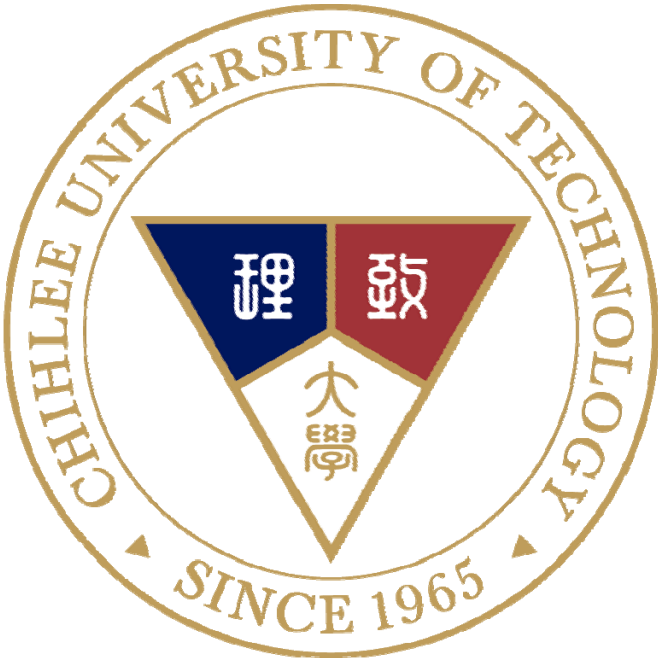
致理科技大學

內部稽核管理程序



機密等級：■一般 □敏感 □機密

編號：P-2-08

版本：2.2

發行日期：112 年 4 月 20 日

文件制／修訂紀錄頁

版次	發行日期	修訂摘要	修訂者	文管人員
1.0	106.4.20	初次發行	呂瑞茹	呂瑞茹
2.0	107.5.28	依據 BS 10012:2017 標準要求修正程序書內容	呂瑞茹	呂瑞茹
2.1	108.5.1	新增內部稽核缺失種類說明	呂瑞茹	呂瑞茹
2.2	112.4.20	修正內部稽核小組為個人資料保護內部稽核小組	呂瑞茹	呂瑞茹

目錄

壹、 目的：

驗證個人資訊管理系統是否被正確實施，適時發掘問題，採取適切之矯正措施，以期維持各項個人資料保護作業之有效性。

貳、範圍：

凡一切與個人資料保護有關之規定事項與實施單位，皆為稽核範圍。

參、權責

文件類別	制/修訂	審查/會簽	核准	稽核執行及矯正追蹤確認
年度稽核計畫	個人資料保護內部稽核小組	個人資料保護內部稽核小組負責人	副校長/主秘	指定稽核人員
不定期稽核公告	個人資料保護內部稽核小組	個人資料保護內部稽核小組負責人	副校長/主秘	指定稽核人員

肆、定義：

組織應在規劃期間內(每年至少一次)或當有重大變更發生時，執行內部稽核以提供資訊了解 PIMS 是否符合組織自身對 PIMS 及 BS 10012 國際標準的要求，本校之內部稽核區分為：

一、 定期稽核：由個人資料內部稽核編組負責研擬年度稽核計畫，經權責主管核准後實施。

二、 不定期稽核：權責主管依據本校個人資料管理系統執行之實際狀況，認為有需要執行內部稽核時，可針對某些單位執行不定期稽核。

伍、作業內容：

一、 應規劃、建立、實施和維持稽核計畫，包括頻率、方法、職責、規劃要求及報告，其應考量所涉及過程的重要性，影響組織的改變及前次稽核的結果；稽核計畫應清楚包括高風險個人資訊的任何處理過程以及委外交由其他組織或資訊處理者處理個人資訊的過程。

二、 稽核計畫及稽核員：

（一） 定期稽核：個人資料內部稽核編組於每次內稽前，需擬定「年度稽核計畫」，陳副校長/主秘核准後，稽核月份依計畫所排訂為主；稽核計畫經副校長/主秘核准後，可公告或 email 通知各單位。

（二） 不定期稽核：當權責主管臨時決定需執行內部個人資料稽核時，則由個人資料內部稽核編組公告或 email 通知相關被稽核單位及稽核日期。

（三） 定期稽核之稽核範圍，可視稽核員之人數及人力負荷，將本校之個人資料管理系統依單位或程序文件予以區隔，分開數次執行部份之稽核；不定期稽核則依權責主管指示範圍或單位執行稽核。

（四） 合格稽核人員，需同時符合下列條件：

1. 曾受相關訓練 3 小時以上，且有相關訓練紀錄者。
2. 稽核前，應先經權責主管核准。

（五） 每次稽核前，由個人資料內部稽核編組負責安排內部稽核人員；被稽核單位內，若有合格之稽核員，不得參與對自己負責業務執行內部稽核。

三、 稽核準備：

（一） 指派資深稽核員為主導稽核員，由主導稽核員召集相關稽核員，說明本次稽核之目的，並協調分配稽核範圍；稽核對象及範圍分配，可依各單位執行狀況、重要性及以前稽核結果做為參考。

（二） 個人資料內部稽核編組在稽核前以電子郵件通知被稽核單位有關稽核項目及稽核日期等資訊，以便被稽核單位做好相關之準備工作。

（三） 通知接受稽核單位之單位個人資料保護代表，在稽核時間內需親自或指派適當人員陪同稽核。

（四） 若委由外部合格稽核員執行稽核規劃作業，則稽核員於排定稽核行程後，經主導稽核員審核，通知相關單位配合執行。

四、 執行稽核：

（一） 稽核員應就所分配之稽核範圍，於稽核前充份瞭解各相關程序及辦法，並制作「內部稽核查檢表」；若委由外部合格稽核員執行，則免製作「內部稽核查檢表」，可直接展開稽核作業。

（二） 稽核員以「內部稽核查檢表」做為稽核指引，請被稽核單位提供相關文件及表單紀錄做為稽核佐證。

（三） 稽核員應秉持公正及客觀的態度，對被稽核單位執行稽核，受稽核單位應全力配合稽核員進行查核。

五、 稽核報告

（一） 稽核員應將稽核過程中所發現之缺失，依據事實紀錄於「內部稽核查檢

表」，交被稽核單位主管簽認，並交稽核小組組長（或主導稽核員）審核。

（二） 被稽核單位依「內部稽核查檢表」所列缺失需檢討，缺失種類區分為「建議」、「觀察」及「不符合」等三種，各單位應建立「矯正與預防處理單」並將該單號做成紀錄以利追蹤。

（三） 稽核員依被稽核單位提出之改善對策進行追蹤確認，並將追蹤狀況紀錄於「內部稽核報告」上，

（四） 個人資料內部稽核負責人應彙整「內部稽核查檢表」，交由主導稽核員審核後，於管理審查會議中提出報告和說明。

（五） 稽核相關紀錄依規定期限加以保存。

六、 績效衡量：內部稽核所發現之缺失，應於規定期限內確實改善完成，並做到類似缺失之再發防止；若其他單位有類似問題時，應提出預防措施並於管理審查會議、個人資料保護推動委員會或其他重要會議中宣導。

陸、相關文件：

P-2-09 矯正與預防管理程序。

柒、使用表單：

一、 年度稽核計畫。(P-2-08-01)

二、 內部稽核查檢表。(P-2-08-02)

三、 矯正與預防處理單。(P-2-09-01)