金耘國際股份有限公司

資訊安全管理規範

2010/11/01 制訂

一、應系統安全管理要求，茲將資訊系統安全部份區分下列項目：

1. 行政安全
2. 應用系統安全
3. 通訊系統安全
4. 軟件安全
5. 硬件安全
6. 備份機制

二、行政安全

指揮體系：

1. Mutto 集團之 MIS，授權統一由蘇州子公司 MIS 主管負責指揮，集團對外 MIS 窗口為總公司之總經理，其代理人為蘇州子公司 MIS 主管。
2. 緊急應變體系為當地最高主管。
3. MIS 相關系統規劃與規格制定，授權統一由蘇州子公司 MIS 主管制訂，並送集團總經理簽核後實施。

作業流程：

1. MIS 作業程序，均依內部控制-電腦資訊系統處理循環之規定辦理。
2. 內部控制如有不足之處，亦統一由 MIS 主管修訂之。
3. 除當地最高主管命令外，各 MIS 對於其它主管之變更系統安全指示，考量整體規畫與安全，必須請主管填寫 IT 需求申請單，依內部控制核決權限簽核後，再予執行。
4. 凡涉及任何系統變更，均需知會 MIS 主管，並取得其同意後實施。
5. 因整體資源有限，總公司有最後調度資源之權限，以應緊急作業、安全防護及其它應變措施。

人員異動：

1. 重要人員異動，包含主管及重要研發人員等，需通知總公司。
2. MIS 於收到人事異動單後，依其職務內容統一調整權限。
3. MIS 需於員工離職時確實關閉系統帳號，有特殊需求且經核准者，依核定內容辦理。
4. 新進人員權限需經申請核可後，MIS 依核准之內容進行相關調整與設定。

三、應用系統安全：

MAIL 管制：

1. 主機實施黑白名單管理，凡對方主機列於黑名單中者，一律拒絕連線。
2. Mutto 集團進出郵件均需備份。
3. 郵件進出一律透過 Mutto 主機，使用者無法於公司透過其它郵件主機對外收發 Mail。
4. Mutto 郵件主機，採統一集中管理模式，設立於蘇州子公司，各廠不得私設任何郵件主機。
5. 員工離職，MIS 依其部門主管之需求，得將其 MAIL 轉至特定人員帳戶。
6. 員工 Email 轉發，需經當事人及該廠最高主管同意後，MIS 依申請單辦理。
7. 員工舊有 Email 資料調閱，需經當事人及該部門主管同意後，由 MIS 於離峰時間進行之。
8. 設有保留 SPAM，TRASH (垃圾，刪除郵件)之員工，系統統一最大保留期間為 7 日。

Windows 管制：

1. 用戶端使用電腦一律需經帳號密碼驗證後，方可使用。
2. 基於整體安全考量，Mutto 不開放 Windows 匿名式存取服務，任何服務都需有帳號密碼管制。
3. 基於整體安全性考量，所有 Windows 用戶端，一律關閉網際網路分享的功能，避免集團資料經由非授權管道流出。
4. 非經申請核准之用戶，不開放本機安裝軟體之權限，以避免盜版安裝，軟件兼容，病毒散播，等問題。
5. 為考量整體安全及用戶端移動需要，Mutto 集團內部 Windows 系統，採統一集中管理機制，下轄廠區不得私設管理原則，管理原則統一由總公司設定。
6. 針對特定用戶，MIS 依主管授權，得另外開啟額外稽核記錄。
7. 為保障資料安全，Windows 檔案主機需有二次備份，以確保資料安全。
8. 考量集團整體資訊安全，所有電腦均需安裝防毒軟體。

ERP 管制：

1. 權限申請及異動依內控規定辦理。
2. MIS 內部控管及制度，依核定之 Mutto 集團系統管理規範辦理。

四、通訊系統安全：

網路管理：

1. 考量公司整體安全，公司對 INTERNET 防火牆，僅開放一般正常使用之端口，非正常使用之端口，在經核定後且經 MIS 判斷無安全問題後，始可開放。
2. 非經申請並經核准，員工不得私接任何路由器、IP 分享器或網際網路閘道器等設備。
3. 非經申請並經核准，員工不得私自安裝任何無線網路基地台、更改基地台位置或改變天線等。

