中山华利实业集团股份有限公司

資訊安全管理辦法 **Management Measures for Information Security**	文件编号/No.：HL-M-IT003	
	生效日期/Effective date：2026 年 6 月 1 日	
	修 订 版 本 /Revised Version：2.4	页次: 1 OF 40

文件修订记录
Document Revision Record

版次 Version	修订日期 Revision Date	变更内容 Revised content	拟编者 Editor(s)
1.0	2022/3/15 March 15, 2022	新订 Formulated	周旭東 Keith Jhou
1.1	2022/12/12 December 12, 2022	增訂「6.營運安全第 12 項」 Added 6.12 in Operation Safety	周旭東 Keith Jhou
1.2	2023/1/5 January 5, 2023	修訂「4.密碼保護第 3、4 項」 Revised 4.3 & 4.4 in Password Protection	周旭東 Keith Jhou
1.3	2023/8/25 August 25, 2023	修訂「1.人力資源管理」項下的「1.1 使用者」和「1.2 系統管理者」 Revised "1.1 Users" and "1.2 System Administrators" in "1. Human Resources Management" 修訂「2.4 媒體檔案管理及報廢程序」 Revised "2.4 Management of Media Files and Disposal Procedures" 新增「7.3 通訊軟體之安全管理」 Added "7.3 Security Management of Communication Software"	陳瑞強、周旭東 Jacky Chen & Keith Jhou
1.4	2023/10/12 October 12, 2023	增訂「7.網路安全」第 8、9 項 Added item 8 and 9 of "7. Internet Security" 增訂「7.4 無線網路之安全管理」 Added "7.4 Security Management of Wireless Network"	周旭東 Keith Jhou
1.5	2023/10/17 October 17, 2023	修訂「二、适用範圍」 Revised "2. Scope" 修訂「7.4 無線網路之安全管理」 Revised "7.4 Security Management of Wireless Network"	周旭東 Keith Jhou
1.6	2023/11/24 November 24, 2023	增訂「2.資訊資產管理」硬體類型「桌上型電腦」、「行動裝置」 Added "2. Management of Information Asset"'s hardware types, "Desktop Computer", and "Mobile Device" 增訂「6.營運安全」下的 6.2、6.3 Added 6.2 and 6.3 in "6. Operational Safety"	周旭東 Keith Jhou
1.7	2024/7/12 July 12, 2024	增訂「2.5 資訊設備借用及歸還程序」 Added "2.5 Information Appliance Borrowing and Returning Procedures"	周旭東 Keith Jhou

1.8	2024/8/30 August 30, 2024	修訂「7.3 通訊軟體與檔案共享平台之安全管理」 Revised "7.3 Security Management of Communication Software and File Sharing Platform"	陳瑞強、周旭東 Jacky Chen & Keith Jhou
1.9	2025/5/7	修訂「1.人員使用權限和責任」 修訂「4.密碼保護」 修訂「6.營運安全」 刪除「8.4 資訊系統上線各階段職責分工」 Revised "1. Personnel use of privileges and responsibilities" Revised "4. Password protection" Revised "6. Operational safety" Deleted "8.4 Division of Responsibilities at Each Stage of Information System Development"	周旭東 Keith Jhou
2.0	2025/7/25	增訂「5.13 UPS 定期檢測與保養」 修訂「7.4 檔案共享平台(Box, OneDrive)之安全管理」 修訂「7.5 無線網路之安全管理」 Added "5.13 UPS Regular Inspection and Maintenance" Revised "7.4 Security Management of File Sharing Platforms (Box, OneDrive) " Revised "7.5 Security Management of Wireless Network"	周旭東 Keith Jhou
2.1	2025/9/16	修訂「7.5 無線網路之安全管理」 Revised "7.5 Security Management of Wireless Network"	周旭東 Keith Jhou
2.2	2025/12/02	增訂「6.16 涉及集團、事業群和工廠內部的重要工作議題，應通過電子郵件、公司網站發送或公布，不應使用個人通訊軟體」 Added "6.16 Important work-related matters involving the group, business units, and factories should be sent or announced via email or the company website, and personal messaging software should not be used"	周旭東 Keith Jhou
2.3	2026/02/26	增訂「7.5.8 外部厂商远程协助安全操作准则」 Added "7.5.8 External Vendor Remote Assistance Safety Operating Guidelines"	梁伟华 Weihua Liang
2.4	2026/06/01	增訂「5.14 客人、厂商设备入驻准入管理规范」 Added "5.14 Guest and Manufacturer Equipment Access Management Standards"	梁伟华 Weihua Liang
版次编号说明：a.b (a 为办法年次，b 为当年修订次数，未修订跨年续用为 a.0 版) Version number description: a.b (a is the year of the measures, and b is the number of revisions in the year, and if it is not revised, it will be version a.0 the following year)			

核准 Approve		复核 Review		审核 Audit	周旭東	制作 Compile	

一、資訊安全管理架構 **Information Security Management Framework**

為強化資訊安全管理，建立安全及可信賴之資訊作業平台，確保資料、系統、網路及相關設備能永續運作，依據中山華利實業集團股份有限公司(以下簡稱本集團)的「資訊安全政策」與「資訊安全組織程序書」訂定本管理辦法，有關本集團的資訊安全管理架構說明如後：

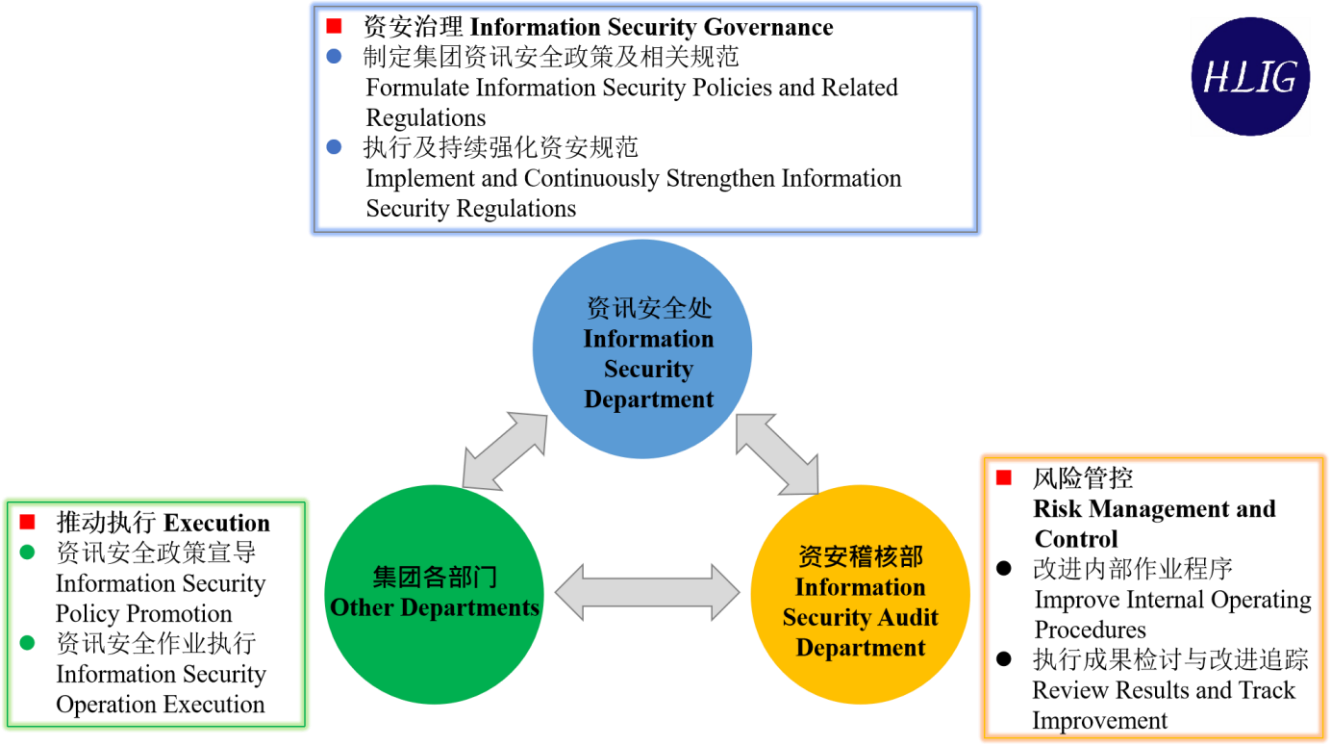
The purpose of these measures is to strengthen information security management, establish a safe and reliable information operation platform, and ensure the sustainable operation of data, system, network and related equipment. These management measures are formulated in accordance with the "Information Security Policy" and "Information Security Organizational Procedures" of Huali Industrial Group Company Limited (hereinafter referred to as Huali Group). The information security management structure of Huali Group is explained as follows:

1. 本集團資訊安全之權責單位為資訊安全處，負責訂定資訊安全政策、規劃和執行資訊安全作業與落實資訊安全政策，並定期向執行長報告集團資安治理概況。

   The Information Security Department of Huali Group is responsible for formulating information security policies, planning and executing information security operations, and implementing information security policies, and regularly reporting to the CEO on the overall situation of Huali Group's information security status.

2. 本集團資安稽核部為資訊安全監理之督導單位，負責稽核內部資安執行狀況，並對外部客戶稽核所見缺失提出矯正和改進措施，定期追蹤改進成效，以降低資安風險。

   The Information Security Audit Department of Huali Group is the supervisory unit for information security activities, responsible for auditing the internal information security implementation status, proposing corrective measures for deficiencies found in audits by external customers, and regularly tracking the improvement results to reduce information security risks.



二、適用範圍 **Scope**

1. 在本集團內部網路使用的各項資訊資產及其使用者。

   Various information assets used on the Huali Group's internal network and their users.

2. 使用者包括正式員工、供應商、訪客及其他經授權使用資訊資產之人員。

   Users include employees, suppliers, visitors and other personnel authorized to use information assets.

三、資訊安全目標 **Information Security Objectives**

1. 防範資訊安全風險威脅之發生，減輕資訊安全事件發生之影響。

   Prevent the occurrence of information security risk/threats, and reduce the impact of information security incidents.

2. 保護集團資料，避免不當使用、存取及防止敏感性與機密性資料外洩或遺失。

   Protect confidential information from being improperly used and accessed, and prevent any leakage or loss of sensitive and confidential information.

3. 提升資訊設備及系統效能，確保資訊系統正常運作。

   Improve the performance of IT devices and systems to ensure the normal operation of IT systems.

4. 確保集團各項業務執行，並符合法令規範。

   Ensure the group's business operations are executed in compliance with legal regulations.

四、資訊安全管理事項 **Information security management categories**

本辦法涵蓋 14 項資訊安全管理事項，除「資訊安全政策」和「資訊安全的組織」兩項定期召開管理階層會議討論，並另行簽核公告外；其他於本辦法提出「人力資源安全」等 12 項作業程序，程序中提到的作業表單及協議書等文件，屬於資安管理系統的第四階文件，於該階文件總覽目錄訂定清單和公告。有關資訊安全管理事項如下：

The measures cover 14 information security management items. Except for "Information Security Policy" and "Information Security Organization", which are subject to discussions in management meetings held regularly and being approved separately for publication, the other 12 items, such as "human resources security", for which operational procedures are set forth in the measures, and documents such as operational forms and agreements mentioned in the procedures are classified as documents at the fourth level of the information security management system; a list of documents at this level should be established based on the general catalog and published. The information security management items concerned are as follows:

1. 人員使用權限和責任 Personnel Use of Privileges and Responsibilities
2. 資訊資產管理 Management of Information Asset
3. 存取控制 Access Control
4. 密碼保護 Password Protection
5. 實體安全與環境需求 Physical Security and setup requirements
6. 營運安全 Operational Safety
7. 網路安全 Internet Security
8. 資訊系統獲取、開發及維護 Information System Acquisition, Development and Maintenance

9. 供應商關係 Supplier relationships
10. 資訊安全事件管理 Management of Information Security Incidents
11. 有關於資訊安全方面的營運持續管理 Information security operation continuity
12. 適法性 Legality

五、資訊安全作業程序 **Information Security Procedures**

1. 人員使用權限和責任 **Personnel use of privileges and responsibilities**

對於接觸資訊系統的人員，依照身分類別不同，規定個人對資訊系統的使用權限和責任歸屬。

Assign different privileges and responsibilities to people according to their roles when they require access to IT systems.

