KEDING

文件名稱	資訊安全規章	等 級	管制	版 次	07
文件編號	M-D-1-001	發 行 日 期			2016/01/01

文 件 變 更 履 歷 頁

版別	生效日期	制(修)訂人	修改說明	
			原內容	修改後內容
01	2011/12/12	顏弘偉	首次發行	
02	2013/01/22	顏弘偉	二版	
03	2013/10/31	林宥任	三版	
04	2015/01/01	林宥任	四版	
05	2015/07/06	林宥任	五版	
06	2015/12/31	林宥任	六版	
07	2016/01/01	林宥任	七版	

文件名稱	資訊安全規章	等 級	管制	版 次	07
文件編號	M-D-1-001	發 行 日 期		2016/01/01	

第一條　目的

資訊時代的來臨，我司為了因應其衝擊，確保所屬資訊資產的機密性、完整性及可用性所面臨的安全問題，特制訂本資訊安全規章(以下通稱本規章)。其旨在保護公司實體軟硬體設施與資訊資產的安全以利管理，並促使免於外在威脅以及內部人員不當管理與使用等風險。以下所編撰之規章條例期許能在安全議題上給予明確的防禦方向。

第二條　目標

本規章目標如下（依據不同政策制定衡量指標，並每年稽核與調整）確保所屬之資訊資產的機密性、完整性及可用性，以提供本司之資訊業務持續運作之資訊環境，並符合相關法規、法令之要求，以避免如因人為疏失、蓄意或天然災害等因素，遭致不當使用、破壞、遺失或洩漏等情事，而對本司可能帶來相關風險及危害。

一、建立資訊管理制度，訂定重要資訊資產及關鍵性業務之防災對策及災變復原計畫，確保本司資訊服務可永續運作。

二、加強內部控制，防止未經授權之不當存取，以確保資訊資產受適當的保護。

三、適當保護資訊資產之機密性與完整性。

四、防止洩漏機密，建立資訊安全，人人有責之觀念，進行資訊安全必要訓練，提高資訊安全意識。

五、推動資安教育訓練及發佈之資訊安全程序、辦法，使得核心之業務人員、相關單位配合人員及網路應用之使用者，皆能充份遵循本規章及措施。

六、確保所有資訊安全意外事故或可疑之安全弱點，依循通報機制向上反應，提升資安狀況處理與應變能力。

第三條　適用範圍

本政策適用於本司全部範圍及所有業務，包括全體員工、離職員工、往來廠商、約聘人員與廠商委派支援本司之工作人員等所有相關文件與紀錄、電腦系統、人員、服務、實體設備、軟硬體之管理。

第四條　定義

一、 網路安全

1. 網路系統安全評估。
2. 防火牆之安全管理。

3. 人員使用網路規定。

二、 系統安全

1. 病毒及惡意程式之防範。
2. 電腦系統軟體之防範。

三、 硬體與機房伺服器控管

1. 硬體設備管理。
2. 機房伺服器控管。

四、 內部機密資料與個資保護

1. 內部機密資料規範。
2. 個人資料保護。

五、 永續運行之規劃

1. 資安事件緊急處理機制。
2. 內部稽核計畫。

第五條 作業內容

一、網路安全

1. 網路系統安全評估:

1-1. 定期評估自身網路系統安全(例如:作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等),並留存相關紀錄。

