唐榮鐵工廠股份有限公司資訊安全管理要點
Tang Eng Iron Works Guidelines for the Information Security Management

中華民國 111 年 1 月 11 日唐董資字第 1111360001 號函頒
Issued by the Letter Tang-Dong-Zi-Zi No. 11111360001 dated January 11, 2022

一、目的
I. Purpose

為強化本公司資訊安全管理，建立可信賴之作業環境，以確保資料、系統、設備及網路等資訊資產之可用性、完整性及機密性，特訂定本要點。

These guidelines have been established to strengthen our information security management and establish a reliable operating environment to ensure the availability, integrity and confidentiality of information assets such as data, systems, equipment and networks.

二、原則
II. Principle

本公司依實際業務需求，訂定資訊安全政策以書面、電子或其他方式告知並要求相關人員遵行。

Based on actual business needs, the Company has established an information security policy that is communicated in writing, electronically or by other means and requires compliance by relevant personnel.

同時建置資訊安全風險管理架構，確定資訊安全組織、權責分工及資訊安全措施。

In addition, the Company has established an information security risk management framework to determine the information security organization, division of authority and responsibility and information security measures.

三、資訊安全政策
III. Information Security Policy

保護公司資訊資產免於各種威脅與破壞，正常穩定運作，提供可信賴之資通訊服務，確保資訊資產之機密性、完整性及可用性，並順利推展公司各項業務，以保障公司權益。

Protect the Company's information assets from various threats and damages, reliable information and communication services to ensure the confidentiality, integrity and availability of information assets and smoothly carry out the Company's various businesses in order to protect the Company's interests.

藉由全體同仁共同努力達成以下目標：

The Company achieves the following goals through the joint efforts of all colleagues:

1. 防範資訊安全威脅之發生，降低資訊安全事件發生之風險。
   Prevent information security threats and reduce the risk of information security incidents.

2. 保護公司資料，避免不當使用及存取，防止敏感性及機密性資料外洩或遺失。
   Protect company data from improper use and access and prevent leakage or loss of sensitive and confidential information.

3. 提高資訊設備及系統效能，確保資訊系統正常運作。
   Improve the performance of information equipment and systems to ensure the proper operation of information systems.

4. 確保公司各項資訊業務之執行，符合法令之規範。
   Ensure that the company's information business is carried out in compliance with the law.

四、資訊安全風險管理架構

IV. Information Security and Risk Management Framework

1. 資訊安全組織及權責分工
   Information security organization and division of authority and responsibility

   公司應依下列原則，將權責賦予相關部門及人員：
   The Company shall delegate authority and responsibility to relevant departments and personnel in accordance with the following principles:

   (1) 管理部門副總經理負責督導資訊安全管理事項。
   The Vice General Manager of the Management Department is responsible for supervising information security management matters.

(2) 本公司資訊安全之專責單位為資訊處，資安專責主管為資訊處長並設至少 1 名資安專責人員，負責資訊安全政策訂定及宣導，以及相關安全措施建置、推動及管理。

The Information Management Division is the dedicated unit for information security, and the Chief Information Officer serves as the dedicated supervisor of information security. At least one dedicated information security staff is responsible for information security policy formulation and promotion, as well as the establishment, promotion and management of related security measures.

(3) 各部門主管負責電腦資料及資訊系統之安全需求研議、使用管理及保護。

Each department supervisor is responsible for the security requirements of computer data and information systems, as well as their usage management and protection.

2. 資訊安全風險評估

Information security risk assessment

評估本公司於營運中資訊安全相關之可能出現的風險與機會，採取管控方案，以維持營運和提供適當資訊服務的能力。

Assess possible risks and opportunities related to information security in our operations and adopt control plans to maintain our operations and ability to provide appropriate information services.

五、資訊安全防護措施

V. Information security protection measures

公司應就下列資訊安全作業，訂定相關管理措施：

The Company shall establish relevant management measures for the following information security procedures:

1. 電腦系統安全管理。
Computer system security management.

2. 網路安全管理。
Network security management.

3. 電子郵件使用資訊安全管理。
   E-mail usage information security management.

4. 系統存取控制管理。
   System access control management.

5. 系統發展及維護安全管理。
   System development and maintenance security management.

6. 資訊資產安全管理。
   Information asset security management.

7. 電腦病毒及惡意軟體之控制。
   Control of computer viruses and malware.