1.1 使用者 **Users**

1.1.1 賦予使用者存取資訊系統的權限，僅限於執行與業務有關工作，個人依業務需求至 BPM 系統填寫「資訊帳號權限申請單」，經由主管核准後始予開放權限。

Granting users access to the information system is limited to performing business-related work. Individuals go to the BPM system to fill in the "Information Account Permission Application Form" based on business needs, and the account privileges are reviewed and approved by the supervisor.

1.1.2 因應人員工作調動負責事項變動下，由人事相關單位至 BPM 系統填寫「人員提升調任申請單」，表單呈核結案後，使用者至 BPM 系統填寫「資訊賬號權限申請單」，送交權責主管審核權限是否符合職務需求，核准後交給 IT 部門進行帳號權限的調整或停用。

When the user's position is transferred, the related department fills out the "Application list for Promotion and internal transfer" in the BPM system. After the application is finished, the system will automatically initiate a "Personnel Transfer Account System To-Do List" to notify the user department to review the account privileges of the transferred staff to check if they are still in compliance with the requirements for continued use and to decide how to proceed.

1.1.3 使用者帳號及權限，應由相關主管與系統負責人依照使用者的職責及分工原則覆核，並檢查及取消閒置帳號。

Account privileges should be reviewed by relevant supervisors and system administrator in accordance with the user's responsibilities and division of labor principles, and idle accounts should be checked and canceled.

1.1.4 使用者權限之設定，依其業務職責及職能分工原則設定權限，每個系統皆需建立使用者帳號並設定密碼，以確保程序及資料存取之安全。

Account privileges are set according to the principles of business responsibilities and functional division of labor. Each system requires the creation of user accounts and the setting passwords to ensure the security of programs and data access.

1.1.5 使用者於入職時簽訂「保密同意書」，應遵守集團訂定的保密規定，約定在職期間不可洩漏集團的營業祕密。

By signing the “Confidentiality Agreement” upon employment, users should abide by the confidentiality regulations set by Huali Group and agree not to disclose business secrets during their employment period.

1.1.6 若有違反資訊安全管理辦法之行為，情節輕微者，將告知當事人及所屬主管，並由總人資培訓組進行資訊安全宣導課程及課後測驗，以加強使用者的安全警覺意識。

If a user violates information security management measures, the information security department will notify relevant personnel and their supervisors, and the HQ human resources training team will implement information security training with after-class tests attached to enhance users' security awareness.

1.1.7 新進人員統一由總人資培訓組規劃和進行資訊安全培訓課程，在職人員每年進行至少一次的資訊安全培訓課程。

Information security training courses are planned and implemented by the HQ human resources training team for new employees, and at least one course is implemented for current employees annually.

1.1.8 不允許使用者將自己的登入身份及密碼提供他人使用。

Users should not provide their login ID and password to others.

1.1.9 不允許使用者存取網路上與業務無關的檔案及存取權限。

Users are not allowed to access files and privileges on the network that are not related to business.

1.1.10 禁止使用者在網路上發送可能涉及人身攻擊或不實報導、任何違法、攻擊性、色情性之訊息或其他與違反工作規則事項之訊息。

Users are prohibited from sending messages online that may involve personal attacks or false reports, any illegal, offensive, pornographic messages, or any other messages that violate working regulations.

1.1.11 禁止使用者以任何手段蓄意干擾或妨害集團的資訊系統，包括但不限於網路安全防護系統、防毒系統的正常運作，違反者由資訊部門通知且安排人員參加資訊安全意識強化培訓，如因蓄意破壞造成公司有形或無形資產損失的情況下，將依損失情況進行懲處，情節嚴重者將依法送辦！

Users are prohibited from deliberately interfering or impeding the normal operation of the Group's information systems by any means.

1.1.12 集團人員如因未能遵守本辦法發生違規行為，造成公司財產或名譽損害時，公司將依法請求損害賠償，情節嚴重者，如有涉及司法單位調查，或有違法情事時，應自負所產生之各項法律責任。

If employees violate the regulations and causes damage to Huali Group's property or reputation, the group will demand compensation for damages in accordance with the law.

If the violations are serious and invested by judicial authority or if there are any violations of the law, the employee will bear the consequences and various legal responsibilities.

1.2 系統管理者 **System Administrator**

1.2.1 系統管理者應負責系統安全政策的制定與執行、網管工具系統設定與操作，以確保集團內部系統主機與資料的安全及完整。

System administrators should formulate and implement system security policies and network management tool settings to ensure the security and integrity of the group's internal system servers and data.

1.2.2 如使用者離職或職務調動，系統管理者應負責將使用者帳號移除或變更使用權限。

If a user leaves or changes positions, the system administrators are responsible for deleting the user account or changing usage rights.

1.2.3 系統管理者未經許可禁止閱覽使用者的個人檔案。

System administrators are prohibited from accessing users' personal files without permission.

1.2.4 系統管理者未經使用者同意，不可增加、刪除及修改個人檔案。如有特殊緊急狀況，必須刪除個人檔案，需先知會檔案擁有者。

System administrators cannot add, delete or modify personal files without the user's consent. In case of special emergency, personal files must be deleted and the file owner must be notified in advance.

1.2.5 對於任何資訊安全違規事件，系統管理者應立即向單位主管反應。

System administrators should immediately report any information security violations to the department supervisor.

1.2.6 系統管理者不得新增、刪除及修改稽核資料檔案，以避免當資訊安全違規事件發生時，產生追蹤查詢的困擾。

System administrators are not allowed to add, delete or modify audit log files to avoid troublesome tracking inquiries when information security violations occur.

1.2.7 為強化系統管理者的資訊安全防護觀念和技術，每年委託第三方專業資安機構，對所有系統管理者辦理至少兩次的培訓課程，以訓練人員具備基本的網路攻、防能力，如：防範社交工程、漏洞利用、DDoS、SQL Injection 等攻擊

In order to strengthen security protection concepts and technologies of system administrators, a third-party professional information security agency is entrusted to enforce at least two training courses for all system administrators every year. The purpose is training personnel to have basic network attack and defense capabilities, such as: Social engineering, Vulnerability exploitation, DDoS, SQL Injection and other attacks.

2. 資訊資產管理 **Management of Information Assets**

資訊資產的定義為集團的硬體和軟體，硬體包括服務器、網路設備、網路安全防護設備、終端機、桌上型電腦、筆記本電腦、行動裝置及相關週邊設備，軟體包括作業系統、應用系統、自行開發系統及 APP。

Information assets are defined as Huali Group's hardware and software. Hardware includes Servers, Network devices, Network security protection devices, Terminals, Desktop computers, Laptops, Mobile devices and Peripheral equipment. Software includes Operating systems, Application systems, Self-developed systems and APPs.

2.1 資訊資產購置程序 **Acquisition of Information Assets**

2.1.1 使用單位填寫設備請購單，經主管覆核及資訊總處審核後，送採購單位進行購買。

The user fills out the equipment purchase requisition form, and after approval by the department supervisor and the General Information Dept., it is sent to the purchasing unit for purchase.

2.1.2 資訊總處負責評估設備的兼容性、擴充性、業務特性及成本效益後，開立符合需求之硬體設備。

The General Information Dept. is responsible for evaluating hardware device that meets compatibility, scalability, business characteristics and cost-effectiveness, and providing professional suggestions to the purchasing unit.

2.1.3 設備購置後由資訊總處協同驗收，並於驗收完成後移交使用單位保管，並登記資訊設備清單列冊管理。

When the equipment is purchased, it will be jointly inspected and accepted by the General Information Department. After the inspection is completed, it will be transferred to the user forpreservation and use, and a list of information assets will be registered and managed by IT Department.

2.1.4 資訊資產購置應配合集團整體短、中、長期的策略與發展方向。

The acquisition of information assets should be consistent with the Huali Group's short, medium and long-term strategies and development directions.

2.2 資訊資產安裝使用程序 **Procedures for Installing and Using Information Assets**

2.2.1 使用單位應按照硬體及軟體操作手冊進行安裝及操作。

IT helps users install and operate according to the software and hardware operating manuals.

2.2.2 硬體及軟體在使用前應予以綜合廣泛地測試，以確定所有已知問題經過評估解決。

Hardware and software should be comprehensively and extensively tested before use to ensure that all known issues have been evaluated and resolved.

2.2.3 禁止使用盜版軟體，應使用合法授權軟體。

The use of pirated software is prohibited; use legally licensed software instead.

2.2.4 管理單位應定期抽查各單位資訊設備，查核是否使用未經授權及其他不當之軟體。

Management department should regularly inspect the information equipment stored & used by other departments, and vet if those there is any unauthorized use and they are using inappropriate softwares.

2.3 資訊資產維護程序

2.3.1 集團的硬體和軟體經資訊總處評估，需委外由廠商提供維護服務者，應與委外廠商簽訂維護合約。

Hardware and software should be comprehensively and extensively tested before use to ensure that all known issues have been evaluated and resolved.

2.3.2 維護合約到期前，由資訊總處評估是否續約及提出續約申請，經相關權責主管核准後進行續約作業。

Before the maintenance contract expires, HQIT Dept. will evaluate whether to renew the contract and submit an application for renewal. The renewal process will be carried out after the approval by the relevant supervisors.

2.3.3 與委外廠商簽訂維護合約，應訂定適當的資訊安全協定，規範委外廠商維護所接觸資料的安全管理措施。

When signing a maintenance contract with an outsourced vendor, appropriate information security protocols should be established to regulate the security management measures for data accessed by the outsourced vendor for maintenance.

2.3.4 主機系統維護工作應避免停機並干擾使用者，盡可能安排在夜間、假日或無人使用狀態下進行停機維護。

Maintenance work for the server system should avoid downtime and interference with its normal service. Whenever possible, downtime maintenance should be scheduled at night, on holidays, or when no one is using the system.

2.3.5 維護作業由委外廠商執行，並由本集團資訊總處確認維護程序皆依照維護合約所述進行，並記錄於「廠商維護記錄單」。

When maintenance operations are performed by the outsourced vendor, HQIT Dept. will confirm that the maintenance procedures are performed in accordance with the maintenance contract and fill in the "Manufacturer Maintenance Record Sheet" accordingly.

2.3.6 一般事務性電腦設備發生故障時，使用者應至集團入口網站的資訊系統填寫「IT 維修申請單」通知資訊總處派員維修，並記錄設備故障原因及維修狀況。

When the computers purchased by company for office use are out of order, the users should fill in the "IT Maintenance Form" on the IT system in the Group's portal, and notify HQIT to perform maintenance. IT personnel should record the cause of the equipment failure and maintenance status.

2.3.7 經資訊總處人員確認設備故障需送交廠商維修者，填寫請修單或相關簽呈等外修申請表單，經申請單位主管核准後，填寫設備放行條發給廠商進行維修。

If it's confirmed by HQIT that the equipment failure needs to be handled by a vendor for repair, the applicant must fill in the "Repair form" for external repair service and after it's approved by the supervisor of the applicant department, the applicant must fill in the "Item Release Form" for sending the faulty equipment out to the vendor for repair.

2.4 媒體檔案管理及報廢程序 **Management and Disposal Procedures of Storage Medium**

2.4.1 磁碟、磁帶、磁(光)盤、移動式儲存媒體等裝置，各單位均應律定專人集中保管，並實施每日上班後、下班前各兩次清點，每日清點記錄交由保管單位的主管審批備查。

Each department must designate dedicated personnel to centrally store disks, tapes, magnetic (optical) disks, removable storage media, and other equipment, and conduct an inventory check at the beginning and end of each workday.. Daily inventory records should be reviewed and approved by the custody department supervisor.