1-2. 定期或適時修補網路運作環境之安全漏洞(含伺服器、攜帶型、個人端及分公司所內供投資人共用之電腦等)。

1-3. 有關電腦網路安全(如資訊安全規章宣導、防範網路駭客入侵事件、電腦防毒等)之事項應隨時公告。

1-4. 各電腦主機、重要軟硬體設備應有專人負責。

2. 防火牆之安全管理

2-1. 防火牆應有專人管理,進出其備份應須妥善保留。

2-2. 重要內部網站及伺服器系統,應以防火牆與外部網際網路隔離。

2-3. 針對職務內容上的不同,不需要使用網際網路的電腦,使用防火牆來限制其存取,減少風險發生。

2-4. 防火牆系統之設定變更須填寫防火牆設定變更申請單,並且應經權責主管之核准。

3. 人員使用網路規定

3-1. 為了防止流量不當使用以及病毒防制，除任務需求可允許連線外部網站，其餘時間皆限制瀏覽。

3-2. 依據不同身分，每部電腦對外部網路流量皆有做限制，並禁止大量下載或觀看串流影片之行為。

3-3. 除任務需求外，公司內一律禁制使用 Yahoo!即時通、Google、hangouts、Line、WeChat、QQ 等通訊軟體。

3-4. 內部網路皆有限制瀏覽社群網站、拍賣網站，除任務需求外，其餘人員上班時間皆不能瀏覽，目前限制網站請閱相關文件一。

3-5. 公司內嚴禁使用 BT、迅雷、PPS..等等的 P2P 通訊協定軟體。

3-6. 公司保留監控員工在公司的通訊與上網內容的權利。

3-7. 公司無線網路僅供大小會議室使用，嚴禁私下使用手機或者筆電連線至公司無線網路，有職務需求者除外。

二、系統安全

1. 病毒及惡意程式之防範：

1-1. 電腦應安裝防毒軟體，並即時更新程式及病毒碼。

1-2. 應定期對電腦系統及資料儲存媒體進行病毒掃瞄(含電子郵件)。

1-3. 勿開啟來歷不明之電子郵件，對於電子郵件中帶有執行檔之附件，尤應特別小心開啟。

1-4. 定期（至少每個月）進行如「Windows Update」之程式更新作業，防範作業系統之漏洞。

1-5. 新系統啟用前，應經過掃毒與更新系統密碼程序，以防範可能隱藏的病毒或後門程式。

2. 電腦系統軟體之防範

2-1. 公司內個人電腦所使用的軟體應有授權，嚴禁安裝各種非法軟體，且禁止私自安裝。

2-2. 公司人員須定期接受資訊安全相關課程宣導，增進資訊安全相關知識並減少發生資安事件的可能性。

2-3. 限制使用個人 USB 或手機等有快取裝置的儲存媒介，如因作業需求可向公司借用公司專用 USB。

2-4. 個人使用電腦，設定帳號密碼時請遵循以下原則:

