國立曾文高級家事商業職業學校109學年度期初校務會議紀錄

日期：109年8月28日10時10分
地點：行政大樓三樓視聽中心
主席：陳校長藝昕　　紀錄：鄭玉秀
參加人員：如簽到單

壹、報告開會人數：

一、應到人數83人，實到人數 81人，達法定開會人數。

二、主席宣布開會。

貳、報告上次會議決議事項執行情形：參閱會議資料P1。

參、人事異動介紹：歡迎家長會代表明哲副會長、親愛的同仁大家好，時間過的很快，新的學年度已經開始，首先介紹兼行政異動及新進教師同仁(略)。

肆、家長會代表(吳副會長明哲)致詞

校長、各位主任、組長、老師大家好，感謝所有的老師在未來新學年度，對學生盡心盡力作最優質的教育，讓孩子能安心就學，我代表家長會向各位老師致上最高敬意，老師辛苦了。

伍、各處室工作報告暨補充報告

甲、 教務處邱鴻錦主任工作報告

一、已完成工作事項暨預定辦理事項請參閱會議資料P2~4。

二、9/3 受理109學年度第1學期課表異動申請截止，本學期除聘任廣告科、幼保科、體育科、資處科、特教科等5位代理教師外，尚邀請英文、物理、音樂、舞蹈、廣告、餐管及體育等7位兼課教師，另有各科專業教室/排課要求及同仁提出個別特殊排課需求，倘課務安排無法如每位同仁預期或有不盡理想處，請多體諒包涵。

三、各科教學研究會今年變更為一時段僅能一科，請各科召集人要召開教學研究會前先到教務處看是否已有他科申請之後，再向教務處登記召開時間。

四、今年高一新生人數302人，高二299人，加高三，全校總人數9佰多，人數也有下滑現象。

五、高三畢業生301人，共241名錄取大學，其中錄取國大大學與國立科大共45名。因自主學習的成效不錯，本學年度將續辦。

六、教育部來文資安提昇，學校的郵件主機10月份必須關閉，所以設備組會教各位教職員至教育部雲端信箱申請帳號。

七、8/31 學習歷程檔案任課教師認證(課程學習成果)截止日。

乙、 學務處劉主任士嘉工作報告

一、學務處報告事項請參閱會議資料P4~5。

二、規劃中工作事項：8/28 教職員工急救研習、9/21 國家防災日地震避難複合式演練、9/21-22 高一公民教育訓練、9/28-30 高三校外教學

參觀活動、10/7 環境教育講座、10/21 校運籌備會(暫定)、12/10-11 全校運動會(暫定)。

三、為建立學生良好用餐習慣並提倡均衡飲食概念，將嚴格禁止學生午餐外訂情形。

四、相關服儀規定皆依照本校學生服儀穿著要點辦理，僅星期三開放學生統一穿著班服及為提供學生舒適且優質之學習環境，開放學生於教室內可穿著非制式服裝，餘上課期間皆須依照服儀穿著要點辦理。

五、感謝本校教職員工發心捐款至學校教育儲蓄專戶，幫助有需要的學生，讓有心向學的孩子能安心上學。

六、新學年度相關防疫作為皆延續辦理，僅增列於教育學習場所或無法維持正常社交距離之空間，教職員工生皆須配戴口罩。

七、開學後一周內，衛生所將辦理登革熱抽查，煩請同仁定期進行環境巡檢並倒掉積水容器，以有效消除孳生源，抑制登革熱疫情。

八、緊急或一般傷病由校方送醫皆需有保健小天使或同學陪同就醫。護理人員不在時，嚴禁學生獨自在健康中心休息，以免發生意外。上課期間勿讓學生獨自到健康中心休息。

丙、 總務處李主任建法工作報告

一、總務處報告請參閱如會議資料 P5~6。

二、學校一直以來未有合格的「甲種職業安全衛生」業務主管人員，校長要我參與受訓，所以目前我已取得資格；上級要學校單位重視職業安全衛生，因此，各位同仁在教學場所若看到不符合職業安全衛生或不安全設備或措施等疑慮，請即時通報總務處，我們會馬上改善。

三、因近日下雨不斷且為颱風頻繁生成時期，請同仁務必注意辦公室及各管理空間之門窗是否於下班前皆確實緊閉，避免雨水潑濺造成室內設備損壞。

丁、 實習處李主任佳珍工作報告

一、報告事項請參閱會議資料 P6~7。

二、剛教務處有報告新生人數，實用技能學程人數不盡理想，有同仁建議是否結束實用技能學程招生，但經實習組長電詢國教署，回覆為因學校附近無其他學校招收商業類實用技能學生，所以本校必須續辦。

三、中餐教室整修進行中，及西餐教室若完成招標，也將陸續搬遷，請各位任課教師提醒學生勿靠近工程工地，以免影響人身安全。

四、教育部已經不提供實用技能班二年級教材，因此請任課教師必須自編教材。

戊、圖書館洪主任思農工作報告：

一、報告事項請參閱會議資料 P8。

二、感謝設備組長及總務處協助愛閱 2.0 及 3.0 空間的有聲書、輕音樂播放設備設置定位，歡迎同仁多加利用。

三、本學期新進圖書書單如(會議資料)所列，歡迎借閱使用。

己、輔導室陳主任姵慈工作報告：報告事項請參閱會議資料 P8~11。

一、期初召開各項會議，請各處室主任、導師、委員及相關成員準時與會。

（一）9/4(五)16:00 召開學生輔導工作委員會議，2 樓會議室。

（二）9/4(五)16:15 家庭教育推動小組會議，2 樓會議室。

（三）9/3-9/11 期初個別化教育計畫會議（IEP 會議），多元學習中心。

（四）9/14(一)12:00 特殊教育推行委員會議，2 樓會議室。

二、10 月 17 日（星期六）上午舉辦全校親職教育座談會，請導師及相關行政同仁參加；下午辦理親子互動工作坊。

三、本學期輔導室辦理 3 場教師(教職員工)知能研習(10/16、11/11、12/23)，歡迎踴躍報名參加。

四、實施學年輔導教師制，王寶慧老師負責高一高二學生，陳姵慈老師負責高三學生。各位教師如需轉介或諮詢，可洽該學年輔導教師。

五、宣導：自殺防治法施行細則第十三條，本法第十一條第一項所定人員應自知悉有自殺行為情事後二十四小時內，依中央主管機關建置之自殺防治通報系統進行通報作業。

六、本學年度除了新進特代理教張 O 詩老師以外，還有一位實習心理師協助團體輔導工作，另聘一位特殊教育助理人員陳 OO 先生，協助電商一陳 O 廷新生行動、用餐或休息，請同仁也多予協助學生。

庚、人事室吳主任瑞禎工作報告：

一、報告事項如會議資料 P12~14。

二、109 學年度第 1 學期子女教育補助費者，請於 109 年 9 月 30 日以前檢證提出申請，國民中、小學無須檢證，公私立高中（職）以上者，請繳驗收費單據，夫妻同為公教人員，僅能一方申領，不得重複報領。

三、108 年 6 月 5 日修正公布之教師法第 35 條規定：「(第一項) 教師因婚、喪、疾病、分娩或其他正當事由，得依規定請假；其基於法定義務出席作證性侵害、性騷擾及霸凌事件，應給予公假。(第二項)前項教師請假之假別、日數、請假程序、核定權責與違反之處理及其他相關事項之規則，由中央主管機關定之。」因原第十八條之一條次變更及內容修正，爰配合修正教師請假規則。修正重點如下:

1.增訂第十款「教師從事進修、研究等專業發展，其公假依教師進修研究等專業發展辦法　規定辦理」，兼任行政職務教師寒暑假期間從事進修、研究等專業發展之公假時數，得不受每週八小時之限制；現行條文第七款無須重複規定，爰予以刪除。

2.教師基於法定義務出席作證性侵害、性騷擾及霸凌事件，應給予公假。

四、同仁申請出差旅費時，請檢附公差單夾帶之經校長簽准公文或簽呈。

五、110 年 1 月 1 日起資深優良教師獎金需列入課稅所得額範圍。

六、國民旅遊補助每年以申請2次為限，每次為8仟元以上。

辛、主計室廖主任家宏工作報告：報告事項詳如會議資料P14~15。

一、出差搭乘高鐵所獲優惠措施或購買早鳥票之優惠，應本誠信原則以優惠後票價報支。

二、上班日或假日報支旅費均應以機關所在地作為報支起訖點。

三、因年底帳務結束時間較為緊迫，若師長有核銷單據(如：差旅費、健康檢查補助費、10人小組文康活動費、國旅卡或代墊款…等等)，煩請盡早提出申請。

壬、 黃秘書淑蘭工作報告

一、報告事項如會議資料P1。

二、完成2020曾文家商宣傳影片(中文版、英文版、日文版、韓文版)，有需要的同仁請告知我。

陸、提案討論：如會議資料P13~15。

案由一：推舉109學年度「國立曾文高級家事商業職業學校代收代辦費審核委員會」教師代表1名。(教務處)

說　明：

一、依據102年02月18日校務會議修正通過之「國立曾文高級家事商業職業學校代收代辦費審核委員會組織要點」辦理。

二、本組織要點第三條，本校代收代辦費審核委員會(以下簡稱本委員會)，本委員會之成員包括行政代表3人、教師代表1人、家長代表6人、社會公正人士1人計11人，其中行政代表及社會公正人士由校長遴聘，家長及教師代表由家長及本校全體教師分別推舉產生。

決　議：由王舜皇教師擔任。

案由二：推舉109學年度「國立曾文高級家事商業職業學校工讀獎助金審查委員會」教師代表2名。(教務處)

說　明：

一、依據107年8月20日行政會報修正通過「國立曾文高級家事商業職業學校學生工讀獎助金實施要點」辦理。

二、本實施要點第3條，應成立工讀獎助金審查委員會(以下簡稱本委員會)，本委員會置委員7人，置主任委員一人由校長兼任，教務主任為總幹事，委員**由行政代表、家長代表、學生會代表及**教師兩名兼任。

決　議：由顏嘉良教師、林有志教師擔任。

案由三：推舉109學年度「學生學習歷程檔案工作小組」教師代表1名、導師代表1名。(教務處)

說　明：

一、依據108年8月29日校務會議修正通過「國立曾文家商建置學生學

習歷程檔案作業補充規定」辦理。

二、補充規定第3點:工作小組成員由校長、教務主任、學務主任、輔導主任、實習主任、圖書館主任、教學組長、註冊組長、訓育組長、生輔組長、課程諮詢教師代表及導師代表、教師代表、家長代表、學生代表各一人，合計15人組成；其中校長擔任召集人，教務主任為執行秘書。

決　議：由翁菽蔚教師、謝依真教師擔任。

案由四：訂定本校「資通安全維護計畫」(如會議資料附件1電子檔)，提請討論。(教務處)　**(本提案之計畫詳細內容及附件，請參照本校網頁-教務處-資訊安全ISMS專區-「資通安全維護計畫校務會議提案區」網址連結如下：**

http://www.twvs.tn.edu.tw/index.php?route=cms/cms&cms_id=867&path=4_36_821_867

說　明：依據109年4月1日國教署臺教國署秘字第1090038348號函辦理暨109年4月28日本校資通安全委員會訂定。

決　議：照案通過。

案由五：訂定「國立曾文高級家事商業職業學校學生在校作息時間規劃注意事項」(如會議資料附件2)，提請討論。(學務處/教官室)

說　明：依據教育部105年12月1日臺教授國字第1050142381號函，檢送「教育部主管高級中等學校學生在校作息時間規劃注意事項」辦理。

決　議：照案通過。

案由六：訂定「國立曾文高級家事商業職業學校校園行動載具使用管理規範」(如會議資料附件3)，提請討論。(學務處/教官室)

說　明：

一、依據教育部108年6月17日臺教資(四)字第1080060697號函高級中等以下學校校園行動載具使用原則辦理。

二、103年6月30日期末校務會議通過「國立曾文高級家事商業職業學校學生行動電話使用規範」停用。

決　議：照案通過。

案由七：修正「國立曾文高級家事商業職業學校性別平等教育委員會設置要點」(如會議資料附件4)，提請討論。(學務處/教官室)

說　明：

一、依據107年12月28日總統華總一義字第10700140861號令修正公布之「性別平等教育法」辦理。

二、因應本校性別平等教育委員會執行秘書所屬處室之調整。

決　議：照修正案通過。

案由八：修正「國立曾文高級家事商業職業學校學生服儀穿著要點」(如會議資料附件 5)，提請討論。(學務處/教官室)

說　明：因應本校科班調整，進行細節內容修正。

決　議：照修正案通過。

案由九：修正「國立曾文家商學生請假實施要點」(如會議資料附件 6)，提請討論。(學務處/教官室)

說　明：配合本校請假及點名系統電子化，擬同時調整要點內容。

決　議：照修正案通過。

案由十：訂定本校「109 學年度第 1 學期行事曆簡表」(如會議資料附件 7)，提請討論。(總務處)

決　議：照案通過。

柒、教育部雲端版郵件帳號申請流程說明(教務處設備組)。

捌、主席結論

一、教育部雲端版郵件帳號，請每位同仁都要申請，尚未完成或有困難者請洽詢設備組協助。

二、體育署前來查核運動場整建工程，願再補助本校一些經費作田徑場改善，請總務處督促廠商進度，切勿延誤本校本年度運動會日期。

三、第 1 學期行事曆提案決議後，請總務處公告學校網頁最新消息。

四、全國技藝競賽時，選手同學在上場的 3 天，尤其是頒獎的殘酷時刻，情緒是無比緊張與激動的，拜託各位老師帶著同學步步為營，多鼓勵同學，新生進入本校時告知他們有得獎學長姐同學馬上會得到企業的肯定，是很榮譽的事情；請實習處追蹤以往有得獎選手同學之目前的學習成就及社會成就。

五、新修正的教師法包含性平法及兒少法之規定，人事室每年必須有 5 次的查核性別平等案件，包括專車司機、社團教師、約聘助理員，人事室僅有主任 1 人，人力有限業務繁忙，因此，請各位教師及全體同仁平日教育學生都要很小心，勿與學生於小空間接觸，以避免誤觸性平法的規定，

或有發現有關性平事件都要及時通報。

六、剛剛實習主任有報告實用技能學程商務科存廢問題，因本校該學程同學也都考升科大為主，但報到人數愈來愈少，請實習處再評估商業事務科的課程如何調整，及校外實習安排、如何抵學分或先改科名..等，或是按現況逐漸停招或是轉型。

七、兼行政同仁的辛苦，是他人不在其位，不知其苦；每人看自己的工作量時會覺得辛苦，看別人時都會覺得別人是輕鬆的，希望大家能以同理心對待，將心比心，大家一起努力，每個人的位置都是很重要的。

玖、臨時動議：無。

壹拾、散會(11 時 57 分)

國立曾文家商 109 學年度期初校務會議資料　1090828

一、 報告上次會議提案決議執行情形：

109 年 7 月 14 日 108 學年度期末校務會議提案決議：

案由一：修正本校「考試試場規則」。(教務處)

決　議：照修正案通過。

執行情形：依決議執行。

案由二：訂定本校「校外人士協助教學或活動要點」。(教務處)。

說　明：依據教育部 109 年 5 月 26 日臺教授國部字第 1090056105A 號函辦理。

決　議：照案通過。

執行情形：依決議執行本要點。

案由三：訂定本校「學生賃居服務要點」。(學務處)。

說　明：依據教育部國民及學前教育署 108 年 11 月 26 日臺教國署學字第 1080127720A 號函「高級中等以下學校學生賃居服務注意事項」辦理。

決　議：照案通過。

執行情形：依決議執行本要點。

案由四：訂定本校「辦理教師進行產業研習或研究作業要點」。(實習處)

說　明：

一、依據 109 年 4 月 8 日國教署臺教國署高字第 1090036955 號函辦理。

二、依據高級中等學校教師進行產業研習或研究實施辦法第 4 條規定辦理。

三、本作業要點，應經最近一次校務會議通過後實施，並將通過之作業要點或規定先行函送國立秀水高級工業職業學校（本署教師赴公民營機構研習委辦學校），再由該校統一彙報國教署。

決　議：照案通過。

執行情形：依決議執行本要點。

案由五：請決議「109 學年度教師成績考核委員會委員總數」。(人事室)

說　明：依據「公立高級中等以下學校教師成績考核辦法」第 9 條規定略以，「教師成績考核委員會由委員 9 人至 17 人組成，除掌理教務、學生事務、輔導、人事業務之單位主管及教師會代表為當然委員外，其餘由本校教師票選產生……委員之總數由校務會議議決。」

決　議：爰往例總數採 11 人。

執行情形：109 學年度教師成績考核委員會委員依決議人數通知開會。

案由六：修正本校「教師聘約約定事項」。(人事室)

說　明：

一、教師法於 108 年 6 月 5 日修正全文 53 條並自 109 年 6 月 30 日施行。

二、有關本校「教師聘約約定事項」爰配合教師法辦理修正。

決　議：照修正案通過。

執行情形：依修正後「教師聘約約定事項」執行辦理。

案由七：修正本校「教師評審委員會設置要點」。(人事室)

說　明：

一、 依據國教署109年6月10日臺教國署人字第1090066301A號函辦理。

二、 查108年6月5日修正公布之教師法第9條第4項規定：「前三項教師評審委員會之 任務、組成方式、任期、議事、迴避及其他相關事項之辦法，由中央主管機關定之。」，高級中等以下學校教師評審委員會設置辦法（以下簡稱本辦法）配合辦理修正。

三、 本辦法於109年6月28日修正發布，且本辦法第3條第5項規定：「本會委員之總額、選舉與被選舉資格、委員選舉方式、依第五條規定增聘校外學者專家擔任本會委員與候補委員遴聘方式、會議規範及相關事項規定，應由學校訂定，經校務會議通過後實施。」

決　議：照修正案通過。

執行情形：依決議執行本要點。

二、 人事異動介紹

三、 校長致詞

四、 家長會會長致詞

五、 各處室工作報告

教務處工作報告

一、教務處各組完成工作事項(109/7/1-109/8/27)：

(一) 109/7/1辦理『立體造型混凝土盆器DIY』研習

(二) 109/7/3高一高二第8節輔導課結束

(三) 109/7/6 辦理高級中等學校校長專業精進支持系統建構與實施計畫-南區校長區域工作坊

(四) 109/7/9　辦理『手機攝影工作坊』研習

(五) 109/7/10 辦理『英文科社群英文繪本』研習計畫

(六) 109/7/10 辦理 109 學年度高一新生報到

(七) 109/7/13 辦理『英文科教師專業社群研習-橋梁書工作坊』研習

(八) 109/7/22 公告高一、高二補考名單

(九) 109/7/27 高一、高二補考

(十)109/8/4 四技聯合登記分發放榜公告

(十一)109/8/10 完成 109 學年度教師任課暨班級配課。

(十二)109/8/3-8/14 暑期輔導課。

(十三)109/8/24~25 新生始業輔導(業務報告)、新課綱介紹、學習歷程檔案介紹

(十四)109/8/26-28 辦理高一新生夏日動能提升計畫

二、預定辦理工作事項：(109/8/28~9/30)

(一)教學組：

1.109/9/3 受理 109 學年度第 1 學期課表異動申請截止。

2.109/9/7~110/元/8 實施第 8 節輔導課。

3.109/10~110/4 辦理 5 次高三學藝競賽。

5.辦理期初及期末各科教學研究會，並彙整會議紀錄。

(二)註冊組：

1.配合後期中等教育長期追蹤資料庫於 110/2~6 月底進行高一新生問卷調查。
2.109/8/31 註冊開學；上傳各類補助名。
3.109/9/9 109-1 各班前三名清寒優秀學雜費減免申請截止。
5.109/9/11 中午前 109-1 工讀生申請截止。
6.109/9/11 前富邦慈善基金會獎助金申請截止。

(三)設備組：
1.109/8/31 前完成欣河系統合約續約。
2.處理教科書數量統計、請購業務。
3.全校教職員教育部雲端信箱帳號彙整
4.機房伺服器向上集中

(四)優質化承辦人
1.109/8/31 前完成 108 學年度高職優質化計畫書核定版上傳。
2.109/8/31 前完成 109 學年度高職優質化成果檢核報告書上傳。

三、商請協助事項/其他：

(一)高一新生報到人數:

	幼兒保育科	商業經營科	資料處理科	電子商務科	廣告設計科	餐飲管理科免試	餐飲管理科特招	商業事務科	廣告技術科	總計
免試	30	62	29	33	30	31	36	17	24	292
續招	2	4	3		3	1				13
總計	32	66	32	33	33	32	36	17	24	305
報到率	91.4%	94.3%	91.4%	94.3%	94.3%	91.4%	102%	48.5%	68.5%	87.2%

感謝全校教職員的協助。

(二) 高三畢業生 301 人，共 241 名錄取大學，其中錄取國大大學與國立科大共 45 名。

	餐管三	幼保三	商經三	資處三	綜三甲學術	綜三甲幼保	綜三乙	綜三丙	綜三丁	商務三	廣告三	總計
人數	34	28	32	34	21	16	23	31	36	20	26	301
升學人數	29	22	29	33	21	10	16	26	28	10	17	241
國立大學	6	6	19	10		1		1	2			45

(三) 感謝各處室配合修訂 109 學年度高職優質化計畫複審暨核定版及撰寫上學年度期末檢核成果報告書。

(四)本學期除聘任廣告科、幼保科、體育科、資處科、特教科等 5 位代理教師外，尚邀請英文、物理、音樂、舞蹈、廣告、餐管及體育等 7 位兼課教師，另有各科專業教室/排課要求及同仁提出個別特殊排課需求，故倘課務安排無法如每位同仁預期或有不盡理想處，請多包涵。

(五)教務工作繁雜，除既定行事外，尚須執行新課綱各項實務，倘有需同仁協助之處或辦理優質化、課綱宣導規劃等研習活動，請同仁們多支持、參與，感謝大

家。

（四）由於資安關係，學校的郵件主機必須關閉，麻煩全校教職員至教育部雲端信箱申請帳號。

（五）109/8/31 學習歷程檔案任課教師認證(課程學習成果)截止日

學務處工作報告

一、學務處完成工作事項：

（一）109學年度高三校外教學招標案，決標完成。

（二）109學年度高一公訓活動，決標完成。

（三）109學年度上學期期初友善校園週規劃。

（四）109學年度新生始業輔導。

（五）彙編109學年度學生手冊。

（六）109學年度社團招生表演。

（七）109學年度上學期綜合活動課表。

（八）109學年度上學期學務處工作計畫。

（九）109年7、8月學生返校打掃。

（十）因應新型冠狀病毒防疫小組工作第十二次會議。

二、學務處規劃中工作事項：

（一）1090828 教職員工急救研習。

（二）1090909 新生體檢。

（三）1090921 國家防災日地震避難複合式演練

（四）1090921-22 高一公民教育訓練。

（五）1090928-30 高三校外教學參觀活動。

（六）1090930 性別平等暨愛滋防治講座。

（七）1091007 環境教育講座。

（八）1091016 班際拔河比賽。

（九）1091021 校運籌備會。

（十）1091028 高一軍校歌比賽。

（十一）1091030 高二實彈射擊體驗。

（十二）1091111 名人講座。

（十三）1091202 班際排球比賽決賽。

（十四）1091210-11 全校運動會。

（十五）1091216 聖誕祈福點燈音樂饗宴活動。

（十六）1091230 歲末感恩班際才藝競賽。

三、商請同仁協助事項：

（一）本校團膳價格為每餐47元，主食以米食為主，麵食為輔，副食每餐4菜1湯，水果每週供應2次，白飯及湯無限量供應，各項餐點皆依照營養師規劃菜單烹調，營養健康、創新味美及衛生安全為主要訴求。同仁針對用餐如有建議或意見，請隨時提供予學務處，將立即提供廠商改善。

（二）為建立學生良好用餐習慣並提倡均衡飲食概念，將嚴格禁止學生午餐外訂情

形，如有活動或相關特殊需求，請師長出具證明後方可准予外訂，學務處亦不定期招開伙食委員會並邀請廠商列席，將各項用餐狀況或菜色建議提供廠商參考，以提升本校團膳及教職員工生用餐品質。

（三）相關服儀規定皆依照本校學生服儀穿著要點辦理，僅星期三開放學生統一穿著班服及為提供學生舒適且優質之學習環境，開放學生於教室內可穿著非制式服裝，餘上課期間皆須依照服儀穿著要點辦理。

（四）感謝本校教職員工發心捐款至學校教育儲蓄專戶，幫助有需要的學生，因為專戶成立之精神為救急不救窮，為使補助款能達最大使用效益，本專戶亦由委員謹慎審核發放資格，所以感謝同仁的無私付出，讓有心向學的孩子能安心上學。

（五）新學年度相關防疫作為皆延續辦理，僅增列於教育學習場所或無法維持正常社交距離之空間，教職員工生皆須配戴口罩。因全球疫情尚未趨緩，且疫苗尚未上市，故請同仁持續協助宣導各項防疫作為

（六）開學後一周內，衛生所將辦理登革熱抽查，煩請同仁定期進行環境巡檢並倒掉積水容器，以有效消除孳生源，抑制登革熱疫情。

（七）緊急或一般傷病由校方送醫皆需有保健小天使或同學陪同就醫。護理人員不在時，嚴禁學生獨自在健康中心休息，以免發生意外。上課期間勿讓學生獨自到健康中心在健康中心留置觀察時間以一小時為原則(健康中心不是讓同學補眠的地方，勿請想睡覺的同學到健康中心睡覺)

（八）教職員體檢調查請於9月4日前洽衛生組報名，若人數達20人即可辦理，辦理時間將另行公告。**40歲以上同仁(含40歲)可至人事室詢問相關健康檢查補助辦法。**

總務處工作報告

一、總務處各組完成工作事項：

（一）參加「甲種職業安全衛生」業務主管教育訓練。

（二）109 學年度全國高級中等學校實習工作會議膳食及研習場地勞務採購案決標。

（三）高壓電停電檢修時，發電機會發電供應電梯及電腦機電力，日後機房伺服器不用再停機，停電同步檢測機房冷氣會自動啟動功能，以避免非上班時間之跳電因應措施。

（四）辦理「109 學年度三年級校外教學採購案」招標事宜。

（五）完成「實習大樓屋頂防水防漏整修工程」驗收事宜。

（六）辦理「109 學年度高一公民教育團體活動」招標事宜。

（七）圖書採購案，辦理驗收。

（八）教育部國民及學前教育署所屬國立學校 109 年度新任總務及庶務主管採購研習。

（九）教育部派員至本校辦理「運動場地整建工程」施工品質查核作業。

（十）109 年度「跳脫框架之設計飯店與獨特文創行銷服務實例研討」驗收事宜。

（十一）行政大樓地下室集水井污泥之清理。

二、預定及進行中工作事項：

（一）109 學年度西餐烹調實習教室修繕之採購事宜。

（二）檢討並規畫實習大樓教室內聽不到消防警報的問題。

檢修圖資大樓 3F、4F 聽不到消防警報的問題（消防設備線路）。

（三）與電子公文簽核之國尊廠商研究改善電子公文簽核之效能。

（四）辦理「109 學年度幼保科、廣設科充實基礎教學實習設備」招標事宜。

（五）辦理 109 年度「國立高級中等學校污水及排水系統建置暨改善工程」。

三、煩請同仁配合事項：

（一）因近日下雨不斷且為颱風頻繁生成時期，請同仁務必注意辦公室及各管理空間之門窗是否於下班前皆確實緊閉，避免雨水潑濺造成室內設備損壞。

（二）因應「職業安全衛生法」之法令，請同仁檢核各辦公室場所、教室、專業教室，如有設備或措施有危機之疑慮，請通免於發生職業災害。

實習處工作報告

一、實習處暑假期間擬定之計畫皆依行事曆日程進行，感謝各位同仁的協助與幫忙，完成工作事項：

(一)109/07/15-07/18 辦理即測即評及發證檢定，職類計有電腦軟體應用、中餐烹調、飲料調製、會計資訊與印前製程等。

(二)109/07/20-07/29 辦理專業教師赴公民營機構研習「跳脫框架之設計飯店與獨特文創行銷服務實例研討」。

(三)完成優質化 108-5 成果報告。

(四)完成遴聘業界專家協同教學計畫成果報告。

(五)完成職場體驗計畫成果報告。

(六)完成提升學生實習實作能力計畫成果報告。

(七)完成 108 學年度均質化成果報告。

(八)完成 109 學年度家事類科與商業類科技藝競賽正式選手選拔。

(九)109/08/05 完成實習工作會議第一次籌備會。

(十)109/08/05 完成實習工作會議膳宿招標。

(十一)109/08/12 完成實習工作會議第二次籌備會。

二、本學年度擬定辦理工作計畫

(一) 109/10/06-07 承辦 109 學年度全國高級中等學校實習工作會議。

(二)校內實習：

1. 本學期幼保科校內實習二年級自 9 月 7 日起開始，一年級自 10 月 5 日起開始，請各指導老師妥善規劃實施，幼保科一二年級學生依照排定輪流表於本校附設幼兒園實習。
2. 各科實習課程特別籲請各指導老師務必利用課程開始第一節上課時間，詳細講解實習場地之安全衛生相關規則事項，並請務必落實執行。

