興富發建設
Highwealth Construction

興富發建設股份有限公司

資訊安全風險管理

經本公司權責單位評估，資訊安全風險雖非屬於本公司重大營運風險項目，但考量網路環境漸趨複雜，相關風險可能逐年增高，本公司於111年08月11日董事會通過資通安全專責人員，並訂定了「資通安全防護與管理辦法」，隸屬管理部並為資訊安全管理之執行單位，進行資訊安全預防及危機處理等具體管理方案，並實施對應的安控措施，持續精進內部異常偵測與防護方法，以降低企業資安風險。本公司每年至少一次向董事會報告。

一、資訊安全具體管理方案：

本公司考量資安險仍屬新興險種，目前尚無適合本公司之資安險，故現階段以本公司既有的資訊安全管理程序來落實資訊安全風險管理。相關具體執行措施如下：

1.網路安全管理：

(1)配置企業級防火牆，阻擋駭客非法入侵。

(2)與北中南分公司使用HiLink VPN企業專屬線路作業，使用資料加密方式，避免資料傳輸過程遭到非法擷取。

(3)配置上網行為管理系統，控管網路存取，可屏蔽訪問有害或政策不允許的網址及內容，強化網路安全且防止頻寬被不當佔用。

2.系統存取控制：

(1)公司內各應用系統的使用，需透過資訊服務需求申請程序，經權責主管核准後，由資訊室建立帳號，且經過各系統管理員依所申請之功能開放權限，方得使用。

(2)帳號的密碼設置，需符合規定之強度，且需文數字參雜，才能通過。

(3)同仁辦理離職手續時，需會辦管理部資訊人員，進行各系統帳號刪除作業。

3.落實資安訓練：

(1)新進人員教育訓練中加入資安課程。

(2)在職同仁教育訓練，每季針對違反資安規定之同仁再特別開課訓練。

(3)定期對全體同仁辦理資訊安全教育宣導課程，強化資訊安全知識。

(4)不定期對全體同仁發起「電子郵件社交工程演練」，全面提高人員資安風險防護意識。

4.病毒防護與管理：

(1)伺服器與同仁電腦設備皆安裝端點防護軟體，病毒碼採自動更新，確保能阻擋最新型病毒。

(2)電子郵件伺服器配置有垃圾信過濾機制，防堵病毒或垃圾郵件進入使用者端PC。

5.確保系統可用性：

(1)建置備份管理系統，定期將每日備份的資料，一份保留在機房，另一份放於異地（台中分公司機房），互相備援。

(2)定期實施災難復原演練，選定還原基準點後，由備份檔回存於系統主機。

6.電腦設備安全管理：

(1)本公司電腦主機、各應用伺服器.....等皆設置於專用機房，機房隨時上鎖嚴格控管人員進出，且保留記錄存查。

(2)資訊機房內有獨立空調及不斷電系統，以維持電腦設備於適合的溫度下運轉，斷電時不會中斷電腦應用系統的運作。

(3)建置設備管理系統，需經過公司認證之移動裝置及USB裝置才可連線至公司內網及存取資料。

二、資訊系統損害對公司業務之影響與因應措施：

目前公司資訊系統架構中，在硬體部份是建置高穩定性伺服器，而軟體部份則是定期將資訊系統、軟體與系統設定參數做映像檔案備援及完整資料備份機制以確保縮短服務中斷時間。

在資訊服務不中斷及資料安全上，管理部資訊單位定期將備份資料送往異地保管存放，並定期演練災後復原措施，以預防及降低無預警天災以及人為疏失帶來的

資訊服務中斷和縮短系統復原的時間。

為了資訊系統在發生損害時能順利恢復業務運作減少損失，除了定期演練災後復原措施之外，應隨著新興科技技術不斷發展來規劃設計與提升軟硬體設備資源，建構安全等級更高的防護機制以降低系統損害風險。

近來資安威脅分析，其威脅來源來自外部駭客攻擊佔大宗，其次是內部員工的疏忽及欠缺資安意識，而這些造成資安事件的根源，就是使用者執行不明惡意程式所造成，因此資安防護需要公司的全面共識和全員參與，惟有從工作習慣與公司文化，逐步養成員工的風險意識與資安防護能力，才能真正強化資安防禦能力。

三、113年度本公司並未發現任何重大的網絡攻擊或事件，已經或可能將對公司業務及營運產生重大不利影響，也未曾涉入任何與此有關的法律案件或監管調查。

資訊安全政策

一、資訊安全管理之目的：

1、確保公司主機、網路設備及網路通訊安全，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，並建立資通安全管理規範。

2、確保公司業務資訊之機密性、完整性與可用性。
機密性：確保被授權之人員才可使用資訊。
完整性：確保使用之資訊正確無誤、未遭竄改。
可用性：確保被授權之人員能取得所需資訊。

二、資訊安全政策內容：

1、本公司參考ISO 27001及CNS27001資訊安全管理系統標準要求，訂頒資通安全防護與管理辦法，藉由制定符合且適當的資訊安全制度及控制措施，持續推動內部資訊安全工作。