2.4.2 使用移動式儲存媒體(USB 設備)應通過 BPM 系統「資訊安全權限申請單」一人一單提出申請以便事件責任規屬，填寫「申請事由」和「裝置 ID」，提交品牌總經理審批同意，並經過資安或資訊部門審查後開放使用。

Before using removable storage media (USB devices), users should fill out the "IT Security Permission Requisition" on the BPM system and each application form can only be used for one person to clarify the responsibilities; users need to fill in the "Application Reason" and "Device ID" in the form, and submit it to the brand's general manager for approval, then it should be reviewed by the Information Security Department/IT before the permission is given..

2.4.3 載有磁性記錄之消耗品報廢時，需消除磁性記錄使其不得再度被使用，並填寫「媒體設備報廢記錄單」進行報廢程序。

When consumables containing magnetic records are being destroyed, the magnetic records must be eliminated so that they cannot be used again, and the "Media Equipment Disposal Form" must be filled out to proceed with the destruction process.

2.5 公司資訊設備借用及歸還程序**(**借還流程如附圖 **1) Borrowing and Returning Procedures of Information Assets (the process is shown in Figure 1)**

2.5.1 筆記型電腦、數位相機、移動式儲存媒體(USB 設備)等裝置，因開會、出差等公務需要借出使用，借用人應填寫紙本「資訊設備借用登記表」(格式如附表 1)，填寫設備名稱、借用人姓名、借用日期、用途等資訊，由設備保管單位留存記錄一年。

Laptops, digital cameras, removable storage media (USB devices) and other devices are loaned out for official purposes such as meetings and business trips. The borrower should fill in the paper version of "Information Appliance Borrowing Form" (the format is as shown in Appendix 1). Fill in the Equipment name, Borrower's name, Borrowing records and reasons on the form, which should be kept for at least one year by the custody department.

2.5.2 借用人歸還資訊設備給保管單位時，保管人應檢查設備外觀是否和借出前情況相同，軟體是否運作正常，並且清除/還原設備內暫存資料，以免造成機敏資料外流等資訊/產品安全疑慮，完成檢查後填寫歸還紀錄備查。

When the borrower returns the information equipment to the custody department, the custodian should check whether the appearance of the equipment is the same as before the loan, whether the software is operating normally, and clear/restore the temporary data in the equipment to avoid information/product security concerns such as the leakage of sensitive data. After completing the inspection, fill in the return record.

2.5.3 非資安、資訊之保管部門不清楚如何清除/還原設備的資料，需主動請求廠區的資安或資訊人員協助教學處理。

Custody departments other than IS/IT who are not sure how to clear/restore the device data, can request assistance from the factory IS/IT personnel.

3. 存取控制 **Access Control**

3.1 程序及資料的存取控制 **Program and Data Access Control**

3.1.1 經權責部門核准人員才能使用終端機或主機，處理資料存取等作業。

Before users access client or server data, they must be approved by the responsible department.

3.1.2 系統(含作業及應用系統)程序、檔案之存取使用，由需求單位提出使用申請，並經權責主管簽核後轉資訊部門辦理。

For All access to and use of system (including operating and application systems) programs and files, an application for use shall be submitted by the requesting department, and shall be transferred to IT after being approved by the responsible supervisor.

3.1.3 系統程序、檔案之存取使用，均需留下記錄。

All access to and use of system programs and files must be recorded.

3.1.4 系統程序之原始碼與執行檔應分開在不同群組存放，並依其存取作業分別管制。

The source code and executable files of system programs should be stored in different group folders and controlled separately according to their access operations.

3.1.5 系統程序應依業務權責限定程序設計人員之資料存取功能及範圍(如：程序之讀、寫)，並由資訊部門主管評估其作業效益及核准存取權限。

The data access function and scope of the system program should be limited according to the business authority and responsibility of the personnel (e.g., reading and writing of the programs), and the IT supervisor should evaluate the operational efficiency and inspect the access privileges.

3.1.6 檔案存取權限為預先許可的工作權限，變更權限應提出申請並經過審核同意。

File access privileges are set based on the pre-approved work duties. Changes to the privileges should be requested and approved.

3.1.7 提供稽核使用之程序及檔案，應僅限稽核人員使用。

The programs and files provided for audit use should be used only by the auditors.

3.1.8 資料存取應透過密碼權限設定，以杜絕未經授權的之存取發生。

Data access should be encrypted to prevent unauthorized access.

3.1.9 程序及檔案應依不同用途存放不同區域。

Programs and files should be stored in different areas per different purposes.

3.1.10 於外部網路取得資料檔時，應先經過資訊總處授權後始得進入存取。

When obtaining data files from the external network, you should obtain authorization from HQIT before accessing the files.

3.2 程序管理 **Program Management**

3.2.1 對重要程序非經授權不得使用。

Unauthorized use of important programs is prohibited.

3.2.2 程序之登錄、使用、刪除或更改，在主機中均應保有記錄。

The login, use, deletion or modification of the program should be recorded in the server.

3.2.3 正式程序說明文件之使用，應設定權限管控。

Access control should be set up for the use of the official program description document.

3.2.4 禁止操作人員變更程序名稱或編錄程序。

The operators are prohibited from changing the program name or programming.

3.2.5 所有程序的修改均應經過核准，並有相關負責之人員，以杜絕程序未經授權而遭更改之情形。

All modifications to programs should be approved and matched with responsible personnel to prevent unauthorized changes to programs.

3.2.6 有關單位均應參與重要程序修改過程。

All departments concerned should be involved in the process of modifying the major programs.

3.2.7 正式程序之修改，需經多次測試以決定其預計結果。

Changes to the formal program are subject to multiple tests to determine the outcome of the estimated result.

3.2.8 程序修改時，備用程序、程序列表及其他說明文件亦應隨同更新。

When the program is modified, the spare program, program list, and other documentation should be updated as well.

3.2.9 當程序執行發生錯誤時，應查明執行錯誤的原因再予繼續執行。

When an error occurs in the execution of a program, the cause of the error should be identified before proceeding.

3.3 資料檔(庫)管理 **Data Files (database) Management**

3.3.1 資料庫的應用程序、作業與測試區應獨立區隔。

Database applications, operations, and test areas should be separately segregated.

3.3.2 資料檔(庫)只有經授權的維護或管理人員有權變更。

Data files (database) can only be changed by authorized maintenance or management personnel.

3.3.3 資料檔(庫)維護人員在未經使用單位同意前不得更改資料。

Data files (database) maintainer should not change the data without the consent of the user organization.

3.3.4 嚴格限制不同使用者對資料檔(庫)檔案之使用權限及所能執行之功能。

Strictly limit the use of data files (database) by different users and the functions they can perform.

3.3.5 對資料檔(庫)的變動，程序宜產出適當稽核軌跡，提供程序與資料關係，以追蹤不正確之資料。

For changes to data files (database), the program should have an appropriate audit trail that provides a relationship between the program and the data to track down incorrect data.

3.3.6 各項資料檔(庫)記錄文件應定期審核，以確保資料檔(庫)之存取安全無虞。

Data files (database) and logs should be audited regularly to ensure that access to the data files (database) is secure.

3.3.7 應定期評估資料檔(庫)效能，並對於效能不佳或警示狀況提出改進措施。

The performance of data files (database) should be evaluated periodically, and improvement measures should be proposed for poor performance or warning conditions.

3.4 系統主機資源管理 **Resource management for system server**

3.4.1 重要之系統公用程序、工具及指令，一般使用者無存取權限，僅有管理者帳號能執行，當持有管理者帳號之人員調、離職時，需由權責主管監管移交程序。

Important common system programs, tools, and commands can't be accessed by general users and can only be accessed with an administrator account. When an administrator account holder is being transferred or about to quit, the supervisor in charge needs to supervise the transfer process.

3.4.2 系統開發及程序撰寫人員對於上線系統之程序與資料檔案無存取權限。

System developers and programmers do not have access to the programs and data files of the online system.

3.4.3 系統主機需設置工作日誌，提供系統操作員記載系統作業之情況，並定期由主管覆核。

A job logbook should be set up for the system server for the system operator to record the operation of the system and to be periodically reviewed by the supervisor.

3.4.4 服務器主機之作業系統、應用系統及資料庫管理系統應設置稽核日誌，以記錄任何可能危害系統安全的事件。

The operating system, application system, and database management system of server, should have audit logs to record any events that may jeopardize system security.

3.4.5 集團外部人員(包括維護廠商)之帳號應由專人妥善監控，並於非使用時期取消其存取權限。

Accounts of personnel outside the Group (including maintenance vendors) should be properly monitored and their access privileges should be revoked during periods of non-use.

3.4.6 選用服務器作業系統時，應對其總工作量、工作型態及安全保護設施等予以考慮，服務器的作業系統版本及相關文件應為同一版本。

When selecting a server operating system, consideration should be given to its total workload, work type and security protection facilities, etc. The server's operating system version and related documents should be of the same version.

3.4.7 各廠 IT 主管每個月應定期評估服務器效能，並對於效能不佳或警示狀況提出改進措施。

The IT supervisor of each factory should regularly evaluate server performance every month and propose improvement measures for poor performance or warning conditions.

4. 密碼保護 **Password Protection**

4.1 集團的資訊系統應建立適當之密碼控管原則，包括限制錯誤登入次數、密碼最短長度、密碼複雜度以及變更週期等。

Appropriate password control principles should be established for the Group's information system, including limiting the number of incorrect logins, minimum password length, password complexity, and period for changing passwords.

4.2 使用者第一次登入系統，應立即變更初始密碼後方可繼續作業。

The first time a user logs on to the system, he/she should change the initial password immediately before continuing the operation.

4.3 密碼設置依照使用者的系統權限區分「一般帳戶」（Standard User Accounts）和「特權帳戶」（Privileged User Accounts），設置標準如下：

Password settings are categorized into “Standard User Accounts” and “Privileged User Accounts” according to the user's system privileges, and are set according to the following criteria:

4.3.1 一般帳戶的密碼長度至少為 8 個字符，特權帳戶的密碼長度至少為 15 個字符。

Passwords are at least 8 characters long for regular accounts and 15 characters long for privileged accounts.

4.3.2 密碼不得設置和個人工號、常用字典詞相同。

Passwords should not be the same as personalized passwords or commonly useddictionary words.

4.3.3 密碼組合應包括大、小寫英文字母、數字及特殊符號。

Password combinations should include upper and lower case letters, numbers and special symbols.

4.4 密碼應 90 天更換一次，同組密碼不得重複使用超過 6 次。

4.4.1 Reebok 品牌工廠：密碼應 30 天更換一次，密碼輸入錯誤超過 3 次鎖定，同組密碼不得重複使用超過 6 次。

4.4.2 其他品牌工廠：密碼應 90 天更換一次，密碼輸入錯誤超過 10 次鎖定，同組密碼不得重複使用超過 6 次。

4.4.1 Reebok brand factory: Passwords should be changed every 30 days. Passwords will be locked if entered incorrectly more than 3 times. The same password group cannot be reused more than 6 times.

4.4.2 Other brand factory: Passwords should be changed every 30 days. Passwords will be locked if entered incorrectly more than 10 times. The same password group cannot be reused more than 6 times.

4.5 密碼不得與任何人共用，包括主管和同事。

Passwords may not be shared with anyone, including supervisors and coworkers.

4.6 不得將密碼插入電子郵件或其他形式的電子通信中，也不得通過電話向任何人透露。

Passwords may not be inserted into emails or other forms of electronic communication or disclosed to anyone over the phone.