(三)校內學生技藝競賽：

1. 109/09/16 幼保科寫故事比賽。
2. 109/10/07 幼保科說故事比賽。

3.109/10/28 PVQC 商管群專業英文詞彙校內賽。

(四)109 學年度全國中等學生技藝競賽：

1.109/11/10-12 家事類科競賽，地點：新北市立樟樹國際實創高級中等學校。

2.109/12/01-03 商業類科競賽，地點：豐原高商。

(五)畢業成果發表：

1.109/12/30 幼保科成果展。

2.109/12/16-18 廣告設計科暨廣告技術學程成果發表會。

(六)技能檢定期程：

1.109/09/01-09/07 受理 109 年度第 3 梯次全國技術士技能檢定報名，開考職類：會計資訊、印前製程、視覺傳達。

2.110/01/03 辦理 CSF 電腦技能檢定。

3.110/01/- 受理 110 年度在校生工業類、商業類技能檢定報名。

(七)109 學年度學生業界實習與職場體驗計畫學生與任課教師之責任：

1.學生應於每次職場體驗實習後繳交報告。

2.職場體驗後須作滿意度調查。

3.任課教師需批閱學生繳交之報告。

(八)遴聘業界專家協同教學計畫學生、業界專家、原任課教師之責任：

1.學生應於每次實習課後撰寫實習報告。

2.原任課教師須與業界專家共同研擬單元教材。

(九)均質化計畫

1.社區職涯試探學習計畫(各科)。

2.大手攜小手人才培育計畫。(南台科大)。

(十)持續進行「優化實作環境-改善實習教學環境及設施計畫」。

(十一)持續進行「優化實作環境-充實基礎教學實習設備計畫」。

(十二)持續進行「老舊實習場域翻新再造計畫」。

三、商請同仁協助與配合事項：

(一)全國技藝競賽選手將於本學期參加競賽，請大家多多給予鼓勵，因密集訓練造成行政及教學上的不便，敬請見諒！感謝各處室的協助。

(二)專業類科實習教室整潔維護工作將拜託全體師生協助，請任課老師協助指導各班同學，於第一次進入實習場所上課時，進行整潔工作，並於實習日誌中記載。

(三)這學期廣告設計科老師支援南科國中技藝學程課程，感謝廣設科老師協助，並感謝教務處排調課上之協助。

(四)這學期均質化重點工作是統籌辦理台南三區餐旅類、商業類、家事類與設計類國中試探實作課程，預計至少有 10 個班級到校參加實作，希望屆時各位老師可以協助實作課程，共同行銷學校。

(五)學生職場體驗及業界實習計畫與業師協同教學計畫皆已通過，請各位老師依照計畫協助執行，並於課程或活動結束時，將記錄或報告繳回實習組。

輔導室工作報告

一、 輔導室暑假工作事項：

(一)完成 108 學年度「辦理家庭教育實施計畫」成果結報。
(二)完成 108 學年度「教師輔導與管教知能工作坊」成果結報。
(三)完成 108 學年度「特殊教育方案計畫」成果結報。
(四)完成 108 學年度第 2 學期「身心障礙學生學習扶助計畫」成果結報
(五)擬定 109 學年度第 1 學期輔導工作實施計畫。
(六)登錄 109 學年度第 1 學期輔導工作行事曆。
(七)擬訂 109 學年度第 1 學期教師輔導知能研習輪流表。
(八)擬定本學期輔導工作各項細部實施計畫。
(九)配合教務處申請高級中等學校學生穩定就學措施實施計畫。
(十)109/8/24-25 配合辦理新生始業輔導。
(十一) 109/8/25 辦理 109 年度下半年輔諮中心臺南二區聯繫會議。
(十二) 109/8/25 辦理特殊需求新生轉銜會議。
(十三) 109/8/26 辦理特殊教育助理人員甄選。

二、 本學期輔導室重點工作事項：

(一)一般性輔導工作

1. 109/8/25 特殊需求新生轉銜會議。
2. 109/9/4 家庭教育推動小組會議。
3. 109/9/4 學生輔導工作委員會議。
4. 109/9/3-9/11 期初個別化教育計畫會議（IEP 會議）。
5. 109/9/14 特殊教育推行委員會議。
6. 109/9/23 認輔會議。
7. 109/12/21-110/1/8 期末 IEP 會議

(二)發展性輔導工作

1. 生活輔導
   (1) 109/8/24-25 配合實施新生始業輔導。
   (2) 109/9 辦理優質化計畫-曾家藝樹園丁活動-心動角落。
   (3) 109/9/1-18 協助高一新生登入線上系統資料。
   (4) 109/9/21 至期末實施輔導志工。
   (5) 109/9/30 特教新生始業輔導。
   (6) 109/11/24-12/11 辦理特殊教育暨家庭教育宣導週。
   (7) 109/12/4 輔導知訊出刊。
   (8) 109/12/3、109/12/17 辦理學生性別平等教育小團體活動。
   (9) 109/12/31 辦理同儕輔導暨輔導志工歲末聯誼活動。
   (10)依各班需求，不定期利用週三第八節實施班級團體輔導活動。
   (11)不定期更新輔導室 FB 粉絲專頁，提供輔導新訊。
2. 學習輔導
   (1) 高一學生於一段後實施並解釋學習診斷測驗（配合生涯規劃課或班會實施）。

(2) 109/9/1 多元學習中心課程開始。
(3) 申請與辦理扶助計畫課程。
(4) 申請與辦理特殊需求方案課程。
(5) 配合教務處申請高級中等學校學生穩定就學措施實施計畫-多元彈性課程。

3. 生涯輔導
(1) 高一學生實施生涯規劃課程。
(2) 高一學生實施並解釋大考中心興趣量表；高三學生(綜三甲學術學程)實施並解釋大學學系探索量表（配合班會實施）。
(3) 109/11/20 高三特殊需求學生升學輔導說明會。
(4) 利用雲端社群提供生涯輔導資訊。
(5) 蒐集升學及面試相關資料提供學生參考。
(6) 10 月下旬辦理轉銜輔導活動(暫定職場參訪+大專參訪一天)。

(三)介入性輔導工作
1. 針對需特殊關懷或感覺困擾的學生進行個別諮商或團體輔導。
2. 實施認輔學生輔導。

(四)處遇性輔導工作
1. 針對疑似罹患精神疾病、嚴重情緒困擾及特別困難學生轉介教育部學生輔導諮商中心臺南二區駐點服務學校接受諮商與治療，並與精神科醫師或諮商心理師協商後續輔導事宜。

(五)提供輔導諮詢
1. 教師知能研習
(1) 109/10/16 辦理教職員工輔導暨特教知能研習「認識自閉症和我做朋友」，講師：赫江老爸(無用老爸)，地點：生規教室，13:00-15:00。
(2) 109/11/11 辦理教職員工輔導暨特教知能研習「就業路上的我懂你-認識身障者職業重建」，講師：陳淑芳督導，地點：生規教室，13:00-15:00。
(3) 109/12/23 辦理優質化計畫-藝樹園丁工作坊「頌缽聲音療癒體驗」，講師:林文博，地點：多元學習中心，13:00-16:00。
(4) 擬訂校內教師研習輪流表，鼓勵教師參加教育部國教署辦理之輔導知能研習。

2. 家庭教育
(1) 109/10/17 辦理全校親職教育座談會。
(2) 109/10/17 親子互動工作坊。
(3) 提供親職教育資料。

3. 諮詢服務
(1) 提供教師輔導諮詢。
(2) 提供家長輔導諮詢。
(3) 承辦教育部學生輔導諮商中心臺南二區駐點服務學校，聘請精神科醫師及諮商心理師，接受台南市二區各高中職個案轉介諮商。

(六)承辦活動

（一）109/8/25 辦理教育部學生輔導諮商中心臺南二區駐點服務學校業務聯繫會議。

（二）109/10/30、11/16、11/20、12/14 辦理教育部學生輔導諮商中心臺南二區駐點服務學校團體督導。

三、 商請相關單位或老師配合的事項:

(一)期初召開各項會議,請各處室主任、導師、委員及相關成員準時與會,謝謝您。

1.109/9/4(五)16:00 召開學生輔導工作委員會議，2 樓會議室。

2.109/9/4(五)16:15 家庭教育推動小組會議，2 樓會議室。

3.109/9/3-9/11 期初個別化教育計畫會議（IEP 會議），多元學習中心。

4.109/9/14(一)12:00 特殊教育推行委員會議，2 樓會議室。

(二)本學期擬於 109 年 10 月 17 日（星期六）上午舉辦全校親職教育座談會，請導師及相關行政同仁參加。

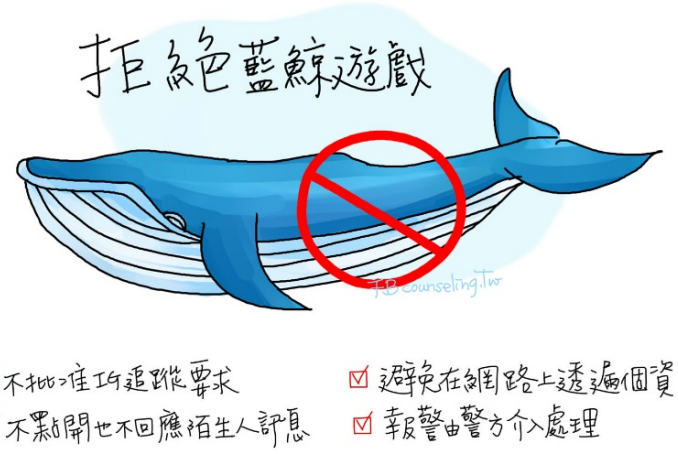
(三)本學期輔導室辦理 3 場教師(教職員工)知能研習，歡迎踴躍報名參加。

(四)持續推動認輔制度，歡迎有意願的老師加入認輔教師的行列。

(五)實施學年輔導教師制，王寶慧師負責高一高二，陳姵慈師負責高三。各位教師如需轉介或諮詢，可洽該學年輔導教師。

四、 宣導事項：

(一)依據 109 年 8 月 6 日以衛部心字第 1091761485 號令訂定發布自殺防治法施行細則第十三條，本法第十一條第一項所定人員應自知悉有自殺行為情事後二十四小時內，依中央主管機關建置之自殺防治通報系統進行通報作業 https://sps.mohw.gov.tw/Account/IndexInform。本法第十一條第二項所定通報內容，包括可得知之自殺方式、自殺行為人資料、自殺原因與處置情形及通報人聯絡方式。



圖片來源：嘿，我是專輔

人事室工作報告

一、人事異動：

新進人員：

廣告設計科教師洪璟婷109年8月1日到職。
幼兒保育科代理教師翁鈺婷109年8月1日到職。
資料處理科代理教師鄭瑞祥109年8月1日到職。
特殊教育科代理教師張保詩109年8月1日到職。
護理師職務代理人廖倩儀109年8月1日到職。
軍訓教官林奕成109年8月16日到職。

離職人員:

軍訓教官游禹琦109年8月1日調私立崑山高級中學。

二、業務報告：

(一)109學年度第1學期子女教育補助費者，請於109年9月30日以前檢證提出申請，國民中、小學無須檢證，公私立高中（職）以上者，請繳驗收費單據，夫妻同為公教人員，僅能一方申領，不得重複報領；於本校地1次申請者，並請檢附戶口名簿影本。

(二)因應108年6月5日修正公布之教師法第35條規定：「(第一項) 教師因婚、喪、疾病、分娩或其他正當事由，得依規定請假；其基於法定義務出席作證性侵害、性騷擾及霸凌事件，應給予公假。(第二項)前項教師請假之假別、日數、請假程序、核定權責與違反之處理及其他相關事項之規則，由中央主管機關定之。」因原第十八條之一條次變更及內容修正，爰配合修正教師請假規則。教師請假規則修正重點如下:

1. 增訂第十款「教師從事進修、研究等專業發展，其公假依教師進修研究等專業發展辦法　規定辦理」，兼任行政職務教師寒暑假期間從事進修、研究等專業發展之公假時數，得不受每週八小時之限制；現行條文第七款無須重複規定，爰予以刪除。
2. 教師基於法定義務出席作證性侵害、性騷擾及霸凌事件，應給予公假。

(三)同仁申請出差旅費時，請檢附公差單夾帶之經校長簽准公文或簽呈。

主計室工作報告

一、法令宣導：

(一)出差搭乘高鐵所獲優惠措施或購買早鳥票之優惠，應本誠信原則以優惠後票價報支

依現行「國內出差旅費報支要點」規定，出差搭乘高鐵當日往返者，已無須檢附票根或購票證明文件，惟仍應注意依行政院主計總處108年12月10日主預督字主預字第1080054410號「主計長信箱」函釋略以：出差係奉機關指派執行一定任務，其實際所發生之必要費用係由機關負擔，爰因公務出差搭乘高鐵所延伸之優惠措施，**出差人實際上既無支付差旅費之事實，自應本誠信原則以優惠後票價報支，或悉數將優惠差價回饋作為政府差旅費支出之抵減**。

(二)上班日或假日報支旅費均應以機關所在地作為報支起訖點

依行政院主計總處106月1月16日主預字第1060050104號「主計長信

箱」函釋略以：依國內出差旅費報支要點第1、3、5及12點規定意旨，旅費係支應機關員工因公奉派出差實際所發生之必要費用，且員工之出差係由機關基於公務需要派遣，爰**旅費之報支自應以機關所在地作為報支起訖點，並以必經之順路計算之，上開規定並未區分上班日或假日**。

二、商請同仁協助事項：

因年底帳務結束時間較為緊迫，若師長有核銷單據(如：差旅費、健康檢查補助費、10人小組文康活動費、國旅卡或代墊款…等等)，煩請盡早提出申請。

秘書工作報告

一、已完成事項：

(一)各項控管業務進度之追蹤。

(二)處理校長交辦事務。

(三)結報家長會經費。

(四)完成108年度學校內部控制自評及內部稽核，並完成內控聲明書簽署。

(五)完成國立曾文家商職業安全衛生相關文件(共計20份)，並放置學校首頁「職業安全衛生專區」。

(六)完成2020曾文家商宣傳影片(中文版、英文版、日文版、韓文版)。

二、預計辦理事項：

(一)持續追蹤控管事務。

(二)持續追蹤學校網頁資料整備情形。

(三)持續彙整曾家新聞剪報、學校大事紀、各處室成果報告書。

三、宣導及感謝各處室配合事項：

感謝各處室組及同仁們對秘書室業務的協助與配合，新學期再煩請賜教。

六、 提案討論

案由一：推舉109學年度「國立曾文高級家事商業職業學校代收代辦費審核委員會」教師代表1名。(教務處)

說　明：

(一)依據102年02月18日校務會議修正通過之「國立曾文高級家事商業職業學校代收代辦費審核委員會組織要點」辦理。

(二)本組織要點第三條，本校代收代辦費審核委員會(以下簡稱本委員會)，本委員會之成員包括行政代表3人、教師代表1人、家長代表6人、社會公正人士1人計11人，其中行政代表及社會公正人士由校長遴聘，家長及教師代表由家長及本校全體教師分別推舉產生。

案由二：推舉109學年度「國立曾文高級家事商業職業學校工讀獎助金審查委員會」教師代表2名。(教務處)

說　明：

(一)依據107年8月20日行政會報修正通過「國立曾文高級家事商業職業學

校學生工讀獎助金實施要點」辦理。

(二)本實施要點第 3 條，應成立工讀獎助金審查委員會(以下簡稱本委員會)，本委員會置委員 7 人，置主任委員一人由校長兼任，教務主任為總幹事，委員由行政代表、家長代表、學生會代表及教師兩名兼任。

案由三：推舉 109 學年度「學生學習歷程檔案工作小組」教師代表 1 名、導師代表 1 名。。(教務處)

說　明：

(一)依據 108 年 8 月 29 日校務會議修正通過「國立曾文家商建置學生學習歷程檔案作業補充規定」辦理。

(二)補充規定第 3 點:工作小組成員由校長、教務主任、學務主任、輔導主任、實習主任、圖書館主任、教學組長、註冊組長、訓育組長、生輔組長、課程諮詢教師代表及導師代表、教師代表、家長代表、學生代表各一人，合計 15 人組成；其中校長擔任召集人，教務主任為執行秘書。

案由四：訂定本校「資通安全維護計畫」(如附件 1 電子檔)，提請討論。(教務處)

(本提案之計畫詳細內容及附件，請參照本校網頁-教務處-資訊安全 ISMS 專區- 「資通安全維護計畫校務會議提案區」網址連結如下：
http://www.twvs.tn.edu.tw/index.php?route=cms/cms&cms_id=867&path=4_36_821_867

說　明：依據 109 年 4 月 1 日國教署臺教國署秘字第 1090038348 號函辦理暨 109 年 4 月 28 日本校資通安全委員會訂定。

案由五:訂定「國立曾文高級家事商業職業學校學生在校作息時間規劃注意事項」(如附件 2)，提請討論。(學務處/教官室)

說　明：依據教育部 105 年 12 月 1 日臺教授國字第 1050142381 號函，檢送「教育部主管高級中等學校學生在校作息時間規劃注意事項」辦理。

案由六：訂定「國立曾文高級家事商業職業學校校園行動載具使用管理規範」(如附件 3)，提請討論。(學務處/教官室)

說　明：

(一)依據教育部 108 年 6 月 17 日臺教資(四)字第 1080060697 號函高級中等以下學校校園行動載具使用原則辦理。。

(二)103 年 6 月 30 日期末校務會議通過「國立曾文高級家事商業職業學校學生行動電話使用規範」停用。

案由七：修正「國立曾文高級家事商業職業學校性別平等教育委員會設置要點」(如附件 4)，提請討論。(學務處/教官室)

說　明：

(一) 依據 107 年 12 月 28 日總統華總一義字第 10700140861 號令修正公布之「性

別平等教育法」辦理。

（二）因應本校性別平等教育委員會執行秘書所屬處室之調整。

案由八：修正「國立曾文高級家事商業職業學校學生服儀穿著要點」(如附件 5)，提請討論。(學務處/教官室)

說　明：因應本校科班調整，進行細節內容修正。

案由九：修正「國立曾文家商學生請假實施要點」(如附件 6)，提請討論。(學務處/教官室)

說　明：配合本校請假及點名系統電子化，擬同時調整要點內容。

案由十：訂定本校「109 學年度第 1 學期行事曆簡表」(如附件 7)，提請討論。(總務處)

說　明：

七、 臨時動議

附件 1　**本校「資通安全維護計畫」**　畫詳細內容及附件，請參閱本校網頁-教務處-資訊安全 ISMS 專區-「資通安全維護計畫校務會議提案區」網址連結如下：http://www.twvs.tn.edu.tw/index.php?route=cms/cms&cms_id=867&path=4_36_821_867

附件 2

國立曾文高級家事商業職業學校學生在校作息時間規劃注意事項(草案)

109 年 8 月 28 日校務會議訂定

一、 依據教育部 105 年 12 月 1 日臺教授國字第 1050142381 號函，檢送「教育部主管高級中等學校學生在校作息時間規劃注意事項」辦理。

二、 為維護學生身心健康發展，培養自主學習及妥善時間規劃，提升學習品質，本校遵循教育部政策，同時參酌學校特性、學生、家長及教職員之意見及需求、校園安全、交通狀況及社會期待等因素，特訂定學生在校作息時間規劃注意事項（以下簡稱本注意事項），俾使師生有所依循。

三、 依「十二年國民基本教育課程綱要總綱」及「教育部函頒學生在校作息時間規劃注意事項」規定，學習節數每週三十五節（每日排課以七節為原則），其中包含必選修課程、團體活動時間及彈性學習時間；另早自修、升旗、午餐、午休、環境清掃及第八節輔導課等，均列屬非學習節數。

四、 為增進師生互動機會、班級經營及生活教育遂行，每週一至週五上午第 1 節學習節數(08:10)前之活動規劃如下：

(一)週一：升旗（屬全校性活動，全體學生均應到校參加）。

(二)週二至週四：學生自主學習規劃運用（各班級可以實施自修、考試、班級活動、社團討論等，以不影響其他班級為原則，學生得決定是否參加）。

(三)週五：朝會（屬年級性活動，年級學生均應到校參加）。

五、 每週一至週五第八節輔導課，均列屬非學習時數，學生得決定是否參加。

六、 每週一至週五上、放學時間及午餐、午休、環境清掃時間等規劃如下：

(一)上學：07:40 前進校。

(二)放學：17:00 放學。

(三)未參加週二至週四自主學習/服務學習之學生，得於上午第 1 節上課前進教室；未參加第 8 節輔導課學生，應於下午第 7 節下課後(16:10)離校。

(四)午餐：11:55-12:30。

(五)午休：12:30-13:00。依寧靜午休原則，除經申請核准之活動外，全體同學應於教室內安靜休息。

(六)環境清掃：16:40-17:00。各班級視掃區狀況進行環境維護。

(七)如遇特殊狀況，學校得調整部分上、放學時間，依學校公布為主。

七、 學生於非學習節數活動之參與狀況，本校不列入出缺席紀錄，但得視其情節，採取適當之正向輔導管教措施。

八、 學生如因個人或家庭特殊因素上學提早到校時(0630 前)，可至校門附近安全處等待，俟校門開啟後再行進校，放學延遲離校學生，可至教官室(或有師長留駐之辦公室)等待家長接

送，以維自身安全。

九、 學生如因活動或課程所需，經完成相關申請程序，得於週一至周五非上課期間使用教室或場地，惟須有申請老師在場陪同指導，學生須遵守申請相關規定並檢附家長同意書。

十、 本校學生專車載送時間、學生宿舍生活作息管理及獎懲規定等，應配合本注意事項增(修)訂之。

十一、 學生在校作息時間如下：

國立曾文高級家事商業職業學校學生在校作息時間表					
	星期一	星期二	星期三	星期四	星期五
06:30 後	進校	進校	進校	進校	進校
07:40-08:00	升旗 全校集合活動	服務學習 (非學習時數)	學生自主學習 (非學習時數)	學生自主學習 (非學習時數)	朝會 年級集合活動
08:10-09:00	第一節 (學習時數)	第一節 (學習時數)	第一節 (學習時數)	第一節 (學習時數)	第一節 (學習時數)
09:10-10:00	第二節 (學習時數)	第二節 (學習時數)	第二節 (學習時數)	第二節 (學習時數)	第二節 (學習時數)
10:10-11:00	第三節 (學習時數)	第三節 (學習時數)	第三節 (學習時數)	第三節 (學習時數)	第三節 (學習時數)
11:05-11:55	第四節 (學習時數)	第四節 (學習時數)	第四節 (學習時數)	第四節 (學習時數)	第四節 (學習時數)
11:55-12:30	午餐 (非學習時數)	午餐 (非學習時數)	午餐 (非學習時數)	午餐 (非學習時數)	午餐 (非學習時數)
12:30-12:55	午休 (非學習時數)	午休 (非學習時數)	午休 (非學習時數)	午休 (非學習時數)	午休 (非學習時數)
13:00-13:50	第六節 (學習時數)	第六節 (學習時數)	第六節 (學習時數)	第六節 (學習時數)	第六節 (學習時數)
14:00-14:50	第七節 (學習時數)	第七節 (學習時數)	第七節 (學習時數)	第七節 (學習時數)	第七節 (學習時數)
15:00-15:50	第七節 (學習時數)	第七節 (學習時數)	第七節 (學習時數)	第七節 (學習時數)	第七節 (學習時數)
15:55-16:40	第八節 (學習時數)	第八節 (學習時數)	第八節 (學習時數)	第八節 (學習時數)	第八節 (學習時數)
16:40-17:00	環境清掃 (非學習時數)	環境清掃 (非學習時數)	環境清掃 (非學習時數)	環境清掃 (非學習時數)	環境清掃 (非學習時數)
17:00	放學	放學	放學	放學	放學

十二、 本注意事項未規定者，依「十二年國民基本教育課程綱要總綱」、相關法令及本校校規辦理，學校得另行修訂決議施行。

十三、 本注意事項如需補充或修訂，經校務會議通過，校長核定之。

附件 3　**國立曾文高級家事商業職業學校校園行動載具使用管理規範（草案）**

109 年 8 月 28 日校務會議訂定

一、 依據教育部 108 年 6 月 17 日臺教資(四)字第 1080060697 號函高級中等以下學校校園行動載具使用原則辦理。

二、 為導引學生、教職員工及其他人（校外人士進入校園）等，於校園內適切使用行動載具，維持學校秩序及安全、教導行動載具使用禮儀，並促進學習成效，特訂定高級中等以下學校校園行動載具使用原則。

三、 本規範所稱行動載具，泛指手機、可攜式電腦、平板電腦、穿戴式裝置等具無線通訊功能之終端裝置。

四、 校園使用管理規範：

(一)使用時間：

1. 課堂下課及午間用餐休息期間。
2. 其餘除教師引導學習或緊急必要聯繫時使用外，其餘時間應以關機為原則。

(二)使用規範：

1. 行動載具於上課期間（含定期評量、自習、輔導課、體育課、實習課)、早自習彈性學習時間、午休、週會或學校重要集會場合，務必將行動載具關機或調整成震動並禁止使用，違者依校規懲處，經報備核可使用者不在此限。
2. 上課鐘響前將手機關機後，擺放行動載具時，須依個人座號依序放置於手機架，不得任意更換擺放位置，各班由風紀股長負責清查管制，未將個人攜帶之行動載具按規定擺放，經各班風紀股長口頭告知後仍未配合立即擺放者，需報告該節課之任課老師及導師，若屬實則可列入平時成績考核參考依據。課程結束後自行取回使用，學校不負行動載具保管責任。
3. 如遇緊急情況或上課需求需要使用行動載具時，應向導師或任課老師報備，經同意後方得使用。
4. 考試期間，行動載具一律管制使用，詳細規範依據本校考試規則辦理。
5. 使用行動載具時，應注意禮節及音量，不得妨礙他人學習。倘認定有違反並影響前揭相關事宜之正常進行，學校得以禁止之。
6. 學生使用行動電話具照相與錄影、錄音功能者，應尊重他人隱私(需徵詢當事人同意後始可為之)，否則不得任意拍攝及上傳散播；如違法播放、錄製(複製)mp3、mp4、影片及音訊或偷拍、糾眾滋事、傳輸(觀賞)不當影片，違反規定者依學生獎懲規定處理並自負法律責任。
7. 同學取、放行動載具需小心，勿損及他人行動載具(違者自負責任)，且不可擅自取用他人手機，違者以竊盜論處。
8. 學校教職員應尊重校園使用管理規定及注意使用安全，並考量使用場域、方法的合宜性。
9. 校外人士進入校園應在不影響學校上課及師生課程教學下使用
10. 違規處置：依據教育部規範原則，使用行動載具應以不影響教學、學習及個人生活 作

息為原則，倘認定有違反相關規定，並影響前揭相關事宜之正常進行，學校得禁止之。本校相關違規處置如下：

(1)上課期間（含定期評量、自習、輔導課、體育課、實習課)、早自習彈性學習時間、午休、週會或學校重要集會場合之使用者，依學生獎懲規定處分。

(2)學生使用行動電話具照相與錄影、錄音功能者，應尊重他人隱私，不得任意拍攝及上傳散播，亦不得下載限制級圖片與影音，違反規定者依學生獎懲規定處理。

(3)行動載具(含行動電源)不得在校內進行充電，違者依學生獎懲規定辦理。

(4)竊取他人行動電話產品者，依學生獎懲規定辦理並自負法律責任。

(5)如違反校園行動載具使用管理規範屢勸不聽者，得予以加重處分。

(6)考試期間，攜帶行動載具違反考場規則或舞弊等，依據本校考試規則辦理。

五、 本使用規範經校務會議通過，校長核定後公布實施，修訂時亦同。

附件 4

國立曾文高級家事商業職業學校性別平等教育委員會設置要點(修正草案)

100年8月31日校務會議訂定
101年6月29日校務會議修正
109年8月28日校務會議修正

一、依據：107年12月28日總統華總一義字第10700140861號令修正公布之「性別平等教育法」規定訂定之。

二、為推動性別平等教育，建立無性別歧視之教育環境，以實現性別平等為目標。

三、任務內容：

（一）統整學校各單位相關資源，擬訂性別平等教育實施計畫，落實並檢視其實施成果。

（二）規劃或辦理學生、教職員工之性別平等教育相關活動。

（三）研發並推廣性別平等教育之課程、教學及評量。

（四）研擬性別平等教育實施與校園性侵害/性騷擾/性霸凌之防治規定，建立機制，並協調及整合相關資源。

（五）調查及處理與性別平等教育法有關之案件。

（六）規劃及建立性別平等之安全校園空間。

（七）推動本校相關社區有關性別平等之家庭教育與社會教育。

（八）其他關於學校或本校相關社區之性別平等教育事務。

四、組織及任期：性平會置委員15人，任期一年，以校長為主任委員，其中女性委員應占委員總數二分之一以上，校長得聘具性別平等意識之教師代表、職工代表為委員。置執行秘書，由校長指派擔任，並指定學務處專人負責處理有關業務(納入分工職掌表)。本委員會委員任期一年，任期為每年八月一日至翌年七月三十一日，期滿得續聘之。