2-4-1. 混合大寫與小寫字母、數字，特殊符號。

2-4-2. 密碼越長越好，最短也應該在 8 個字以上。

2-4-3. 至少每二個月改一次密碼。

2-4-4. 密碼務必妥善保存，勿直接將密碼放置於桌面上。

以上違者，懲處請參考相關文件二。

三、硬體與機房伺服器控管

1. 硬體設備管理

1-1. 公司內同仁所分配電腦隨人事調動而移動時，須負妥善保管與維護責任。

1-2. 進出機房皆要進行登記，無相關業務需求，禁止進入機房。

1-3. 針對機房溫濕度與電源供應品質，應做良好的控管機制。

1-4. 禁止資訊設備在未經授權之情況下攜離所屬區域，若需將設備攜出應留下相關紀錄。

1-5. 公司內入冊之電子設備、電子周邊設備與機器皆保有安全環境之需求，公司保留追訴權利。

2. 機房伺服器控管

2-1. 針對伺服器內資料皆應實施備份，若資源允許至少保存一個月的資料(含電子郵件)。

2-2. 公司內各電腦系統一律存放公司作業需求資料，限制儲存私人資料。

2-3. 公司內系統帳號密碼，不能隨意透露於第三方。

2-4. 各伺服器備援機制須依照標準流程，並進行紀錄追蹤，以評估改善。

2-5. 針對不同的系統的使用部門和階級皆要設定不同的存取控制權限，如需變更權限，需填寫應用系統使用者權限申請單。

四、內部機密資料與個資保護

1. 內部機密資料規範：

1-1. 公司內部資料，無論是紙本文件或是電子檔案一律標明撰寫人與民國日期以示負責與維護任務。

1-2. 公司有權利監控業務上的電子郵件往來，並限制開啟非關業務、標題聳動的電子郵件，如發現疑似有問題信件請回報資訊部門處理。

1-3. 公司保留審查公司個人電腦內資料的權利，並嚴禁再非公司電腦處理公司相關事務。

1-4. 公司內機密帳號密碼資料，勿使用便利貼隨意貼至公開的地方。

1-5. 公司內同仁帳號(個人電腦系統以及伺服器帳號)有效日期至離職日當天為止。

2. 個人資料保護：

2-1. 向客戶蒐集個人資料時，應明確告知使用範圍與目的，且應依客戶之請求，就蒐集的之個人資料進行答覆查詢。

2-2. 個人資料蒐集之特定目的消失時或者期限屆滿時，應主動或依客戶請求、刪除、停止利用該個人資料。

2-3. 個人資料之使用，只可在執行法定職務及蒐集之特定目的必要範圍內進行，嚴禁洩漏客戶的個人資料給予第三方人員使用。

五、永續營運之規劃

1. 資安事件緊急處理機制：

1-1. 應建立資訊安全事件的正式通報程序及管道，並訂定通報之後應採行之行動及措施。

1-2. 如發現或懷疑有資訊安全事件時（包括系統有安全漏洞、受威脅、系統弱點及功能不正常事件等），應依事前訂定的通報管道，迅速通報權責主管單位及人員立即處理。

1-3. 建立 Log File 機制，紀錄檔應定期備份轉出檔案後保存，作為日後調查及監督之用。

1-4. 評估各種災害對公司作業上可能的衝擊，且應準備相關備援復原機制及緊急應變程序。

2. 資訊安全稽核計畫：

2-1. 定期進行資訊安全的稽核，協助組織對本身做更深、更全面的檢視，以防範未來事故的發生。

2-2. 檢視公司內員工對於資訊安全的防範與認知程度，進一步進行面談或相關的資訊安全測驗。

2-3. 資安稽核依組織制度進行長、短期規劃且稽核計畫應經過正式授權與核准程序。

2-4. 針對內部系統進行稽核後，相關缺失部分需要擬定改善計，並追踪改善情形。

第六條　相關文件

一、限制網頁表

（台灣）

網頁名稱	網址
Facebook	http://www.facebook.com
twitter	http://twitter.com
噗浪	http://www.plurk.com
Momo 購物	http://www.momoshop.com.tw/main/Main.jsp
博客來	http://www.books.com.tw/
森森購物	http://www.u-mall.com.tw/Homepage.aspx
東森購物	http://www.etmall.com.tw/Pages/Home.aspx
autobuy	http://www.autobuy.tw/
Udn 買東西	http://shopping.udn.com/mall/Cc1a00.do
Pchome 商店街	http://www.pcstore.com.tw/
樂天市場	http://www.rakuten.com.tw/
Mall123	http://www.mall123.com.tw/
Pchome24	http://shopping.pchome.com.tw/index/
Google mail	http://mail.google.com/
Yahoo mail	https://login.yahoo.com/config/mail?.intl=tw
Hotmail mail	https://login.live.com/
奇摩拍賣	http://tw.bid.yahoo.com/
露天拍賣	http://www.ruten.com.tw/
淘寶網	http://tw.taobao.com/
LINE	https://line.naver.jp
Google disk	https://drive.google.com
Google tools	https://tools.google.com
線上看 TV	http://kr.wavestone.com/
線上看 TV	http://www.fun-tv.net/
線上看 TV	http://www.lovetvshow.com/
線上看 TV	http://www.maplestage.com/
線上看 TV	http://livetv.sx
線上看 TV	http://vigortv.net/