4.7 密碼宜採用多因素身份驗證，包括郵件發送認證碼、Google 身分驗證器等，與密碼合併一起使用，以確認使用者的身分。

Passwords are recommended to use multi-factor authentication, including emailed authentication codes, Google Authenticator, etc., in conjunction with passwords to confirm the identity of the user.

5. 實體與環境安全 **Physical and Environmental Security**

5.1 電腦機房應建立門禁管制機制，包括採用密碼辨識、接觸式卡片、指紋辨識及人臉辨識等系統，非公司內部作業人員進出電腦機房，應登記於「電腦機房進出管制登記表」，並於資訊人員陪同下方可進入，嚴禁未經許可人員擅入電腦機房。

The server room should be equipped with an access control mechanism, including password identification, contact card, fingerprint identification, and face recognition systems. Non-internal operators should register in the ”Server Room Access Control Registration Form” and be accompanied by IT personnel when entering the server room, and it is strictly prohibited for unauthorized personnel to enter the server room without permission.

5.2 電腦機房內應設置獨立之空調設備、高架地板、自動電壓穩定裝置、不斷電系統(UPS)、自動火警偵測及緊急照明等機房防護設備。

Server room should be equipped with independent air-conditioning, raised floors, automatic voltage stabilizers, uninterruptible power supply (UPS) systems, automatic fire detection and emergency lighting, and other protective equipment.

5.3 各項支援防護設備及外圍設備應定期檢查與維護，以測試其堪用性。

Supporting protective equipment and peripherals should be regularly inspected and maintained to test their serviceability.

5.4 電腦機房內不應放置易燃或爆裂物等危險物品，需設置滅火設備，並定期檢測其有效期限。

Hazardous materials such as flammable or explosive substances should not be placed in the server room. Fire extinguishing equipment should be installed and its expiration date should be checked regularly.

5.5 電腦機房管理辦法應訂定環境標準，如：溫度、濕度、防火設備及門禁管制等標準。

The server room management system should set environmental standards such as temperature, humidity, fire prevention equipment and access control.

5.6 重要服務器及通訊設備應設置於電腦機房防護，對於人員的進出，應以門鎖及錄像設備管控，未經授權者不得擅自進入。

Important servers and communication equipment should be set up in the computer room for protection. The access of personnel should be controlled by door locks and video recording equipment, and unauthorized persons should not be allowed to enter the room.

5.7 資訊單位操作人員需每日檢查機房設備運作情形，並填寫於「主機房操作日誌」(Daily Check)。

Information unit's operators are required to check the operation of the equipment in the server room on a daily basis and fill in the "Daily Check" (Server Room Operation Log).

5.8 電腦機房各項裝置或設施之運轉及故障，均需記錄所有修護情形，相關主管亦應定期至該系統中執行核閱作業。

The operation and failure of each device or facility in the computer room should be recorded, and the relevant supervisor should check the system regularly.

5.9 電腦機房中的各項設備故障，應採取適當之復原措施，處理情形亦應作成紀錄。

The failure of each equipment in the server room should be properly recovered and the situation should be recorded.

5.10 機房設備應與維護廠商訂定書面契約，以確定維護範圍及內容。

Server room equipment should have a written contract with the maintenance vendor to determine the scope and content of the maintenance.

5.11 通訊網路之線路配置圖，維護人員應了解及保存，對各線路應定期檢測其功能，以確保網路之暢通。

The maintenance personnel should understand and keep the configuration map of the communication network circuit. The function of each line should be checked regularly to ensure the network connectivity.

5.12 電腦機房維護人員應建立緊急應變計畫，以處理各種突發意外狀況。

Server room maintenance staff should establish an emergency response plan to deal with any unforeseen circumstances.

5.13 目前不斷電系統(UPS)電池的壽命最多至三年，使用超過三年除了蓄電力下降外，亦可能出現電池漏液等安全隱患，為確保 UPS 正常供電及保護機房安全，各工廠除了每年需要定期檢測及保養外，對於使用時間超過三年的 UPS 應評估蓄電能力等情況，最多延長使用不超過一年，即需要更換電池。

Currently, the lifespan of uninterruptible power supply (UPS) batteries is at most three years. Beyond three years, in addition to reduced power capacity, battery leakage and other safety hazards may occur. To ensure normal UPS power supply and protect the data center, factories need to conduct regular annual inspections and maintenance. For UPS systems older than three years, the power capacity should be assessed, and the batteries should be replaced within a maximum of one more year.

5.14 品牌及合作廠商設備入駐機房代管規範 Regulations for Brand and Partner Equipment Colocation

5.14.1 品牌及合作廠商（以下簡稱甲方）需提供設備清單，含設備型號、數量、介面規格、電壓規格等，以確認機房週邊設施，如：符合供電規格，未經本集團（以下簡稱乙方）審核通過不得進場。

The Brand and Partner (hereinafter referred to as "Party A") shall submit an equipment inventory, including model numbers, quantities, interface specifications, and voltage requirements, to verify compatibility with the data center's infrastructure (e.g., power supply standards). No equipment shall be permitted on-site without prior approval from the Group (hereinafter referred to as "Party B").

5.14.2 硬體需提供設備出廠合格證書、檢測報告等文件，軟體須提供原廠授權證明，硬、軟體的系統安全與維運作業由甲方負責，乙方僅提供機房環境。

For hardware, Party A must provide factory certificates of conformity and inspection reports; for software, original manufacturer authorization proof is required. Party A assumes full responsibility for the system security and maintenance operations of both hardware and software. Party B solely provides the physical data center environment.

5.14.3 甲方應提供授權操作設備人員名單，乙方將依據授權人員名單放行進入機房，並由機房管理員全程陪同，嚴禁攜帶食品、飲料及易燃（爆）物品入內。

Party A shall provide a list of authorized personnel. Access to the data center will be granted strictly based on this list and must be accompanied by data center administrators at all times. Food, beverages, and flammable/explosive materials are strictly prohibited.

5.14.4 甲方應自行提供設備的專用機櫃，不與乙方共用機櫃，乙方僅提供機房環境，包括電力、環控、門禁系統等。

Party A shall provide its own dedicated server cabinets and shall not share cabinets with Party B. Party B's scope of provision is limited to the data center environment, including power, environmental controls, and access control systems.

5.14.5 甲方應遵守本辦法第七條「網路安全」規範，不得於廠內自行架設有（無）線網路，以及在乙方的網路儲存資料、進行攻擊或「挖礦」等違規操作。

Party A must comply with Article 7 ("Network Security") of these Measures. It is strictly forbidden to set up any wired or wireless networks within the premises, store data on Party B's network, launch attacks, or engage in "cryptocurrency mining" or other unauthorized operations.

5.14.6 甲方需提供乙方主機關機之標準作業程序，於必要時（如機房停電）由乙方代為進行關機作業。

Party A shall provide Party B with the Standard Operating Procedures (SOP) for host shutdowns, enabling Party B to perform shutdown operations on behalf of Party A when necessary (e.g., during power outages).

6. 營運安全 **Operation Security**

6.1 集團的公發電腦（含終端機、桌上型、筆記型及連網設備等），均需下載及安裝集團採購的防毒軟體，可由集團內部網站下載並運行當前版本，安裝後應定期更新病毒碼。

The Group's public computers (including terminals, desktops, notebooks and networked devices, etc.) are required to download and install the Group's purchased anti-virus software, which can be downloaded from the Group's intranet site and run the current version, and should be regularly updated with the virus code after installation.

6.2 集團人員不得攜帶私人電腦進入廠區連接內網使用，因公務需要「臨時使用」，除了需要通過 BPM 簽呈，經過單位最高主管（廠區、品牌總經理）同意（讓單位最高主管知悉使用私人電腦辦公，會產生資料外洩及單位內網中毒的風險），並且在開始使用前，電腦要依照集團規定安裝相應的防毒及反入侵軟體。

Group personnel are not allowed to bring their personal computers into the factory to connect to the intranet for use. For "temporary use" due to business needs, in addition to the need to sign through the BPM, after the unit's highest level of supervision (factory, brand general manager) agreed (so that the highest level of supervision of the unit to know the use of private computers for office work, which will result in the risk of data leakage and poisoning of the unit's intranet), and before the start of the use of computers, the computer should be in accordance with the Group's information security regulations to install the appropriate anti-virus and anti-intrusion software.

6.3 6.2 中所述「臨時使用」私人電腦，仍需盡快購買公發電腦進行替換。申請臨時使用的期限以 90 天為限，超過期限需以簽呈再報請單位最高主管核准，否則就必須將私人設備帶出廠區。

For “temporary use” of private computers as described in 6.2, it is still necessary to purchase a replacement public computer as soon as possible. Temporary use applications are limited to 90 days, beyond which a signed letter must be submitted to the top supervisor for approval, or else the personal equipment must be taken out of the factory.

6.4 郵件系統用戶不得開啟來自未知、可疑或不可信賴來源的電子郵件，包括附件中的任何文件或程式。對於來路不明被郵件系統判別為隔離的信件，應立即刪除這些信件夾帶的附件，然後通過清空垃圾箱來「雙重刪除」這些郵件。

Users of the mail system should not open emails from unknown, suspicious or untrustworthy sources, including any files or programs attached. For emails from unknown sources that are recognized as quarantined by the mail system, attachments attached to these emails should be deleted immediately, and the emails should be “double-deleted” by emptying the trash folder.

6.5 用戶應刪除垃圾郵件及附件，不得轉發給其他帳戶。

Users should delete spam emails and attachments and not forward them to other accounts.

6.6 除非有經過主管核准的業務需求，否則應避免使用具有讀/寫訪問權限的直接磁盤共享。

Direct disk sharing with read/write access should be avoided unless there is a supervisor-approved business need.

6.7 集團的資訊部門應定期備份關鍵數據和系統配置，關鍵數據由各業務單位訂定及提供清單，交予資訊部門將數據存儲在安全的地方。

The Group's information department should regularly back up critical data and system configurations. Critical data is defined and inventoried by each business unit and handed over to the information department to store the data in a secure location.

6.8 如果軟體測試與防毒軟體產生衝突，在停用防毒軟體後，不得運行任何可能傳播病毒的應用程序，例如：電子郵件或文件共享。在完成軟體測試後，應啟用防毒軟體，並進行病毒掃描程序，以確保電腦未存在病毒或惡意程序。

If the software test conflicts with the anti-virus software, do not run any applications that may transmit viruses, such as e-mail or file sharing, after disabling the anti-virus software. After completing the software test, the anti-virus software should be turned on and a virus scan should be performed to ensure that no viruses or malicious programs are present on the computer.

6.9 所有電子郵件使用均必須符合本集團的政策、道德操守及安全性，遵守適用法律和適當商業慣例的程序。

All e-mail use must be consistent with the Group's policies, ethics and security, complying with applicable laws and procedures of appropriate business practices.

6.10 電子郵件帳戶應主要用於與公司相關的業務用途，允許在有限的基礎上進行個人通訊，但禁止與非本集團相關的商業用途。

Email accounts should be used primarily for business purposes related to the Group, allowing personal communications on a limited basis, but prohibiting business purposes not related to the Group.

6.11 電子郵件或附件中包含的所有與本集團有關的數據必須進行保護，本集團業務記錄的電子郵件保留至少 6 個月。

All data relating to the Group contained in emails or attachments must be protected and emails of the Group's business records retained for at least 6 months.

6.12 禁止用戶使用第三方電子郵件系統和存儲服務器(例如：Google，Yahoo 和 MSN Hotmail 等) 進行華利集團業務，此類通信和交易應使用本集團核准的文件通過適當的渠道進行。

Users are prohibited from using third party email systems and storage servers (e.g. Google, Yahoo and MSN Hotmail, etc.) to conduct business, and such communications and transactions should be conducted through the appropriate channels using documents approved by the Group.

6.13 有關郵件系統的帳戶申請、異動等申請與管理程序，依據本集團訂定的「電子郵件系統管理辦法」說明及執行。

The procedures for application and management of the e-mail system, such as account application and change of account, are described and implemented in accordance with the "HL-M-IT004 Email System Management Regulations" established by the Group.