五、本委員會每學期應至少開會一次，由主任委員召集，主任委員不能出席時，應指定委員代理之。本委員會議應有委員二分之一以上之出席，始得開會。~~委員會議之決議，以出席委員過半數同意行之。~~委員對於會議討論事項（無論議案或調查報告）採共識決之方式決議。本委員會開會時得邀請諮詢顧問、相關行政人員及專家學者列席或報告，但法律另有規定者，從其規定。

六、組織分工與職掌：

七、性平會下設置行政與防治組、課程與教學組、諮商與輔導組、環境與資源組、圖書與刊物推行組、實習與教學組、人事行政組、會計組，各組分工如下：

（一）行政組（~~學務處~~）（執行秘書所屬處室）

1. 統整各單位相關資源，督導各組研擬推動性平相關活動業務，擬定性別平等教育實施計畫，落實並檢視其成果。
2. 研擬修訂性別平等教育實施規定及校園性侵害/性騷擾/性霸凌防治規定等相關規定。
3. 召開性平會會議，並處理性別案件之調查及相關行政事宜。

（二）宣導與防治組(學務處)

1. 規劃辦理學生及家長性別平等教育相關活動。
2. 受理校園性侵害/性騷擾/性霸凌事件（以下簡稱性別事件）之~~申訴~~申請、檢舉與處理相關行政事宜。
3. 建立校園性別事件及行為人檔案資料，並負責於行為人轉至其他學校就讀時之通報事宜。
4. 涉及校園性別案件通報及其協調聯繫事宜。
5. 指派專人擔任性別案件調查記錄者及負責承辦相關行政業務者。
6. 加強社團老師之選聘、管理和性平教育宣導。
7. 其他有關推動性別平等教育宣導與防治之業務。

（三）課程與教學組（教務處）

1. 發展性別平等教育課程之教學、教材及評量；教材之編寫、審查及選用，應符合性別

平等教育原則。

2. 規劃性別平等教育（含性侵害防治、家庭暴力防治、情感教育、性教育、同志教育等）融入各科教學，並且每學年應實施性別平等教育相關課程或活動至少四小時。
3. 協助處理與性別平等教育法有關案件之學生當事人學籍、課程、成績及相關人員課務。
4. 安排性別事件當事人接受性別平等教育課程相關事宜。
5. 加強實習教師之培訓、管理與性平宣導、教育和研習。
6. 其他有關本校性別平等教育課程與教學事務。

（四）諮商與輔導組（輔導室）

~~1. 統整各單位相關資源，擬定性別平等教育實施計畫，落實並檢視其成果。~~
~~2. 研擬修訂性別平等教育實施規定及校園性侵害/性騷擾/性霸凌防治規定等相關規定。~~
~~3. 召開性平會會議。~~

1. 協助辦理性別平等教育相關活動。
2. 擬定與執行性別事件相關當事人之輔導計畫，並向性平會提出報告。
3. 提供性別事件之當事人、家長、證人等之心理諮商、諮詢、轉介相關資源及追蹤輔導等服務。
4. 提供懷孕學生諮商輔導、家長諮詢及社會資源之協助。
5. 其他有關性別平等教育案件之輔導事宜。

（五）環境與資源組（總務處）

1. 建立安全及性別平等之環境。
2. 辦理校園安全空間檢視說明會，公告檢視成果、並作成紀錄。
3. 繪製並更新校園危險地圖，改善校園空間安全。
4. 加強固定或定期執行學校事務人員之管理與性平宣導活動。
5. 其他有關性別平等教育之環境與資源業務。

（六）圖書與刊物推行組(圖書館)

1. 購置性別平等教育相關圖書、刊物，供親師生借閱賞析。
2. 辦理性別平等教育讀書會、心得寫作與徵文活動，潛移默化學生性平價值觀。
3. 印製並發行性別平等教育相關之文宣刊物。

（七）實習與教學組(實習處)

1. 檢視性別平等實習教育空間，建構友善性別實習環境。
2. 協調與監督建教廠提供友善的性別工作場域。
3. 發展性別平等教育實習課程之教學、教材及評量；實習教材之編寫、審查及選用，應符合性別平等教育原則。

（八）人事行政組(人事室)

1. 將性侵害/性騷擾/性霸凌防治規定納入教師聘約。
2. 規劃並推動校內性別主流化，建構教職員性別平等意識。
3. 辦理教職員性別平等教育研習或相關進修活動。
4. 檢視並統計教職員參與性別平等教育情形，建構教職員性別平等規範。
5. 受理教職員工性別事件之申訴與處理相關行政事宜。

（九）會計組(主計室)

依據性平會所擬各項實施方案，編列經費預算。

八、如案情內容牽涉性平會委員本人或親屬時，依行政程序法之規定，應主動迴避。

九、參與處理性別相關事件調查之人員或推動性平業務之有功人員核實給予獎勵。

十、本要點如有未盡事宜，悉依「性別平等教育法」、「校園性侵害/性騷擾/性霸凌防治準則」相關規定處理之。

十一、本要點經性平會提案討論，校務會議決議通過，陳請校長核定後公告實施，修正時亦同。

附件 5

國立曾文高級家事商業職業學校【學生服儀穿著要點】(修正草案)

中華民國 99 年 08 月 30 日校務會議訂定
中華民國 102 年 06 月 05 日臨時校務會議修正
中華民國 103 年 02 月 10 日校務會議修正
103 年 6 月 30 日期末校務會議修正
105 年 6 月 30 日期末校務會議修正
109 年 8 月 28 日期初校務會修正

壹、服裝規定

一、上衣(校服):

(一)制服及運動服均需依規定繡製校名及學號,退色及模糊不清者應立即予以更新。

(二)穿長袖時不得捲袖子,釦子亦應扣好。

(三)女生著夏季制服時應配戴領結;男、女生著冬季制服均需配戴領帶。

(四)制服及運動服外套:應以學校製作之制式外套為標準,校名、科別及學號均應繡於左側校徽上緣,拉鍊拉至定位(約與制服第一顆扣子齊高)。

二、褲、裙(校服):

(一)校服裙子穿著應長短合宜,長度以在膝蓋上緣附近(約一拳頭距離),如裙子之長度過短者即屬違規。

(二)校服褲(裙)子之顏色、款式均應符合學校規定,並依實際需要配合班上規定統一穿著。

(三)長褲之材質,應以學校製作之學生制式長褲為標準,其它材質(如牛仔、休閒、韻律等質料)之長褲與和學校規定顏色不符之長褲(裙)均嚴格禁止穿著,長褲長度以覆蓋鞋帶為宜,惟不可觸地。

(四)同學可視個人需求自由選擇校褲、校裙穿著,惟以校服為限。

三、運動服:

(一)運動服應以學校製作之學生制式外套、衣褲為標準,其它材質(如牛仔、休閒、韻律等質料)之長褲與和學校規定顏色不符之長褲均嚴格禁止穿著。

(二)進入校門以本校制式服裝(含運動服)為限,並可視天候及個人需求調整穿著。惟正式場合(典禮儀程)需配合穿著正式服裝。

(三)著校服或運動服外套,應將釦子扣好、拉鍊拉上(校服外套上的釦子如有脫落,應即時將其修復,以求服裝之整齊一致)。

四、鞋子:

(一)穿著學校制服時鞋子應配合穿著黑色之學生皮鞋(以繫鞋帶種類為主,不得穿厚底及高跟皮鞋),嚴禁穿著球鞋;穿著運動服時以穿著白色底布(球)鞋為主,不得穿著休閒鞋、涼(拖)鞋、膠鞋。

(二)不得穿著涼(拖)鞋到校,否則一律登記處分(受傷明顯可見者及特殊天候因素除外)。如有特殊之理由,則應先請導師或輔導教官出具證明,再至生輔組辦理註銷或更正之手續。

五、髮式以尊重、自主、自然為原則。

六、眉毛以自然為主不得修剪或畫眉,指甲應按時修剪不可抹指甲油、黏貼假指甲。

七、不得配戴耳環。

貳、一般規定:

一、每位學生之服裝(含校服、運動服等)建議備妥兩套以供換洗,日後不得再以任何理由作為規避登記之藉口。

二、進出校門應依規定背制式書包及手提帶,如手提帶無法容納所攜帶之物品時,得以加提素色為主非制式提袋。

三、除定期(有預先告知)之統一服儀檢查外,其他在平日上、放學時被登記之服儀違規項目均可以申請複檢(生輔組),每個項目每人均有一次之複檢機會,由生輔組管制,同項目累犯者即不再受理複檢而將逕予簽處。

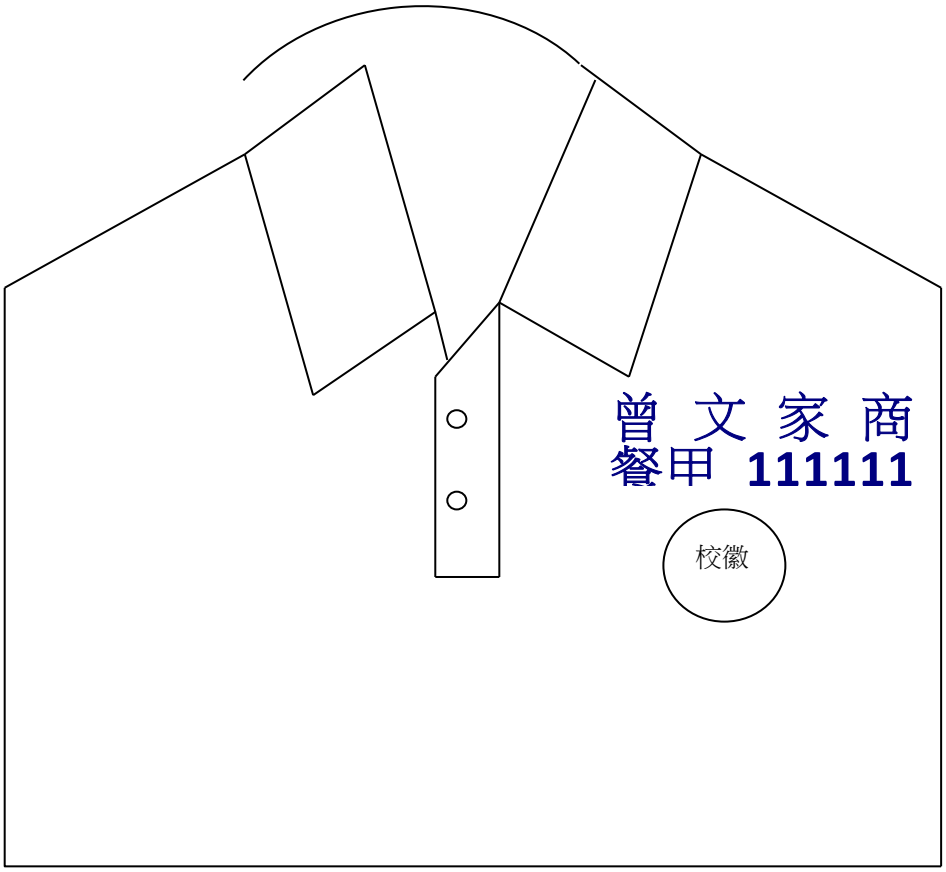
四、學生違規被登記時應虛心接受，凡態度惡劣不服糾正者，加重其處分。(有疑慮或委屈時可向值勤教官或生輔組長請求申覆，嚴禁當場和執勤學生發生衝突)。

五、各班級每週至少穿著制服乙次、**經班級共識開放星期三穿著班（科）服。**

六、102 學年度起，冬季制服修改為短版(同夏季制服下擺)，不需紮入褲（裙）之內。

叁、本實施要點校務會議通過後，呈校長核示後實施，修正時亦同。

國立曾文家商運動服學號規定



一、長短袖運動服：

校名、科別及學號繡~~蓋色~~**指定顏色**，由鈕釦往袖子方向繡，有口袋之制服，學號切齊口袋上緣，無口袋之制服，學號切齊第 2 顆鈕釦。

二、科別代號：

餐甲(餐飲管理科甲班)、餐乙(餐飲管理科乙班)

商甲(商業經營科甲班)、商乙(商業經營科乙班)

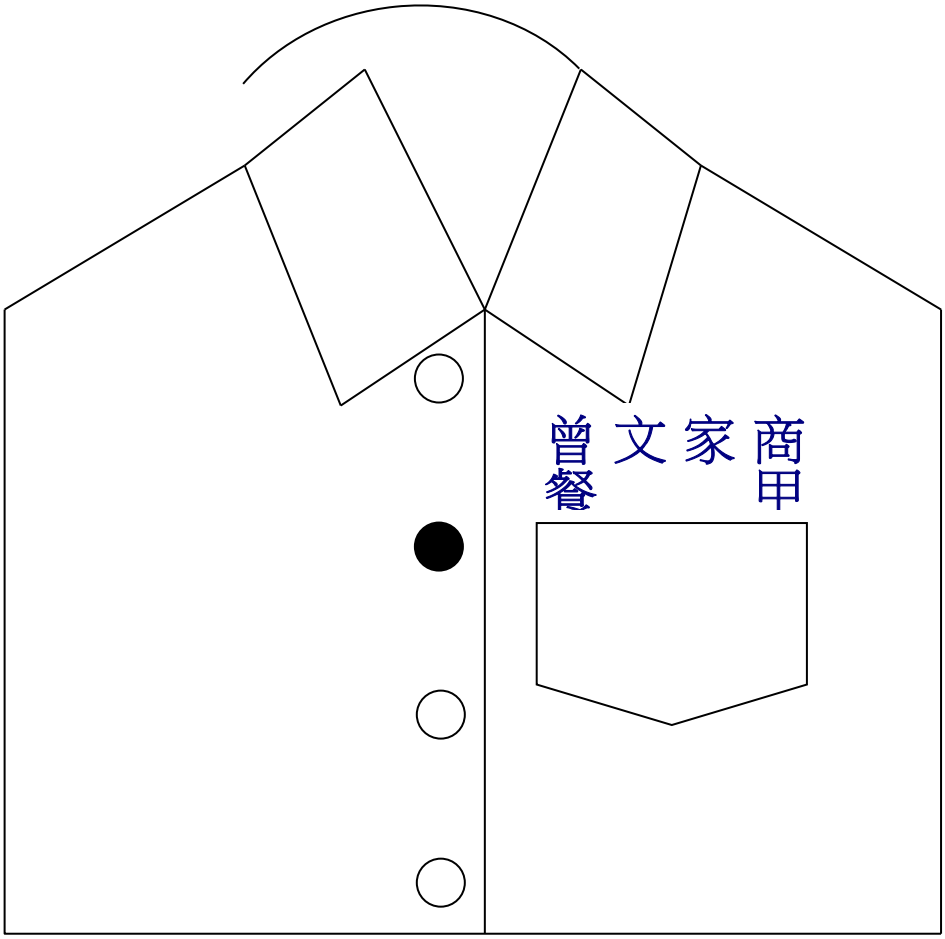
幼保(幼兒保育科)、資處(資料處理科)

電商(電子商務科)、廣設(廣告設計科)

商務(商業事務科)、廣技(廣告技術科)

三、自 108 學年度，電繡顏色依年級而有不同指定。

國立曾文家商制服學號規定



一、長短袖制服：

校名、科別及學號繡~~藍色~~**指定顏色**，由鈕釦往袖子方向繡，有口袋之制服，學號切齊口袋上緣，無口袋之制服，學號切齊第 2 顆鈕釦。

二、科別代號：

餐甲(餐飲管理科甲班)、餐乙(餐飲管理科乙班)

商甲(商業經營科甲班)、商乙(商業經營科乙班)

幼保(幼兒保育科)、資處(資料處理科)

電商(電子商務科)、廣設(廣告設計科)

商務(商業事務科)、廣技(廣告技術科)

三、自 108 學年度，電繡顏色依年級而有不同指定。

國立曾文家商外套學號規定

一、運動服外套：

校名、科別及學號繡~~金黃色~~**指定顏色**，由拉鍊往袖子方向繡。

二、科別代號：

餐甲(餐飲管理科甲班)、餐乙(餐飲管理科乙班)

商甲(商業經營科甲班)、商乙(商業經營科乙班)

幼保(幼兒保育科)、資處(資料處理科)

電商(電子商務科)、廣設(廣告設計科)

商務(商業事務科)、廣技(廣告技術科)

三、自 108 學年度，電繡顏色依年級而有不同指定。

四、制服外套：因應 105 學年度起，制服外套改為西服款式，學號與姓名由個人書寫於內裡標示牌，以資識別。

附件 6

國立曾文高級家事商業職業學校學生請假規則實施要點(修正草案)

中華民國 98 年 1 月 20 日校務會議訂定
中華民國 101 年 2 月 1 日校務會議修正
中華民國 109 年 8 月 28 日校務會議修正

一、 依高級中學學生成績考查辦法及本校實際狀況。

二、 學生在上課期間，遇有親喪疾病或其他重大事故，不能到校上課或出席各種集會時，須先辦妥請假手續，非因重病或特殊事故不得請人代辦或事後補辦。

三、 學生因患重病或特殊事故，不能~~到校~~辦理請假手續時，得由家長代理並於當日來電~~函~~代為請假。

四、 請假種類：病假、事假、喪假、公假、產前假、娩假、流產假、育嬰假、生理假、不可抗力假。

五、 病假：已到校者須辦好請假手續後方准離校；未到校者，准於當日來電聲明，事後辦理補假事宜，除按規定事項辦理外，規定病癒來校上課三天內辦理補假手續，逾期無效並以曠課論。

六、 事假：應於事假前一日檢附家長簽章證明完成請假手續。如有特殊事故，最遲須於三日內完成請假手續。~~須在前一日經家長在請假單上蓋章證明，經核准登記後方可離校，事後不得補假，否則以曠課論。(如特別事故，准以當日來函聲明)。~~

七、 喪假：限直系血親之喪或有特殊情誼經家長書面證明者，須於請假前檢附死亡證明或訃文等文件辦理請假手續，如情況特殊無法事先辦理請假手續時，經核准後始可事後補辦請假手續。

八、 不可抗力假：學生在上學途中交通臨時受阻或其他因不可抵抗之事件發生時應提出證件，始予核准不可抗力假。

九、 因微病或病後健康未復原或生理上之影響而不能參加術科或運動操作等得請求見習，但見習須至解散時，始得離開操場，否則仍以缺席論。

十、 請假理由及呈繳證明文件或家長印章如有虛構偽造等情事，除缺席之時數以曠課論外，並依情節之輕重議處。

十一、 請假期滿即須返校辦理銷假手續，如仍不能返校上課，家長來電續假，否則以曠課論。

十二、 在考試期間請假者，應先報教務處核准，再照章辦理請假手續，並須將請假單送教務處登記，以作日後補考依據。

十三、 學生在課間及午休期間遇有特殊事故須外出辦理時，先填妥臨時外出請假單經核准後，始得外出，次日銷假時需附臨時請假單辦理正式請假手續。

十四、 各班副班長於每天第一節下課到教官室填寫缺席學生名單~~，並通知家長~~。

十五、 每兩週由生活輔導組公佈各班學生缺曠及請假時數，如有錯誤應於公佈後三日內至生活輔導組更正，逾期概不受理。

十六、 落實點名制，請授課教師清點人數；導師班級幹部於集會、早讀、午休、升旗等活動時確實點名工作。學生事務處將不定期抽查，點名不確實之班級幹部予以議處。

十七、 學生請假應按照規定於請假系統~~在請假卡上~~填寫日期、節數、事由並夾帶證明檔案完成請假相關程序，~~填寫請假事由、日期及節數，經家長蓋章後~~，按級呈報不得越級申請。

十八、 學生請病假：

(一)因病無法到校請假，請家長先以電話或書信通知導師或學務處，病癒返校三日內，持就診證明，補辦請假。

(二)病假連續兩天以上時須持有醫師證明，連續六天(含)以上者須持有公立醫院或地區醫院以上診斷證明。

十九、 **病假**、產前假、娩假、流產假、育嬰假~~及生理假~~，應附呈相關就醫證明文件與**家長簽章證明**。事假、喪假及生理假，應附呈有關證明文件與**家長簽章證明**。

二十、 凡請假在三日以內者由導師轉生活輔導組核准,三日以上七日以內者送導師經生活輔導組由學務主任核准，七日以上者須轉呈校長核准。

二十一、凡因執行公務或代表學校參加校外競賽者，應於前一日**完成公假程序**，~~填妥公假單，經有關師長核准後送生活輔導組登記，否則以曠課論~~。如有特殊事故，最遲須於三日內完成請假手續。

~~第 22 條、凡請假經核准後，須將請假卡連同請假證明送生活輔導組登記，俟登記完畢蓋有「登記」字戳後發還。~~

~~第 23 條、本冊遺失，酌收工本費 50 元後補發。所收費用統一於學期末簽送會計室納入學校相關經費運用。~~

二十二、本規則經校務會議通過，校長核准後施行之。

附件 7

國立曾文高級家事商業職業學校 109 學年度第 1 學期行事曆簡表(草案)

週別	月份	星期 日	一	二	三	四	五	六	各處室重要行事
預備週	八	23	24	25	26	27	28	29	8/24-25 新生始業輔導 8/25 輔諮中心業務聯繫會議(上午)、特殊需求新生轉銜會議(第 8 節) 8/27 丙級技能檢定全國第三梯次報名 8/28 109 學年度期初學務會議(9:00)、期初實習會議(9:30)、期初校務會議(10:10)、教職員工急救研習(13:00-17:00)
第 1 週	八、九	30	31	1	2	3	4	5	8/31 開學日、下午正式上課 8/31-9/4 友善校園週教育宣導 9/1 閱讀心得比賽及小論文比賽投稿開始、多元學習中心課程開始 9/1-9/7 丙級技能檢定全國第三梯次報名 9/1-18 高一新生登入線上系統資料 9/2 校長叮嚀與學生活動分享(第 5 節)、全校迎新活動(6-7 節) 9/3 期初 IEP 9/4 108 學年度學習歷程檔案學生勾選截止日、學生輔導工作委員會議、家庭教育推動小組會議(第 8 節)、教室佈置比賽開始
第 2 週	九	6	7	8	9	10	11	12	9/1-9/7 丙級技能檢定全國第三梯次報名 9/1-18 高一新生登入線上系統資料 9/7 第 8 節輔導課開始、曾家藝樹園丁活動 9/9 班級經營暨教室佈置(5-6 節)、班會(第 7 節)
第 3 週	九	13	14	15	16	17	18	19	9/1-18 高一新生登入線上系統資料 9/14 109 年度國家防災日地震避難掩護預演、特殊教育推行委員會(中午) 9/16 環境教育講座-你所不知道的台灣「謎」猴(5-6 節)、班會(第 7 節)、幼保科寫故事比賽(第 7 節)
第 4 週	九	20	21	22	23	24	25	26	9/21 109 年度國家防災日地震避難掩護正式演練、輔導志工服務開始 9/21-22 高一公民教育訓練活動 9/23 認輔會議(中午)、教師節班際才藝競賽(第 5 節)、班會(第 6-7 節) 9/26 補行上班(補上 10/2)(本日 16:20 放學)
第 5 週	九.十	27	28	29	30	1	2	3	9/28-30 高三校外教學參觀活動 9/30 特教新生始業輔導(中午) 、性別平等暨愛滋防治講座(5-6 節)、班會(第 7 節)、教室佈置比賽結束評分 10/1 中秋節 10/2 調整放假
第 6 週	十	4	5	6	7	8	9	10	10/6 第 1 次段考試卷繳交截止日 10/6-7 全國高級中等學校實習工作會議 10/7 自主學習(5-6 節)、班會(第 7 節)、幼保科說故事比賽(6-7 節) 10/9 補假(國慶日) 10/10 國慶日、閱讀心得比賽投稿結束
第 7 週	十	11	12	13	14 ●	15 ●	16 ●	17	10/14-16 第 1 次段考 [10/14(週三)與 10/16(週五)下午課程對調] 10/14 第 1 次導師會議(第 8 節) 10/15 小論文比賽投稿截止 10/16 班際拔河比賽(5-7 節)、輔導管教暨特教知能研習(5-6 節) 10/17 親職座談會(上午)、親子工作坊(下午)

週別	月份	星期 日	一	二	三	四	五	六	各處室重要行事
第8週	十	18	19	20	21	22	23	24	10/19 學習診斷測驗開始實施 10/19-20 高三第 1 次學藝競賽 10/21 社團活動 1(5-6 節)、班會(第 7 節)、109 年校運籌備會(第 8 節) 10/23 第 1 次段考成績上傳截止
第9週	十	25	26	27	28	29	30	31	10/28 高二、高三自主學習(5-6 節)、高一軍校歌比賽(5-6 節) 、PVQC 校內賽(5-6 節)、班會(第 7 節)、高二實彈射擊行前說明會(第 7 節) 10/30 高二實彈射擊體驗(1-4 節)、輔諮中心團督 1
第10週	十一	1	2	3	4	5	6	7	11/2-6 一般科目作業檢查 11/4 社團活動 2 (5-6 節)、班會(第 7 節)
第11週	十一	8	9	10	11	12	13	14	11/9-13 專業科目作業檢查 11/10-12 109 學年度家事類全國技藝競賽 11/11 名人講座(5-6 節)、班會(第 7 節)、輔導管教暨特教知能研習(5-6 節)
第12週	十一	15	16	17	18	19	20	21	11/16 輔諮中心團督2 11/18 社團活動3 (5-6節)、班會(第7節) 11/20 輔諮中心團督 3、身障甄試說明會及報名(中午)
第13週	十一	22	23	24	25	26	27	28	11/23 第 2 次段考試卷繳交截止日 11/24 特教暨家庭教育宣導週 11/25 自主學習(5-6 節)、高一高二英文朗讀比賽(5-6 節)、班會(第 7 節)
第14週	十一.十二	29	30 ●	1 ●	2 ●	3	4	5	11/30-12/2 第 2 次段考 11/30 第 2 次導師會議(第 8 節) 12/1-3 109 學年度商業類全國技藝競賽 12/2 班際排球決賽(5-7 節)、109 年度下半年消防自衛編組訓練(全體教職員工) (6-7 節) 12/3 學生性平小團體 12/4 輔導知訊出刊
第15週	十二	6	7	8	9	10	11	12	12/9 第 2 次段考成績上傳截止(中午)、社團活動 4 (5-6 節)、班會(第 7 節) 12/10 109 年全校運動會預賽、預演 12/11 109 年全校運動會
第16週	十二	13	14	15	16	17	18	19	12/14 輔諮中心團督 4 12/16 社團活動 5 (5-6 節)、聖誕祈福點燈音樂饗宴活動(7-8 節) 12/17 週記抽查、學生性平小團體 2 12/17-18 高三第 2 次學藝競賽
第17週	十二	20	21	22	23	24	25	26	12/21 高一大考中心興趣量表開始實施、期末 IEP 開始 12/23 社團活動 6 (5-6 節)、藝樹園丁工作坊(第 5-7 節)、班會(第 7 節) 12/23-25 廣告科成果展
第8週	十二.一	27	28	29	30	31	1	2	12/30 幼保科成果展(第 1-4 節)、班會(第 5 節)、高一高二歲末感恩班際才藝競賽(6-7 節) 12/31 同儕輔導暨輔導志工聯誼活動(中午)、本日 16:20 放學 1/1 元旦

週別	月份	星期							各處室重要行事
		日	一	二	三	四	五	六	
第19週	一	3	4	5	6	7	8	9	1/6 班級經營暨感恩茶會(5-6 節)、班會(第 7 節) 1/8 期末考試卷繳交截止日、第 8 節輔導課結束
第20週	一	10	11	12	13	14	15 ●	16	1/10 校內 CSF 電腦技能檢定 1/13 自主學習(5-6 節)、班會(第 7 節)、第 1 學期期末暨第 2 學期期初實習會議(第 6 節) 1/15 -19 期末考 1/15 期末學務會議(第 8 節)
第21週	一	17	18 ●	19 ●	20	21	22	23	1/15 -19 期末考 1/19 除舊佈新大掃除(5-7 節) 1/20 休業式、第 1 學期期末暨第 2 學期期初校務會議
寒假	一	24	25	26	27	28	29	30	1/26 日常考、期末考、學期總成績上傳截止(中午)
寒假	二	31	1	2	3	4	5	6	2/1 公告補考名單 2/5 學期成績補考 2/8 補考成上傳截止

備註：□放假日 ●段考

國立曾文高級家事商業職業學校
資通安全維護計畫

目　　錄

壹、依據及目的

依據資通安全管理法第10條及施行細則第6條訂定資通安全維護計畫，作為資訊安全推動之依循及應符合其所屬資通安全責任等級之要求，訂定、修正及實施資通安全維護計畫(以下簡稱本計畫)。為因應資通安全管理法及資通安全責任等級應辦事項要求，以符合法令規定並落實本計畫之資通作業安全。