針對以上封鎖有辦公室內部所有電腦，理級以上以及行銷課不在封鎖範圍內，及另外提出申請單者開通相關網頁部分則排除上面其中規則。

（中國）

網頁名稱	網址
愛奇藝	http://www.iqiyi.com
土豆	http://www.tudou.com
搜狐	http://tv.sohu.com
迅雷看看	http://www.kankan.com
鳳凰視頻	http://v.ifeng.com
QQ 影音	http://v.qq.com
新浪影音	http://video.sina.com.cn
56 影視	http://www.56.com
酷 6 網	http://www.ku6.com
暴風影音	http://www.baofeng.com
樂視影音	http://www.letv.com
PPS 影音	http://www.pps.tv
風行	http://www.fun.tv
PPTV	https://www.pptv.com
百度影音	https://v.baidu.com
芒果 TV	http://www.hunantv.com
激動網	http://www.joy.cn
第一視頻	http://www.v1.cn
YY 影音	https://www.yy.com
愛奇藝	http://www.iqiyi.com
土豆	http://www.tudou.com
搜狐	http://tv.sohu.com
天貓	https://www.tmall.com
京東	http://www.jd.com
蘇甯易購	http://www.suning.com
一號店	http://www.yhd.com
唯品會	http://www.vip.com
麥樂購	http://www.gou.com

二、資訊軟硬體使用懲處規定

1. 軟體:
   - 未經申請採購,在本機或公用桌機與筆電上,私自安裝非本司授權軟體綠色軟體、免安裝版軟體者者。
2. 硬體:
   - 分配之個人使用資訊設備，未妥善保管與維護責任，遺失資訊設備者。
   - 未經申請，私自交換螢幕、主機者，造成管控不易者。
   - 未經主管同意，私自帶個人電腦至公司使用者。
   - 下班後，未關閉電腦者，有業務需求除外。
   - 借用資訊設備歸還時，未關閉電源者。
   - 使用個人隨身碟或手機等有快取裝置的儲存媒介至本司電腦者,如有業務需求可申請公司專用隨身碟。
   - 借用資訊設備逾時未還，且未辦理續借作業或通知資訊人員者。
3. 網路:
   - 除業務需求有申請者，公司電腦內一律禁制使用Google hangouts、Line等通訊軟體。
   - 嚴禁使用BT、PPS等P2P軟體。
   - 開啟來歷不明之電子郵件，並執行有執行檔之附件，造成病毒、木馬等傳送於內部造成公司網路癱瘓之電腦者。
   - 開啟來歷不明之網頁，造成本機中毒者。
   - 私自分享手機網路至本司電腦使用者。
   - 公司無線網路僅提供各會議室使用,嚴禁私下使用手機或筆電連線至公司無線網路，有提出申請之業務需求者除外。
   - 業務上與客戶、廠商有信件往來，一律使用公司信箱(xxx@twkd.com)，勿使用個人信箱。
4. 其他：
   - 上列之細則懲處，主管可依情節輕重，給予加重或減輕處分。
   - 上列之懲處所扣年終績效獎金轉入職工福利。

三、即時通訊軟體使用規範

於公司電腦使用 Skype、Line、QQ、Webchat 等即時通訊工具軟體，需遵循以下規定：

一、一般規範

1. 即時通訊若設定同公司 3 人(含)以上之群組，需加入同單位直屬副理級以上主管，於 2015 年 7 月 1 日起開始執行，違者將視情節輕重進行懲處。例如：
   1-1. 甲、乙、丙 3 名業務於 Skype 設定一群組，需加入業務部副理 1 名；
   1-2. 甲、乙業務和丙會計副理於 Skype 設定一群組，需加入業務部副理和管理部經理各 1 名。
2. 使用即時通訊軟體，應以公務使用為限，並遵循使用禮儀，嚴禁聊天過於浮濫。
3. 各單位所屬員工使用即時通訊系統者，主管應負管理與督導責任，若發現違反規定事宜，主管得視情節輕重進行懲處。

二、網路安全

1. 禁止使用即時通訊軟體傳送或散播電腦病毒、惡意程式、惡意連結網址或惡意語言。
2. 禁止點選來路不明之即時通訊軟體連結網址或接受檔案之傳送，以避免惡意程式入侵或病毒感染。
3. 使用者如發現疑似即時通訊軟體中毒事件，應立即關閉個人之即時通訊軟體，並通報資訊課處理。

三、公司保留監看權利，得視情節輕重進行懲處。