6.14 為了保護帳戶的安全，使用者登入集團的應用系統在 15 分鐘內沒有任何操作後，系統會將該帳戶從網上自動登出，以防其他人使用帳戶。

To protect the security of the account, after a user logs in to the Group's application system and does not perform any action for 15 minutes, the system will automatically log out the account from the Internet to prevent others from using the account.

6.15 IT 部門對於集團開發和建立的電子郵件、應用系統的帳戶擁有完全和即時的管理權，包括但不限於登入帳號、密碼、完整的管理設定、歷史記錄、刪除和停權，除非獲得集團資訊安全最高主管同意授權，否則 IT 人員不得以任何方式或工具任意瀏覽、變更或刪除使用者的郵件內容。

The IT department has full and immediate management rights over accounts for email and application systems developed and established by the group, including but not limited to login accounts, passwords, complete management settings, history, deletion, and suspension. Unless authorized by the group's top information security officer, IT personnel are not allowed to arbitrarily view, modify, or delete users' email content in any way or with any tool.

6.16 涉及集團、事業群和工廠內部的重要工作議題，如：正式的命令、要求、工作報告、公告等，包括傳達訊息的文字、圖片、影像或文件，應通過電子郵件、公司網站發送或公布，不應使用個人通訊軟體，如：微信、Zalo、Teams、WhatsAPP 等發送業務相關資訊。

Matters of significance involving the Group, Business Units, or factory internal operations—such as formal directives, requests, work reports, and announcements, including text, images, videos, or documents conveying messages—shall be distributed or published via official corporate channels (e.g., email or the company website). The transmission of business-related information via personal communication software (e.g., WeChat, Zalo, Teams, WhatsApp) is strictly prohibited.

7. 網路安全 **Cyber Security**

7.1 網路安全管理 **Management of Cyber Security**

7.1.1 基於網路安全考量，集團網路規劃為內部及外部網段，其間以防火牆區隔。

For cyber security reasons, the Group's network is organized into internal and external segments, which are separated by firewalls.

7.1.2 內部網段完全與網際網路隔絕，外部網段及任何外界均不得直接存取內部網段。

The internal network segment is completely isolated from the Internet, and neither the external network segment nor any outside party can directly access the internal network segment.

7.1.3 對於非合法授權的使用者，網路管理人員應立即停用或刪除其使用人員帳號。

For users who are not legally authorized, the network administrator shall immediately deactivate or delete their user accounts.

7.1.4 網路管理人員若發現使用者有影響網路安全情形，得使用自動搜尋(檢測)工具檢查檔案。

Network administrators may use automated search (detection) tools to check the files of users who are found to have compromised the security of the network.

7.1.5 網路管理人員未經使用者同意，不得增加、刪除及修改個人檔案，如需刪除檔案，應以電子郵件或其他方式事先知會檔案擁有者。

Network administrators are prohibited from adding, deleting, or modifying personal files without the user's consent, and if deletion is necessary, the owner of the file should be notified in advance by e-mail or other means.

7.1.6 網路使用人員發現任何網路安全事件，應立即反應，通知網路管理人員進行處理，並向主管報告，無法獨立處理時，需由網路管理人員迅速連絡相關廠商。

When network users discover any network security incident, they should respond immediately, notify the network administrator to respond the incident, and report it to their supervisor. If they cannot handle the incident independently, the network administrator should contact the relevant vendors promptly.

7.1.7 網路管理人員不得新增、刪除、修改稽核資料檔案，以避免違反安全事件發生時，造成追蹤查詢的困擾。

Network administrators are prohibited from adding, deleting, or modifying audit data files in order to avoid tracking and inquiring troubles when security violations occur.

7.1.8 集團內部人員使用公司的資訊設備連接網路，應至 BPM 系統填寫「資訊帳號權限申請單」，依照業務需求申請上網，並且經過品牌總經理或廠主管審批同意方能開通連網。

Group employees use the company's information equipment to connect to the Internet should go to the BPM system to fill out the “Information Account Privilege Application Form” to apply for Internet access in accordance with their business needs, and only with the approval of the brand general manager or the plant supervisor can they open the Internet connection.

7.1.9 廠區主管對於所屬員工使用個人資訊設備(包括手持行動裝置)上網，必須進行控管，以確保員工不得在上班時間從事與工作無關的上網行為。

Plant supervisors are required to control the use of personal information devices (including hand-held mobile devices) for Internet access by their employees to ensure that employees are not allowed to engage in non-work related Internet activities during work hours.

7.2 防火牆與主機之安全管理 Security management of firewall and host

7.2.1 本集團與網際網路連接的網路節點上加裝防火牆，以控管外界與內部網路之間的資料傳輸與資源存取。

The Firewall is installed on the Group's network nodes connected to the Internet to control data transmission and resource access between the Internet and intranet.

7.2.2 防火牆應具備網路服務的轉送服務器，以提供網路服務的轉送與控管。

The firewall should have a network service forwarding server to provide network service forwarding and control.

7.2.3 防火牆主機只能由系統終端機登入，不得以其他任何方式登入，以確保防火牆主機安全。

The firewall host can only be logged in through the system terminal and cannot be logged in by any other means to ensure the security of the firewall host.

7.2.4 防火牆進行變更時，系統需進行記錄並由主管人員進行變更之合理性與正確性。

When changes are made to the firewall, the system must log the changes, and the reasonableness and correctness of the changes must be checked by the supervisor.

7.2.5 防火牆主機設置應符合相關規定或內稽內控管理建議。

The firewall host settings should comply with relevant regulations or internal management control recommendations.

7.3 通訊軟體與檔案共享平台之安全管理 **Security Management of Communication Software and File Sharing Platform**

7.3.1 使用通訊軟體如：微信、Zalo 收、發檔案(包括圖片)，應通過 BPM 系統「資訊安全權限申請單」一人一單提出申請以便事件責任規屬，並經過資安或資訊部門審查，提交品牌總經理審批同意後開放使用(使用及權限管控如附表 2)。

The use of communication software, such as WeChat and Zalo to receive and send files (including pictures), should be applied through the BPM system “Information Security Authorization Application Form”, so that the responsibility for the incident belongs to a single person, and after examination by the information security or information department, and submitted to the general manager of the brand for approval and consent to open for use (the use and authority control are as shown in the attachement 2).

7.3.2 品牌客戶如有明確規範不得使用通訊軟體收、發檔案，除非獲得客戶同意開放使用，否則一律按照客戶的要求禁止使用，或是按照客戶指定的其他方式進行檔案交換。

If the brand customer has a clear specification that they shall not use the communication software to receive and send files, unless the customer agrees to the permission granting, it shall be prohibited according to the customer's requirements or send/receive files in other ways specified by the customer.

7.4 檔案共享平台**(Box, OneDrive)**之安全管理 **Security Management of File Sharing Platforms (Box, OneDrive)**

7.4.1 因為工作及業務往來，需要使用檔案共享平台(以下簡稱雲盤)，如：Box, OneDrive, Google Drive 等與客戶、供應商、政府部門及其他非集團組織/人員進行檔案交流，相關規範和帳號申請流程比照 7.3.1。

For work and business transactions, it is necessary to use file sharing platforms (hereinafter referred to as cloud storage), such as Box, OneDrive, Google Drive, etc., to exchange files with customers, suppliers, government departments and other non-group organizations/personnel. The relevant specifications and account application process are the same as in 7.3.1.

7.4.2 目前集團的品牌客戶 Nike 指定使用 Box、Adidas 指定使用 OneDrive 與我們進行檔案交換共享，原則上品牌指定使用的雲盤應區隔各自管理，不允許人員使用非客戶指定的雲盤進行資料存取與交換，也禁止人員在未獲得客戶的同意下，通過雲盤分享與所屬品牌有關的機敏資料給其他品牌的內、外部人員。

Currently, our group's brand clients Nike and Adidas use Box and OneDrive respectively for file exchange and sharing. In principle, the cloud drives designated by the brands should be managed separately. Personnel are not allowed to use cloud drives not designated by the clients for data access and exchange. Furthermore, personnel are prohibited from sharing sensitive information related to their respective brands with internal or external personnel of other brands through cloud drives without the client's consent.

7.4.3 雲盤帳號的密碼設定規則比照「4.密碼保護」的作業流程，除了密碼保護外，宜開啟二步驗證機制，以防範發生帳號及密碼外洩或被盜用的情形。

The password setting rules for cloud storage accounts should follow the procedures outlined in "4. Password Protection". In addition to password protection, it is advisable to enable a two-step verification mechanism to prevent account and password leaks or theft.

7.4.4 雲盤帳號的申請、變更及刪除流程如 7.3.1 敘述，對於未經過申請同意的新增帳號，雲盤後台管理員會發郵件通知使用者，提醒人員要填寫資訊安全權限申請單，若未能在規定時間完成申請，則刪除該帳號。

The application, modification, and deletion process for cloud storage accounts is described in section 7.3.1. For new accounts added without prior application approval, the cloud storage administrator will send an email to the user reminding them to fill out an information security permission application form. If the application is not completed within the specified time, the account will be deleted.

7.4.5 一般使用者的檔案存取預設僅有讀取權限，檔案的管理員則具有讀取和編輯的權限，除非獲得檔案管理員的授權，否則沒有被授權的帳號不能對該檔案進行任何存取。

The users are only allowed read access to files by default, while file administrators have read and edit permissions. Unless authorized by the file administrator, no unauthorized account can access the file.

7.4.6 雲盤帳號登入錯誤超過 3 次即被列入黑名單不得再登入，經過後台管理員審查及確認非惡意攻擊行為後方能解除帳號的鎖定。

If a cloud drive account logs in incorrectly more than 3 times, it will be blacklisted and unable to log in again. The account can only be unlocked after the backend administrator reviews and confirms that the attack was not malicious.

7.4.7 雲盤如有內建偵測及清除惡意程式的功能模塊，預設保持開啟防護功能，後臺管理員每週定期審查，並且通知檔案被感染惡意程式的使用者，對電腦進行病毒掃描，以確認設備無存在資訊安全的風險。

If the cloud storage service has a built-in module for detecting and removing malware, the protection function is enabled by default. The backend administrator will conduct a regular weekly review and notify users whose files are infected with malware to scan their computers for viruses to confirm that there are no information security risks to the devices.

7.4.8 雲盤允許分享網址鏈接，包括資料夾、文件、Hubs，預設分享的對象為集團內部人員，檔案管理員亦可視作業需求將網址鏈接提供給協作者，包括外部帳號，預設有效期為 7 天。

The cloud drive allows sharing URL links, including folders, files, and hubs. The default sharing recipients are internal group personnel, but file administrators can also provide the URL links to collaborators, including external accounts, as needed. The default validity period is 7 days.

7.4.9 雲盤如有內建浮水印功能模塊，由檔案管理員視業務需要再啟用。

If the cloud drive has a built-in watermarking function module, the file administrator can enable it as needed for business operations.

7.4.10 雲盤應開啟控制登入工作階段時長，限制至少為登入超過 24 小時即強制帳號登出。

The cloud drive should enable control over the duration of the login process, with a minimum restriction of 24 hours before the account is forcibly logged out.

7.5 無線網路之安全管理 **Security Management for Wireless Network**

為了保障集團內部網路的資訊安全，對於人員使用資訊設備連接無線網路(WIFI)，管理對象及方式說明如下：

In order to safeguard the information security of the Group's internal network, the objects and methods of managing the use of information devices by personnel to connect to wireless networks (WIFI) are described below:

7.5.1 集團一般用戶：使用公司電腦連接「HLIG Group」名稱的無線網路，申請人至 BPM 系統填寫「資訊帳號權限申請單」-『無線網絡上網權限』，勾選「公司」選項，經過品牌總經理審批同意後開放使用。一般用戶通過 AD 帳號驗證登錄，只能使用內網資源，不連接網際網路。

General users of the Group: To use the company computer to connect to the wireless network of “HLIG Group”, the applicant goes to the BPM system to fill in the “Information Account Privilege Application Form” - “Wireless Network Access Privilege”, checking the “Company” option, and then opens up the use of the wireless network after the approval of the General Manager of the brand. General users can only use the internal network resources through the AD account authentication, not connected to theInternet.