貳、適用範圍

本計畫適用範圍涵蓋國立曾文高級家事商業職業學校全機關（以下簡稱本校）

參、核心業務及重要性

一、 核心業務及重要性：

本校之核心業務及重要性如下表：

核心業務	核心資通系統	重要性說明	業務失效影響說明	最大可容忍中斷時間	資通系統分級
校務學生資料管理	校務行政系統	為本校依組織法執掌，足認為重要者	違反法遵義務：依個人資料保護法應善盡個人資料保護責任，如違反該法致足生損害他人者將依受罰。影響校務運作	24小時	中

各欄位定義：

1. 核心業務：請參考資通安全管理法施行細則第7條之規定列示。
2. 核心資通系統：該項業務內各項作業程序的名稱。

3. 重要性說明：說明該業務對機關之重要性，例如對機關財務及信譽上影響，對民眾影響，對社會經濟影響，對其他機關業務運作影響，法律遵循性影響或其他重要性之說明。

4. 業務失效影響說明：當系統失效時對學校所造成的衝擊及影響。

5. 最大可容忍中斷時間單位以小時計。

6. 資通系統分級：依據資通安全責任等級分級辦法附件九資通系統防護需求分級原則進行分級。

二、 非核心業務及說明：

本校之非核心業務及說明如下表：

非核心業務	業務失效影響	最大可容忍中斷時間	資通系統分級
公文系統	電子公文無法即時送達機關，影響機關行政效率	24小時	低
請購系統	教職員無法線上辦理各項請購業務，影響機關行政效率	24小時	低
差勤服務	教職員無法線上簽到退，影響機關行政效率	24小時	低
郵件服務	教職員信件無法收寄，影響機關行政效率	72小時	低

各欄位定義：

1. 非核心業務：公務機關之非核心業務至少應包含輔助單位之業務名稱，如差勤服務、郵件服務、用戶端服務等。

2. 業務失效影響：說明該業務失效對機關之影響。

3. 最大可容忍中斷時間單位以小時計。

4. 資通系統分級：依據資通安全責任等級分級辦法附件九資通系統防護需求分級原則進行分級。

肆、資通安全政策及目標

依本校「資通安全政策」如附件一施行。

伍、資通安全推動組織

依本校「資通安全組織」辦法如附件二成立資通安全委員會並成立資訊安全小組，「資通安全組織成員表」如附件三。

陸、專職(責)人力及經費配置

一、專職(責)人力及資源之配置

1. 依據行政院108年7月24日院臺護字第1080180748號函，依據資通安全責任等級分級辦法第6條辦理，並考量本校已有核心系統向上集中規劃，依同法第10條第4款調降等級為 D 級。在未完成向上集中前本校應設置資通安全專責人員，其業務內容如下，本校現有資通安全專責人員名單及職掌應表列於「資通安全組織成員表」如附件三，並適時更新。

   (1) 資通安全管理面業務，負責推動資通系統防護需求分級、資通安全管理系統導入及驗證、內部資通安全稽核及教育訓練等業務之推動。

   (2) 資通系統安全管理業務，負責資通系統分級及防護基準、安全性檢測、業務持續運作演練等業務之推動。

   (3) 資通安全防護業務，負責資通安全監控管理機制、資通安全防護設施建置及資通安全事件通報及應變業務之推動。

2. 本校之承辦單位於辦理資通安全人力資源業務時，應加強資通安全人員之培訓，並提升校內資通安全專責人員之資通安全管理能力。本校之相關單位於辦理資通安全業務時，如資通安全人力或經驗不足，得洽請相關學者專家或專業機關（構）提供顧問諮詢服務。

3. 資安專責人員專業職能之培養(如證書、證照、培訓紀錄等)，應參加主管機關辦理之相關專業研習，並鼓勵取得資通安全專業證照及資通安全職能評量證書。

4. 本校負責重要資通系統之管理、維護、設計及操作之人員，應妥適分工，分散權責，若負有機密維護責任者，應簽屬「保密切結書」如附件四，並視需要實施人員輪調，建立人力備援制度。

5. 校長及各級業務主管人員，應負責督導所屬人員之資通安全作業，防範不法及不當行為。

6. 專責人力資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

二、經費之配置

1. 資訊安全小組於規劃配置相關經費及資源時，應考量本校之資通安全政策及目標，並提供建立、實行、維持及持續改善資通安全維護計畫所需之資源。

2. 各單位於規劃建置資通系統建置時，應一併規劃資通系統之資安防護需求，並於整體預算中合理分配資通安全預算所佔之比例。

3. 各單位如有資通安全資源之需求，應配合機關預算規劃期程向資訊安全小組提出需求，由資訊安全小組視整體資通安全資源進行分配，並經資通安全長核定後，進行相關之建置。

4. 資通安全經費、資源之配置情形應每年定期檢討，並納入資通安全維護計畫持續改善機制之管理審查。

柒、資訊及資通系統之盤點

一、資訊及資通系統盤點

依本校「資訊資產管理」規定如附件五施行。

二、機關資通安全責任等級分級

依據行政院108年7月24日院臺護字第1080180748號函，依據資通安全責任等級分級辦法第6條辦理，並考量本校已有核心系統向上集中規劃，依同法第10條第4款調降等級為D級機關。

捌、資通安全風險評估

一、資通安全風險評估

依本校「風險評鑑與管理」規定如附件六施行。

二、核心資通系統及最大可容忍中斷時間

核心資通系統	資訊資產	核心資通系統主要功能	最大可容忍中斷時間
校務行政系統	1. 網站前台主機計1台	學籍管理、學生修課、出缺席、輔導狀	24小時

	2. 網站後台主機計1台 3. 骨幹網路交換器	況資料。	

最大可容忍中斷時間以小時計。

玖、資通安全防護及控制措施

本校依據前章資通安全風險評估結果、自身資通安全責任等級之應辦事項及核心資通系統之防護基準，採行相關之防護及控制措施如下:

一、資訊及資通系統之管理

依本校「資訊資產異動作業」規定如附件七施行。

二、存取控制與加密機制管理

依本校「存取控制管理」規定如附件八施行。

三、作業與通訊安全管理

依本校資通安全管理制度文件「實體安全管理」規定如附件九、「通信與作業管理」規定如附件十施行。

四、系統獲取、開發及維護

1. 本校之資通系統應依「資通安全責任等級分級辦法」附表九之規定完成系統防護需求分級，依分級之結果，完成附表十中資通系統防護基準，並注意下列事項：

(1) 開發過程請依安全系統發展生命週期(Secure Software Development Life Cycle, SSDLC)納入資安要求，並參考行政院國家資通安全會報頒布之最新「安全軟體發展流程指引」、「安全軟體設計指引」及「安全軟體測試指引」。

(2) 於資通系統開發前，設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾，並檢討執行情形。

(3) 於上線前執行安全性要求測試，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試，並檢討執行情形。

(4) 執行資通系統源碼安全措施，包含源碼存取控制與版本控管，並檢討執行情形。

2. 餘依本校「系統開發與維護」規定如附件十一施行。

五、 業務持續運作演練

本校應針對核心資通系統制定業務持續運作計畫，並每二年辦理一次核心資通系統持續運作演練。

六、執行資通安全健診

1. 本校每二年應辦理資通安全健診，其至少應包含下列項目，並檢討執行情形：

(1) 網路架構檢視。

(2) 網路惡意活動檢視。

(3) 使用者端電腦惡意活動檢視。

(4) 伺服器主機惡意活動檢視。

(5) 安全設定檢視。

七、 資通安全防護設備

1. 本校應建置防毒軟體、網路防火牆、電子郵件過濾裝置，持續使用並適時進行軟、硬體之必要更新或升級。

2. 資安設備應定期備份日誌紀錄，定期檢視並由主管複核執行成果，並檢討執行情形。

壹拾、資通安全事件通報、應變及演練相關機制

為即時掌控資通安全事件，並有效降低其所造成之損害，本校應訂定資通安全事件通報、應變及演練相關機制，詳如附件十二「資通安全事件通報應變程序」。

壹拾壹、資通安全情資之評估及因應

本校接獲資通安全情資，應評估該情資之內容，並視其對本校之影響、本校可接受之風險及本校之資源，決定最適當之因應方式，必要時得調整資通安全維護計畫之控制措施，並做成紀錄。

一、資通安全情資之分類評估

本校接受資通安全情資後，應指定資通安全專職人員進行情資分析，並依據情資之性質進行分類及評估，情資分類評估如下：

(一) 資通安全相關之訊息情資

資通安全情資之內容如包括重大威脅指標情資、資安威脅漏洞與攻擊手法情資、重大資安事件分析報告、資安相關技術或議題之經驗分享、疑似存在系統弱點或可疑程式等內容，屬資通安全相關之訊息情資。

(二) 入侵攻擊情資

資通安全情資之內容如包含特定網頁遭受攻擊且證據明確、特定網頁內容不當且證據明確、特定網頁發生個資外洩且證據明確、特定系統遭受入侵且證據明確、特定系統進行網路攻擊活動且證據明確等內容，屬入侵攻擊情資。

(三) 機敏性之情資

資通安全情資之內容如包含姓名、出生年月日、國民身份證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病例、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接識別之個人資料，或涉及個人、法人或團體營業上秘密或經營事業有關之資訊，或情資之公開或提供有侵害公務機關、個人、法人或團體之權利或其他正當利益，或涉及一般公務機密、敏感資訊或國家機密等內容，屬機敏性之情資。

(四) 涉及核心業務、核心資通系統之情資

資通安全情資之內容如包含機關內部之核心業務資訊、核心資通系統、涉及關鍵基礎設施維運之核心業務或核心資通系統之運作等內容，屬涉及核心業務、核心資通系統之情資。

二、資通安全情資之因應措施

本校於進行資通安全情資分類評估後，應針對情資之性質進行相應之措施，必要時得調整資通安全維護計畫之控制措施。

(一) 資通安全相關之訊息情資

由資訊安全小組彙整情資後進行風險評估，並依據資通安全維護計畫之控制措施採行相應之風險預防機制。

(二) 入侵攻擊情資

由資通安全專職(責)人員判斷有無立即之危險，必要時採取立即之通報應變措施，並依據資通安全維護計畫採行相應之風險防護措施，另通知各單位進行相關之預防。

(三) 機敏性之情資

就涉及個人資料、營業秘密、一般公務機密、敏感資訊或國家機密之內容，應採取遮蔽或刪除之方式排除，例如個人資料及營業秘密，應以遮蔽或刪除該特定區段或文字，或採取去識別化之方式排除之。

(四) 涉及核心業務、核心資通系統之情資

資訊安全小組應就涉及核心業務、核心資通系統之情資評估其是否對於機關之運作產生影響，並依據資通安全維護計畫採行相應之風險管理機制。

壹拾貳、資通系統或服務委外辦理之管理

本校委外辦理資通系統之建置、維運或資通服務之提供時，應考量受託者之專業能力與經驗、委外項目之性質及資通安全需求，選任適當之受託者，並監督其資通安全維護情形。

一、選任受託者應注意事項

1. 受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。
2. 受託者應配置充足且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗之資通安全專業人員。
3. 受託者辦理受託業務得否複委託、得複委託之範圍與對象，及複委託之受託者應具備之資通安全維護措施。

二、監督受託者資通安全維護情形應注意事項

1. 受託業務包括客製化資通系統開發者，受託者應提供該資通系統之第三方安全性檢測證明；涉及利用非自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。
2. 受託者執行受託業務，違反資通安全相關法令或知悉資通安全事件時，應立即通知委託機關及採行之補救措施。

3. 委託關係終止或解除時，應確認受託者返還、移交、刪除或銷毀履行委託契約而持有之資料。

4. 與委外廠商簽訂契約時，應審查契約中保密條款，並要求委外廠商之業務執行人員簽署委外廠商執行人員保密切結書、保密同意書，格式如：附件十三「委外廠商執行人員保密切結書」、附件十四「委外廠商執行人員保密同意書」。

5. 本校應定期或於知悉受託者發生可能影響受託業務之資通安全事件時，以本校「委外廠商查核項目表」如附件十五進行稽核以確認受託業務之執行情形。

壹拾參、資通安全教育訓練

一、資通安全教育訓練要求

1. 本校資安及資訊人員每年至少接受12小時以上之資安專業課程訓練或資安職能訓練。

2. 本校之一般使用者與主管，每人每年接受3小時以上之一般資通安全教育訓練。

二、資通安全教育訓練辦理方式

1. 資通安全小組應於每年年初，考量管理、業務及資訊等不同工作類別之需求，擬定資通安全教育訓練計畫，以建立教職員生資通安全認知，提升機關資通安全水準，並應保存相關之資通安全認知宣導及教育訓練紀錄（如：「教育訓練簽到表」）。

2. 本校資通安全認知宣導及教育訓練之內容得包含：

(1) 資通安全政策(含資通安全維護計畫之內容、管理程序、流程、要求事項及人員責任、資通安全事件通報程序等)。

(2) 資通安全法令規定。

(3) 資通安全作業內容。

(4) 資通安全技術訓練。

3. 教職員報到時，應使其充分瞭解本校資通安全相關作業規範及其重要性。

4. 資通安全教育及訓練之政策，除適用所屬教職員生外，對機關外部的使用者，亦應一體適用。

壹拾肆、公務機關所屬人員辦理業務涉及資通安全事項之考核機制

本校所屬人員之平時考核或聘用，依據公務機關所屬人員資通安全事項獎懲辦法、本校公務人員平時獎懲標準表及各相關規定辦理之。

壹拾伍、資通安全維護計畫及實施情形之持續精進及績效管理機制

一、資通安全維護計畫之實施

為落實本安全維護計畫，使本校之資通安全管理有效運作，相關單位於訂定各階文件、流程、程序或控制措施時，應與本校之資通安全政策、目標及本安全維護計畫之內容相符，並應保存相關之執行成果記錄。

二、資通安全維護計畫實施情形之稽核機制

(一) 稽核機制之實施

1. 資訊安全稽核小組應定期(至少每二年一次)或於系統重大變更或組織改造後執行一次內部稽核作業，以確認人員是否遵循本規範與機關之管理程序要求，並有效實作及維持管理制度。

2. 辦理稽核前資通安全小組應擬定「內部稽核計畫」如附件十六並安排稽核成員，稽核計畫應包括稽核之依據與目的、期間、重點領域、稽核小組組成方式、保密義務（稽核委員簽署「保密切結書」如附件四）、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核之結果納入稽核範圍。

3. 辦理稽核時，資訊安全稽核小組應於執行稽核前30日，通知受稽核單位，並將稽核期程、「稽核項目紀錄表」如附件十七及稽核流程等相關資訊提供受稽單位。

4. 本校之稽核人員應受適當培訓並具備稽核能力，且不得稽核自身經辦業務，以確保稽核過程之客觀性及公平性；另，於執行稽核時，應填具稽核項目紀錄表，待稽核結束後，應將稽核項目紀錄表內容彙整至「內部稽核報告」如附件十八中，並提供給受稽單位填寫辦理情形。

5. 稽核結果應對相關管理階層(含資通安全執行秘書)報告，並留存稽核過程之相關紀錄以作為資通安全稽核計畫及稽核事件之證據。

6. 稽核人員於執行稽核時，應至少執行一項特定之稽核項目（如

是否瞭解資通安全政策及應負之資安責任、是否訂定人員之資通安全作業程序與權責、是否定期更改密碼)。

(二) 稽核改善報告

1. 受稽單位於稽核實施後發現有缺失或待改善項目者，應對缺失或待改善之項目研議改善措施、改善進度規劃，並落實執行。
2. 受稽單位於稽核實施後發現有缺失或待改善者，應判定其發生之原因，並評估是否有其類似之缺失或待改善之項目存在。
3. 受稽單位於判定缺失或待改善之原因後，應據此提出並執行相關之改善措施及改善進度規劃，必要時得考量對現行資通安全管理制度或相關文件進行變更。
4. 機關應定期審查受稽單位缺失或待改善項目所採取之改善措施、改善進度規劃及佐證資料之有效性。
5. 受稽單位於執行改善措施時，應留存相關之執行紀錄，並填寫稽核結果及改善報告。

三、 資通安全維護計畫之持續精進及績效管理

1. 本校之資通安全委員會應於二、十月(每年至少二次)召開資通安全管理審查會議，確認資通安全維護計畫之實施情形，確保其持續適切性、合宜性及有效性。
2. 管理審查議題應包含下列討論事項：
   (1) 過往管理審查議案之處理狀態。
   (2) 與資通安全管理系統有關之內部及外部議題的變更，如法令變更、上級機關要求、資通安全推動小組決議事項等。
   (3) 資通安全維護計畫內容之適切性。
   (4) 資通安全績效之回饋，包括：
      A. 資通安全政策及目標之實施情形。
      B. 資通安全人力及資源之配置之實施情形。
      C. 資通安全防護及控制措施之實施情形。
      D. 稽核結果。
      E. 不符合項目及矯正措施。

(5) 風險評鑑結果及風險處理計畫執行進度。

(6) 重大資通安全事件之處理及改善情形。

(7) 利害關係人之回饋。

(8) 持續改善之機會。

3. 持續改善機制之管理審查應做成「矯正與預防處理單」如附件十八，相關紀錄並應予保存，以作為管理審查執行之證據。

壹拾陸、資通安全維護計畫實施情形之提出

本校依據資通安全法第12條之規定，應於十月前向上級或監督機關，填報「資通安全維護計畫實施情形」，使其得瞭解本校之年度資通安全計畫實施情形。

壹拾柒、相關法規、程序及表單

一、相關法規及參考文件

1. 資通安全管理法
2. 資通安全管理法施行細則
3. 資通安全責任等級分級辦法
4. 資通安全事件通報及應變辦法
5. 資通安全情資分享辦法
6. 公務機關所屬人員資通安全事項獎懲辦法
7. 資訊系統風險評鑑參考指引
8. 政府資訊作業委外安全參考指引
9. 無線網路安全參考指引
10. 網路架構規劃參考指引
11. 行政裝置資安防護參考指引
12. 政府行動化安全防護規劃報告
13. 安全軟體發展流程指引
14. 安全軟體設計指引

15. 安全軟體測試指引

16. 資訊作業委外安全參考指引

二、附件資料表單

附件一：資訊安全政策
附件二：資訊安全組織
附件三：資訊安全組織成員表
附件四：保密切結書
附件五：資訊資產管理
附件六：風險評鑑與管理
附件七：資訊資產異動作業
附件八：存取控制管理
附件九：實體安全管理
附件十：通信與作業管理
附件十一：系統開發與維護
附件十二：資通安全事件通報及應變程序
附件十三：委外廠商執行人員保密切結書
附件十四：委外廠商執行人員保密同意書
附件十五：委外廠商查核項目表
附件十六：內部稽核計畫
附件十七：稽核項目紀錄表
附件十八：內部稽核報告
附件十九：矯正與預防處理單

國立曾文高級家事商業職業學校

資通安全政策

機密等級：一般

文件編號：TWVS-ISMS-A-001

版 次：2.0

發行日期：109.04.28

修 訂 紀 錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	102.11.26		文管人員	初版
2.0	109.04.28		文管人員	二版

資通安全政策					
文件編號	TWVS-ISMS-A-001	機密等級	一般	版次	2.0

目　錄

資通安全政策					
文件編號	TWVS-ISMS-A-001	機密等級	一般	版次	2.0

1 目的

為確保國立曾文家事商業職業學校（以下簡稱本校）所屬之資訊資產的機密性、完整性、可用性及符合相關法規之要求，導入資訊安全管理系統，強化本校資訊安全管理，保護資訊資產免於遭受內、外部蓄意或意外之威脅，維護資料、系統、設備及網路之安全，提供可靠之資訊服務，訂定本政策。

2 依據

2.1 資通安全法(及施行細則)

2.2 個人資料保護法（及施行細則）

2.3 行政院及所屬各機關資訊安全管理要點

2.4 教育體系資通安全暨個人資料管理規範

3 適用範圍

3.1 本政策適用範圍為本校之全體人員、委外服務廠商與訪客等。

3.2 資訊安全管理範疇涵蓋 14 項領域，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本校造成各種可能之風險及危害，各領域分述如下：

3.2.1 資訊安全政策訂定與評估。

3.2.2 資訊安全組織。

3.2.3 人力資源安全。

3.2.4 資產管理。

3.2.5 存取控制。

3.2.6 密碼學(加密控制)。

3.2.7 實體及環境安全。

3.2.8 運作安全。

3.2.9 通訊安全。

3.2.10 系統獲取、開發及維護。

3.2.11 供應者關係。

3.2.12 資訊安全事故管理。

3.2.13 營運持續管理之資訊安全層面。

3.2.14 遵循性。

4 目標

維護本校資訊資產之機密性、完整性與可用性，並保障使用者資料隱私。藉由本校全體同仁共同努力來達成下列定性及定量目標：

4.1 定性目標：

4.1.1 確保相關資通安全措施或規範符合政策與現行法令的要求每年至少進行一次內部稽核。

4.1.2 每年至少進行一次業務持續計畫之測試或檢核。

4.2 定量目標：

4.2.1 確保資訊資產受適當之保護,每年未經授權或因作業疏失對資產所造成的損害 0 件。

4.2.2 確保所有資通安全事件或可疑之安全弱點,每年不依適當通報程序反應，並予以適當的調查及處理 0 件。

4.2.3 符合政府資通安全相關政策、規訂及相關法令要求。

4.2.4 定期實施資通安全教育訓練。

4.3 本校完成指標時，考量下列項目：

4.3.1 所需配置之人員、預算、設備技術與程序表單。

4.3.2 活動或事項負責人員。

4.3.3 活動或事項預計完成時間。

4.3.4 管理目標是否達成之評估方式。

5 責任

5.1 本校應成立資訊安全組織統籌資訊安全事項推動。

5.2 管理階層應積極參與及支持資訊安全管理制度,並授權資訊安全組織透過適當的標準和程序以實施本政策。

5.3 本校全體人員、委外服務廠商與訪客等皆應遵守相關安全管理程序以維護

本政策。

5.4 本校全體人員及委外服務廠商均有責任透過適當通報機制，通報資訊安全事件或弱點。

5.5 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本校之相關規定進行議處。

6 審查

本政策應每年至少審查乙次，以反映政府法令、技術及業務等最新發展現況及關注方之關注議題，以確保本校資訊安全管理制度之運作。

7 實施

本政策經「資通安全委員會」核定後實施，修訂時亦同。

國立曾文高級家事商業職業學校

資通安全組織程序書

機密等級：限閱

文件編號：TWVS-ISMS-B-001

版 次：2.0

發行日期：109.04.28

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	102.11.26		文管人員	初版
2.0	109.04.28		文管人員	二版

目錄

資通安全組織程序書					
文件編號	TWVS-ISMS-B-001	機密等級	一般	版次	2.0

1 目的

確保 XXXX（以下簡稱「本校」）資通安全管理制度之資通安全責任，落實資通安全政策之推行，並符合下列「教育體系資通安全管理暨個人資料保護規範」之控制目標：

1.1 為確保本校內部資通安全管理事項之推動，應建立適當管理架構，以審核資通安全政策、分配安全責任，並協調本校各項資通安全措施之實施。

1.2 建立與外部資通安全專家之聯繫管道，以利於安全事件處理及專家意見徵詢。

2 適用範圍

本校承辦之資通安全制度相關業務作業流程。

3 權責

無。

4 名詞定義

無。

5 作業說明

5.1 建立組織全景

5.1.1 應依據行政管理會議(如主管會報、行政會議或校務會議等校內行政管理會議)中有關資訊安全暨個人資料保護需求決議事項，或上級機關來文要求事項進行評估，並據此建立或調整管理範圍與目標。

5.1.2 應依據相關法令要求、行政院及教育主管機關所下達之重要決定或指導(包括主管機關之行政指導、重要會議決議事項等)、組織透過相關會議所做成之決議(包括主管會報、行政會議或校務會議等)，針對

管理制度之維護需求進行評估，並據此建立或調整相關之管理範圍與目標。

5.1.3 應依據決議事項確認與該事項有關之利害相關團體及其要求，並留存文件化紀錄。

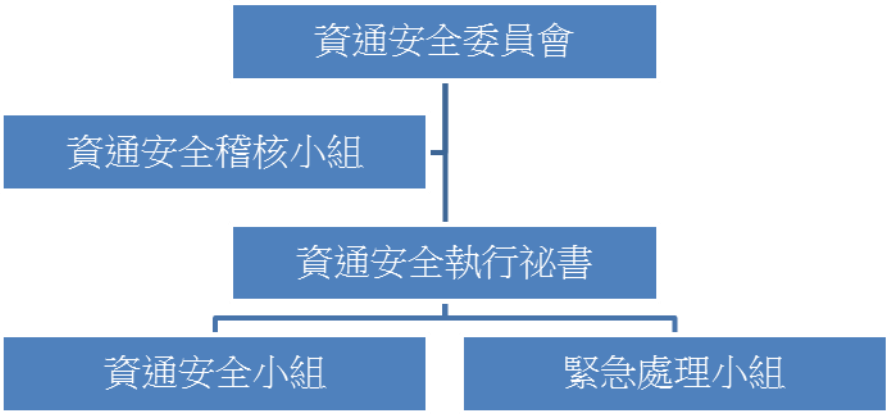
5.1.4 上述事項之識別與分析應每年至少審查一次，或於發生下列事件後重新檢視，並供管理審查時評估管理制度及其適用範圍調整之必要性。

5.1.4.1 組織重大變更後三月內。

5.1.4.2 新業務建立前或執行後一個月內。

5.2 資通安全組織架構與工作執掌

5.2.1資通安全組織架構如下圖所示，資通安全組織成員應填寫於「資通安全組織成員表」，若遇人員異動應加以更新。



5.2.2資通安全委員會：由本校校長擔任召集人，各單位一級主管（含祕書）、主任教官、設備組長、各科主任及電腦技士為委員會委員，負責資通安全管理制度相關事項之決議。

5.2.3

5.2.3.1 每年定期或視需要召開會議，審查資通安全管理相關事宜。

5.2.3.2 視需要召開跨單位之資源協調會議，負責協調資通安全管理制度執行所需之相關資源分配。

5.2.4資通安全執行秘書：由資通安全委員會召集人指派專人擔任。

5.2.4.1 負責協調資通安全小組與緊急處理組執行資通安全相關作業。

5.2.4.2 負責對資通安全狀況進行預警、監控，並對資通安全狀況與事件進行處置。

5.2.4.3 對於資通安全管理之改善提出建議，以及協助執行資通安全之自我檢核。

5.2.4.4 對於存取控制管理定期進行事件紀錄檢核，以及管理程序檢核。

5.2.5資通安全小組：由資通安全委員會召集人指派人員組成，負責規劃及執行各項資通安全作業。

5.2.5.1 制定資通安全管理相關規範。

5.2.5.2 推動資通安全相關活動。

5.2.5.3 辦理資通安全相關教育訓練。

5.2.5.4 建立風險管理制度，執行風險管理。

5.2.5.5 建立安全事件緊急應變暨復原措施。

5.2.5.6 執行稽核改善建議事項。

5.2.5.7 執行預防措施之改善。

5.2.5.8 研討新資通安全產品或技術。

5.2.5.9 執行資通安全委員會決議事項。

5.2.5.10 鑑別資通安全相關之法規。

5.2.5.10.1 資通安全小組應針對本校所提供之資訊服務，識別資通安全相關法令、法規及相關要求，明確定義至「外來文件一覽表」中，並定期檢討與更新。

5.2.6緊急處理小組：緊急處理組為任務編組，由資通安全委員會召集人

指派人員組成。成員相關權責及作業內容分述如下：

5.2.6.1 緊急處理組組長：

5.2.6.1.1 當重大資安事件發生時，負責聯絡及召集緊急處理組。

5.2.6.1.2 協調及督導各關鍵業務流程負責人執行作業，並協調資源之調派使用。

5.2.6.1.3 依據事件評估之結果，得依現況建請資通安全委員會召集人決議是否宣布災變並啟動業務永續運作計畫。

5.2.6.1.4 當災變發生時，配合救災單位負責搶救人員、物資與設備等，以及現場指揮工作。

5.2.6.1.5 負責災後協調、指揮清理災害現場。

5.2.6.1.6 負責規劃原營運場所之現場復原工作。

5.2.6.2 各關鍵業務流程負責人員：

5.2.6.2.1 負責召集相關人員，發展、維護、更新修訂及執行各災害復原程序。

5.2.6.2.2 每年負責召集相關人員進行業務永續運作計畫之測試演練。

5.2.6.2.3 負責原營運場所或異地備援場所之應變、處理、復原及運轉測試工作。

5.2.6.2.4 負責災害現場證據收集,俾利未來訴訟與損害求償事宜。

5.2.6.2.5 災害現場評估損害狀況及執行原營運場所之現場復原工作。

5.2.7資通安全稽核小組：由資通安全委員會召集人指派，負責評估資通安全管理制度之執行情形。

5.2.7.1 擬定資通安全內部稽核計畫。

5.2.7.2 執行資通安全內部稽核。

5.2.7.3 撰寫資通安全內部稽核報告。

5.2.7.4 追蹤不符合事項之改善執行情形。

5.3 管理審查會議

5.3.1資通安全委員會應每年至少召開一次管理審查會議，必要時得召開臨時會議。

5.3.2管理審查會議審查內容建議如下：

5.3.2.1 資通安全稽核結果及建議改善事項。

5.3.2.2 上級指導單位、內部同仁及外部單位等利害相關團體的建議。

5.3.2.3 新資通安全產品或技術導入之審查。

5.3.2.4 矯正及預防措施檢討。

5.3.2.5 風險評鑑適切性審查。

5.3.2.6 前次管理審查會議決議執行狀況。

5.3.2.7 影響資通安全制度之任何變更事項。

5.3.2.8 資通安全組織成員所提出之改善建議。

5.3.2.9 資通安全目標執行狀況報告。

本校依據「資通安全政策」所列之範圍及目標制定「ISMS有效性量測表」,並以該量測結果做為評估本校資通安全目標達成情形。

5.3.3管理審查會議之結論建議如下：

5.3.3.1 資通安全制度執行之各項改進措施。

5.3.3.2 更新風險評鑑與風險改善計畫。

5.3.3.3 針對可能影響資通安全制度之內、外部事件，修正資通安全管理流程與控制措施，包括：

5.3.3.3.1 營運需求的變更。

5.3.3.3.2 安全需求的變更。

5.3.3.3.3 影響現行營運需求的業務程序變更。

5.3.3.3.4 管理或法規需求的變更。

5.3.3.3.5 契約要求的變更。

5.3.3.3.6 可接受風險等級或標準的變更。

5.3.3.4 針對資通安全制度之需要，協調所需之資源。

5.3.3.5 控制措施有效性評量方式的改善。

應每年檢視「ISMS 有效性量測表」之量測結果與執行情形，並檢討量測項目與目標水準是否需進行調整之必要，做成改善決議。

5.3.4管理審查紀錄

管理審查會議為資通安全管理制度重要之活動，「資通安全管理審查會議紀錄」應依「文件管理程序書」辦理。

5.4 權責機關、特殊利害相關團體的聯繫

5.4.1為確保資訊安全、個人資料保護事件發生時，儘速執行事件處理，須與權責或外部單位隨時保持聯繫，例如：主管機關、資通安全會報、消防單位等；並建立與管理制度相關之「外部單位聯絡清單」。

