中臺科技大學資訊網路遭入侵應變處理辦法

文件編號：CAR105
891106第六次行政會議通過
940629校務會議通過更改校名
951122行政會議修訂通過
1051026行政會議修訂通過
1071128行政會議修訂通過
提1100811主管會報審議
1100825行政會議修訂通過更改單位或主管名稱

第一條　目的隨著網際網路使用人數激增，網路安全問題也日漸嚴重，被入侵破壞者常不知情，並極少曝光。為防止資訊網路破壞者如駭客（Hacker）或怪客（Cracker）等非法入侵本校網路系統，竊取或損毀或竄改網路伺服器之資料，特制定此辦法。

第二條　編組及責任區分

一、資訊網路遭入侵時，圖書資訊處成立網路遭入侵緊急應變小組(以下簡稱緊急應變小組)。

二、圖資長為緊急應變小組召集人，負責指揮圖書資訊處人員，並隨時將相關情況呈報校長。

三、圖書資訊處行政及技術人員為緊急應變小組成員，負責排除故障及呈報損壞情形。

第三條　通報程序

一、圖書資訊處發現資訊網路遭入侵時，呈報圖資長。

二、圖書資訊處成立緊急應變小組，由召集人呈報校長，並通報各單位。

三、緊急應變小組成員依據資訊網路遭入侵應變程序處理。

四、狀況排除後，由緊急應變小組召集人呈報校長，並通報各單位。

第四條　資訊網路遭入侵應變程序

一、立即切斷電腦網路伺服器之連線，並記錄遭入侵之相關資料。

二、還原電腦網路伺服器之軟體及資料。

三、追查電腦網路駭客之入侵方式，檢查網路安全系統漏洞，提昇系統安全，以防堵電腦網路駭客再次以相同方式入侵。

四、統計損壞情形，呈報主管，通報受損資料之單位。

五、追查駭客身分，報請相關司法單位依法究辦並要求賠償。

第五條　預防措施

一、設置有效資訊網路防火牆，防止不合法使用者進入本校網路。

(一)資料查詢系統應採三層式組織架構，分為瀏覽系統、應用系統及資料庫系統等三層。

(二)視實際系統架構於適當地點建置防火牆。

(三)利用防火牆將資料查詢系統與內部及外部資訊網路有效隔開。

(四)防火牆主機與資料查詢系統主機放置於安全地點。

(五)防火牆主機系統功能設定最簡化，排除安裝所有非必要系統。

(六)防火牆主機系統不建置使用者帳號。

(七)執行安全稽核，建立自動監測功能。

二、定期備份資訊網路伺服器之軟體及資料。

第六條　本辦法經行政會議通過後實施，修正時亦同。