7.5.2 集團訪客及特別權限用戶：使用個人裝置或公司電腦連接「HLIG Group VIP」名稱的無線網路，申請人(或代理人)至 BPM 系統填寫「資訊帳號權限申請單」-『無線網絡上網權限』，勾選「個人」選項，經過品牌總經理審批同意後開放使用。訪客及特別權限用戶需要綁定設備的網卡序號，只能連接網際網路，不使用內網資源。

Group visitors and privileged users: use personal devices or company computer to connect to the wireless network under the name of “HLIG Group VIP”, the applicant (or agent) should fill in the “Information Account Privilege Application Form” - “Wireless Network Access Privilege” in the BPM system, check the “Personal” option, and then open to use the service after the approval of the brand general manager. Guests and users with special privileges need to bind the serial number of the device's network card, and can only connect to the Internet, without using the internal network.

7.5.3 使用個人行動裝置的用戶：因工作需要申請使用個人行動裝置連接「HLIG Group Limited」名稱的無線網路，申請人至 BPM 系統填寫「資訊帳號權限申請單」-『無

線網絡上網權限』，勾選「個人」選項，經過品牌總經理審批同意後開放使用。個人行動裝置除了只能連接外網、不使用內網資源，另外需遵守相關安全措施如下：

Users of personal mobility devices: To apply for the use of personal mobility devices to connect to the wireless network of "HLIG Group Limited" for work purposes, applicants should fill out the "Information Account Permission Application Form" - "Wireless Network Access" in the BPM system, check the "Personal" box, then get the approval of the brand general manager before being allowed to use. In addition to connecting to the external network and not using the internal network resources, the personal mobility device is required to comply with the relevant security measures as follows:

7.5.3.1 只能使用微信、Zalo、Skype 等通訊軟件，不得從事與工作無關的上網行為。

For communication software, only WeChat, Zalo, Skype, etc. are acceptable for work purposes, and any non-work related internet activities are prohibited.

7.5.3.2 開放使用個人行動裝置連網的工廠需付費加購無線網路安全模塊。

Factories that are open to using personal mobility devices to connect to the Internet are required to purchase wireless security modules at a cost.

7.5.4 因業務或辦公空間配置需要，用戶申請架設個人使用的 WIFI AP，應至 BPM 系統填寫簽呈，說明申請用途及會簽資訊總處審查，獲得品牌總經理同意後交給 IT 部門安裝。

If a user needs to install a personal Wi-Fi Access Point (AP) due to business requirements or office space configuration, they shall submit a formal request via the BPM system. The request must specify the purpose of use and be countersigned by the Information Division for review. Upon approval by the Brand General Manager, it shall be forwarded to the IT Department for installation.

7.5.5 個人使用的 WIFI SSID 預設的網路型態為「隱藏」，WIFI AP 需綁定用戶設備的 MAC Address, 用戶只能連接外網不得接入內網，IT 人員需要對設備設定重啟時間，如：00:00~03:00，以防止閒置連線用戶及降低效能。

7.5.5 Personal Wi-Fi SSIDs shall default to "Hidden" mode. The MAC Address of the user's device must be bound to the Wi-Fi AP. Users are restricted to the external network (Internet) only and are prohibited from accessing the internal network. IT personnel must configure automatic reboot schedules (e.g., 00:00–03:00) to disconnect idle sessions and optimize performance.

7.5.6 公共使用的 WIFI AP 原則上需與集團採購的無線網路設備品牌相同，以利統一派送安全政策管控；如因個別需求採購他牌 WIFI AP，相關安全設定比照 7.5.5 辦理。

7.5.6 Public Wi-Fi APs must, in principle, be of the same brand as those procured by the Group to facilitate unified security policy deployment. If alternative brands are procured for specific needs, their security configurations shall follow the provisions outlined in Section 7.5.5.

7.5.7 OT 網路架構下的 WIFI AP 不能連接外網及 IT 內網，只能連入 OT 內網，如果有特殊需求情況要跨接網路，比照 7.5.4 流程進行申請，需經過資訊總處審查及品牌總經理審批同意後，再提交給 IT 部門安裝。

7.5.7 Wi-Fi APs under the OT network architecture must not connect to the external network (Internet) or the IT internal network; they may only connect to the OT internal network. If cross-network connectivity is required for special circumstances, the application process defined in Section 7.5.4 must be followed. Approval from the Information Division and the Brand General Manager is mandatory before submission to the IT Department for installation.

7.6 外部厂商远程协助安全操作准则 **Security Operating Guidelines for External Vendor Remote Support**

为规范外部厂商远程协助处理技术问题的操作流程，确保公司网络与数据安全，防止未经授权的访问与信息泄露，特制定本准则，本准则适用于所有需接入公司内部网络进行远程技术支持的外部厂商、合作伙伴及公司内部对接人员。

In order to standardize the operational procedures for external vendors providing remote technical assistance, ensure the security of the corporate network and data, and prevent unauthorized access and information leakage, these Guidelines are hereby established. These Guidelines apply to all external vendors and partners required to access the internal corporate network for remote technical support, as well as relevant internal personnel acting as liaisons.

7.6.1 远程接入基本要求 Basic Requirements for Remote Access

认证方式强制要求： Mandatory Authentication Methods:

7.6.1.1 VPN 通道：厂商必须使用公司提供的 Fortinet SSL VPN 账号接入公司网络，禁止直接通过公网暴露内部系统端口。

VPN Tunnel: Vendors must use Fortinet SSL VPN accounts provided by the company to access the corporate network. Direct exposure of internal system ports to the public internet is strictly prohibited.

7.6.1.2 双因子认证（2FA）：所有 VPN 账号需启用双因子认证。厂商人员需使用动态令牌（如 FortiToken Mobile）生成一次性验证码，结合静态密码完成登录。

Two-Factor Authentication (2FA): 2FA must be enabled for all VPN accounts. Vendor personnel must use dynamic tokens (e.g., FortiToken Mobile) to generate one-time verification codes, combined with static passwords, to complete login.

7.6.1.3 IP 白名单绑定：仅允许厂商预先报备的固定公网 IP 地址通过 VPN 接入。需由 IT 部门在防火墙规则中配置 IP 白名单，拒绝非授权 IP 的所有连接请求

IP Whitelisting: Only pre-registered, fixed public IP addresses declared by vendors are permitted to connect via VPN. The IT Department must configure IP whitelists in firewall rules to reject all connection requests from unauthorized IPs.

7.6.2 远程软件限制 Remote Software Restrictions

禁用第三方工具：严禁使用向日葵、TeamViewer、AnyDesk 等未经授权的第三方远程控制软件。

Prohibition of Third-Party Tools: The use of unauthorized third-party remote control software (e.g., Sunlogin, TeamViewer, AnyDesk) is strictly prohibited.

7.6.3 过程监控 Process Monitoring

操作审计：所有远程会话需开启日志记录功能（如火绒支持的操作追溯），包括屏幕录像、命令行操作记录等。

Operation Auditing: All remote sessions must have logging enabled (including operation traceability supported by Huorong Security). This includes screen recording and command-line operation logs.

7.6.4 事后清理 Post-Incident Cleanup

远程协助结束后，立即关闭 VPN 账号的临时访问权限。

Access Revocation: Temporary VPN access permissions must be revoked immediately upon completion of the remote assistance session.

8. 資訊系統獲取、開發及維護 **Information System Acquisition, Development and Maintenance**

8.1 資訊系統獲取、開發程序 **Information system acquisition and program development**

8.1.1 資訊部門應評估使用單位實際作業需求，確認可行且有開發新系統之必要，簽呈送請相關單位主管會簽，以判定是否執行系統開發作業。

IT should evaluate the actual operational needs of the user unit, confirm that it is feasible and necessary to develop a new system, then sign and submit it to the supervisor of the relevant department for signature in order to determine whether or not to carry out the system development operation.

8.1.2 資訊部門辦理委外開發採購作業，需依據使用者需求邀集相關單位共同規劃解決方案，實際查詢廠商的成功案例，評選有能力按需求完成系統開發工作的最佳廠商。

In order to handle outsourced development and procurement, the information department needs to invite relevant units to jointly plan solutions based on user requirements, actually inquire about successful cases of vendors, and select the best vendor that is capable of completing the system development work according to the requirements.

8.1.3 委外開發(維護)的合約內容需包含：開發時程表、完成時間、維護方式、付款方式、版權、軟硬件需求、交付文件、相關賠償方式及安全要求等。

The contract for outsourced development (maintenance) should include: development schedule, completion time, maintenance method, payment method, copyright, software

and hardware requirements, delivery documents, related compensation and security requirements.

8.2 資訊系統開發文件規範 **Specifications for Information System Development files**

資訊系統之開發，資訊部門人員或委外廠商應編寫完整之系統文件，包含：系統開發文件、系統測試紀錄及驗收紀錄、系統操作說明書等，文件內容規範如下：

For the development of the information system, IT personnel or the outsourced vendor s should prepare complete system files, including: system development files, system test records and acceptance inspection records, system operation manuals, etc. The contents of the files are standardized as follows:

8.2.1 系統文件應統一規定使用相同語言及編碼。

System files should be standardized for using the same language and code.

8.2.2 系統文件使用之符號體系應有統一使用規定及填寫說明。

The symbol system used in the system files should have standardized rules for use and instructions for filling in the symbol system.

8.2.3 系統文件應有撰寫標準說明。

System files should be written with standard descriptions.

8.2.4 系統文件應有使用者閱讀說明。

System files should have user readable instructions.

8.2.5 系統文件應標明控制點及審計軌跡。

System files should identify control points and audit trails.

8.2.6 系統開發單位應將完成之各項資料歸檔備查。

The system developers should archive the completed data for reference.

8.2.7 系統文件應詳細分類編號統一歸檔。

System files should be classified and numbered for uniform filing.

8.2.8 系統文件應備份存放於安全處，並由專人負責保管。

System files should be backed up and stored in a safe place under the responsibility of a person.

8.2.9 當系統修改時，文件應隨之修改，並註明修改時間。

When the system is modified, the files should be modified accordingly with the time of modification.

8.2.10 系統文件保管人員離職時，主管應指派交接之保管人員。

When the custodian of the system files leaves , the supervisor shall assign a replacement custodian.

8.2.11 若確定舊版本之系統文件、使用手冊已無需再使用，經過資訊部門主管核准後，保管人方可將文件報廢。

If it is determined that the old version of the system files and user manuals are no longer usable, the custodian can scrap the files only after the approval of the IT supervisor.

8.3 資訊系統修改控制作業

8.3.1 資訊系統修改需由使用單位填寫「系統開發需求申請單」，經過資訊部門主管審核通過始得變更，以確保相關權責人員充分考量修改程序的必要性及其風險。

Modifications to the information system must be made by the user unit by completing the "Form of Needs for IT System" and approved by the supervisor of the IT department to ensure that the relevant responsible personnel fully consider the necessity of the modification process and its risks.

8.3.2 系統開發人員需編制「系統開發文件」(SA/SD)，與使用單位進行討論了解細部需求，並留存各階段會議紀錄與使用單位確認。

System developers are required to prepare "System Development Documents" (SA/SD), discuss with the user units to understand the detailed requirements, and keep the minutes of each stage of the meeting to confirm with the user units.

8.3.3 資訊人員應建置獨立之開發及測試環境，以維護正式環境之資料，系統開發及程序修改作業皆於開發及測試環境下執行。

IT personnel should establish an independent development and testing environment to maintain the data of the official environment, and the system development and program modification operations are performed in the development and testing environment.