5.4.2應隨時與資訊安全、個人資料保護技術相關團體維持聯繫，獲取相關之技術及產品資訊與知識，以及處理相關事件或執行系統修補資訊等，亦將資訊建立於「外部單位聯絡清單」。

5.4.3「外部單位聯絡清單」由各單位自行建立與保管，或以任何可行之方式保存之。

須建立與資通安全管理制度相關之「外部單位聯絡清單」，並由資通安全小組負責維護及更新。

5.5 法規遵循性

5.5.1識別適用之法令、法規

「資通安全小組」應定期識別管理制度適用之法令、 法規，並彙整或修訂於「外來文件一覽表」。

5.5.2智慧財產權

員工應遵守智慧財產權等相關法令，並依據本校軟體管理相關 規定辦理。為確保員工均遵守智慧財產權，於稽核時，將一併 查核軟體使用情形。

5.5.3個人資訊的資料保護與隱私

員工應遵守個人資料保護法、行政院所屬各機關資訊安全管理 要點及相關規定。

5.5.4組織紀錄的保護

紀錄依紀錄型式進行分類(例如：變更紀錄、資料庫紀錄、錯誤 日誌、稽核日誌和運作程序)，訂定保存期間和儲存媒體型式(例 如：紙張、磁片、磁帶、硬碟或光碟片等儲存媒體)。並應依據 資訊等級進行適當地處置與保護。

6 相關文件

6.1 資通安全政策。

6.2 文件管理程序書。

6.3 資通安全組織成員表。

6.4 外來文件一覽表。

6.5 外部單位聯絡清單。

6.6 ISMS 有效性量測表。

6.7 資通安全管理審查會議紀錄。

資通安全組織成員表					
文件編號	TWVS-ISMS-D-001	機密等級	限閱	版次	2.0

紀錄編號：　　填表日期：109 年 04 月 28 日

職務	職稱	姓名	電話	手機	電子郵件
資通安全委員會					
召集人	校長	陳藝昕	100		twvs0101@twvs.tn.edu.tw
委員	教務主任	邱鴻錦	201		twvs0201@twvs.tn.edu.tw
委員	學務主任	顏嘉良	301		twvs0301@twvs.tn.edu.tw
委員	總務主任	劉士嘉	501		twvs0501@twvs.tn.edu.tw
委員	實習主任	李佳珍	601		twvs0601@twvs.tn.edu.tw
委員	輔導主任	陳姵慈	701		twvs0701@twvs.tn.edu.tw
委員	圖書館主任	洪思農	661		twvs0711@twvs.tn.edu.tw
委員	人事主任	吳瑞禎	104		twvs0801@twvs.tn.edu.tw
委員	主計主任	廖家宏	106		twvs0901@twvs.tn.edu.tw
委員	秘書	黃淑蘭	101		twvs0102@twvs.tn.edu.tw
委員	主任教官	吳昭震	302		twvs0302@twvs.tn.edu.tw
委員	商業經營科主任	王介伶	604		twvs0604@twvs.tn.edu.tw
委員	餐飲管理科主任	王舜皇	605		twvs0605@twvs.tn.edu.tw
委員	資料處理科主任	黃佩純	602		twvs0607@twvs.tn.edu.tw
委員	幼兒保育科主任	許滋芸	606		twvs0606@twvs.tn.edu.tw

委員	廣告科主任	洪嘉南	606		twvs0609@twvs.tn.edu.tw
委員	資訊技士	胡忠志	608		twvs0610@twvs.tn.edu.tw
資通安全執行秘書					
資通安全執行祕書	教務主任	邱鴻錦	201		twvs0201@twvs.tn.edu.tw
資通安全小組					
組長	教務主任	邱鴻錦	201		twvs0201@twvs.tn.edu.tw
組員	設備組長	孔祥櫻	209		twvs0204@twvs.tn.edu.tw
組員	資訊專長教師				
組員	資訊技士	胡忠志	608		twvs0610@twvs.tn.edu.tw
資通安全稽核小組					
組長	祕書	黃淑蘭	101		twvs0102@twvs.tn.edu.tw
組員	人事主任	吳瑞禎	104		twvs0801@twvs.tn.edu.tw
組員	具稽核專長之專業人員	李建法	608		twvs703@twvs.tn.edu.tw
緊急處理小組					
組長	教務主任	邱鴻錦	201		twvs0201@twvs.tn.edu.tw
組員	設備組長	孔祥櫻	209		twvs0204@twvs.tn.edu.tw
組員	資訊技士	胡忠志	608		twvs0610@twvs.tn.edu.tw

保密切結書					
文件編號	TWVS-ISMS-D-016	機密等級	機密	版次	1.0

紀錄編號：

本人 _____ 將嚴守工作保密規定與國家相關法令對業務機密負完全保密之責，並尊重智慧財產權。絕不擅自洩漏、傳播職務上任何業務相關資料及任職期間經辦、保管或接觸之所有須保密訊息資料；絕不擅自複製、傳播任何侵害智慧財產權之任何程式、軟體。保密之義務，不因調職或離職而終止。如有違反，依法負刑事、民事及行政責任。

此致

國立曾文高級家事商業職業學校

立 同 意 書 人：_____

身 分 證 字 號：_____

電　　話：_____

地　　址：_____

中　華　民　國　　年　　月　　日

國立曾文高級家事商業職業學校

資訊資產管理程序書

機密等級：限閱

文件編號：TWVS-ISMS-B-003

版 次：2.0

發行日期：109.04.28

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	102.11.26		文管人員	初版
2.0	109.04.28		文管人員	二版

目錄

資訊資產管理程序書					
文件編號	TWVS-ISMS-B-003	機密等級	限閱	版次	2.0

1 目的

建立國立曾文家事商業職業學校（以下簡稱「本校」）資訊資產管理規範，訂定資訊資產分類、分級、價值評估、標示及處理之遵循原則，並據以辦理各項資訊資產管理及作業方法。用以保護各類資訊資產，避免因人為疏失、蓄意或自然災害等風險所造成之傷害。

2 適用範圍

本校承辦相關資訊業務作業流程之資訊資產。

3 權責

3.1 資通安全執行祕書：

負責定期審議資訊資產清單及價值評估結果，並督導相關活動之進行。

3.2 資通安全小組：

負責定期辦理資訊資產異動調查與彙整，提供最新之資訊資產清單，並陳報資通安全委員會。

3.3 資訊資產權責單位：

負責所管轄內資訊資產之存取授權，並評估與審核資訊資產分類分級及價值之結果，得另指定資訊資產保管單位。

3.4 資訊資產保管單位：

對於指定資訊資產，具有落實資訊資產權責單位所委託之保護管理責任。

3.5 資訊資產使用單位：

對於資訊資產之使用，必須依據權責單位要求，並具有正確使用操作之責任。

4 名詞定義

4.1 機密性（Confidentiality）

確保只有經授權的人，才可以存取資訊。

4.2 完整性（Integrity）

確保資訊與處理方法的正確性與完整性。

4.3 可用性（Availability）

確保經授權的使用者在需要時可以取得資訊及相關資產。

4.4 資訊資產權責單位

對該項資訊資產具有判斷資產價值、決定存取權限或新增、刪除、修改權限之單位，同時也是資訊資產的擁有單位。

4.5 資訊資產保管單位：

依據權責單位之需求標準，執行資訊資產日常保護、異動與維護之執行單位。

4.6 資訊資產使用單位：

因業務需求，經授權可直接或間接使用該資訊資產之單位。

5 作業說明

5.1 資訊資產鑑別

5.1.1各資訊資產權責單位應鑑別所管轄之資訊資產，並建立「資訊資產清單」。

5.1.2各資訊資產權責單位應定期更新與維護所管轄之資訊資產清單。

5.1.3資訊資產清單由各權責單位提供，資通安全小組負責彙整，並陳報至資通安全委員會，以確保資訊資產編號及清單之完整性。

5.2 資訊資產分類

5.2.1資訊資產依其性質不同，分為 7 類：人員、文件、軟體、通訊、硬

體、資料、環境。

5.2.1.1 人員（People / PE）：包含全體同仁，以及委外廠商。

5.2.1.2 文件（Document / DC）：以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫等紙本文件。

5.2.1.3 軟體（Software / SW）：作業系統、應用系統程式、套裝軟體等，包含原始程式碼、應用程式執行碼、資料庫等。

5.2.1.4 通訊（Communication / CM）：網路設備、網路安全設備、提供資訊傳輸、交換之線路或服務。

5.2.1.5 硬體（Hardware / HW）：主機設備等相關硬體設施。

5.2.1.6 資料（Data / DA）：儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。

5.2.1.7 環境（Environment / EV）：相關基礎設施及服務，包含辦公室實體、實體機房、電力、消防設施等。

5.2.2各類資訊資產機密等級分為 4 級：一般、限閱、敏感、機密。各等級之評估標準如下：

5.2.2.1 一般：無特殊之機密性要求，可對外公開之資訊。

5.2.2.2 限閱：僅供組織內部人員或被授權之單位及人員使用。

5.2.2.3 敏感：僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用。

5.2.2.4 機密：為組織、主管機關或法律所規範之機密資訊。

5.2.3資訊資產之機密等級應定期審核，視實際需要予以調整。

5.2.4不同等級之資訊資產合併使用或處理時，以其中最高之等級為機密等級。

5.3 資訊資產價值鑑別

5.3.1資訊資產權責單位應鑑別其所管轄內所有資訊資產之價值。

5.3.2資訊資產價值除考量資訊資產機密等級之外，尚需考量資訊資產之可用性及完整性，其評估標準如下：

5.3.2.1 機密性評估標準

評估標準	數值
此資訊資產無特殊之機密性要求	1
此資訊資產僅供組織內部人員或被授權之單位及人員使用	2
此資訊資產僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用	3
此資訊資產所包含資訊為組織或法律所規範的機密資訊	4

5.3.2.2 完整性評估標準

評估標準	數值
該資訊資產本身完整性要求極低	1
該資訊資產本身具有完整性要求，當完整性遭受破壞時，不會對組織造成傷害	2
該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，但不至於太嚴重	3
該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，甚至造成業務終止	4

5.3.2.3 可用性評估標準

評估標準	數值
該資訊資產可容許失效3工作天以上	1
該資訊資產可容許失效8工作小時以上，3工作天以下	2
該資訊資產僅容許失效4工作小時以上，8工作小時以下	3
該資訊資產僅容許失效4工作小時以下	4

5.3.2.4 資訊資產價值之決定將依據資訊資產之機密性、完整性及可用性評估之後，取 3 者之最大值以為資訊資產之價值。

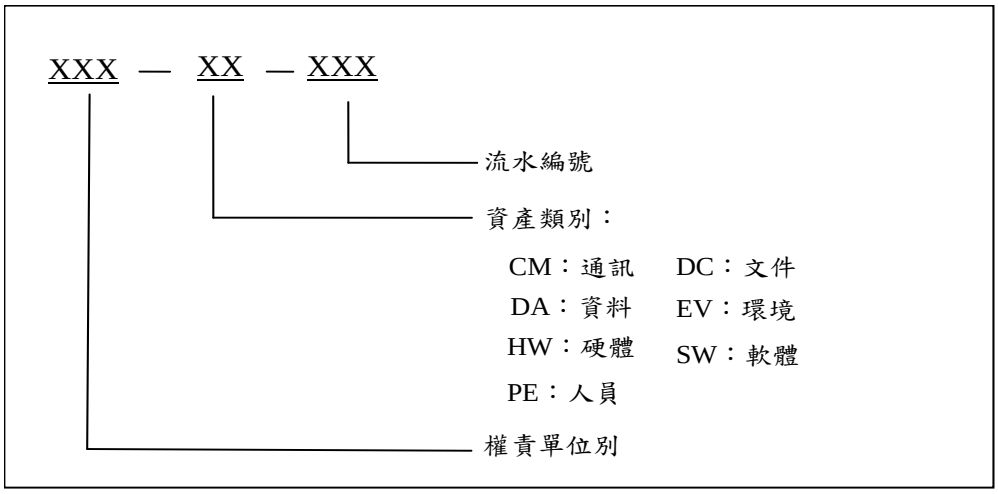
5.4 資訊資產清單及價值確認

5.4.1資訊資產權責單位應依據資訊資產清單之機密性、可用性及完整性之評估標準，確認資產價值。

5.4.2資訊資產清單及價值評估結果，應陳報至資通安全委員會審議。

5.5 資訊資產編號及標示

5.5.1除「資通安全管理制度文件」外的資訊資產編碼方式，第 1~3 碼為權責單位別，第 4~5 碼為資產類別，第 6~8 碼為資訊資產流水編號。



資訊資產編碼方式圖

5.5.2已列入機密等級分類的資訊資產，應明確標示其機密等級，避免其機密性遭破壞。

5.5.3實體設備之重要等級標示方式：

5.5.3.1 實體設備之重要等級應以不同顏色標籤區分（資產價值 2 為綠色標籤，資產價值 3 為黃色標籤，資產價值 4 為藍色標籤）。

5.5.3.2 文件之機密等級應於文件封面做明確的標示。系統輸出機密等級為敏感以上的報表，如系統未自動標示，則由資訊資產權責單位做額外的明顯註記。

5.6 資訊資產管理作業

5.6.1有關文件、紀錄、相關電子檔及儲存媒體控管原則及方式，請參閱「文件管理程序書」。

5.6.2有關人員之控管原則及方式,請參閱「人員安全與教育訓練程序書」。

5.6.3有關實體資產，包括：軟體、硬體、通訊及環境等之控管原則及方式，請參閱「實體安全管理程序書」。

5.6.4資訊資產異動管理，如：新增、刪除、修改等控管原則，請參閱「資訊資產異動作業說明書」。

5.7 覆核

5.7.1權責單位每年至少進行 1 次資產盤點與資訊資產清單覆核，以更新及確保資訊資產清單的正確性及完整性。

5.7.2當範圍內有以下的狀況發生時，則實施不定期的覆核，以更新及確保資訊資產清單的正確性及完整性。

5.7.2.1 有新增、變更或移除資訊資產。

5.7.2.2 系統有重大異動。

5.7.2.3 作業環境改變。

5.8 資訊資產之報廢

資訊資產之報廢（或銷毀）應依「資訊資產異動作業說明書」之相關規定，採取適當之方式進行銷毀。

5.9 資訊資產之處理規範

5.9.1針對價值 3 或 4 之資訊資產，應加強安全保護及存取控制管控措施，以防止洩漏或不法及不當的使用。

5.9.2價值 3 或 4 文件類資訊資產之安全處理應符合以下作業要求：

5.9.2.1 紙類文件不再使用時，應銷毀處理。

5.9.2.2 系統流程、作業流程、資料結構及授權程序等系統相關文件，

應予適當保護，以防止不當利用。

5.9.2.3 系統文件應指定專人管理，並鎖在安全的儲櫃或其他安全場所，且發送對象應以最低必要的人員為限。

5.9.2.4 電腦產製的文件，應與其應用檔案分開存放，且應建立適當的存取保護措施。

5.9.3價值 3 或 4 軟體類資訊資產之安全處理作業，請參閱「存取控制管理程序書」及「系統獲取、開發及維護管理程序書」之相關程序。

5.9.4價值 3 或 4 硬體類資訊資產之安全處理作業，請參閱「實體安全管理程序書」中重要設備之相關程序。

5.9.5應定期檢討價值 3 或 4 之資訊資產清單內容，以確保重要資產受到適當的安全保護。

5.10 實體媒體傳送

實體媒體傳送之管理原則及方式依據「可攜式設備與儲存媒體管理使用作業要點」。

6 相關文件

6.1 文件管理程序書

6.2 人力資源安全管理程序書

6.3 存取控制管理程序書

6.4 系統獲取、開發及維護管理程序書

6.5 實體安全管理程序書

6.6 資訊資產異動作業說明書

6.7 資訊資產清單

6.8 可攜式設備與儲存媒體管理使用作業要點

國立曾文高級家事商業職業學校

風險評鑑與管理程序書

機密等級：限閱

文件編號：TWVS-ISMS-B-004

版　　次：2.0

發行日期：109.04.28

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	102.11.26		文管人員	初版
2.0	109.04.28		文管人員	二版

目錄

風險評鑑與管理程序書					
文件編號	TWVS-ISMS-B-004	機密等級	限閱	版次	2.0

1 目的

建立國立曾文家事商業職業學校（以下簡稱「本校」）資通安全管理制度（以下簡稱 ISMS）風險評鑑與管理規範，提供本校資訊資產之權責單位、保管單位，以及使用單位，共同遵行之風險評鑑標準，有效執行風險控管，預防資通安全事件之威脅。

2 適用範圍

本校承辦相關資訊業務作業流程之風險管理。

3 權責

3.1 資通安全委員會：

負責可接受風險值、風險評鑑結果、風險改善計畫與控制措施之審查及核定。

3.2 資通安全小組：

負責相關資訊資產風險評鑑結果之複核，並針對超過可接受風險值之項目提出建議之控管措施，並產出風險改善計畫。

3.3 權責單位主管：

負責所屬單位業務範圍之風險評鑑結果審核作業。

3.4 資訊資產權責單位：

負責執行資訊資產之威脅與弱點評估、風險值計算等程序項目。

4 名詞定義

4.1 機密性 (Confidentiality)

確保只有經授權的人，才可以存取資訊。

4.2 完整性 (Integrity)

確保資訊與處理方法的正確性與完整性。

4.3 可用性（Availability）

確保經授權的使用者在需要時可以取得資訊及相關資產。

4.4 可接受風險值

各類資訊資產之最低風險容忍度。

4.5 殘餘風險（Residual Risk）

在採用相關控制措施之後剩餘的風險。

4.6 威脅（Threat）

可能對系統或組織造成傷害之意外事件。

4.7 弱點（Vulnerability）

因資訊資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受到損害之因子。

4.8 風險（Risk）

可能對團體或組織的資產發生損失或傷害的潛在威脅，通常利用弱點所產生之影響及發生可能性來衡量。

5 作業說明

5.1 鑑別資產

5.1.1資訊資產之鑑別應依據「資訊資產管理程序書」進行鑑別及分類。

5.2 鑑別風險

5.2.1威脅及弱點評估

參考 ISO 27005 將各類資訊資產可能面臨之威脅與弱點項目，分別建立「威脅及弱點評估表」。

5.2.2事件發生機率與影響程度評估

5.2.2.1 依威脅的等級對應表（表 1）評估各事件之威脅等級：

表 1 威脅的等級對應表

評估標準	評估值
威脅發生之可能性為低	1
威脅發生之可能性為中	2
威脅發生之可能性為高	3

5.2.2.2 依弱點的等級對應表（表 2）評估各事件之弱點等級：

表 2 弱點的等級對應表

評估標準	評估值
該弱點不容易被威脅利用	1
該弱點容易被威脅利用	2
該弱點非常容易被威脅利用	3

5.2.3風險值的計算

評估威脅發生之可能性及弱點受到威脅利用之容易度，計算出風險值。

風險值=（資訊資產價值 × 威脅等級 × 弱點等級）

5.3 風險管理

5.3.1可接受風險值的決定

5.3.1.1 資訊資產之可接受風險值，需經資通安全委員會開會決議，並記載於會議紀錄中。

5.3.1.2 資通安全委員會每年召開會議檢討可接受風險值。可接受風險必須考量組織環境及作業之安全需求,並進行適當地調整。

5.3.1.3 資通安全小組應針對高於可接受風險值項目，產出「風險評鑑彙整表」作為風險管理之依據。

5.3.2選擇控制措施

5.3.2.1 超出可接受風險值之項目，應選擇適當之控管措施，並產出

「風險改善計畫表」，說明風險控管措施之執行辦法。

5.3.2.2 「風險改善計畫表」應陳報資通安全委員會開會審核，並列入追蹤管理程序。

5.3.2.3 資通安全小組依據風險控管措施產出「適用性聲明書」。

5.3.3風險改善狀況的後續追蹤

5.3.3.1 資通安全小組應針對「風險改善計畫表」彙整控管，持續追蹤至完成改善為止。

5.3.3.2 應於各項風險改善措施完成後，應進行風險再評鑑，以確保相關改善措施的有效性。

5.4 覆核

5.4.1監控

控制措施的實施必須建立相對應的指標或紀錄，以反應出控制措施實施的狀況及成效，便於管理階層及相關人員做定期或不定期審視。

5.4.2持續改善

為保持本風險評鑑方法之有效性與適用性，資通安全小組得定期檢討可接受風險值與「威脅及弱點評估表」之項目。以期確保資訊資產均處於最佳保護之下，提供持續不中斷的營運。

5.4.3風險重新評鑑

5.4.3.1 每年應至少執行 1 次風險評鑑。

5.4.3.2 當有新增系統、系統有重大異動或作業環境改變時則應執行不定期之風險評鑑。

6 相關文件

6.1 資訊資產管理程序書

6.2 風險評鑑彙整表

6.3 風險改善計畫表

6.4 適用性聲明書

6.5 威脅及弱點評估表

7 附件

7.1 事件風險權值對照表

威脅等級（發生之可能性）		低(1)			中(2)			高(3)		
弱點等級（受到威脅利用之容易度）		低(1)	中(2)	高(3)	低(1)	中(2)	高(3)	低(1)	中(2)	高(3)
資產價值	1	1	2	3	2	4	6	3	6	9
	2	2	4	6	4	8	12	6	12	18
	3	3	6	9	6	12	18	9	18	27
	4	4	8	12	8	16	24	12	24	36

國立曾文高級家事商業職業學校

資訊資產異動作業說明書

機密等級：敏感

文件編號：TWVS-ISMS-C-001

版　　次：2.0

發行日期：109.04.28

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	102.11.26		文管人員	初版
2.0	109.04.28		文管人員	二版

目錄

資訊資產異動作業說明書					
文件編號	TWVS-ISMS-C-001	機密等級	敏感	版本	2.0

1 目的

本作業說明書制訂之目的，在於保護國立曾文家事商業職業學校（以下簡稱本校）之資訊資產於新增、異動、報廢時，能依據適當之程序，進行安全可靠之處置。

2 適用範圍

本校承辦相關資訊業務之資訊資產新增、異動、報廢作業。

3 權責

本校相關人員、約聘（僱）人員與工讀生：遵守本作業說明書之相關規定，確實執行資訊資產新增、異動、報廢作業之程序。

4 名詞定義

無。

5 作業說明

5.1 資訊資產之新增、異動

5.1.1 資訊資產新增或異動時，資訊資產使用單位應填寫「資訊資產異動申請表」，資訊資產價值為 4 者，須呈核至資通安全執行秘書；其餘由權責主管核定。

5.1.2 「資訊資產異動申請表」經審核後，交由文件管理人員保管，並定期更新「資訊資產清單」。

5.2 資訊資產之報廢

5.2.1 硬體及通訊資產報廢

5.2.1.1 硬體及通訊資訊資產需報廢或移作他用，硬體及通訊資產之相關設定與儲存媒體之資料必須清除。

5.2.1.2 硬體及通訊資訊資產報廢時，資訊資產使用單位應填寫「資

訊資產異動申請表」,經本校審核並確認資料清除後,方可進行資訊資產報廢程序。

5.2.1.3 資訊資產保管單位依據「資訊資產異動申請表」經本校審核後,辦理更新「資訊資產清單」,可重複使用之資料儲存媒體,於不再繼續使用時,應將儲存之內容完全消除,敏感級以上的資料必須確認資料清除後無法還原其內容。

5.2.1.4 硬體及通訊資訊資產價值為 4 者,經呈報資訊安全官核准後,方可執行報廢;資訊資產價值為 4 以下者,經各權責主管核准後,方可執行報廢。

5.2.2 儲存媒體報廢

5.2.2.1 儲存媒體如要報廢或移作他用時,儲存媒體上之資料必須清除。

5.2.2.2 當儲存媒體須報廢時,應採用以下任一種合宜之措施進行銷毀:

5.2.2.2.1 清除硬碟資料

以覆寫方式覆蓋硬碟資料或以工具進行實體之破壞,使其無法使用。

5.2.2.2.2 光碟

於光碟表面塗抹層製造刮痕後,再進行絞碎作業。

5.2.2.2.3 磁帶或磁片

使用強力磁鐵消磁後,磁帶應抽出後剪斷,磁片則進行絞碎作業。

5.2.2.3 儲存機密級以上資料之儲存媒體,嚴格禁止使用格式化方式進行資訊資產之報廢程序,應採用上述之方式進行銷毀。

5.2.3 軟體版權到期與移除

5.2.3.1 當軟體版權到期而需移除時，資訊資產使用單位應填寫「資訊資產異動申請表」，經審核後，方可進行軟體移除程序。

5.2.3.2 資訊資產保管單位依據「資訊資產異動申請表」經審核後，辦理更新「資訊資產清單」。

5.2.3.3 軟體資訊資產價值為 4 者，經呈報資訊安全官核准後，方可執行移除；資訊資產價值為 4 以下者，經各權責主管核准後，方可執行移除。

5.2.4 文件報廢

當資訊安全管理制度相關文件報廢時，依照文件管理程序書辦理。

6 相關文件

6.1 文件管理程序書

6.2 資訊資產異動申請表

6.3 資訊資產清單

國立曾文高級家事商業職業學校

實體安全管理程序書

機密等級：限閱

文件編號：**TWVS-ISMS-B-006**

版　　次：**2.0**

發行日期：**109.04.28**

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	102.11.26		文管人員	初版
2.0	109.04.28		文管人員	二版

目錄

實體安全管理程序書					
文件編號	TWVS-ISMS-B-006	機密等級	限閱	版本	2.0

1 目的

本程序書制訂之目的，在於保護 XXXX 學校（以下簡稱「本校」）資訊資產及周邊環境設施，減少環境安全問題所引發的危險，以便達成本校安全控管之目的。

2 適用範圍

本校機房及周邊環境與設備安全管理。

3 權責

本校相關人員、約聘（僱）人員與委外人員：遵守本程序書之相關規定，以確保本校安全區域與人員辦公區域及資訊資產設備之安全。

4 名詞定義

無。

5 作業說明

5.1 安全區域

5.1.1 本校之機房為安全區域。

5.1.2 為確保相關設施之安全，非權責單位授權之人員不得擅自進入安全區域或使用相關資訊設備。

5.1.3 若外部人員或本校未具機房進出權限之人員，因執行業務需求進入機房時，必須由資訊資產權責單位或保管單位指派人員隨行並填寫「人員進出機房登記表」後方可進出機房，並遵守相關設備管理之規定。