8. 業務永續運作計畫。
   Business sustainability plan.

六、電腦系統安全管理措施

VI. Computer system security management measures

針對使用者控制、資料、檔案程式及機房控制等作安全管理，確保電腦系統能正常運作。

Conduct security management for user control, data, file programs and server room control to ensure the normal operation of the computer system.

1. 使用者控制安全管理

   1. User control security management

   為保護本公司電腦系統儲存之資料檔案並避免遭受破壞，非經授權人員不得進入電腦系統。

   Unauthorized personnel are not allowed to access the computer system to protect the data files stored in our computer system and prevent damage.

   相關詳細規定請參照 ISO9001 編號 ISA6403「電腦系統安全管理辦法」之「使用者控制安全管理作業說明」。

   For detailed regulations, please refer to the "Explanations for User Control Security Management Procedures" of ISO9001 No. ISA6403 "Computer System Security Management Regulations".

2. 資料、檔案程式安全管理

2. Data and file program security management

為避免資料及檔案程式因意外狀況發生而毀損，電腦程式作業人員應遵守安全規定。

Computer programmers should observe safety regulations to prevent data and file programs from being damaged by accidental occurrences.

相關詳細規定請參照 ISO9001 編號 ISA6403「電腦系統安全管理辦法」之「資料、檔案程式安全管理作業說明」。

For detailed regulations, please refer to the "Explanations for Data and File Program Security Management Procedures" of ISO9001 No. ISA6403 "Computer System Security Management Regulations".

3. 機房控制安全管理

3. Computer room control security management

為防止不相干人員進入機房及維護機房環境確保電腦系統運作正常，資訊處人員應依安全規定辦理。

The staff of the Information Management Division should follow the security regulations to prevent unauthorized personnel from entering the server room and maintain the environment of the server room to ensure the normal operation of the computer system.

相關詳細規定請參照 ISO9001 編號 ISA6403「電腦系統安全管理辦法」之「機房控制安全管理作業說明」。

For detailed regulations, please refer to the "Explanations for Computer Room Control Security Management Procedures" of ISO 9001 No. ISA6403 "Computer System Security Management Regulations".

七、網路安全管理措施

VII. Network security management measures

1. 與外界網路連接之網點，資訊處以防火牆及其他必要安全設施，控管外界與公司內部網路之資料傳輸及資源存取。

1. For the network points connected to the external network, the Information Management Division uses firewalls and other necessary security facilities to control the transmission of data and access to resources between the external

and internal networks of the company.

2. 開放外界連線作業之資訊系統，必要時應以代理伺服器等方式提供外界存取資料，避免外界直接進入資訊系統或資料庫存取資料；且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。

2. Information systems that are open to external connection operations shall be provided with proxy servers and other means of external access to information when necessary, and direct access to information systems or databases should be avoided. Depending on the importance and value of the information and system, different security technologies or measures such as data encryption, identity authentication, electronic signature, firewall, and security vulnerability detection shall be used to prevent intrusion, destruction, tampering, deletion, and unauthorized access to the information and system.

3. 資訊處針對公司網站加強對客戶資料及機敏檔案保護，以防止資料外洩。

3. The Information Management Division has strengthened the protection of customer information and sensitive files on the Company's website to prevent data leakage.

4. 若因業務需求欲從公司外部連線至公司內網作業，須填寫「電腦連線帳號申請單」申請 VPN 連線帳號，經資訊處處長核准後，由資訊處建立其帳號並安裝軟體後，方可透過加密通訊管道進入公司內網特定電腦進行相關系統作業。

4. If you want to connect to the Company's intranet for business needs, you must fill out the "Computer Connection Account Application Form" to apply for a VPN connection account. After approval by the Director of Information Technology Division, the Information Management Division will create the account and install the software before you can access specific computers on the company's intranet through encrypted communication channels for related system operations.

5. 為避免網路使用者未經申請或公司同意，擅自使用公司網路資源，資訊處網路管理人員先報備資訊處處長經其核准後，以不干擾正常網路使用之原則下，採取主動管制措施。

5. To prevent network users from using the company's network resources without application or the company's consent, the network administrator of the Information Management Division will first report to the Director of Information Management Division for approval, and then take the proactive control measures under the principle of not interfering with normal network usage.