8.3.4 資訊部門應會同申請單位於測試環境測試開發或修改完成之系統或程序，將測試結果記錄於系統測試文件(ST1/ST2)，並檢附相關報表及畫面。

The IT department, together with the applicant, should test the developed or modified system or program in a test environment, record the test results in the system test file (ST1/ST2), and attach the related reports and pictures.

8.3.5 系統負責人於程序修改前，應上線變更申請程序並發送系統上線申請紀錄，經資訊部門主管確認簽核並確認預定上線日期，由經授權之執行人員負責將系統上線至系統正式環境。

The system PIC should make an application for the program change and send record of the system release application before modifying the program, after the supervisor of IT department approves the application and confirms the scheduled release date, the authorized executive will be responsible for uploading the updated programs to the official environment of the system.

8.3.6 系統上線至正式環境，資訊人員應建立軟件更新的版本控制機制。

When the system is upgraded to the official environment, IT personnel should establish a version control mechanism for software updates.

8.3.7 系統上線使用後，資訊部門應用系統管理組人員應將「系統開發/程序變更申請單」、「系統規格需求說明書」及「系統上線申請單」編號歸檔留存。

After the system is online, staff of application & system management unit of IT should serialize & file the “System Development/Program Change Request Form”, “System Specification Request form” and “System roll-out Request Form”.

8.3.8 系統上線使用後，資訊部門需評核其使用情形，如有執行結果不當或錯誤時，應使用「問題反饋通知單」轉發系統分析人員，系統分析人員依使用者反饋的訊息，執行系統分析、程序設計、系統發展等步驟，逐一進行系統錯誤檢核及修正，並定期執行系統轉換環境後之運轉績效評估。

After the system goes live, IT needs to evaluate its usage condition, and if there are improper or incorrect execution results, they should be forwarded to the system analysts using the “Problem Feedback Notification Sheet”. The system analysts, based on the user's feedback, will perform system analysis, program design, and system development, and will carry out the system errors checking and fixing them step by step and periodically regularly evaluate the operating performance of the system after changing the operating environment.

8.4 資訊系統上線各階段職責分工 **Division of responsibilities at various stages of information system rollout**

資訊系統上線區分三個階段，由程式組和資料庫組共同執行相關作業，有關各階段職責分工如下：

There are three stages for the rollout of information system, which will be carried out by the programming team and the database team, and the division of responsibilities for each stage is as follows:

8.4.1 開發階段(DEV)：程式組執行程序的開發、異動及維護。

Development Stage (DEV): The programming team executes the development, changes and maintenance of the program.

8.4.2 測試階段(QAS)：程式組執行測試檢驗程序，確保軟件品質符合標準，並持續改進測試流程。

Test stage: The programming team test and verify procedures to ensure software quality meets standards and continuously improve the testing process.

8.4.3 部署階段(PRD)：資料庫組執行程序的部署及版本控制。

Deployment stage (PRD) : The database team performs the deployment and versioning of the program.

9. 供應商關係 **Supplier Relationships**

9.1 本集團透過內部資安管理制度，對於供應商在集團資訊系統內的資訊，採用系統的權限設定保護其隱私。

The Group protects the privacy of suppliers' information in the Group's information system by adopting systematic authority setting through an internal information security management system.

9.2 對於外部供應商的資安管理，於簽訂合約時檢附資訊安全條款及保密協議，要求合作的供應商簽署；供應商需於年度稽核時填寫資訊安全管理自評表，並由本集團資安部門審查內容，每兩年實地稽核供應商。

For information security management of external vendors, information security clauses and confidentiality agreements are attached to contracts and required to be signed by cooperating suppliers; vendors are required to fill in "Self-assessment form for Information Security Management" during annual audits and the contents are reviewed by the Group's IS department, which conducts on-site audits against suppliers every two years.

9.3 有關與供應商簽定的資訊安全條款項目如下：

The clauses of the information security agreement with suppliers are as follows:

9.3.1 供應商交付產品不應有影響集團營運的資安疑慮，如病毒(Virus)、後門(Back Door)或木馬程式(Trojan Horse) 等惡意程序。

Vendors should not deliver products with security concerns that affect the Group's operations, such as viruses, back doors, or malware such as Trojan Horse.

9.3.2 軟硬件產品需提供必要的修正程式與安全更新，以確認無資安漏洞。

For hardware and software products, vendors are required to provide necessary fixes and security updates to ensure that there are no security vulnerabilities.

9.3.3 供應商如發生資安事件，應提供快速有效的解決方案，並研擬改善及預防措施，以將損失降到最低的程度。

In the event of an information security incident, vendors should provide quick and effective solutions and develop improvement measures to minimize losses.

10. 資訊安全事件管理 **Management of information security incidents**

10.1 資訊安全事件依其影響範圍及損失程度分為四級，依嚴重性由高至低定義如下：

Information security incidents are categorized into four levels according to their scope of impact and degree of loss and are defined as follows in descending order of severity:

10.1.1 第四級：本集團骨幹網路或對外網路無法運作、郵件系統無法運作、核心系統遭入侵或破壞、集團重要的機密資料外洩。

Level 4: The Group's backbone network, external network, or mail system is unavailable; the core system has been intruded on or damaged, and important confidential information of the Group is leaked.

10.1.2 第三級：本集團骨幹網路或對外網路遭受攻擊，導致 2 或多個網段無法運作、2 或多個資訊系統無法運作、集團入口網站遭受攻擊導致業務停擺、2 或多個廠區的個人電腦遭大規模入侵、破壞或感染電腦或木馬等惡意程序。

Level 3: Attacks on the Group's backbone network or external network, resulting in 2 or more network segments or information systems being inoperable; attacks on the Group's portal resulting in business shutdowns; computers in 2 or more plants are subjected to

large-scale intrusion and damage, or infected with Trojan horses and other malicious programs.

10.1.3 第二級：本集團單一網段因遭受攻擊導致無法運作、單一資訊系統無法運作、2 或多個部門的個人電腦遭入侵、破壞、感染病毒或木馬等惡意程序。

Level 2: A single network segment of the Group is rendered inoperable due to an attack, a single information system is rendered inoperable, or personal computers of 2 or more departments are invaded, damaged, or infected with viruses, Trojans, and other malicious programs.

10.1.4 第一級：個人電腦遭受入侵、破壞或感染電腦病毒、個人電腦的非機密資料遭竊取、感染病毒或木馬等惡意程序。

Personal computer is invaded, damaged or infected with computer virus; non-confidential data stored in the office computer is stolen, infected with virus or Trojan horse and other malicious programs.

10.2 資訊總處負責下列資訊安全事件通報與處理事項：

The following information security incident notifications and responding are under the purview of HQIT:

10.2.1 本集團資訊安全事件分類與分級。

Classify the Group's information security incidents.

10.2.2 通報本集團的資訊安全事件。

Notification of information security incidents in the Group.

10.2.3 規劃資訊安全事件處理程序。

Plan for procedures for responding information security incidents.

10.2.4 協助各單位處理資訊安全事件。

Assist departments in responding information security incidents.

10.2.5 集團的資訊安全長交辦事項。

Matters assigned by the Group Chief Information Security Officer.

前項所稱處理，包括調查事件原因、確認其影響範圍並評估損失及執行緊急應變措施。

The responding of an incident, as referred to in the preceding items, includes investigating the cause of the incident, ascertaining the scope of its impact, assessing the damage, and implementing emergency response measures.

10.3 資訊安全事件處理時效依影響等級區別「優先權」，不同等級之優先權有對應的通報和應變時間，事件發生後最晚不得超過 2 天完成通報，並於 5 天內完成復原及損害管制。以下為資安事件的優先權等級和處理時效：

The priority of responding information security incidents is based on its level of impact. Different levels of priority have corresponding notification and response times. The notification should be completed no later than 2 days after the occurrence of the incident, and the recovery and damage control should be completed within 5 days. Below are the

priority levels and response times for information security incidents:

10.3.1 事件優先權為「緊急」：1 天內完成事件通報，2 天完成應變處理。

Priority of the incident is “Urgent”: 1 day for incident notification and 2 days for response.

10.3.2 事件優先權為「高」：1 天內完成事件通報，3 天完成應變處理。

Priority of the incident is is “High”: 1 day for incident notification and 3 days for response.

10.3.3 事件優先權為「一般」：2 天內完成事件通報，4 天完成應變處理。

Priority of the incident is “Normal”: 2 days for incident notification and 4 days for response.

10.3.4 事件優先權為「低」：2 天內完成事件通報，5 天完成應變處理。

Priority of the incident is “low”: 2 days for incident notification and 5 days for response.

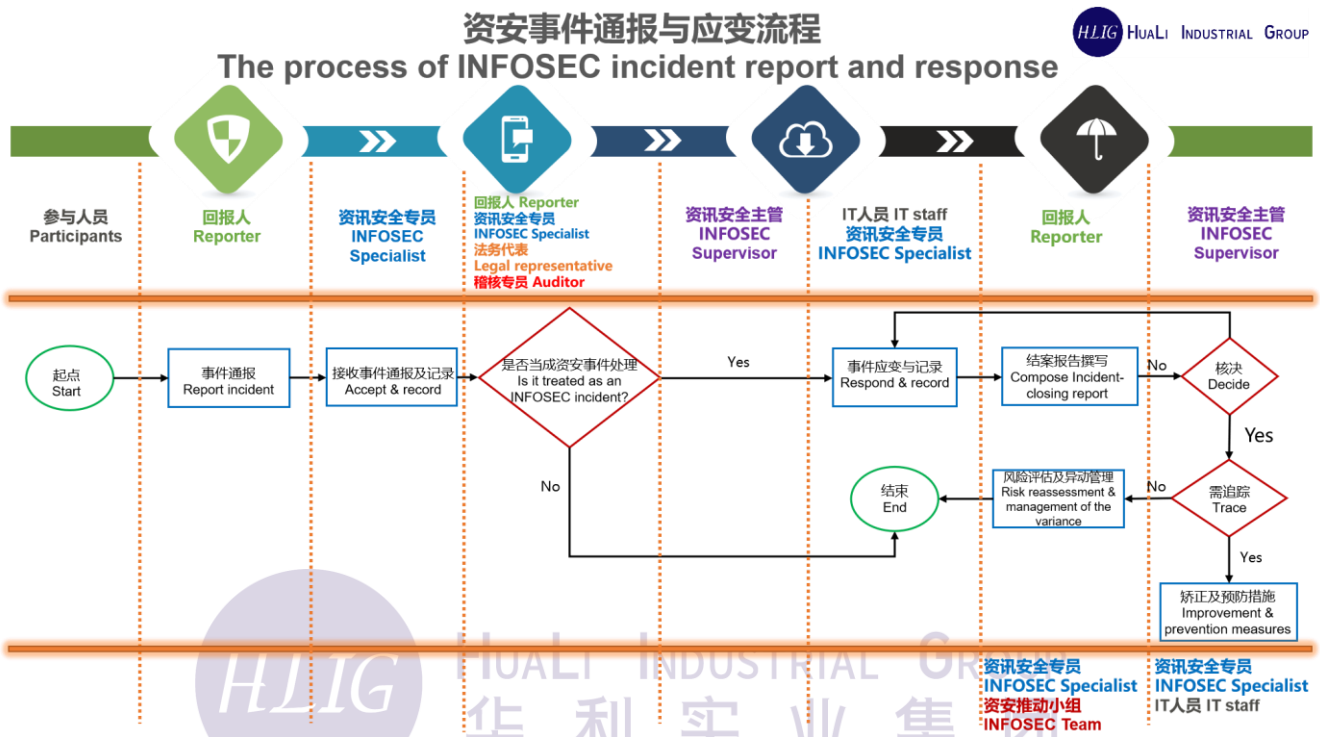
如資安事件為內部通告預警，不具實質危害資訊作業之風險，比照事件優先權「低」的處理時效。

If a security incident is an internal warning notice that does not materially jeopardize the information operations, it will be responded according to the “low” priority.