5.1.4 安全區域之門禁紀錄，該紀錄應適當保存與定期審閱。

5.2 一般控制措施

5.2.1 無人時或下班最後一人離開時，需將辦公室關門上鎖。

5.2.2 為防止未經授權之存取，同仁應於下班後，遵守桌面淨空政策，並將敏感等級（含）以上之文件與可攜式資訊設備皆存放於儲櫃並上鎖，避免資訊外洩之機會。

5.2.3 同仁於本校安全區域與辦公室內需隨時注意身分不明或可疑的人員。發現不明身分之人員時，需主動詢問並儘速通知相關部門進行處理。

5.2.4 同仁需隨時清理個人電腦的資源回收筒，以確保已經刪除的重要資料不會因為遺留在資源回收筒未清理，而遭未經授權之使用。

5.2.5 未經授權不得將設備、軟體、儲存資訊之媒體或文件攜出安全區域。如有需要，則須經主管人員核准，始得進行。

5.3 一般設備安全

5.3.1資訊資產與相關設備安全之維護需考量設備之使用、安置、儲存、監控、移出與報廢等安全管理。

5.3.2可攜式電腦，需以密碼保護，免於被偷取、遺失而遭未經授權的盜用，並於使用完畢後，刪除電腦中非一般等級之資料及清理資源回收筒內之資料。

5.3.3個人電腦、伺服器或電腦終端機不使用時，需採用密碼保護、鎖定或登出離線等安全控制措施。

5.3.4無人看管的使用者設備

5.3.4.1 個人電腦限制執行資源分享，必要時應由權責主管同意，並設定密碼保護。

5.3.4.2 使用者離開電腦設備時，應退出使用環境或電腦螢幕鎖定，以確保資料之安全。

5.3.5無人看管暨場所外之公用資訊設備，應安裝防毒軟體及合法有版軟體，若安裝相關服務性應用系統，應具備身分識別之帳密管制功能，其內亦不能存放敏感性資料。

5.4 硬體資訊資產安全維護

5.4.1 重要之儲存媒體，應上鎖或由專人管理，並且僅經授權之使用者方能使用。

5.4.2 謹慎使用電源延長線，以免電力無法負荷而導致火災，於新增硬體設備時，應先評估電力負荷。

5.4.3 設備異動（包含新增、報廢、變更用途），應重新評估相關系統設定。

5.5 機房設備安全維護

5.5.1 重要資訊設備，應放置於機房，並落實安全管理。

5.5.2 電力、網路、通信設備應予以保護，以防止遭有心人士截取或破壞。

5.5.3 機房內應保持整齊清潔，並嚴禁吸菸、飲食或堆置易燃物。

5.5.4 電腦機房應設置專用空調設備以維持電腦主機正常運作。

5.5.5 經評估後，確定將資訊設備（如：伺服器、防火牆...等）委外維護時，應簽訂維護契約，並定期實施保養與維護，以確保設備完整性及可用性之持續使用。

5.5.6 重要電腦主機之資訊設備及警報系統等應定期檢修測試。

5.5.7 冷氣機、不斷電系統（UPS）等機電設備之使用，應依照設備說

明書指示操作，並施行定期檢查作業。

5.5.8 機房應設置足量之不斷電系統（UPS），供應重要資訊設備電源之使用，以保障資訊設備之正常作業。

5.5.9 機房溫溼度應維持在機器可正常運轉的範圍內，並需 24 小時維持空調運轉。

5.5.10 資訊設備專用電源插座，不得使用於資訊及空調設備以外之設備，以免耗用電源，發生跳電當機情形，影響正常作業。

5.5.11 資訊設備保管單位應於每工作日檢核各設備之運作狀況，發現異常時，應填寫「異常事件紀錄表」並進行必要之處置。

5.6 移轉資產之安全管理

5.6.1 機房中資訊設備之進出應填寫「設備進出紀錄表」敘明其設備進出原因或目的。

5.6.2 資訊設備、資料或軟體之移轉，應依「資訊資產管理程序書」辦理，並由資訊安全小組負責更新「資訊資產清單」。

5.6.3 硬體資產報廢前應確實清除限閱等級（含）以上之資訊，以避免資訊外露，並確實清點報廢資產後，方可進行報廢，相關作業規範請參閱「資訊資產異動作業說明書」。

5.7 送修作業

5.7.1 資訊設備送修前，資訊設備之權責單位應依該設備之資訊資產價值選擇適當之備援方案，並備註說明於「設備進出紀錄表」。

5.7.2 資訊設備若具敏感等級以上之資料，於送修前應請廠商簽署「委外廠商保密切結書」。

5.8 維護契約

5.8.1 所有資訊設備維護契約，應由專人負責保管與定期審查契約時間是否過期與該資訊設備是否仍有維護需求，若仍有維護需求則應依「委外管理程序書」簽訂維護契約。

6 相關文件

6.1 資訊資產管理程序書

6.2 委外管理程序書

6.3 資訊資產異動作業說明書

6.4 資訊資產清單

6.5 人員進出機房登記表

6.6 設備進出紀錄表

6.7 異常事件紀錄表

6.8 委外廠商保密切結書

國立曾文高級家事商業職業學校

存取控制管理程序書

機密等級：限閱

文件編號：**TWVS-ISMS-B-008**

版　　次：**2.0**

發行日期：**109.04.28**

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	102.11.26		文管人員	初版
2.0	109.04.28		文管人員	二版

目錄

存取控制管理程序書					
文件編號	TWVS-ISMS-B-008	機密等級	一般	版次	2.0

1 目的

為保護資訊資產，降低未經授權存取系統之風險，以達成國立曾文家事商業職業學校（以下簡稱「本校」）安全控管之目的。

2 適用範圍

本校資訊資產之存取控管原則。

3 權責

本校相關人員、約聘（僱）人員與委外人員：遵守本程序書之相關規定，以確保本校相關軟體與資料等資訊資產之安全。

4 名詞定義

無。

5 作業說明

5.1 存取控制政策

5.1.1 資訊資產之存取應與本身業務相關之範圍為主，任何人未經授權不得存取業務範圍外之資訊資產。

5.1.2 應正確地使用資訊資產，以維護資訊資產之可用性、完整性與機密性。

5.1.3 非因業務需求不得將系統存取帳號提供給外部人員，若因業務需要開放帳號予外部人員，應有適當安全控管措施，該安全控管措施應考量業務需求及資訊資產之機密性，授與適當之存取權限及有效日期。

5.1.4 被賦予系統管理最高權限之人員、掌理重要技術及作業控制之特定人員，應經審慎之授權評估。

5.1.5 因處理系統當機與異常狀況需視狀況授與適當存取權限，並避免共

用帳號。

5.1.6 可攜式電腦儲存媒體，例如：筆記型電腦、隨身碟、外接式硬碟、光碟、磁帶等，應採取適當之控管措施，以防止未經授權之資料、系統、網路存取或病毒傳播。

5.1.7 資料、資訊之存取，必須符合「個人資料保護法」、「電子簽章法」及「智慧財產權」等相關法規、法令之規定，或契約對資料保護及資料存取使用控管之規定。

5.1.8 系統主機之公用程式路徑之存取權限應適當控管，禁止一般使用者存取。

5.1.9 針對無人看管的資訊資產設備，應有適當控管程序，以防未經授權之存取或濫用。

5.1.10 個人桌上型電腦、可攜式電腦應設定於一定時間不使用或離開後，應自動清除螢幕上的資訊並登出或鎖定系統，以避免被未經授權之存取。

5.2 網路存取控制

5.2.1 網路系統應依其性質之不同，分開成不同的領域，各領域應以特定的安全設施（如防火牆及網路閘門）加以保護，以降低可能的安全風險。

5.2.2 網路管理人員應定期檢視網路存取之紀錄，並留存查核紀錄。

5.2.3 對於開放提供外部客戶或廠商存取之服務，必須限制使用者之網路功能以確保網路安全。

5.2.4 網路路由之規劃必須確保任何網路連線或資訊傳輸符合網路存取之安全需求。

5.3 使用者存取管理

5.3.1 各項系統資源使用權限之申請、註冊及註銷應遵循作業管理程序，

並維護相關之申請、註冊、註銷資料與紀錄，以備查核。

5.3.2 使用者職務異動或離職時,部門主管應即時通知相關單位調整或終止使用者之存取權限。

5.3.3 系統相關作業人員需經正式授權存取業務相關之資訊資產,其識別資料與帳號必須為唯一，禁止借用他人之帳號或共用帳號。

5.3.4 各項設備與系統相關之使用權限（例如使用者帳戶與作業權限）應留存紀錄。

5.3.5 應妥善管理久未登錄系統之帳戶，若超過 6 個月未曾登錄，則視需要清除閒置帳號。

5.3.6 應要求使用者變更初始密碼並定期變更密碼;重要資訊系統及特殊權限之存取帳號之密碼變更期間應較一般權限之帳號頻繁。

5.3.7 使用者存取權限應定期審查，週期不得超過 6 個月。

5.3.8 重要系統稽核資料應由專人定期審核，系統管理者不得新增、刪除或修改稽核資料，審查週期不得超過 6 個月。

5.3.9 每半年將學籍系統、主機、網路設備等帳號權限設定資料印出，或填寫於「帳號清查紀錄表」，進行帳號權限清查，並將查核結果記錄於「帳號清查結果報告」呈資訊安全官審查。

5.4 帳號與密碼管理

5.4.1 新購置之應用軟體或系統，安裝完成後應立即更新預設之密碼，並刪除或關閉不必要之帳號。

5.4.2 使用者帳號管理

5.4.2.1 使用者帳號申請應填寫「資訊服務申請表」，經部門主管核准後，由帳號管理人員進行使用者帳號建立作業。

5.4.3 管理者帳號管理

5.4.3.1 系統管理者應避免共用系統管理者帳號，系統管理者帳號與密

碼應存放於安全之處。

5.4.3.2 系統管理者密碼設置，至少 8 碼，且應符合密碼設置原則。

5.4.4 密碼管理

5.4.4.1 使用者首次使用系統時，應要求更改密碼設定，並妥善保管帳號與維持密碼之機密性，保存帳號密碼之檔案應以加密方式處理。

5.4.4.2 使用者應避免將帳號密碼記錄在書面上，張貼在個人電腦、螢幕或其他容易洩漏秘密之場所。

5.4.4.3 使用者禁止共用帳號密碼。

5.4.4.4 使用者發現密碼可能遭破解時，應立即更改密碼。

5.4.4.5 使用者每次存取系統時應輸入密碼登入系統，避免使用記錄密碼功能，導致開機時自動登入系統。

5.4.4.6 系統管理者應至少 6 個月更換密碼一次，一般系統之使用者(學校行政人員)應至少 12 個月更換密碼一次。

5.4.4.7 使用者密碼設置至少 8 碼，且應符合密碼設置原則。

5.4.4.8 密碼設置原則

應儘量避免使用易猜測或公開資訊為設定，例如：

A. 個人姓名、出生年月日、身分證字號

B. 機關、單位名稱或其他相關事項

C. 使用者 ID、其他系統 ID

D. 電腦主機名稱、作業系統名稱

E. 電話號碼

F. 空白

密碼設定可考慮下列原則：

A. 參雜數字、英文字母、特殊符號、大小寫

B. 特殊意義詞彙

5.4.4.9 使用者遺忘密碼時，須填具「資訊服務申請表」，經部門主管核准後，由帳號管理人員重新設定。

5.5 作業系統存取控制

5.5.1 系統設定應避免於終端機登入程序中以明碼方式顯示密碼相關資訊。

5.5.2 只有在完成所有的登入資料輸入後，系統才開始查驗登入資訊的正確性；若登入發生錯誤，系統不應顯示錯誤發生之原因。

5.5.3 在系統登入被拒絕後，應立即中斷登入程序，並不得給予任何的協助。

5.5.4 應設定系統登入程序之時間限制，如果超出時間限制，系統將自動中斷登入。

5.5.5 使用者帳號避免顯示任何足以辨識使用者特別權限的訊息，例如：顯示其為管理者或監督者。

5.5.6 系統管理人員結束系統維護作業後，應結束應用系統及網路連線，清除螢幕上的資訊，登出系統，並鎖定主控台螢幕。

5.5.7 系統之存取使用應留存查核紀錄。

5.6 遠端存取之限制

5.6.1 所有資訊資源使用者，非經主管授權或允許，禁止執行遠端存取作業。

5.7 資料庫存取控制

5.7.1 資料庫之存取權限，應經適當程序之授與及移除，且須使用獨立之帳號及密碼登入。

5.7.2 資料庫存取之身分驗證機制，須由系統內部安全機制提供。

5.7.3 資料庫使用者之帳號密碼設定必須符合本程序書及相關系統之帳

號密碼管理規範之要求。

5.7.4 資料庫公用程式路徑之存取權限應適當控管，禁止一般使用者存取。

5.7.5 資料庫最高權限帳號之存取授權應僅限於資料庫管理員。

5.7.6 資料庫預設帳號應變更密碼，或是關閉使用。

5.7.7 資料庫之存取紀錄應留存查核紀錄。

5.8 系統被入侵時的異常處理

5.8.1 立即拒絕入侵者任何存取動作（例如關閉可疑帳號），防止災害繼續擴大。

5.8.2 關閉受侵害的主機，或立即與網路離線。

5.8.3 檢查防火牆及系統紀錄，研判入侵管道之方式，必要時作安全漏洞修補。

5.8.4 通知主機供應商提供必要的回復協助。

5.8.5 如伺服主機的完整性受侵害，應將完整的系統備份資料存回受害主機上，並測試其功能，直至完全回復為止，最後再將該主機重新上線。

5.9 具特殊存取權限之管理

5.9.1 特殊權限之使用者必須與一般權限之使用者區分管理；針對特殊權限帳號，應妥善管理。

5.9.2 特殊權限之授權管理，必須依執行業務系統別之需求，例如作業系統、資料庫管理系統、網路服務系統、監控管理系統等賦予系統存取特殊權限的授權，且以執行業務及職務所必要的最低資源存取授權為限。

5.10 應用系統之存取控制

5.10.1 資訊存取之限制

5.10.1.1 應用系統資訊之使用，僅限業務相關之授權使用者，並應適當控制。例如：新增、刪除或執行等。

5.10.1.2 應用系統之敏感與機密性資訊，應與一般資訊作適當區隔，並加強權限控管措施。

5.10.2 原始程式資源之存取控制

5.10.2.1 應用程式原始碼，應集中存放，並由系統負責人管理程式之增修作業。

5.10.2.2 開發中之原始程式碼，應與線上程式碼分開放置與控管。

5.10.2.3 舊版的原始程式應妥慎保管，並詳細記錄使用的明確時間，以備新版失敗回復使用。

5.10.2.4 應用程式之異動需經適當控管。

5.10.2.5 應用程式管理人員，應檢視程式目錄清單，如有異常情形，應即查明原因及處理。

6 相關文件

6.1 個人資料保護法

6.2 智慧財產權相關法令

6.3 電子簽章法

6.4 資訊服務申請表

6.5 帳號清查紀錄表

6.6 帳號清查結果報告

國立曾文高級家事商業職業學校

通信與作業管理程序書

機密等級：限閱

文件編號：TWVS-ISMS-B-007

版　　次：2.0

發行日期：109.04.28

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	102.11.26		文管人員	初版
2.0	109.04.28		文管人員	二版

目錄

通信與作業管理程序書					
文件編號	TWVS-ISMS-B-007	機密等級	一般	版次	2.0

1 目的

為防止國立曾文家事商業職業學校（以下簡稱「本校」）資訊在不安全之網路環境下，遭致可能之破壞，或非預期及非經授權之修改，以確保資訊系統與資料之安全性、可用性及完整性。

2 適用範圍

本校所轄之範圍內，相關網路服務與設備及核心業務系統之管理。

3 權責

本校網路管理人員應遵守本程序書之相關規定，以確保本校網路之安全。

4 名詞定義

4.1 機密性 (Confidentiality)

確保只有經授權的人，才可以存取資訊。

4.2 完整性 (Integrity)

確保資訊與處理方法的正確性與完整性。

4.3 可用性 (Availability)

確保經授權的使用者在需要時可以取得資訊及相關資產。

4.4 可接受風險值

各類資訊資產之最低風險容忍度。

4.5 殘餘風險 (Residual Risk)

在採用相關控制措施之後剩餘的風險。

4.6 威脅 (Threat)

可能對系統或組織造成傷害之意外事件。

4.7 弱點 (Vulnerability)

因資訊資產本身狀況或所處環境之下，可能受到威脅利用而造成資產受

到損害之因子。

4.8 風險 (Risk)

可能對團體或組織的資產發生損失或傷害的潛在威脅，通常利用弱點所產生之影響及發生可能性來衡量。

4.9 行動計算與通信設施

如筆記型電腦、掌上型電腦、行動電話等。

4.10 儲存媒體

如磁片、磁碟、磁帶、IC 卡、匣式磁帶、外接式硬碟、光碟、隨身碟、各式記憶卡、錄影帶、錄音帶等。

5 作業說明

5.1 資訊系統安全規劃作業

5.1.1 應建立資訊系統之安全控管機制，以確保資訊資料之安全，保護系統及網路作業，防止未經授權之系統存取。

5.1.2 資訊系統管理職務與責任應加以區隔，足以影響業務經營管理的資訊，不可只由單獨一人知悉。如因人力資源限制，無法區隔責任，則應加強監督與稽核等措施。

5.1.3 伺服主機及網路設備應指定負責人，負責該主機之正常運作，包括應用程式之執行、資料庫之維護及相關作業系統與主機硬體資源之分配管理。主機或網路設備負責人無法進行管理時應由代理人負責，未指定負責人之主機及網路設備由機房管理負責人員負責。

5.1.4 網路管理人員應妥為規劃網路架構、設定網路參數，並依規定備份相關檔案。

5.1.5 應規劃系統與設備的開發與測試環境，避免於已上線運作設備及環境進行開發或測試工作。

5.1.6 系統及設備建置前，主辦單位應對系統需求做適當規劃，以確保足夠的電腦處理及儲存容量。如需委外開發或採購，則依「委外管理程序書」辦理。

5.1.7 系統設備與軟體之建置，均應依照「系統獲取、開發及維護程序書」之程序進行測試及驗收。

5.2 變更管理

5.2.1 新增設備及網路變動，應即時修改網路架構圖及設備資料。

5.2.2 架構調整：架構變動之影響性甚大者應經資訊安全官以上核准，並遵循下列規定：

5.2.2.1 設備之功能性及設定方式應熟悉掌握。

5.2.2.2 新增對外網路連線，需注意安全性考量，從嚴審核對外網路連線與內部之連接之方式。

5.2.2.3 如有廠商參與安裝或設定，必須全程陪同參與並記錄。

5.2.3 系統若有相關文件（如系統文件、參考文件或作業準則）時，系統相關負責人員於變更程序同時，應同步修改維護相關文件。

5.2.4 各項系統變更作業依據「系統開發與維護程序書」變更作業控制措施辦理。

5.3 容量管理

5.3.1 依據資通訊設備資源使用狀況及資源容量之需求，適時進行系統調整與系統容量擴充規劃，以確保獲得必要之系統作業資源。

5.3.2 系統容量評估與規劃時，須注意硬體設備及軟體系統版本更新、使用與維護之生命週期，及硬軟體系統運作相容性。

5.3.3 儲存設備之容量應予以監控，以維持系統之正常運作。當儲存設備

之使用容量達 85%時，系統管理人員應進行必要之資料移轉或處理。

5.4 惡意軟體之防範

5.4.1 禁止使用或下載未經授權或與業務無關之軟體。

5.4.2 應安裝病毒偵測與修復軟體，並定期更新病毒資訊，以防止病毒之攻擊。伺服器主機防毒軟體系統應設定主動掃瞄檢查，或由網路管理人員定期執行掃瞄檢查作業。

5.4.3 應定期檢查支援重要業務之作業系統是否有任何未核准的檔案或未經授權的修改。

5.4.4 應於使用來源不明、來源未經授權、或從未經信任網路接收之檔案前，檢查該檔案是否藏有病毒。

5.4.5 應於使用前檢查電子郵件附件和下載檔案有無惡意軟體。

5.4.6 使用者如偵測到電腦病毒入侵或其他惡意軟體，應立即通知系統或網路管理人員；管理者亦應將已遭病毒感染的資料及程式等資訊隨時提供使用者，以避免電腦病毒擴散。

5.4.7 系統或電腦設備如遭病毒入侵感染，應立即與網路離線並隔離，直到網路管理人員確認病毒已消除後，才可重新連線，並留存處理紀錄。

5.5 資料備份

5.5.1 各項系統設定檔、網頁資料、伺服器檔案及資料庫資料均應由各系統負責人員訂定備份週期，並依據週期執行系統排程或手動備份，備份狀況應記錄於「備份狀況紀錄表」、「系統備份狀況紀錄表」，或利用各項監控系統予以監測、紀錄。

5.5.2 應定期於測試主機上測試備份資料是否正確、可用。

5.5.3 重要系統資料應考量建立異地備份機制。

5.5.4 備份作業之執行依據「備份作業說明」相關規範辦理。

5.6 存錄及監視

5.6.1稽核存錄

5.6.1.1 應針對之重要系統，在不影響效能運作下開啟相關日誌，包括：事件（成功或失敗）發生的時間。事件的資訊（如已處置檔案）或失效的資訊（如已 發生錯誤並採取矯正措施）。所涉及的帳號和管理者或操作者。

5.6.1.2 應用系統若有提供紀錄功能應予啟動，若無則視系統之重要性，以書面方式紀錄之。除預設之系統紀錄功能外，應考量紀錄以下事件：系統管理者及具備特殊權限帳號之登入成功及失敗事件紀錄。使用者帳號異動及對密碼檔案之讀取與變更。變更正式應用系統的程式原始碼及程式執行碼。對於作業系統設定檔之存取及變更。

5.6.1.3 各系統的系統紀錄存取,應限定僅由系統管理者或具讀 取權限者存取。

5.6.1.4 資訊設備保管單位應於每工作日檢核各設備之運作狀況，發現異常時，應執行相關處置，並依據「異常事件 處理作業說明」辦理。

5.6.2日誌資訊保護的控制措施

5.6.2.1 系統需開啟系統日誌及適當稽核記錄功能，並將關鍵性系統(如防火牆)之紀錄匯出存檔備查，並保留至少三個月。

5.6.2.2 系統管理人員需確實檢視系統日誌（含各式通訊服務之連線

紀錄)、系統資源使用狀態、系統漏洞與修補程式安裝情形。

5.6.3管理者與操作者日誌

5.6.3.1 資訊設備、網路安全設備、應用系統與資料庫之管理者與操作者所有執行的管理或異動作業，應加以記錄。

5.6.3.2 系統管理者與操作者日誌宜定期予以審查。

5.6.4資訊與通訊設備時序同步

5.6.4.1 重要資訊設備、網路安全設備、主機伺服器應盡可能與單一參考時間源同步。以確保系統時間的一致性。若設定自動校時，每日應至少校時一次。

5.6.4.2 資訊設備如無法設定單一參考時間源，則應約定同步之時間源，由設備管理員定期(至少每季一次)或於設備異動時進行系統時間同步作業。

5.7 安全稽核事項

5.7.1 對各項系統視需要留存系統最新參數設定檔。

5.7.2 系統管理、技術諮詢與機房操作人員工作應依職務與相關規定確實記錄其工作內容於「巡查紀錄表」內。

5.7.3 每月應檢視一次各設備中系統時間是否一致，並進行校正及同步作業。

5.7.4 系統稽核資料應依系統重要性進行備份保護作業，並由專人定期審核，系統管理者不得新增、刪除或修改稽核資料，審查週期不得超過 6 個月。

5.7.5 應定期查核技術符合性，進行弱點掃描或滲透測試，以確定資訊系統及網路環境符合安全實施標準。掃描週期如下：

5.7.5.1 每年至少針對伺服器及網管設備執行一次。

5.7.5.2 當系統有重大變動時。

5.7.5.3 新系統上線前。

5.7.6 系統異常及安全事件記錄與分析，依據「矯正及預防管理程序書」辦理。

5.7.7 弱點掃瞄報告與修補作業

5.7.7.1 執行弱點掃描應產出弱點掃描報告，弱點掃描報告格式不拘，惟應包含下列內容：

5.7.7.1.1 弱點掃描檢測範圍。

5.7.7.1.2 弱點掃描檢測時程。

5.7.7.1.3 弱點風險等級說明。

5.7.7.1.4 安全弱點列表與建議修補措施。

5.7.7.2 掃描出之弱點應限期改善，並填寫「弱點處理報告單」，且於修補後進行複掃。

5.7.7.3 於安裝修正程式前，需先行測試並確認運作正常後，方可進行安裝。

5.7.8 殘餘弱點管理

5.7.8.1 弱點若因故無法修補，應於「弱點處理報告單」說明無法修補之原因與防禦因應方法。

5.8 網路安全管理

5.8.1 網路服務之管理

5.8.1.1 避免利用公共網路傳送敏感等級（含）以上資訊，應保護資料在公共網路傳輸之完整性及機密性，並保護連線作業系統之安全性。

5.8.1.2 網路管理人員應利用網路管理工具，偵測及分析網路流量。

5.8.1.3 開放相關人員從遠端登入內部網路系統之網路服務，應執行嚴謹之身分辨識作業，或提供連線設備之識別機制。

5.8.1.4 如果系統使用者為非合法授權之使用者時，應立即撤銷其系統使用權限；離（休、退）職人員應依資訊安全規定及程序，調整或終止其存取網路及系統之權限。

5.8.1.5 網路管理人員除依相關法令或規定，不得閱覽使用者之私人檔案；但如發現有可疑之網路安全情事，網路系統管理人員得依授權規定，使用工具檢查檔案。

5.8.1.6 網路管理人員除有緊急狀況外，未經使用者同意，不得增加、刪除及修改私人檔案。

5.8.1.7 網路設備軟硬體應限定由網路系統管理人員依規定辦理設定異動，並應留存紀錄備查。

5.8.1.8 對任何網路安全事件，網路管理人員應依「安全事件管理程序書」辦理。

5.8.1.9 網路管理人員應於每工作日檢查所有網路設備並記錄於「巡查紀錄表」，每月送主管簽核。如發現異常應依本程序之異常處理流程辦理。

5.8.2 網路使用者之管理

5.8.2.1 經授權之網路使用者，只能在授權範圍內存取網路資源。

5.8.2.2 網路使用者於使用行動碼（如 ActiveX、JAVA Applet）之前，應先確認其授權資料，並禁止執行未經授權之行動碼。

5.8.2.3 網路使用者應遵守網路安全規定，並確實瞭解其應負之責任；如有違反網路安全情事，應依資訊安全規定，限制或撤銷其網路資源存取權利，並依相關規定處理。

5.8.2.4 網路使用者不得將自己之登入身分識別與登入網路之密碼交

付他人使用。

5.8.2.5 禁止網路使用者以任何方法竊取他人之登入身分與登入網路密碼。

5.8.2.6 禁止網路使用者以任何儀器設備或軟體工具竊聽網路上之通訊。

5.8.2.7 禁止網路使用者在網路上取用未經授權之檔案。

5.8.2.8 網路使用者不得將色情檔案建置在網路，亦不得在網路上散播色情文字、圖片、影像、聲音等不法或不當之資訊。

5.8.2.9 禁止網路使用者發送電子郵件騷擾他人，導致其他使用者之不安與不便；或以任何手段蓄意干擾或妨害網路系統之正常運作。

5.8.2.10 網路使用者不得任意修改網路相關參數。

5.8.2.11 為維護本校網路安全，網路管理人員於發現網路使用者之電腦發送異常封包或使用非經允許之服務時，依『校園網路使用規範』相關規定辦理。

5.8.3 無線網路使用之管理

5.8.3.1 無線網路基地台之使用應經適當控管。

5.8.3.2 無線網路設備之安裝設定應經核准。

5.8.3.3 無線網路設備之使用應取得授權，禁止於內部網路私自使用任何無線網路產品。

5.8.3.4 無線網路設備之使用應有適當管理機制，例如：授權使用之IP 數量、連接埠、網卡位址（MAC）過濾等。

5.8.3.5 無線網路之資料傳輸應使用加密機制，並就安全與資訊風險之考量，增加適當之防護機制以避免資料外洩。

5.8.4 防火牆之安全管理

5.8.4.1 所有與外界網路連接之連線，應透過加裝防火牆，以控管外界與本校內部網路間之資料傳輸與資源存取。

5.8.4.2 防火牆設定異動時，應填寫「防火牆進出規則申請表」，經主管簽准後，交由網路管理人員設定。

5.8.4.3 防火牆應由網路管理人員執行控管設定，並依制定之資訊安全規定、資料安全等級及資源存取之控管策略，建立包含身分辨識機制與系統稽核之安全機制。

5.8.4.4 防火牆設置完成時，應測試防火牆是否依設定之功能正常及安全地運作。如有缺失，應立即調整系統設定，直到符合既定之安全目標。

5.8.4.5 網路管理人員應配合資訊安全政策及規定之修正，以及網路設備之變動，隨時檢討及調整防火牆系統設定，調整系統存取權限，以反映最新狀況。

5.8.4.6 視業務需要及設備功能，對於通過防火牆之特定網路服務，應予確實紀錄。

5.8.4.7 網路管理人員應避免採取遠端登入方式登入防火牆主機，以避免登入資料遭竊取，危害網路安全。如果必須使用遠端登入方式管理，應訂定嚴謹之遠端登入控管措施。

