壹、 目的(Purpose):

隨著網際網路的盛行，企業與外界的交流日益頻繁，如何在便利與安全中取得一個平衡點，讓企業在網際網路業務上能順利推行，成為企業在網際網路架構規劃上重要課題；因此，如何制定一個完善的安全策略，足以影響日後整個公司運作機制是否順暢，並能防範系統可能漏洞，以確保公司資料安全性，以下為本公司防火牆安全政策，將逐一作說明。

貳、 範圍(Scope):

本政策涵蓋中鋼公司廠區及總部大樓所有連結至公司網路之電腦設備(個人電腦、伺服器等)及使用者。

參、 安全管理準則(Policy):

內部網路與外部網路間，設置非軍事區(DMZ, de-military zone)，將企業開放資源放置於本區域(如電子商務、電子信件伺服器、檔案傳輸(FTP)伺服器..)，以區隔內部與外部網路，避免駭客及病毒長驅直入，產生更大破壞。

內部網路與 DMZ 區連線

1. 此類連線多屬中鋼內部程式開發所使用。新開發之伺服器連線業務需要並經評估及書面審核許可後，才開放特定連線服務；現行既有伺服器連線修改及異動可由 Email 作為往來異動證明。

內部網路/DMZ 區對外部網路連線

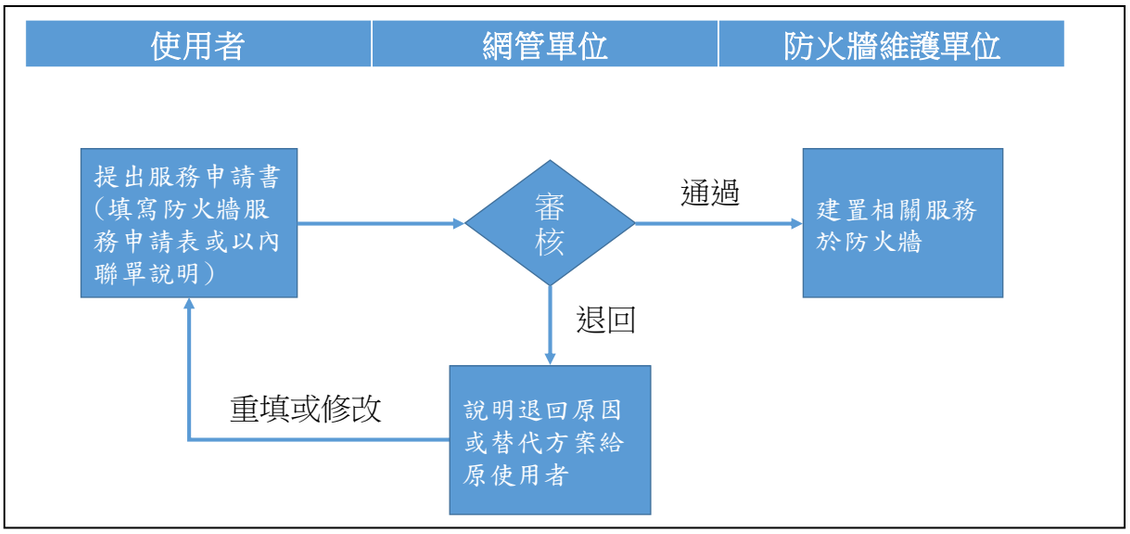
1. 限制公司電腦對外上網，經專案申請並核准者，始可使用網際網路資源。
2. 除業務需要並經評估及許可後，才開放特定連線服務，否則一律關閉其餘服務，以降低通訊流量節省頻寬；開放特定服務時，亦僅針對特定 IP、IP 範圍以及特定網段開放。

外部網路對內部網路/DMZ 區連線

1. 由外部進入內部連線存取服務，採用限制特定服務至特定主機為原則。
2. 可依業務需要並經檢核之政策，針對特定對外開放連線服務及主機， 於防火牆上設定安全連線規則，以減少被入侵可能性。
3. 出外洽公人員，若有需要使用公司資訊，經專案申請 VPN
4. 防火牆設置規則(Policy)，皆須經由網管單位主管簽核通過，將討論之規則建置成調查表內容，做為設定防火牆規則依據，並不定期討論，防止系統漏洞產生。
5. 定期檢視防火牆出入記錄，以確保防火牆運作正常。
6. 定期檢視防火牆官方更新，檢查防火牆作業系統是否存在漏洞，避免駭客攻擊，造成資訊外流及惡意破壞情事發生。
7. 每年一次以上(含)滲透測試服務，針對本公司指定之對外重要伺服器或主機作業系統、網站系統伺服器（Web Server），模擬駭客進行取得未經授權存取權限之滲透測試，測試完成後，請資安廠商提供『滲透測試結果報告』，並提出具體可行之建議及協助改善，以提供後續架構調整、系統強化作業之參考。
8. 針對公司非戰事區域(DMZ)內重要服務，請委外資安廠商提供每年定期一次以上(含)網頁弱點掃描服務，掃描完成後提供檢測報告，並提出具體可行之建議及協助改善，以提供後續架構調整、系統強化作業之參考。

肆、 防火牆安全政策實施程序說明：

防火牆服務之訂定，由使用單位提出申請，經由公司安管人員審核後，交由防火牆維護人員設置實施，程序如下：



伍、 政策強制性(Enforcement):

公司員工應遵守上述安全政策規定，若有違反者，則依公司人事管理制度來辦理。