10.4 資訊安全事件通報依照事件處理流程，參與人員身份區分為「回報人」、「IT 人員」、「資訊安全專員」及「資訊安全主管」，當事件發生時由回報人於本集團的「資安事件通報應變平台」(CSIRT)先進行通報記錄，接著由資訊安全專員進行事件審查，如確認立案，則交由資訊安全主管覆核，並指派專責 IT 或資訊安全人員進行事件應變處理。完成事件處理，回報人將事件經過報告填寫於平台記錄，再交給資訊安全主管進行事件審核與結案，若該事件影響集團的資安風險管控方案，需調整風險等級或管控措施，則交由本集團資安推動小組進行風險複評及異動管理；若無影響資安風險管控方案，則逕行辦理結案，本集團資安事件通報與應變流程如下圖所示。

The information security incident notification is based on the incident handling process, and the personnel concerned are categorized as “reporter”, “IT staff”, “information security specialist” and “information security supervisor”. When an incident occurs, the reporter will first make a notification record in the Group’s “Information Security Incident Notification and Response Platform” (CSIRT), then the information security specialist will carry out an incident review, and if it is confirmed that a case needs to be filed, the case will be reviewed by the information security supervisor and assigned to a dedicated IT or information security staff to respond to the incident. Upon completion of the incident processing, the reporter will fill in the incident report in the platform for the record, and then submit it to the information security supervisor for incident review and closure. If the incident affects the Group’s information security risk control program, the risk level or

control measures need to be adjusted, which will be handed over to the Group's information security promotion team to conduct a risk reassessment and management of the variance; if the incident does not affect the information security risk control program, it will be directly closed. The information security incident notifications and handling flow is shown in the figure below:



10.5 資訊安全事件發生之原因、影響範圍、損失情況、分類、分級及應變措施等，事件回報人員應詳加記錄於 CSIRT 平台，作為改善資訊安全缺失、因應未來類似事件及修訂各類資訊安全事件處理程序之參考。

The causes, scope of impact, damage, classification, categorization, and contingency measures of information security incidents should be recorded in the CSIRT platform by the incident reporting personnel as a reference for improving information security deficiencies, responding to similar incidents in the future, and revising the procedures for handling various types of information security incidents. This will serve as a reference for improving information security deficiencies, responding to similar incidents in the future, and revising various information security incident responding procedures.

10.6 資訊總處應定期評估本集團資訊安全事件預防需求，建置和維護適當防護設備及相關技術，以協助各單位加強防範發生資訊安全事件之能力。

The Group's information security incident prevention needs should be regularly assessed by the HQIT, and appropriate protective equipment and related technologies should be installed and maintained to assist each unit in strengthening its ability to prevent information security incidents.

11. 有關於資訊安全方面的營運持續管理 **Ongoing management of information security operations**

11.1 訂定資訊安全的業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，劃分緊急應變及復原作業程序及相關人員之權責，並定期演練及調整更新計畫。

To establish a business continuity plan for information security, assess the impacts of various man-made and natural disasters on business operations, delineate the emergency response and recovery procedures and the authority and responsibility of related personnel, and regularly rehearse and adjust the plan.

11.2 建立資訊安全事件緊急處理機制，當集團發生資訊安全事件時，應依資安事件通報與應變程序，立即向資訊部門人員通報，採取相對應變措施，以降低及控制損害範圍。

Establish an emergency responding mechanism for information security incidents. When an information security incident occurs in the Group, immediately notifying IT personnel for them to take contingency measures to minimize and control the scope of damages is necessary in accordance with the information security incident notifications and responding flow.

11.3 當發生資訊安全事件，若有損及客戶權益疑慮時，經資訊安全主管裁決，透過業務單位人員通報客戶相關內容。

When an information security incident occurs and there is a suspicion of damage to customers' rights and interests, we will notify customers of the contents of the incident through our business unit personnel at the discretion of the information security officer.

11.4 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訊安全措施。

To define and differentiate the level of data security, and to take appropriate and sufficient information security measures according to the different levels of security.

12. 適法性 **Legality**

12.1 本集團之內部人員、供應商與訪客，皆應遵守集團的資訊安全政策與管理辦法，承擔安全相關義務和責任，並及時報告資訊安全事件。

The Group's internal staff, suppliers and visitors should comply with the Group's information security policies and management measures, assume security-related obligations and responsibilities, and report information security incidents in a timely manner.

12.2 適法性目標及量測指標：每年進行資訊安全管理辦法檢驗，違反國家有關法律、法規等相關件數不得發生。

Legality targets and measurement indicators: the Management Measures for Information Security will be examined every year, and no violation of relevant national laws and regulations is allowed to occur.

附表 1

华 利 实 业 集 团 Huali Industrial Group

资讯设备（笔记本、数位相机、U 盘）借用&归还登记表

Record form of Information Equipment Borrowed & Returned (Notebook, Digital Camera, USB Storage, etc.)

设备名称 Name of Equipment	借用人 Borrower	借用日期 Date of borrowing	用途 Purpose	归 还 纪 录			
				归还日期 Date of Return	归还人 Returner	设备状况 Equipment Status	保管人 Keeper
						☐正常 Normal ☐异常 Abnormal	
						☐正常 Normal ☐异常 Abnormal	
						☐正常 Normal ☐异常 Abnormal	
						☐正常 Normal ☐异常 Abnormal	
						☐正常 Normal ☐异常 Abnormal	
						☐正常 Normal ☐异常 Abnormal	
						☐正常 Normal ☐异常 Abnormal	
						☐正常 Normal ☐异常 Abnormal	
						☐正常 Normal ☐异常 Abnormal	
						☐正常 Normal ☐异常 Abnormal	
						☐正常 Normal ☐异常 Abnormal	
						☐正常 Normal ☐异常 Abnormal	
						☐正常 Normal ☐异常 Abnormal	

附表 2

通訊軟體使用及權限管控表

Permission Settings for Communication Software

通訊軟體預設權限 Permission Settings for Communication Software						
項目 Items	使用及文字傳輸 Use and text transmission	傳送權限 Permission to transfer		接收權限 Permission to receive		備註 Remark
		檔案 File	圖片 Pic	檔案 File	圖片 Pic	
SKYPE	No	No	No	No	No	如需使用請依下表方式申請 If you need any permission, please apply per the form below
WECHAT	No	No	No	No	No	
ZALO	No	No	No	No	No	

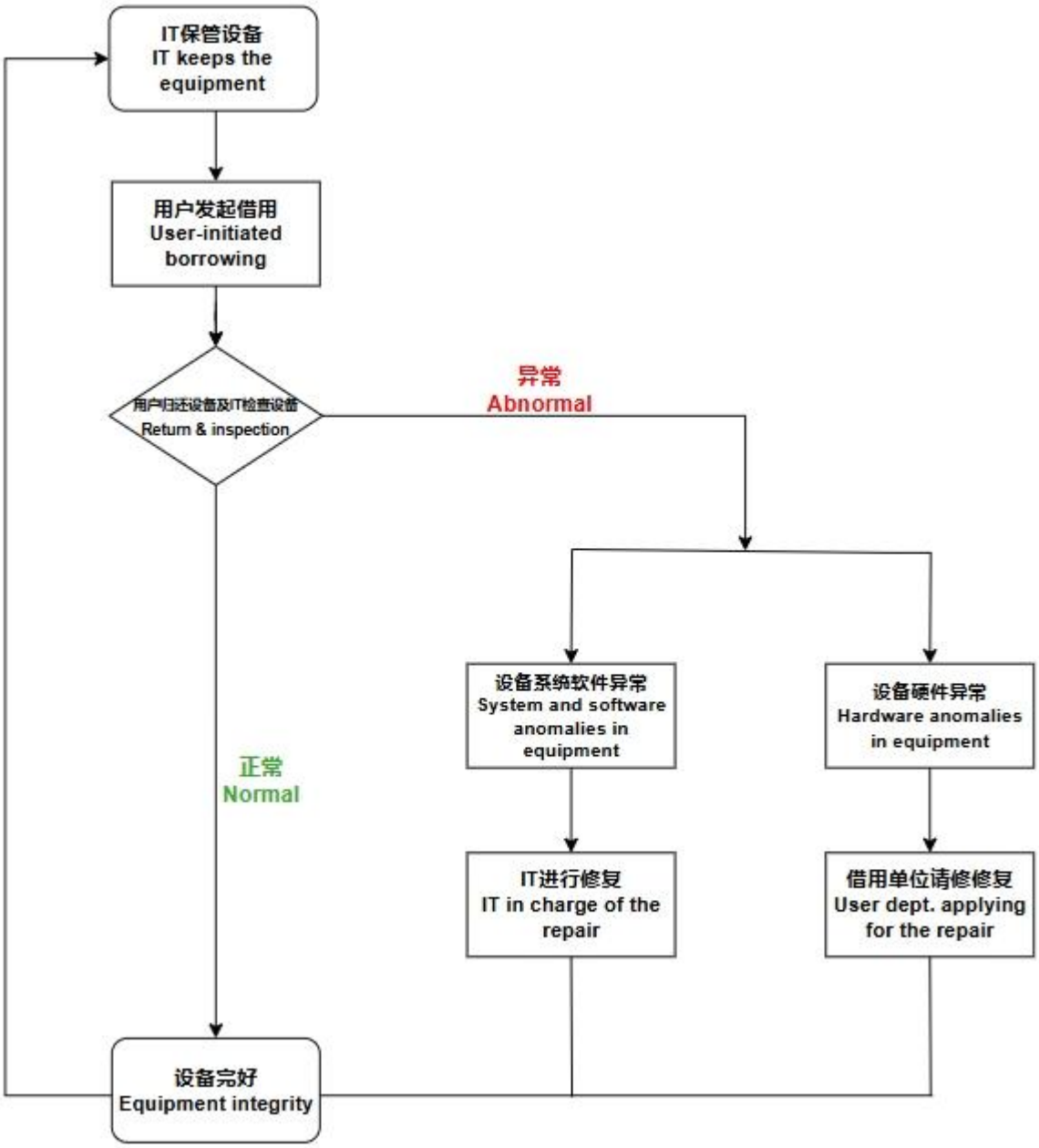
通訊軟體使用及檔案/圖片傳輸權限申請方式 Permission Settings for Transferring Files/Pics on Communication Software							
項目 Items	使用及文字傳輸 Use and text transmission	傳送權限 Permission to transfer		接收權限 Permission to receive		簽核層級 Approval level	備註 Remark
		檔案 File	圖片 Pic	檔案 File	圖片 Pic		
SKYPE	資訊帳號權限申請單 Requisition of Account-Authority	簽呈(需加簽總部資安稽核、資訊單位和上傳備註欄位所述附件) Application form (Countersigning HQIS & IT is needed, and upload				品牌總經理 Brand GM	申請檔案傳輸權限只限對外、客戶的主要連絡窗口，且需政府/客戶提供相關證明，WECHAT/ZALO 圖片傳輸權限除外 Application

		attachment per the "Remark" column)		for file transfer permission is limited to main contact windows for external parties/customers, and requires related evidence from government/customers, except for WECHAT/ZALO image transfer permission.
WECHAT ZALO	資訊帳號權限申請單 Requisition of Account-Authority	資訊安全權限申請單 IT Security Permission Requisition	品牌總經理 Brand GM	

附圖 1

華利實業集團資訊設備借出/歸還流程

HLIG's Borrowing & Returning Procedure for Information Equipment


IT保管设备
IT keeps the equipment
用户发起借用
User-initiated borrowing
用户归还设备及IT检查设备
Return & inspection
异常
Abnormal
正常
Normal
设备系统软件异常
System and software anomalies in equipment
设备硬件异常
Hardware anomalies in equipment
IT进行修复
IT in charge of the repair
借用单位请修修复
User dept. applying for the repair
设备完好
Equipment integrity