5.8.4.8 若資源許可應建立防火牆設備之備援機制；防火牆之環境建置檔等需定期執行備份作業。

5.8.4.9 防火牆政策及設定應每月定期覆核，並記錄於「巡查紀錄表」中，若已屆期限或該 IP 不再使用，請系統負責人確認後刪除，並填寫「防火牆進出規則申請表」。

5.8.4.10 網路管理人員每週將防火牆之 log 轉出存放於備份機器上，並記錄於「巡查紀錄表」。

5.8.4.11 於防火牆設定變更之前，將各防火牆之設定檔備份，並依「備份狀況紀錄表」之表列進行備份，存放於備份設備上。

5.8.5 網路資訊之管理

5.8.5.1 敏感等級（含）以上之業務資料或文件不得存放於對外開放之資訊系統中，若因特殊業務功能之需求，必須採取加強之安全管控機制，如：資料加密。

5.8.5.2 網路管理人員應負責監督網路流量及使用情形，並對可能導致系統作業癱瘓等情事，預作有效的防範，以免影響網路服務品質。

5.8.5.3 對外開放的資訊系統所提供之網路服務，如：HTTP、FTP等，應採取適當之存取控管機制。

5.8.5.4 對校外開放的資訊系統，如：存放教職員、學生或家長申請或註冊之個人資料檔案，其傳輸過程應考量以加密方式處理，並妥善保管資料，以防止被竊取或移作他途之用，侵犯個人隱私。

5.8.5.5 網路管理人員於偵測收到資訊系統異常狀況或駭客入侵之警示訊息時，應立即通報權責主管，依據相關作業管理規範採取適當之緊急應變處理，並留存系統異常處理紀錄。

5.8.6 網路管理作業流程

5.8.6.1 網路檢查作業

5.8.6.1.1 以指令方式 ping 各網段之 Gateway，以回應時間初步判斷網路狀態。

5.8.6.1.2 檢查防火牆之 log 及狀態。

5.8.6.1.3 防火牆發現異常情形應設定自動寄發通知信給網路管理人員，嚴重時網路管理人員應立即採取阻擋作為，並通

知主管。

5.8.6.2 網路監控作業

5.8.6.2.1 利用工具自動 ping 各 IP，用以監控網路各節點，由其回應數值判斷網路狀態是否正常。

5.8.6.2.2 收集防火牆之 log，並統計 log 資料。

5.8.6.2.3 監控內部網路頻寬使用狀況，於頻寬使用率達 60%以上時，應評估增加頻寬之必要性。

5.8.6.3 異常監控作業

5.8.6.3.1 定期監控各伺服器提供之各項服務是否正常，若設備服務狀態不正常時，應通知相關負責人員處理。

5.8.6.4 異常處理作業

5.8.6.4.1 以節點方式由內而外檢測，由回應數值推知問題點。

5.8.6.4.2 確認與問題點相關之實體設備和網路線是否正常。

5.8.6.4.3 如為設備問題可尋找替用設備更換，並連絡廠商維修，並將處理情形記錄於「異常事件紀錄表」。

5.8.7 網路入侵之處理

5.8.7.1 網路被入侵時，應依「安全事件管理程序書」辦理。

5.8.7.2 應建立網路入侵事件之調查程序，除利用工具及稽核檔案提供之資料外，應協請相關單位（如網路服務提供者），追蹤入侵者。

5.8.7.3 入侵者之行為若觸犯法律規定，構成犯罪事實，應立即告知相關單位，請其處理入侵者之犯罪事實調查。

5.9 電腦軟體與程式著作權保護

5.9.1 應訂定使用授權軟體與遵守著作權規範，違反規範者應依相關程序

議處。

5.9.1.1 使用軟體與資訊產品不得超過允許的最高使用人數。

5.9.1.2 使用軟體與資訊產品應遵守相關規定，例如限制於指定之機器使用、限制僅於備份時方可複製等。

5.9.1.3 取得之合法軟體不得從事或轉讓予非授權範圍之使用。

5.9.1.4 從公共網路取得之合法軟體與資訊須遵守原著作權者與電腦處理個人資料保護法之規定。

5.9.1.5 對公共系統的存取不得擅自存取其所相連的網路。

5.9.2 應妥善保管採購軟體產品之授權書、原版光碟、手冊等等證明。

5.9.3 經由網際網路下載之公開授權軟體，應在確認安全無虞及不違反智慧財產權前提下，方得下載執行。

5.10 電子郵件安全管理

5.10.1 電子信箱帳號之註冊、離職、異動申請，應遵循電子郵件相關管理規範之規定，除學生帳號由本校批次建立外，其餘則填寫「電子郵件帳號申請表」提出申請，經各單位部門主管核准後，再交由系統管理者或經授權之管理者建置相關資料。

5.10.2 應建立電子郵件之安全管理機制，以降低電子郵件可能帶來之業務上及安全上之風險。

5.10.3 應禁止發送匿名信，或偽造他人名義發送電子郵件騷擾他人，導致其他使用者之不安與不便。

5.10.4 敏感等級（含）以上的資料或文件，應避免以電子郵件傳送。

5.10.5 不得傳遞大量且非必要的資訊，避免網路壅塞及資源浪費。

5.10.6 電子郵件附加之檔案，應事前檢視內容有無錯誤後方可傳送。

5.10.7 對來路不明之電子郵件，不宜隨意打開電子郵件，以免啟動惡意執

行檔，使網路系統遭到破壞。

5.10.8 郵件伺服器異常處理及故障排除作業

5.10.8.1 發現郵件伺服器系統異常，資訊人員應進行診斷，辨識異常原因及影響範圍，評估系統回復時間，並進行排除作業。

5.10.8.2 異常處理人員應定時回報權責主管最新狀況及處理進度。

5.10.8.3 如異常發生無法立即排除故障時，應通知相關部門異常影響程度及預估回復時間，並採取因應措施。

5.10.8.4 如診斷可能係硬體設備故障造成，則通知廠商人員到場檢測。

5.10.8.5 系統經復原並確實檢查測試後，終止緊急應變作業，並通知相關部門及主管。

5.10.8.6 將處理過程及結果記錄於「異常事件紀錄表」中。

5.11 全球資訊網（WWW）

5.11.1 對 HTTP 伺服器開放可存取的範圍，應限制僅能存取資訊系統之某一特定區域之功能與權限，HTTP 伺服器應透過組態的設定，使其啟動時不具備系統管理者身分。

5.11.2 公告之資訊，應經由權責管理人員之審查與核定，確認未含機密性或敏感性的資訊、違反本系統資訊安全管理之相關資訊，以及違反智慧財產權或法令所明定禁止之資訊。

5.11.3 開放外界連線作業之資訊系統，應避免外界直接進入資訊系統或資料庫存取資料。

5.11.4 內部使用的瀏覽器，對下載之檔案應設定掃描是否隱藏電腦病毒或惡意內容。

5.11.5 當伺服器執行之應用程式需接收自使用者回傳資料時，應予嚴密監

控，以防止不法者利用來執行系統指令，獲取系統內重要的資訊或破壞系統。

5.12 電腦管理及安全防護

5.12.1 系統負責人應定時檢查作業系統及硬體設備之效能，並注意作業系統版本更新及問題資訊，做最適建議及導入。

5.12.2 主機負責人應進行伺服器主機監控，檢查系統、安全及應用程式日誌紀錄、或其它有關之系統狀況。一旦發現任何問題得請相關人員協同處理，必要時並通知廠商處理。

5.12.3 為提升伺服器主機連線作業之安全性，應視需要使用加密通道（如VPN、SSH）等各種安全控管技術。

5.12.4 應關閉不需要之服務。

5.12.5 系統負責人需定期檢視更新系統安全修補、防毒軟體及防毒碼，以維持系統正常運作。

5.12.6 應保存稽核紀錄，並定期審查。

5.12.7 系統負責人應於每工作日上班時依「巡查紀錄表」所列項目檢查各主機狀況，以確保系統正常運作。

5.12.8 軟體由系統負責人安裝，安裝時應視狀況通知相關技術人員支援或通知使用者，以避免資訊服務中斷或影響業務。

5.12.9 系統軟體測試由系統負責人辦理，測試時應事先公告並通知及協調相關人員支援，且視狀況需要通知相關人員及使用者以避免因資訊服務中斷而影響業務。

5.12.10 異常狀況排除

5.12.10.1 遇異常狀況時系統負責人應先行回報資訊安全官，視需要採適當方式處理。

5.12.10.2 通知本校相關人員協助，並說明詳細原因、先行處理步驟及相關資料。如無法自行排除則向維護廠商報修維護，並將故障情形公告及通知使用者及相關人員。

5.12.10.3 將處理過程及結果記錄於「異常事件紀錄表」中。

5.12.11 系統入侵之處理

5.12.11.1 立即拒絕入侵者任何存取動作（例如關閉可疑帳號），以防止災害繼續擴大。

5.12.11.2 關閉受侵害的主機，並立即與網路離線。

5.12.11.3 檢查防火牆及系統紀錄，研判入侵管道之方式，必要時作安全漏洞修補。

5.12.11.4 通知主機供應商提供必要的回復協助。

5.12.11.5 如伺服主機的完整性受侵害，應將完整的系統備份資料存回受害主機上，並測試其功能，直至完全回復止，最後再將該主機重新上線。

5.12.11.6 將處理過程及結果記錄於「異常事件紀錄表」中。

5.13 可攜式電腦儲存媒體管理

5.13.1 系統資料若需以可攜式媒體保存時，該媒體應存放於安全設備或處所。

5.13.2 儲存媒體所使用之密碼或編碼技術不應透露予遞送人員或與業務無關之人員。

5.13.3 儲存媒體遞送前應加以妥善包裝保護，避免發生實體損壞。

5.13.4 儲存媒體如委由外部單位（例如：郵局或快遞公司）運送，應選擇具有信譽之廠商，並採取以下控制措施：

5.13.4.1 放置於上鎖之容器或以彌封方式處理。

5.13.4.2 當面送達並簽收。

5.13.4.3 資料內容應使用密碼保護。

5.13.5 該儲存媒體之報廢，請詳「資訊資產異動作業說明書」，且須經核准。

6 相關文件

6.1 資訊安全政策

6.2 委外管理程序書

6.3 系統獲取、開發及維護程序書

6.4 安全事件管理程序書

6.5 資訊資產異動作業說明書

6.6 矯正及預防管理程序書

6.7 巡查紀錄表

6.8 防火牆進出規則申請表

6.9 備份狀況紀錄表

6.10 異常事件紀錄表

6.11 電子郵件帳號申請表

6.12 弱點處理報告單

國立曾文高級家事商業職業學校

系統獲取、開發及維護程序書

機密等級：限閱

文件編號：TWVS-ISMS-B-009

版　　次：2.0

發行日期：109.04.28

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	102.11.26		文管人員	初版
2.0	109.04.28		文管人員	二版

目錄

系統獲取、開發及維護程序書					
文件編號	XXXX-B-009	機密等級	一般	版本	2.0

1 目的

本程序書制訂之目的在於確保 XXXX 學校（以下簡稱「本校」）資訊系統開發、測試與維護作業之安全管理。

2 適用範圍

資訊系統之程式開發相關支援活動，如既有線上系統之測試、修改、維護、上線變更、原始碼之管控與儲存等作業。

3 權責

本校相關資訊系統開發、維護人員與委外人員：遵守本程序書之相關規定，以確保本校相關軟體與資料等資訊資產之安全。

4 名詞定義

無。

5 作業說明

5.1 一般控制措施

5.1.1 當發展新資訊系統，或現有系統功能之強化，於系統規劃需求分析階段，即將安全需求要項納入系統功能。

5.1.2 除由系統自動執行之安全控管措施之外，亦可考量由人工執行相關控管措施。

5.1.3 在採購套裝軟體時，視其安全需求，進行分析。除事前經權責單位主管核准外，應避免修改套裝軟體，如需修改應依本程序書之變更作業控制措施加以控管。

5.1.4 系統之安全需求及控制程度，應與資訊資產價值相稱，並考量安全措施不足，可能帶來之傷害程度。

5.1.5 資訊系統應保護敏感等級（含）以上之資料，防止洩漏或被竄改，

必要時應使用資料加密之相關機制保護。

5.1.6 在作業系統上執行應用軟體，應建立控制程序並嚴格執行，為減少可能危害作業系統之風險，應用程式之更新作業應限定只能由授權之管理人員才可執行，且應建立應用程式之更新稽核紀錄。

5.1.7 真實資料被複製到測試系統時，應依複製作業之性質及內容，在取得授權後始能進行，敏感資料欄位應予模糊化。

5.1.8 系統若需委外建置或維護，請參考「委外管理程序書」之相關管理規範。

5.1.9 系統弱點管理，請參考「通信與作業管理程序書」之相關管理規範。

5.1.10 各單位若有資料需求申請時，申請人視情況應依電子公文程序或填寫『資料需求申請表』經單位主管同意後，呈資通安全執行祕書核決，本校始得提供資料內容。

5.2 軟體控制措施

5.2.1 作業系統變更時，應審查與測試重要營運系統，以確保對組織作業或安全無不利之衝擊。

5.2.2 系統軟體安裝

系統軟體應由系統負責人進行安裝，安裝時應視狀況通知相關技術人員支援或通知使用者，以避免資訊服務中斷或影響業務。

5.2.3 系統軟體測試

5.2.3.1 軟體測試由系統負責人辦理，測試時應事先通知協調相關人員支援。

5.2.3.2 系統負責人應通知相關人員及使用者以避免資訊服務中斷或影響業務。

5.2.4 系統軟體更新

系統負責人需定期檢視更新系統安全修補、防毒軟體及防毒碼，以維持系統正常運作。

5.3 開發作業控制措施

5.3.1 提案與回覆

5.3.1.1 申請單位提出「系統需求申請與回覆單」敘明需求理由。

5.3.1.2 承辦人員於完成與申請單位之訪談與系統分析後，於「系統需求申請與回覆單」中回覆評估結果，包含功能細項、預估人力與時程、建議方案等。

5.3.1.3 經評估系統修改幅度不大，且不涉及系統流程變更者，於「系統需求申請與回覆單」中回覆處理結果並結案。

5.3.2 分析規劃與程式撰寫

5.3.2.1 程式開發者應於程式開發前進行系統分析，系統分析時應將系統安全需求納入考量。如涉及重要資料之傳輸，應使用 SSL 加密金鑰，並依下列規定管理金鑰：

5.3.2.1.1 金鑰應有明確的啟動與止動日期，並於可用期間，保護其不被修改、遺失和破壞。

5.3.2.1.2 金鑰之使用與存取，應限於使用金鑰之系統管理者，不可由其他非系統管理者任意存取。

5.3.2.1.3 對於金鑰之使用、啟動、止動，皆應留存相關之紀錄。

5.3.2.2 輸入應用系統之資料，應檢查主要欄位或資料檔案的內容，以確保資料的有效性及真確性。

5.3.2.3 對高敏感性的輸入資料，必要時應採用資料保密機制，在傳輸或儲存過程中應採加密方法保護。

5.3.2.4 輸出之資料，應於輸出之前，確認其正確性；對於系統內之

訊息，則需保護其完整性。

5.3.3 測試

5.3.3.1 測試環境與線上環境應予以分開。

5.3.3.2 程式設計初步完成後，準備「系統測試記錄表」通知申請單位進行聯合測試，並請申請單位於「系統測試記錄表」中填寫測試結果。

5.3.3.3 程式功能若無法達成申請單位預定需求，則請系統開發人員另行修改程式後，擇期再測試，直至符合預定需求為止。

5.3.4 上線與驗收

5.3.4.1 聯合測試進行順利完成後，進行相關驗收作業，並請申請單位簽收「系統測試記錄表」。

5.3.4.2 若原系統已經存在，應於系統上線前訂定「系統上線及緊急復原計畫表」，內容包含系統轉換規劃，轉換備援處理等。

5.3.4.3 系統上線後，程式開發者應提出系統設計與功能規格書，內容包含『系統作業流程圖』、『系統資料庫說明表』，以及『系統程式碼清冊』。

5.3.4.4 系統若委由其他單位開發時，應請開發單位交付系統設計與功能規格書，由本校程式開發權責單位審閱，並留存備查。

5.3.5 後續系統增修維護

5.3.5.1 專案上線後功能如需修補，申請單位應填「系統需求申請與回覆單」，程式開發權責單位依需求規格進行訪談規劃設計。

5.3.5.2 程式開發權責單位完成系統增修作業後與申請單位進行測試驗收結案。

5.4 變更作業控制措施

5.4.1 變更作業應考量之事項：

5.4.1.1 在實際執行變更作業前，變更作業之細項建議，應取得權責主管人員之核准。

5.4.1.2 應確保系統變更作業不致影響或破壞系統原有的安全控制。

5.4.1.3 系統開發或變更，應更新系統文件。

5.4.1.4 程式維護時，應在程式內以註解說明異動部分。

5.4.1.5 所有系統變更作業請求，皆應建立紀錄供稽核運用。

5.4.2 變更作業之控制流程：

5.4.2.1 在實際執行變更作業前，申請者應先填具「系統需求申請與回覆單」提出變更需求，並經權責主管人員核准確認。

5.4.2.2 變更作業如有需要，應會辦相關人員配合。

5.4.2.3 上線前應先進行測試,必要時請相關人員配合建置測試環境。

5.4.2.4 除非事先經由權責主管人員核准外，測試不應在線上營運系統執行。

5.4.2.5 測試完成後，程式開發權責單位應擬定「系統上線及緊急復原計畫表」,決定上線日期,經權責主管人員確認後始得上線。

5.4.2.6 上線後應立即於線上營運系統再行測試，以確認系統運作正常。測試人員不宜與程式開發者為同一人，以減少錯誤機會發生。

5.4.2.7 上線後測試如發現狀況，應嘗試可否立即排除，如無法立即排除，應依緊急復原計畫，回復上線前原狀。

5.4.2.8 變更作業完成後應修改相關系統設計與功能規格書。

6 相關文件

6.1 通信與作業管理程序書

6.2 委外管理程序書

6.3 系統需求申請與回覆單

6.4 系統測試紀錄表

6.5 系統作業流程圖

6.6 系統資料庫說明表

6.7 系統上線及緊急復原計畫表

6.8 系統程式碼清冊

6.9 資料需求申請表

國立曾文高級家事商業職業學校

資通安全事件通報及應變管理程序

目錄

壹、 目的

國立曾文高職家事商業職業學校(以下簡稱本校)為遵照資通安全管理法第14 條及本校資通安全維護計畫之規定，建立資通安全事件之通報及應變機制，以迅速有效獲知並處理事件，特制定本資通安全事件通報及應變管理程序(以下稱本管理程序)。

貳、 適用範圍

發生於本校之事件，系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅者。

參、 責任

一、本校於發現資通安全事件時，應依本程序或權責人員之指示，執行通報及應變事務。

二、本校應視必要性，與受託機關約定，使其制定其資通安全事件通報及應變管理程序，並於知悉資通安全事件後向本部進行通報，於完成事件之通報及應變程序後，依本校指示提供相關之紀錄或資料。

三、本校應於知悉資通安全事件後，應依本程序之規定，儘速完成損害控制、復原與事件之調查及處理作業。完成後，應依教育部指定之方式進行結案登錄作業，並送交調查、處理及改善報告。

肆、 事件通報窗口及緊急處理小組

一、臺灣學術網路資通安全事件委託由臺灣學術網路危機處理中心之教育機構資安通報應變小組(簡稱通報應變小組)負責，聯繫資訊如下：

（一） 聯絡電話：(07)525-0211

（二） 網路電話：98400000

（三） 電子郵件：service@cert.tanet.edu.tw

二、本校應至少指派二位以上資安聯絡人員，並於「教育機構資安通報應變平台」(https://info.cert.tanet.edu.tw)登錄相關聯絡資料，如有異動亦應立即上網更新。

三、本校之資通安全事件通報窗口及聯繫專線為：

（一） 聯絡電話：(06)572-2079 轉 209

（二） 網路人：設備組長

（三） 電子郵件：equip@ms2.twvs.tn.edu.tw

四、本校應以適當方式使相關人員明確知悉本機關之通報窗口及聯絡方式。

五、本校所屬人員知悉資通安全事件後，應立即至教育機構資安通報平台(https://info.cert.tanet.edu.tw)通報登錄資安事件細節、影響等級及支援申請等資訊。

六、本校應確保通報窗口之聯絡管道全天維持暢通，若因設備故障或其他情形導致窗口聯絡管道中斷，該中斷情況若持續達一小時以上者，應即將該情況告知相關人員，並即提供其他有效之臨時聯絡管道。

七、負責事件處理之單位(該事件發生之單位)權責人員應與相關單位密切合作以進行事件之處理，並使通報窗口適時掌握事件處理之進度及其他相關資訊。

八、事件經初步判斷認為可能屬重大(第「三」級、第「四」級)資安事件或事態嚴重時，應即向資通安全執行秘書報告，由資通安全執行秘書成立緊急處理小組，立即協助進行處理；接獲受託廠商所通報之資通安全事件時，亦同。

九、緊急處理小組成員由資通安全執行秘書指派機關之資通安全相關技術人員擔任，或亦得由其他機關資通安全相關技術人員或外部專家擔任之。

十、各相關權責人員應紀錄事件處理過程，並檢討事件發生原因，著手進行改善，並留存必要之證據。

伍、 通報程序

一、通報作業程序

(一)判定事件等級之流程及權責

本校之權責人員或緊急處理小組應依據以下事項，於知悉資通安全事件後，依規定完成「資通安全事件通報及應變辦法」之資通安全事件等級判斷：

1.事件涉及核心業務或關鍵基礎設施業務之資訊與否。

2.事件導致業務之資訊或資通系統遭竄改之影響程度，屬嚴重或輕微。

3.事件所涉資訊是否屬於國家機密、敏感資訊或一般公務機密。

4. 機關業務運作若遭影響或資通系統停頓，是否可容忍中斷時間內能回復正常運作。

5. 事件其他足以影響資通安全事件等級之因素。

(二)本校因網路或電力中斷等事由，致無法依前項規定方式為通報者，應於確認資安事件條件成立後 1 小時內，與所隸屬區縣市網路中心及通報應變小組聯繫，先行提供該次資安事件應通報之內容及無法通報依規定方式通報之事由，並於事由解除後，依原方式補行通報。

(三)資通安全事件等級如有變更，本校權責人員或通報應變小組應告知通報單位，使其續行通報作業。

(四)本校於委外辦理資通系統之建置、維運或提供資通服務之情形時，應於合約中訂定委外廠商於知悉資通安全事件時，應即向委託單位所屬之權責人員通知，以指定之方式進行通報。

(五)本校於知悉資通安全事件後，如認該事件之影響涉及其他機關或應由其他機關依其法定職權處理時，權責人員或通報應變小組應於知悉資通安全事件後一小時內，將該事件依教育部或行政院所指訂或認可之方式，通知該機關。

(六)本校執行通報應變作業時，得視情形向所隸屬區縣市網路中心人員提出技術支援或其他協助之需求。

陸、 應變程序

一、事件發生前之防護措施規劃

本校應於平時妥善實施資通安全維護計畫，並以組織營運目標與策略為基準，透過整體之營運衝擊分析，規劃業務持續運作計畫並實施演練，以預防資安事件之發生。

二、損害控制機制

(一)負責應變之權責人員或緊急處理小組，應完成以下應變事務之辦理，並留存應變之紀錄

1. 資安事件之衝擊及損害控制作業。

2. 資安事件所造成損害之復原作業。

3. 重大(第「三」級、第「四」級)資安事件相關鑑識及其他調查作業。

4. 重大(第「三」級、第「四」級)資安事件之調查與處理及改善報告之方式。

5. 重大(第「三」級、第「四」級)資安事件後續發展及與其他事件關聯性

之監控。

6. 資訊系統、網路、機房等安全區域發生重大事故或災難，致使業務中斷時，應依據本機關事前擬定之緊急計畫，進行應變措施以恢復業務持續運作之狀態。

7. 其他資通安全事件應變之相關事項。

(二)對於第一級、第二級資通安全事件，本校應於知悉事件後七十二小時內完成前項事務之辦理，並應留存紀錄；於第三級、第四級資通安全事件，本校應於知悉事件後三十六小時內完成損害控制或復原作業，並執行上述事項，及留存相關紀錄。

(三)本校完成資安事件處理後，須至教育機構資安通報平台填報資安事件處理辦法及完成時間。

(四)本校於知悉受託廠商發生與受託業務相關之資通安全事件時，應於知悉委外廠商發生第一、二級資通安全事件後七十二小時內，確認委外廠商已完成損害控制或復原事項之辦理；於知悉委外廠商發生第三、四級資通安全事件後三十六小時內，確認委外廠商完成損害控制或復原事項之辦理。

柒、 重大(第「三」級、第「四」級)資安事件後之復原、鑑識、調查及改善機制

一、本校若發生重大(第「三」級、第「四」級)資通安全事件時，於完成資通安全事件之通報及應變程序後，應針對事件所造成之衝擊、損害及影響進行調查及改善，並應於事件發生後一個月內完成資通安全事件調查、處理及改善報告。

二、重大(第「三」級、第「四」級)資通安全事件調查、處理及改善報告應包括以下項目：

(一)事件發生、完成損害控制或復原作業之時間。

(二)事件影響之範圍及損害評估。

(三)損害控制及復原作業之歷程。

(四)事件調查及處理作業之歷程。

(五)為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。

(六)前款措施之預定完成時程及成效追蹤機制。

三、本校應向所隸屬之上級機關及教育部提出前項之報告，以供監督與檢討。

捌、 紀錄留存及管理程序之調整

一、本校應將資通安全事件之通報與應變作業之執行、事件影響範圍與損害程度以及其他通報應變之執行情形，於「教育機構資安通報平台」上填報完整之紀錄，該平台事件通報應變紀錄由通報應變小組於年度彙整後，提交至本部資訊及科技教育司覆核備查。

二、本校於完成資通安全事件之通報及應變程序後，應依據實際處理之情形，於必要時對本管理程序、人力配置或其他相關事項進行修正或調整。

玖、 演練作業

一、本校應配合教育部依資通安全事件通報應變辦法之規定所辦理之社交工程演練、資通安全事件通報及應變演練。

二、本校應配合行政院依資通安全事件通報應變辦法之規定所辦理之下列資通安全演練作業：

(一)社交工程。

(二)資安事件通報及應變

(三)網路攻防

(四)情境演練

(五)其他資安演練

委外廠商保密切結書					
文件編號	TWVS-ISMS-D-022a	機密等級	機密	版次	2.0

紀錄編號：

立切結書人＿＿＿＿＿＿（簽署人姓名）等，受＿＿＿＿＿＿＿＿＿＿（廠商名稱）委派至國立曾文高級家事商業職業學校（以下稱本校）處理業務，謹聲明恪遵本校下列工作規定，對工作中所持有、知悉之資訊系統作業機密或敏感性業務檔案資料，均保證善盡保密義務與責任，非經本校權責人員之書面核准，不得擷取、持有、傳遞或以任何方式提供給無業務關係之第三人，如有違反願賠償一切因此所生之損害，並擔負相關民、刑事責任，絕無異議。

一、 未經申請核准，不得私自將本校之資訊設備、媒體檔案及公務文書攜出。

二、 未經本校業務相關人員之確認並代為申請核准，不得任意將攜入之資訊設備連接本校網路。若經申請獲准連接本校網路，嚴禁使用數據機或無線傳輸等網路設備連接外部網路。

三、 經核准攜入之資訊設備欲連接本校網路或其他資訊設備時，須經電腦主機房掃毒專責人員進行病毒、漏洞或後門程式檢測，通過後發給合格標籤，並將其粘貼在設備外觀醒目處以備稽查。

四、 廠商駐點服務及專責維護人員原則應使用本校配發之個人電腦與週邊設備，並僅開放使用本校內部網路。若因業務需要使用本校電子郵件、目錄服務，應經本校業務相關人員之確認並代為申請核准，另欲連接網際網路亦應經本校業務相關人員之確認並代為申請核准。

五、 本校得定期或不定期派員檢查或稽核立切結書人是否符合上列工作規定。

六、 本保密切結書不因立切結書人離職而失效。

七、 立切結書人因違反本保密切結書應盡之保密義務與責任致生之一切損害，立切結書人所屬公司或廠商應負連帶賠償責任。

此致

國立曾文高級家事商業職業學校

立切結書人：

具 切 書 廠 商：

代　　表　　人：

統 一 編 號：

地　　址：

中　華　民　國　　年　　月　　日

委外廠商保密同意書					
文件編號	TWVS-ISMS-D-022b	機密等級	機密	版次	2.0

紀錄編號：

茲緣於簽署人＿＿＿＿＿＿（簽署人姓名，以下稱簽署人）參與＿＿＿＿＿＿（廠商名稱，以下稱廠商）得標國立曾文高級家事商業職業學校（以下稱本校）資通業務委外案＿＿＿＿＿＿（案名）（以下稱「本案」），於本案執行期間有知悉或可得知悉或持有政府公務秘密及業務秘密，為保持其秘密性，簽署人同意恪遵本同意書下列各項規定：