2、本公司建置異地備援系統並維持各資訊系統永續運作。

3、防止駭客、各種病毒入侵及破壞。

4、防止機敏資料外洩。

5、維護實體環境安全。

6、加強內部及外部網路攻擊防護。

7、加強教育訓練及防駭意識宣導。

三、資訊安全風險管理架構及人員配置：

1、本公司依據「公開發行公司建立內部控制制度處理準則」相關規定，設置資安長及設置資安專責單位，以統籌進行資訊安全制度之規劃、監控及執行資訊安全管理作業。

2、本公司現由管理部所轄資安專責單位負責規劃、執行及推動資訊安全管理事項，並推展資訊安全意識，目前配置資安人員有：資安長1名、資安主管1名、資訊安全人員2名，共計4名。

3、本公司稽核處為資訊安全監理之查核單位，如有查核發現缺失，立即要求受查單位提出相關改善計畫並呈報董事會，且定期追蹤改善成效，以降低內部資安風險。

四、資訊安全政具體管理方案：

1、本公司電腦主機、各應用伺服器等設備均設置於專用機房。

2、機房內部備有獨立空調，維持電腦設備於適當的溫度環境下運轉。

3、機房主機配置不斷電與穩壓設備，確保臨時停電不會中斷電腦應用系統運作。

4、提醒宣導：要求同仁定期更換系統密碼，以維帳號安全。

5、資安宣導：提供資訊安全實例文件給同仁參考。

五、資訊安全管理措施說明如下：

1、制度規範：本公司內部訂定多項資安規範與制度，以規範本公司人員資訊安全行為，每年定期檢視相關制度是否符合營運環境變遷，並依需求適時調整。

2、系統防護：本公司為防範各種內/外部資安威脅，除採多層式網路架構設計外，更建置各式資安防護系統，以提昇整體資訊環境之安全性。此外，為確保內部同仁之作業行為符合公司制度規範，亦設計作業程序稽核機制和導入資安管理工具，落實人員資訊安全管理措施。

3、人員訓練：本公司定期實施新進人員資訊安全教育訓練實務課程，並不定期實施資訊安全機會宣導，藉以提昇公司同仁資安知識與專業技能。

六、投入資通安全管理之資源：

1、加入「台灣電腦網路危機處理暨協調中心」，提升整體資安防護能量。

2、透過內部完善資訊安全措施協助管理，以降低資訊安全所面臨的各種風險與威脅。

3、定期進行全公司電子郵件社交工程釣魚郵件演練，並對全集團進行資訊安全宣導，藉以加深同仁資訊保護與資訊安全風險意識。

4、定期辦理內部網路弱點分析及對主機與個人電腦進行全面性資安檢測。

5、定期更新資訊安全防護設備，以確保各項業務能有效運作。

七、資訊安全會議及教育訓練受訓情形：

時間及地點	內　　容
每月例會	針對每月的資安情資等相關議題，與廠商進行討論及溝通。
【教育訓練】 時間： 113年10月17日 地點： 公司108會議室	課程名稱：資安意識宣導
資訊安全測試	對全集團實施內部的社交工程演練,強化同仁資安應變能力(內部email滲透測試，每年實施1次)
參加「2024台灣資安通報應變年會」	113/11/22資安長代表參加國家資通安全研究院「2024台灣資安通報應變年會」

113年度興富發建設資訊安全軟硬體設備投資暨教育訓練費用	
項次	投資項目
1	系統備份還原軟體年度維護
2	CP EDR for Server
3	防火牆年度維護
4	防毒軟體
預算	新台幣150萬

113年度興富發建設資訊安全團隊暨同仁專業培訓課程		
項次	課程名稱	實施日期
1	Check Point Gateway教育訓練	4/16
2	無法預測的危機：生成式AI如何顛覆資安防線	8/27
3	零信任架構下導入AI應用與資安防護策略研討會	9/18
4	從智能革命到數位戰場—AI時代的零信任資安新格局	9/25
5	上市(櫃)公司資安長資通教育訓練課程-國家資通安全研究院	9/27
6	全體同仁資安教育宣導課程-外聘專業資訊安全講師	1017
7	台灣資安通報應變年會-國家資通安全研究院	11/22
8	資安人力與預算，專家怎麼做？	11/26
9	資安事件說明及預防措施暨上市上櫃公司資通安全管控指引說明-金融研訓院	12/11
10	每月定期對全企業發布資訊安全宣導與資安教材	每月

113年度興富發建設資訊安全專業證照暨資安防護演練實施說明		
項次	專業項目	執行期間
1	資安長具備ISO 27001：2013 資訊安全管理系統主導稽核師及ISO 27001：2022 資訊安全管理系統主導稽核師證照	113年度
2	資安主管參加ISO 27001：2022資訊安全管理系統主導稽核師證照訓練	113年度
3	公司參加台灣電腦網路危機處理暨協調中心TWCERT/CC聯盟(資安聯防組織)	113年度
4	公司參加中華民國資訊軟體協會-資安長聯誼會(資安聯防組織)	113年度
5	113年實施全企業資安模擬社交工程滲透演練，受測人次共912人	6/11~7/19日

113年度興富發建設資訊安全防護作業	
項次	執行項目
1	建置資訊安全設備監控系統
2	設置24小時資訊安全監控及緊急應變小組
3	建置完整備份系統及安全防護措施
4	每日下班執行個人電腦關機及連線管制措施
5	強制定期更換個人電腦帳密及防毒軟體更新作業