八、電子郵件使用資訊安全管理措施

VIII. Information security management measures for e-mail usage

1. 留職停薪人員郵件帳號不移除。

1. The email account of the staff on leave without pay will not be removed.

2. 電子郵件主機系統對外(網際網路)提供 SMTP、POP3 信件收發服務協定，且 POP3 服務設置加密認證防護，可安全收取公司電子郵件信箱資源。

2. The e-mail host system provides SMTP and POP3 mail sending and receiving service protocols to the outside (Internet), and the POP3 service is set up with encryption authentication protection, so you can safely receive company e-mail resources.

3. 內部人員只能由公司電子郵件主機發送信件，除業務需要專案申請並經部門副總經理同意外，限制於外網使用 SMTP 發信，僅提供 POP3 收信協定。

3. Internal staff can only send letters from the Company's e-mail server, except for business needs and project application and approval by the department vice president, the use of SMTP to send letters on the external network is restricted, and only POP3 receiving protocol is provided.

4. 公司電子郵件主機啟動拒絕轉發(Relay Deny)機制，避免電子信箱伺服器被當成轉發伺服器，造成公司信譽受損情事發生。

4. The Company's e-mail host activates the Relay Deny mechanism to prevent

the e-mail server from being used as a forwarding server and causing damage to the company's reputation.

5. 所有進出電子郵件主機信件，皆經公司防毒軟體掃描，避免病毒蔓延情事發生，若遇信件攜帶病毒，除加以隔離或刪除外，系統應主動通知發送者、接收者及管理者，以隨時掌握病毒發作狀態。

5. All incoming and outgoing emails are scanned by the Company's anti-virus software to prevent the spread of viruses. If a virus is carried in a letter, the system should take the initiative to notify the sender, receiver and administrator, in addition to isolating or deleting it, in order to keep track of the virus status.

6. 為避免病毒時常寄居之副檔名，利用電子郵件散播造成電腦中毒，凡寄發下列之副檔名檔案，公司防毒伺服器一律會將下列附加檔加以隔絕及刪除：*.bat,*.chm,*.com,*.eml,*.exe,*.hta,*.js,*.jse,*.lnk,*.nws,*.pif, *.scr,*.shs,*.vbe,*.vbs,*.wsf。

6. To prevent viruses from spreading by e-mail and causing computer poisoning, the company's anti-virus server will block and delete the following additional files if the following files are sent:
.bat,.chm,*.com,*.eml,*.exe,*.hta,*.js,*.jse,*.lnk,*.nws,*.pif, *.scr,*.shs,*.vbe,*.vbs,*.wsf.

7. 使用者之電子郵件信箱容量，以 1000MB 為限，除特殊需求經專案申請並經部門副總經理同意，始可增加其大小；另外，為避免影響線上作業，每封電子郵件含本文、附加檔，外寄或內送信件不得超過 20MB(含)。

7. The capacity of the user's e-mail box is limited to 1000MB, except for special needs, which may be increased upon project application and approval of the departmental vice president. In addition, to avoid affecting online operations, each email containing this document and additional files, outgoing or incoming mail should not exceed 20MB (inclusive).

九、系統存取控制管理措施

IX. System access control management measures

1. 公司僅賦予各級人員執行系統時所必要之權限。

1. The Company grants only the necessary authority to each level of personnel to executing the system.
   人員職務調整或調動時，其權限配合調整。
   When the duties of the personnel are adjusted or transferred, their authority will be adjusted accordingly.

2. 新系統使用者應填寫「電腦連線帳號申請單」申請帳號，經資訊處處長核准後，由資訊處建立其帳號。

2. New system users shall fill out the "Computer Connection Account Application Form". After approved by the Director of Information Management Division, the Information Management Division will create the account.
   資訊處對新系統使用者會先給予預設密碼，使用者在初次進入系統後應立即更改密碼。
   Information Management Division will first give default passwords to new system users. However, users shall change their passwords immediately after first entering the system.

3. 針對公司離職人員，應立即取消其系統權限，並列入人員離職程序要求；系統作業使用者於職務異動時，作業單位主管應督導作業人員立即修改共用帳號之密碼；每位系統使用者密碼皆設定使用期限，強制使用者定期更新密碼，以維護資訊安全。

3. For the company's departed personnel, the system privileges should be immediately revoked and included in the personnel departure procedure requirements. When the system users change their duties, the supervisor of the operating unit should supervise the operators to immediately modify the password of the shared account. Each system user's password is set for an expiration date, and it is mandatory for users to update their passwords regularly to maintain information security.
   資訊處每半年依「資通安全自我檢查表」檢核時確實記錄檢核。
   The Information Management Division will verify the records every six months in accordance with the "Information Security Self-Check Sheet".

