南開科技大學資訊安全矯正與改善辦法

壹、目的

南開科技大學(以下簡稱本校) 為持續增進資訊安全管理系統的有效性，落實資訊安全管理系統矯正與持續改善活動，特訂定「南開科技大學資訊安全矯正與改善辦法」(以下簡稱本辦法)。

貳、依據

一、南開科技大學資訊安全政策。

二、南開科技大學資訊安全營運持續計畫。

三、國際資訊安全標準 2013 年版(ISO/IEC 27001:2013)。

四、國際資訊安全作業規範 2013 年版(ISO/IEC 27002:2013)。

參、通則

本校實施資訊安全管理系統，遭遇下列情形時，即應啓動本辦法：

一、資訊安全管理系統適用對象，有三分之一(含)以上人員對同一程序作法不符規定。

二、對同一個活動的認知或做法不一致。

三、任何會使本校暴露於可接受風險值以上的事件。

四、資安稽核紀錄為重要缺失、次要缺失與觀察事項等不符合事項。

肆、程序

一、本校人員實施資訊安全管理系統，當發現影響資訊安全有效性的事件發生或有可能發生時，應對資安處理小組提出建議，由小組鑑別是否啓動本辦法。

二、資安處理小組應將啓動本辦法之項目，填寫於「南開科技大學資訊安全管理系統稽核不符合事項與矯正措施摘要表」(詳參「南開科技大學資訊安全管理系統稽核作業要點」)，並簽報資訊安全管理委員會執行祕書。

三、受稽核單位應針對需矯正的事件進行矯正、改善與追蹤作業，並將結果記載於「南開科技大學資訊安全管理系統稽核不符合事項與矯正措施摘要表」。相關作業說明如下：

(一)事件分析

分析原因並評估可以防止同樣事件再度發生的方法，可分短期方案和長期方案。

(二)矯正措施

1.決定採取的矯正措施與矯正時程。

2.如需取得實施矯正措施所需資源時，應簽報資訊安全管理委員會。

3.完成矯正後，須將矯正成效證據記載於「南開科技大學資訊安全管理系統稽核不符合事項與矯正措施摘要表」。

(三)持續改善

1. 鑑別潛在的問題及其發生的原因，進行事件分析。
2. 決定採取的改善措施與實施時程。
3. 如需取得實施改善措施所需資源時，應簽報資訊安全管理委員會。
4. 將措施證據記載於「南開科技大學資訊安全管理系統稽核不符合事項與矯正措施摘要表」。

四、追蹤查核

(一)資安處理小組至少每月一次，應追蹤查核尚未結案的資安矯正措施摘要表記錄項目，由各負責人就記錄項目於每月底提交相關資料予資安處理小組進行彙報與討論。

(二)結案的資安矯正措施摘要表應簽報資安處理小組召集人。

五、有效性確認

(一)負責單位應確認矯正預防事件實施結果的有效性。

(二)資安處理小組召集人應將年度矯正預防措施的實施結果，於資訊安全管理委員會會議報告。

伍、輸出紀錄

南開科技大學資訊安全管理系統稽核不符合事項與矯正措施摘要表(編號：AU01)

陸、資訊安全矯正與改善辦法之修訂

本辦法經「資訊安全管理委員會」會議審議通過，陳請校長核可後施行。修訂時亦同。

附件一：

南開科技大學資訊安全矯正與改善辦法項目對照表

項次	規範要項	參照 ISO/IEC 27001:2013 項目
參	通則	10.1。
肆	程序	9.1、9.3、10.1 與 10.2。

第 1.0 版 97 年 6 月 20 日資訊安全管理委員會會議審議通過

第 1.01 版 97 年 6 月 24 日校務會議通過

第 1.1 版 98 年 6 月 8 日資訊安全管理委員會會議審議通過

第 1.2 版 100 年 9 月 13 日資訊安全管理委員會會議審議通過

第 1.3 版 102 年 5 月 31 日資訊安全管理委員會會議審議通過

第 2.0 版 103 年 11 月 27 日資訊安全管理委員會會議審議通過