4. 非經申請並經核准，員工不得私自異動網路集線器(HUB)或網路交換機(SWITCH)等接線，或更換其位置。
5. Mutto 內部網站，僅提供內部使用，於公司外存取需透過 VPN。
6. 有在外撥接式 VPN 需求者，需經總公司同意後，MIS 依核准內容，依順序視公司現有資源開放。
7. 非經申請並經核准，員工及 MIS 不得安裝或設定非 Mutto 集團之 VPN 軟件，防止資料未經授權管道流出。
8. 考量集團整體資訊安全，凡公司內部電腦，於公司內部使用時，一律使用受防火牆保護的內部 IP 位置，公司除對外主機因對外連線需求者，任何用戶端的電腦均不開放。
9. Mutto 集團之 DNS，統一由蘇州子公司管理。
10. 非經申請並核准，員工不得私自安裝 DNS、DHCP、BOOTP 及 WINS 等服務，以避免干擾整體網路之正常運作。
11. Mutto 集團之 WWW，統一由蘇州子公司管理。
12. Mutto 集團對各廠之 VPN 線路，統一由蘇州子公司管理。
13. Mutto 各廠之網段或 VLAN(虛擬網段)，統一由蘇州子公司規劃後，各廠依規劃進行設定，各廠不得私設網段或 VLAN。
14. 各廠之上網 PROXY 主機，授權與各廠自行管理，但其設定不得違反總公司之相關規定。

五、軟件安全：

1. 為保障安裝軟件是安全的，所有軟件安裝來源，需經 MIS 確認過，且經申請核准後，由 MIS 統一安裝。
2. 為確保員工電腦安全，免於病毒、木馬或版權問題。Mutto 集團下轄廠區，一般員工上網均強制透過代理伺服器。凡軟件安裝執行程式一律攔截，若因公務需求需要者，於申請核可後，由 MIS 代為下載並經檢測正常後安裝。
3. 軟件安裝光盤，磁盤，應統一集中於各廠 MIS 保管。
4. MIS 不得將公司軟件安裝序號，安裝於非公司電腦中。

六、硬件及機房安全：

1. 凡資訊產品之規格，為確保運作之兼容性，其規格均需由 MIS 制定。
2. 硬件攜出需有放行單，放行單上需有 MIS 簽名。
3. 集團重要核心硬件，如主機、重要網路設備等，考量整體之運作穩定性及兼容性，統一以總公司定義之標準實施。
4. 硬盤報廢時，MIS 需進行資料清空，重要硬盤應進行物理性破壞後，始可丟棄或回收。
5. 機房一律設定門禁控管，非 MIS 人員若須進出機房者，須由 MIS 人員陪同。

七、資料備份

主機系統備份：

1. 主機包含 Windows 與 LINUX 主機等，定義為影響公司營運之系統，使用之電腦主機。
2. 採影像式備份系統，備份影像統一存放至該廠之檔案主機中。
3. 系統設定有調整或異動時，需作備份。
4. 影像備份版本保留次數至少為 3，可視主機儲存空間增加。

資料庫備份：

5. 裝有資料庫主機，硬碟安裝必須採 RAID 方式。
6. 各廠資料庫統一集中管理，不得分散。
7. 採日備份機制，每日備份至該主機備份資料夾，並統一資料夾名稱為 backup。
8. 當日將最近一週之異動備份至另一台電腦。
9. 每週將資料庫統一備份至 Mutto 資料備份中心。

檔案備份：

1. 各廠主要之檔案主機，硬碟安裝必須採 RAID 方式。
2. 主機檔案於每日進行覆蓋式備份至另一台電腦，或是同機另一顆硬盤。
3. 每週將資料統一備份至 Mutto 資料備份中心。

郵件備份：

1. 郵件主機之進出郵件，每日均做日備份。
2. 採用 IMAP 之格式之用戶，備份郵件主機採每 2 小時同步之方式。
3. 郵件主機做之日備份系統，統一每月底以壓縮方式，移轉到另一台備份主機。
4. 郵件有效備份週期定為 3 年，超過的時間之資料依規定銷毀。

備份中心：

1. 集團統一設置備份中心，並做為各廠之近線資料備份。
2. 為降低整體維護成本與備份還原能力，近線式備份採用硬碟式備份。
3. 近線式備份，儲存資料與在線式之時間差為一週。
4. 備份資料統一由 MIS 保管。
5. 集團可視需要建立異地的次要近線備份系統。