4. 對系統服務廠商以遠端登入方式進行系統維修者，為加強安全控管，應

先申請連線並經核准後才可連線至相關設備，並責其遵守相關安全保密責任。

4. For system service providers who perform system maintenance by remote login, in order to strengthen security control, they should apply for connection and be approved before connecting to the relevant equipment, and they should be obliged to comply with the relevant security and confidentiality responsibilities.

5. 公司之重要資料委外建檔者，不論在公司內外執行，均應採取適當及足夠之安全管制措施，防止資料被竊取、竄改、販售、洩漏及不當備份等情形發生。

5. The Company shall take appropriate and adequate security control measures to prevent theft, manipulation, sale, leakage and improper backup of important information, regardless of whether it is performed inside or outside the Company.

十、系統發展及維護安全管理措施

X. System development and maintenance security management measures

1. 公司發展系統，應在系統生命週期初始階段，將資訊安全需求納入考量；辦理資訊委外作業，亦應明訂廠商之資安責任及保密規定。

1. When developing systems, the Company should take information security requirements into consideration at the initial stage of the system life cycle; when outsourcing information operations, they should also specify the information security responsibilities and confidentiality regulations of vendors.

2. 系統之維護、更新、上線執行及版本異動作業，應作備份之安全措施。

2. The system maintenance, update, online execution and version change operations should be made as a backup security measure.

3. 對廠商之軟硬體系統建置及維護人員，應限制其可接觸之系統與資料範圍，並嚴禁核發長期性之系統辨識碼及通行密碼。

3. The software and hardware system installation and maintenance personnel of

the vendor shall be restricted from accessing the system and data, and the issuance of long-term system identification codes and passwords is strictly prohibited.

基於實際作業需要，得核發短期性及臨時性之系統辨識及通行密碼供廠商使用。

Based on the actual operation needs, short-term and temporary system identification and access codes may be issued for the use of the vendor.

但使用完畢後應立即取消其使用權限。

However, the permission should be canceled immediately after the vendor users have finished using it.

4. 公司委託廠商建置及維護重要軟硬體設施時，應在公司相關人員監督及陪同下始得為之。

4. When entrusting the vendor to build and maintain important software and hardware facilities, the Company shall do so only under the supervision and accompaniment of the company's relevant personnel.

十一、資訊資產安全管理措施

XI. Information asset security management measures

1. 建立與資訊系統有關的資訊資產目錄，訂定資訊資產的項目及保管者。

1. Establish an inventory of information assets related to the information system and define the items and custodians of information assets.

2. 軟體由資訊處依各單位需求購買，由資訊處統一安裝軟體並將版權證明書交由會計處保管，並定期查核，確保公司每部電腦中只安裝合法軟體。

2. The software is purchased by the Information Management Division according to the needs of each unit. The Information Management Division installs the software centrally and assigns the copyright certificate to the Accounting Department for safekeeping and regular checking to ensure that only legal software is installed on each computer in the company.

3. 若非本公司資訊部門人員或指定維修人員，不得自行拆卸各項資訊硬體設備及更換內部零組件。

3. If not a member of our Information Management Division or designated

maintenance personnel, such personnel are not allowed to disassemble each information hardware equipment and replace the internal parts themselves.

十二、電腦病毒及惡意軟體之控制措施

XII. Control measures for computer viruses and malware measures

1. 應採行必要的事前預防及保護措施，防制及偵測電腦病毒、特洛依木馬及邏輯炸彈等惡意軟體的侵入。

1. Necessary preventive and protective measures should be taken to prevent and detect the intrusion of malware such as computer viruses, Trojan horses and logic bombs.

2. 應依「事前預防重於事後補救」的原則，採行適當及必要的電腦病毒偵測及防範措施，促使同仁正確認知電腦病毒的威脅，進一步提升同仁的資訊安全警覺，健全系統之存取控制機制。

2. In accordance with the principle of "prevention beforehand is more important than remediation afterwards", appropriate and necessary measures should be taken to detect and prevent computer viruses, to promote proper awareness of the threat of computer viruses among employees, to further enhance their awareness of information security, and to improve the access control mechanism of the system.

