 Information Security Officer	職稱 Designation	:	總經理 General Manager
日期 Date	:	16/3/2023	日期 Date	:	16/3/2023