3. 電腦病毒防範的重要原則如下：

3. The important principles of computer virus prevention are as follows:

(1) 使用者應遵守軟體授權規定，禁止使用未取得授權的軟體。
Users shall comply with the software licensing regulations and are prohibited from using unlicensed software.

(2) 選用信譽良好、功能健全的電腦病毒防制軟體，並依下列原則使用：
Select reputable and functional computer virus prevention software and use it according to the following principles:

a. 電腦病毒防治軟體應定期更新，並在廠商的指導下使用。
Computer virus control software shall be updated regularly and used under the guidance of the vendor.

b. 使用防毒軟體事前掃瞄電腦系統及資料儲存媒體，以偵測有無感

染電腦病毒。
Use anti-virus software to scan your computer system and data storage media in advance to detect any computer virus infection.

c. 視需要安裝可偵測軟體遭更改的工具軟體，並偵測執行碼是否遭變更。
Install a tool that detects software changes if necessary and detects if the executable code has been changed.

d. 應謹慎使用可掃除電腦病毒及回復系統功能的解毒軟體；使用前應充分瞭解電腦病毒的特性，以及確定解毒軟體的功能。
Users should be cautious in using antivirus software that can scan your computer for viruses and restore system functions; users should fully understand the characteristics of computer viruses and determine the functions of the antivirus software before using it.

e. 應定期檢查軟體及檢查重要的系統資料內容，如發現有偽造的檔案或是未經授權的修正事項，應立即調查，找出原因。
The software should be checked regularly and important system data content should be inspected. If forged files or unauthorized corrections are found, they should be investigated immediately to find the cause.

f. 對來路不明及內容不確定的儲存媒體，應在使用前詳加檢查是否感染電腦病毒。
Storage media from unknown sources and with uncertain contents should be carefully checked for computer viruses before use.

g. 應建立防制電腦病毒攻擊及回復作業的管理程序，並給予相關人員必要的責任。
Management procedures for prevention of computer virus attacks and recovery operations should be established, and the necessary responsibilities should be given to relevant personnel.

h. 為使電腦病毒影響機關正常運作之程度降至最低，應建立妥適的業務永續運作計畫，將必要的資料及軟體備份，事前訂定回復作業計畫。
To minimize the extent to which computer viruses affect the normal operation of the organization, a proper business sustainability plan should be established, necessary data and software should be backed up, and a recovery operation plan should be set in advance.

十三、業務永續運作計畫之規劃與管理

XIII. Planning and management of business sustainability plans

1. 為因應各種人為及天然災害對營運之影響，資訊部門須針對系統及資料安排自動備份且安裝救援回復軟體，訂定緊急應變及回復作業程序，並定期演練與檢查最近備份磁帶是否完整。

1. To the impact of various man-made and natural disasters on operations, the Information Management Division must arrange automatic backups of systems and data, install rescue recovery software, establish emergency response and recovery procedures, and regularly rehearse and check the integrity of recent backup tapes.

2. 資訊處應建立資訊安全事件緊急通報及處理機制，在發生資訊安全事件時，依規定之程序，立即逐級通報，採取反應措施，控管資安風險。

2. The Information Management Division shall establish an emergency reporting and handling mechanism for information security incidents, and in the event of an information security incident, immediately report the incident at all levels in accordance with the prescribed procedures, and take countermeasures to control information security risks.
若情節重大時應聯繫檢警調單位協助偵查。
If the situation is significant, the Company shall contact the police investigation unit to assist with the investigation.
(資訊安全事件通報程序如附件一)
(Information security incident reporting procedures are shown in Annex 1)

3. 依照公司內部控制之資訊循環作業的控制重點，稽核室定期進行資訊安全稽核作業。

3. The audit office conducts information security audits operation regularly in accordance with the control keypoints of the information circulation operations in the Company's internal control system.

4. 發生符合「財團法人中華民國證券櫃檯買賣中心對有價證券上櫃公司重大訊息之查證暨公開處理程序」規範之重大資安事件，應依相關規定辦理。

4. In the event of a material information security incident that complies with the "Taipei Exchange Procedures for Verification and Disclosure of Material

Information of Companies with TPEx Listed Securities", the Company shall follow the relevant regulations.

十四、本要點奉董事長核可後實施，修正時亦同。

XIV. These Guidelines will be implemented after approved by the chairman of the board of directors. The same applies when the guidelines are amended.

附件一：資訊安全事件通報程序

Annex 1: Information Security and Incident Notification Procedures