第一條 簽署人承諾於本契約有效期間內及本契約期滿或終止後，對於所得知或持有一切本校未標示得對外公開之公務秘密，以及本校依契約或法令對第三人負有保密義務之業務秘密，均應以善良管理人之注意妥為保管及確保其秘密性，並限於本契約目的範圍內，於本校指定之處所內使用之。非經本校事前書面同意，不得為本人或任何第三人之需要而複製、保有、利用該等秘密或將之洩漏、告知、交付第三人或以其他任何方式使第三人知悉或利用該等秘密，或對外發表或出版，亦不得攜至本校或本校所指定處所以外之處所。

第二條 簽署人知悉或取得本校公務秘密與業務秘密應限於其執行本契約所必需且僅限於本契約有效期間內。簽署人同意公務秘密與業務秘密，應僅提供、告知有需要知悉該秘密之履約廠商團隊成員人員。

第三條 簽署人在下述情況下解除其所應負之保密義務：

原負保密義務之資訊，由本校提供以前，已合法持有或已知且無保密必要者。

原負保密義務之資訊，依法令業已解密、依契約本校業已不負保密責任、或已為公眾所知之資訊。

原負保密義務之資訊，係自第三人處得知或取得，該第三人就該等資訊並無保密義務。

第四條 簽署人若違反本同意書之規定，本校得請求簽署人及其任職之廠商賠償本校因此所受之損害及追究簽署人洩密之刑責，如因而致第三人受有損害者，簽署人及其任職之廠商亦應負賠償責任。

第五條 簽署人因本同意書所負之保密義務，不因離職或其他原因不參與本案而失其效力。

第六條 本同意書一式叁份，本校、簽署人及.....（廠商）各執存一份。

此致

國立曾文高級家事商業職業學校

立切結書人：

具 切 書 廠 商：

代　　表　　人：

統 一 編 號：

地　　址：

中　　華　　民　　國　　年　　月　　日

委外廠商查核項目表					
文件編號	TWVS-ISMS-D-022C	機密等級	機密	版次	2.0

紀錄編號：

查核項目	查核內容	查核結果	說明
1.人員及資源配置	1.1 配置專責人員或組織？	□符合□不符 □不適用	
	1.2 配置適當資源？	□符合□不符 □不適用	
2.界定個人資料	2.1 進行個資盤點？	□符合□不符 □不適用	
	2.2 個資盤點是否確實？	□符合□不符 □不適用	
	2.3 建立盤點清冊？	□符合□不符 □不適用	
3.風險評估	3.1 進行風險評估？	□符合□不符 □不適用	
	3.2 製成風險評鑑表？	□符合□不符 □不適用	
	3.3 針對風險進行因應？	□符合□不符 □不適用	
4.事故通報應變	4.1 有通報及應變程序？	□符合□不符 □不適用	
	4.2 事故發生時確實通報？	□符合□不符 □不適用	當年度無事故者 4.2~4.6 免填
	4.3 事故發生後採取應變措施？	□符合□不符 □不適用	
	4.4 於期限內通知當事人？	□符合□不符 □不適用	
	4.5 事後採取預防措施？	□符合□不符 □不適用	
	4.6 將事故處理情形通知？	□符合□不符 □不適用	
5.蒐集處理利用之內部管理程序	5.1 資料蒐集、處理具備特定目的並具有法定要件？	□符合□不符 □不適用	
	5.2 依規定取得當事人同意（當事人同意之情形）？	□符合□不符 □不適用	
	5.3 履行告知義務（未履行告知義務時，是否符合免告知之情形）？	□符合□不符 □不適用	
	5.4 個人資料之利用，符合特定目的之範圍？	□符合□不符 □不適用	
	5.5 是否有目的外之利用？	□符合□不符 □不適用	
	5.6 目的外利用是否符合法定要件？	□符合□不符	

委外廠商查核項目表					
文件編號	TWVS-ISMS-D-022C	機密等級	機密	版次	2.0

查核項目	查核內容	查核結果	說明
		□不適用	
	5.7 是否利用因執行本契約所蒐集之個人資料進行行銷？	□符合□不符 □不適用	
	5.8 是否提供個人資料予第三人？	□符合□不符 □不適用	
	5.9 是否有進行複委託？	□符合□不符 □不適用	無複委託時5.8免填
	5.10 對複委託方進行監督？	□符合□不符 □不適用	
	5.11 當事人權利行使流程？	□符合□不符 □不適用	
	5.12 將當事人權利行使回覆情形做成紀錄供備查？	□符合□不符 □不適用	
	5.13 契約終止或解除，是否刪除、銷毀所持有之個人資料？	□符合□不符 □不適用	
	5.14 契約終止或解除，是否返還個人資料之載體？	□符合□不符 □不適用	
6.資料安全與人員管理	6.1 是否進行去識別化作業？	□符合□不符 □不適用	
	6.2 是否有資料存取控制措施？	□符合□不符 □不適用	
	6.3 是否進行加密？	□符合□不符 □不適用	
	6.4 資料之傳送是否進行管控？	□符合□不符 □不適用	
	6.5 保有資料者是否遵守保密協定？	□符合□不符 □不適用	
	6.6 人員進出情形是否具體掌控？	□符合□不符 □不適用	
7.認知宣導與教育訓練	7.1 是否確實進行認知宣導與教育訓練？	□符合□不符 □不適用	
	7.2 是否進行課後評量？	□符合□不符 □不適用	
	7.3 是否對新進人員進行教育訓練？	□符合□不符 □不適用	
8.設備安全管理	8.1 是否對設備及環境進行控管與保護？	□符合□不符 □不適用	
	8.2 是否定期檢查或維護更新設備？	□符合□不符 □不適用	
9.稽核機制	9.1 是否設有稽核制度？	□符合□不符 □不適用	
	9.2 是否定期實施稽核？	□符合□不符 □不適用	

委外廠商查核項目表					
文件編號	TWVS-ISMS-D-022C	機密等級	機密	版次	2.0

查核項目	查核內容	查核結果	說明
10.紀錄保存	10.1 是否保存個資管理紀錄？	□符合□不符 □不適用	
11.持續改善	11.1 是否定期檢視個資保護措施？	□符合□不符 □不適用	
	11.2 是否針對缺失進行改善？	□符合□不符 □不適用	
	11.3 是否依所提出之建議進行改善？	□符合□不符 □不適用	

國立曾文高級家事商業職業學校

資通安全管理制度內部稽核計畫

機密等級：限閱

文件編號：**TWVS-ISMS-C-004**

版　　次：**2.0**

發行日期：**109.04.28**

修　訂　紀　錄				
版次	修訂日期	修訂頁次	修訂者	修訂內容摘要
1.0	102.11.26		文管人員	初版
2.0	109.04.28		文管人員	二版

目錄

資通安全管理制度內部稽核計畫					
文件編號	TWVS-ISMS-C-004	機密等級	敏感	版次	2.0

1 主旨

為落實國立曾文高級家事商業職業學校（以下簡稱「本校」）資通安全管理制度執行，以反映政策、法令、技術及現行業務之最新狀況，確保資通安全政策與資通安全實務作業之有效性及可行性。

2 目標

符合本校所訂定之資通安全政策及各項安全管理規定。

3 稽核範圍

本校資訊機房維運服務營運相關資訊業務。

4 稽核項目

4.1 適用性聲明書之確認

4.2 ISMS 建置步驟

4.3 ISMS 建置需求

4.4 資訊安全政策訂定與評估。

4.5 資訊安全組織。

4.6 人力資源安全。

4.7 資產管理。

4.8 存取控制。

4.9 密碼學(加密控制)。

4.10 實體及環境安全。

4.11 運作安全。

4.12 通訊安全。

4.13 系統獲取、開發及維護。

4.14 供應者關係。

4.15 .資訊安全事故管理。

4.16 營運持續管理之資訊安全層面。

4.17 遵循性。

5 資通安全稽核小組成員

組長：ＸＸＸ

組員：ＸＸＸ、ＸＸＸ

6 稽核時程

日 期	時 間	項 目	稽核人員	地點
	10:00-10:20	啟始會議	ＸＸＸ ＸＸＸ ＸＸＸ	
	10:20-10:30	高階主管訪談		
	10:30-12:00	● 適用性聲明書之確認 ● ISMS 建置步驟 ● ISMS 建置需求 ● 資訊安全政策訂定與評估。 ● 資訊安全組織。 ● 人力資源安全。 ● 資產管理。 ● 存取控制。 ● 密碼學(加密控制)。 ● 實體及環境安全。		
	12:00-13:00			

	13:00-15:30	● 運作安全。 ● 通訊安全。 ● 系統獲取、開發及維護。 ● 供應者關係。 ● .資訊安全事故管理。 ● 營運持續管理之資訊安全層面。 ● 遵循性之符合性	XXX XXX XXX	
	15:30-16:00	稽核結果彙整		
	16:00-16:30	結束會議		

7 稽核程序

7.1 執行日期：XX 年 XX 月 XX 日。

7.2 啟始會議

- 資通安全稽核小組成員介紹
- 確認稽核目的及範圍
- 稽核程序報告
- 稽核方法說明

7.3 高階主管訪談

- 透過與高階主管訪談方式，瞭解本校推動資通安全管理制度之決心、資源分配以及所面臨之問題

7.4 實地稽核

- 實地驗證資通安全管理系統執行之有效性
- 以面談、觀察、抽樣檢查方式進行

7.5 稽核結果彙整

- 資通安全稽核小組根據稽核事實討論所發現之缺失事項
- 彙整稽核結果
- 總結報告

7.6 結束會議

- 資通安全稽核小組報告發現之缺失事項
- 改善建議
- 問題澄清與討論
- 稽核總結

8 附件

8.1 資通安全管理制度內部稽核表

8.2 矯正與預防處理單

資通安全管理制度內部稽核紀錄表					
文件編號	TWVS-ISMS-D-039	機密等級	限閱	版次	2.0

紀錄編號：　　填表日期：　　年　　月　　日

評分標準說明：

A：相關資訊安全管理制度規範已建立，且落實執行

B：相關資訊安全管理制度規範未建立，但已實施替代性資安控管措施

C：相關資訊安全管理制度規範已建立，但未落實執行

D：相關資訊安全管理制度規範未建立，且未實施替代性資安控管措施

E：不適用

稽核項目 – 規範本文

條款章節	依據條文	稽核評分					稽核發現與說明
		A	B	C	D	E	
陸、	關於適用性聲明(Statement of Applicability)						
	本標準之設計為適用於教育體系與相關單位，但鑑於類型、規模、資源、業務性質等因素，若本標準列出之任何條款無法適用於某單位時，可考慮予以排除，但必須在不影響該單位提供資訊安全能力與責任之情況下，並提出理由。在建置完該單位之 ISMS 後，必須提出符合的適用性聲明，其中應包含選擇之控制目標與控制措施項目與理由，以及排除條款之內容、理由，作為稽核時的依據。	☐	☐	☐	☐	☐	
捌、	關於資訊安全管理系統 (ISMS)建置步驟						

資通安全管理制度內部稽核紀錄表					
文件編號	TWVS-ISMS-D-039	機密等級	限閱	版次	2.0

條款 章節	依據條文	稽核評分					稽核發現與說明
		A	B	C	D	E	
捌、三	ISMS 之建立：依據該單位之類型、規模、資源、業務性質等特性，定義 ISMS 之範圍；考慮相關法律、法規，以及合約之要求，於適度評估風險及應對措施後，訂出經由管理階層核准之 ISMS 政策，並擬定一份適用性聲明書文件。	☐	☐	☐	☐	☐	
捌、四	ISMS 之實施與操作：施行單位應確實實施控制措施，以符合控管的目標，並執行訓練與認知計畫，確保偵測安全事件的能力，以及迅速回應和應對處理的時效。	☐	☐	☐	☐	☐	
捌、五	ISMS 之監控及審查：施行單位應針對 ISMS 進行監控程序與其他控制措施，即時鑑別資安事件的發生、處理順序與解決方法；定期審查 ISMS 之有效性（建議一學年至少一次），並將相關有顯著影響之活動與事件記錄下來。	☐	☐	☐	☐	☐	
捌、六	ISMS 之維持及改進：施行單位應定期實行改進活動，採取適當的矯正與預防措施，並得到管理階層之同意，並確保各項措施達到預期目標。	☐	☐	☐	☐	☐	
玖、	關於資訊安全管理系統 (ISMS)建置需求						
玖、七	文件要求：關於 ISMS 文件化（電子檔案或紙本），必須包含安全政策、安全目標、ISMS 範圍、適用性聲明、資安事件記錄，以及其他有助於提升 ISMS 成效之文件；上述之文件需接受保護與管制，並定期的審查及更新，確保文件之最新版本；任何過期文件需保留或銷毀，應予以適當的鑑別。	☐	☐	☐	☐	☐	
玖、八	管理階層責任：施行單位之管理階層，最為重要的是給予承諾及實	☐	☐	☐	☐	☐	

條款 章節	依據條文	稽核評分					稽核發現與說明
		A	B	C	D	E	
	際的支持，並適度的提供資源以助 ISMS 程序的進行，必要時審查 ISMS 的控制措施與有效性；另外，確保於 ISMS 範圍內之員工，具備足夠之能力及認知，並定期進行教育訓練。						
玖、九	管理階層審查：管理階層應在規劃期間內，審查該單位的 ISMS 與適用範圍，確保其持續的適用性、適切性及有效性；其中應審查包含變更需求與改進時機，並將其結果確實文件化。	☐	☐	☐	☐	☐	
玖、十	ISMS 之改進：ISMS 的改進是持續的，必須藉由各資安事件與審查結果，做出適度的反應與改進，持續系統之有效性；另外，對應的矯正措施以及防範未然的預防措施，亦須予以制定並文件化。	☐	☐	☐	☐	☐	

稽核項目 – 控制目標與控制項目

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A5	資訊安全政策訂定與評估							
A.5.1	資訊安全政策訂定與評估							
A.5.1.1	資訊安全政策制定	資訊安全政策應參考資安相關法令及施行單位業務上的需求，並經由管理階層核准，以適當方式向所有員工公佈與宣導，在必要時告知相關單位及合作廠商，以利共同遵守。	☐	☐	☐	☐	☐	
A.5.1.2	資訊安全政策評估	面對資安事件的發生、資安相關法令與其他影響因素的改變時，資訊安全政策應進行即時的評估，並定期審查政策的可行性與有效性。	☐	☐	☐	☐	☐	
A6	資訊安全組織							
A.6.1	資訊安全組織推動與權責							
A.6.1.1	資訊安全組織推動以及權責之分配	由管理階層舉辦定期之資訊安全會報，召集相關單位代表進行工作與責任的分屬，確保資安相關計畫的進行，並展現管理階層的支持。	☐	☐	☐	☐	☐	
A.6.1.2	資訊設施使用之授權	資訊處理設備的移轉（包含新設備），應由權責主管人員進行授權、移交的程序，確保該設備後續的順利運作及責任所屬。	☐	☐	☐	☐	☐	
A.6.1.3	保密條款之簽訂	施行單位之員工（包含正職員工、臨時雇員）應簽署獨立或包含保密條款之合約，確保其了解應有之資安責任與相關限制。	☐	☐	☐	☐	☐	

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.6.1.4	跨單位合作及協調	為確保資訊安全作業的順利運行，需與執法機關、主管機構、資訊服務廠商及電信公司建立適當的溝通管道。	☐	☐	☐	☐	☐	
A.6.1.5	資訊安全諮詢與顧問	在必要時，須向單位內部專業人員或外部專業諮詢人員徵詢、協調資訊安全建議。	☐	☐	☐	☐	☐	
A.6.1.6	資訊安全政策的獨立檢視	機關制訂之資訊安全政策，應進行獨立及客觀的評估。	☐	☐	☐	☐	☐	
A.6.2	施行單位外部人員存取安全管理							
A.6.2.1	施行單位外部人員存取之安全掌控	面對外部人員存取施行單位資訊處理設施的可能風險，應視狀況採取適當的安全控制措施，並條列安全規定於正式合約中。	☐	☐	☐	☐	☐	
A.7	資訊資產分類與管制							
A.7.1	資訊資產分類與責任分屬							
A.7.1.1	資訊資產目錄建立	應製作所有資訊資產之清冊，並定期維護、更新。	☐	☐	☐	☐	☐	
A.7.1.2	資訊安全等級分類	資訊資產應進行分級與標示，並考量重要資產的需求，於必要時制定保護措施及處理流程。	☐	☐	☐	☐	☐	
A.8	人員安全管理與教育訓練							
A.8.1	聘任前之處理							

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.8.1.1	所屬角色與責任	施行單位之員工、廠商及第三方使用者的資訊安全角色及責任應適需求以書面或其他方式清楚定義，並與資訊安全政策一致。	☐	☐	☐	☐	☐	
A.8.2	聘用中之處理							
A.8.2.1	資訊安全教育訓練	施行單位內所有員工、合作廠商與第三方使用者應接受適當之資安訓練與有關資安政策、程序之宣導課程。	☐	☐	☐	☐	☐	
A.8.2.2	違反規定之處理	依據既定之條款或合約，違反施行單位之資訊安全政策與程序之人員，應予以適當之懲處。	☐	☐	☐	☐	☐	
A.8.3	結束聘任或改變職務							
A.8.3.1	結束聘用之處理	負責執行結束聘用或改變職務之權責，其職掌應清楚定義並指派。	☐	☐	☐	☐	☐	
A.8.3.2	資產繳回	離職時，應有正式的資產繳回程序，顯示其已繳回單位資產。	☐	☐	☐	☐	☐	
A.8.3.3	存取權移除	所有員工、合約商及第三方使用者的存取權限應根據既有的規範或協定進行移除或改變。	☐	☐	☐	☐	☐	
A.9	實體與環境安全							
A.9.1	區域之安全							
A.9.1.1	實體環境安全	施行單位應採用適當防護措施保障資訊處理設施所在區域（機房設備、人員辦公區域）的安全。	☐	☐	☐	☐	☐	
A.9.1.2	人員進出控制	施行單位應實施控制措施，確保只有授權人員可以進出安全區域。	☐	☐	☐	☐	☐	

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.9.1.3	資訊處理設施安全	在資訊處理設施所在區域工作，應採取適當的控制措施與指引，確保該區域的安全性。	☐	☐	☐	☐	☐	
A.9.2	設備之安全							
A.9.2.1	設備安置地點之保護措施	施行單位應安置或保護設備，降低環境之威脅、災害，以及未授權存取所造成的可能損失。	☐	☐	☐	☐	☐	
A.9.2.2	電源供應	施行單位應保護資訊處理設備，降低電力故障或異常的影響。	☐	☐	☐	☐	☐	
A.9.2.3	電纜線安全防護	施行單位應保護通訊纜線及資訊處理設備之電源，降低受竊聽或破壞的可能損失。 —較適用於第一群	☐	☐	☐	☐	☐	
A.9.2.4	設備之維護	資訊處理設備應予以適當的維護，確保其持續運作。	☐	☐	☐	☐	☐	
A.9.2.5	設備報廢與再使用	資訊處理設備在報廢或再使用的過程中，應避免內存資料的外洩，進行必要之清除動作。	☐	☐	☐	☐	☐	
A.9.2.6	預防未經授權之移動	施行單位所屬之設備、資訊或軟體未經授權禁止移動。	☐	☐	☐	☐	☐	
A.10	通訊與作業安全管理							
A.10.1	作業程序與責任							
A.10.1.1	作業程序文件化	安全政策所規定之作業程序，應文件化並定期維護。	☐	☐	☐	☐	☐	

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.10.1.2	作業變更之管理	資訊處理設施、系統之變更，應進行管制。	☐	☐	☐	☐	☐	
A.10.1.3	資訊安全責任之分散	職務與責任範圍需予區分，降低資訊或服務遭未授權修改或誤用之機會。 —較適用於第一群	☐	☐	☐	☐	☐	
A.10.1.4	系統發展、測試及實務作業之分散	開發或測試用之設備、軟體轉換至作業狀態，應制定規則分隔開來，並加以文件化。 —較適用於第一群	☐	☐	☐	☐	☐	
A.10.2	資訊作業委外服務之安全管理							
A.10.2.1	資訊作業服務之管控	施行單位執行資訊業務委外時，應與廠商簽訂適當的資訊安全協定及課予相關的安全管理責任，納入契約條款。	☐	☐	☐	☐	☐	
A.10.2.2	服務之監控與審查	施行單位應監視和審查廠商提供的服務，確保服務標準達到協議的要求。	☐	☐	☐	☐	☐	
A.10.2.3	廠商服務異動	面對廠商服務異動的管理程序，應注意相關的系統及程序，確實的掌控以避免導致新資安危機。 —較適用於第一群	☐	☐	☐	☐	☐	
A.10.3	系統規劃與驗收							
A.10.3.1	系統作業容量之規劃	施行單位應適時預估系統容量需求，確保有充分處理資料與儲存的空間。 —較適用於第一群	☐	☐	☐	☐	☐	

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.10.3.2	新系統上線作業之安全評估	新資訊系統、系統升級與新版本正式上線前應予以適當的測試，建立固定的驗收程序。	☐	☐	☐	☐	☐	
A.10.4	電腦病毒、惡意軟體							
A.10.4.1	電腦病毒及惡意軟體之控制	施行單位應進行防備電腦病毒與惡意軟體之偵測及預防的控制措施，以及使用者認知程序。	☐	☐	☐	☐	☐	
A.10.5	備份作業之管控							
A.10.5.1	資料備份	重要資訊與軟體應進行定期的備份。	☐	☐	☐	☐	☐	
A.10.6	網路安全管理 —較適用於學術網路系統							
A.10.6.1	網路安全規劃與管理	應實施網路控制措施，維護網路安全。	☐	☐	☐	☐	☐	
A.10.6.2	網路服務之安全控制	使用公用或私用網路，應評估網路服務提供者之安全措施是否足夠，並提供明確的安全措施說明，另應考量使用該項網路對維持機關資料傳輸機密性、資料完整性及可用性等各種安全影響。	☐	☐	☐	☐	☐	
A.10.7	儲存媒體的處理與安全							
A.10.7.1	電腦媒體之安全管理	電腦儲存媒體、可攜式媒體或印出報表，應制定控管措施。	☐	☐	☐	☐	☐	

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.10.7.2	電腦媒體處理之安全	應訂定電腦媒體的處理作業程序，以降低可能的安全風險。	☐	☐	☐	☐	☐	
A.10.7.3	資料檔案之保護	重要資料檔案應進行控管，並安全的保存。	☐	☐	☐	☐	☐	
A.10.7.4	系統文件之安全	重要系統文件應受到保護，避免未授權之存取。	☐	☐	☐	☐	☐	
A.10.8	資訊與軟體交換							
A.10.8.1	資訊與軟體交換安全政策與協定	單位間交換資訊與軟體的行為（具機密性或敏感性內容）應有安全保護措施及協議規範，必要時制定正式合約。	☐	☐	☐	☐	☐	
A.10.8.2	電子郵件安全管理	應制定電子郵件使用政策，並實施控制措施降低安全風險。	☐	☐	☐	☐	☐	
A.10.8.3	電子辦公系統安全	視需求應制定並實施控制措施，以管制和電子辦公系統有關之單位及安全風險。	☐	☐	☐	☐	☐	
A.10.8.4	對外公告資訊之管理	對外公告資訊前應有正式授權程序，並避免未授權之竄改。	☐	☐	☐	☐	☐	
A.10.9	系統存取及應用之監督							
A.10.9.1	事件記錄	建立及製作例外事件及資訊安全事項的稽核軌跡，並保存一段的時間，以作為日後調查及監督之用。	☐	☐	☐	☐	☐	
A.10.9.2	系統使用之監控	為確保使用者只能執行授權範圍內的事項，應建立系統使用監督程序。	☐	☐	☐	☐	☐	

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.10.9.3	記錄的保護	單位應保護未授權的變更及防止記錄設備操作發生問題。	☐	☐	☐	☐	☐	
A.10.9.4	系統管理者與作業人員之記錄	應忠實紀錄系統管理者與作業人員之相關操作記錄。	☐	☐	☐	☐	☐	
A.10.9.5	系統錯誤事項之紀錄	系統發生錯誤之事項時，應予以忠實的記錄，並進行適當的處理程序。	☐	☐	☐	☐	☐	
A.10.9.6	系統時鐘應予同步	應定期校正系統作業時間，維持系統稽核紀錄的正確性及可信度，最為事後法律上或是紀律處理上的重要依據。	☐	☐	☐	☐	☐	
A.11	存取控制安全							
A.11.1	使用者存取控制							
A.11.1.1	使用者註冊管理	應制定正式使用者註冊、註銷流程和條款，以供存取資訊系統及服務。	☐	☐	☐	☐	☐	
A.11.1.2	系統存取特別權限管理	限制與控管特許權限的分配及使用方式。 —較適用於第一群	☐	☐	☐	☐	☐	
A.11.1.3	一般通行碼之控管	應建立使用者通行碼之管理制度。	☐	☐	☐	☐	☐	
A.11.1.4	系統存取權限之評估	施行單位應定期審查使用者存取權限。 —較適用於第一群	☐	☐	☐	☐	☐	
A.11.2	使用者責任							

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.11.2.1	桌面淨空安全管理	應考量採用辦公桌面的淨空政策，以減少文件及儲存媒體等在正常的辦公時間之外遭未被授權的人員取用、遺失、竄改或是被破壞的機會。	☐	☐	☐	☐	☐	
A.11.3	網路存取控制措施							
A.11.3.1	網路服務之限制	施行單位須清楚限定使用者只能直接存取准許使用之服務。	☐	☐	☐	☐	☐	
A.11.3.2	遠端使用者身分鑑別	遠端連線使用者之存取需進行身分鑑別。 —較適用於第一群	☐	☐	☐	☐	☐	
A.11.3.3	診斷埠(Diagnostic Ports)存取控制	診斷埠的存取行為必須嚴密控管。 —較適用於第一群	☐	☐	☐	☐	☐	
A.11.3.4	網路分隔控制	網路應視需求控制措施，將資訊服務、使用者及各資訊系統區隔。 —較適用於第一群	☐	☐	☐	☐	☐	
A.11.3.5	網路連線控制	使用者連線能力應視需求予以限制。 —較適用於第一群	☐	☐	☐	☐	☐	
A.11.3.6	網路路由控制	共享網路應有路由控制措施，確保電腦連線及資訊流依循應用系統之存取控管政策。 —較適用於第一群	☐	☐	☐	☐	☐	
A.11.4	作業系統存取控制							

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.11.4.1	系統登入程序	使用者存取電腦系統應經由安全的系統登入程序。	☐	☐	☐	☐	☐	
A.11.4.2	使用者通行碼管理	應以安全有效的使用者通行碼管理系統鑑別使用者身份。	☐	☐	☐	☐	☐	
A.11.4.3	系統公用程式管理	系統上公用程式的使用，應予限制並控管。 —較適用於第一群	☐	☐	☐	☐	☐	
A.11.4.4	連線作業時間之控制	必要時限制使用者在高風險應用系統的連線作業時間。 —較適用於第一群	☐	☐	☐	☐	☐	
A.11.5	應用系統的存取控制 —較適用於行政資訊系統							
A.11.5.1	資訊存取限制	依資訊存取規定，配予應用系統的使用者與業務需求相稱的資料存取及應用系統的使用權限。	☐	☐	☐	☐	☐	
A.11.5.2	機密及敏感性系統之獨立作業	必要時對機密性及敏感性系統，考量建置獨立的或是專屬的電腦作業環境。 —較適用於第一群	☐	☐	☐	☐	☐	
A.11.6	行動式電腦作業與遠距工作管理 —較適用於第一群							
A.11.6.1	行動式電腦作業控制	必要時應針對行動式電腦設施制定適當的控制措施及政策。 —較適用於第一群	☐	☐	☐	☐	☐	

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.11.6.2	遠距工作管理	施行單位應制定遠距工作活動的政策、流程及標準，控管相關活動的進行。 —較適用於第一群	☐	☐	☐	☐	☐	
A.12	系統開發與維護之安全							
A.12.1	系統安全要求 —較適用於行政資訊系統 —較適用於第一群							
A.12.1.1	安全需求分析及規格訂定	應詳述新系統或既有系統之各項控制措施要求。 —較適用於第一群	☐	☐	☐	☐	☐	
A.12.2	應用系統安全 —較適用於行政資訊系統							
A.12.2.1	資料輸入之驗證	輸入應用系統之資料須確認其正確性與適當性。	☐	☐	☐	☐	☐	
A.12.2.2	系統內部作業處理之驗證	系統需建立確認檢查機制，以偵知所處理資料的塗改。	☐	☐	☐	☐	☐	
A.12.2.3	訊息真確性之鑑別	必要時應採用訊息鑑別機制，保護訊息內容的完整性。 —較適用於第一群	☐	☐	☐	☐	☐	
A.12.2.4	資料輸出控管	應用系統的資料輸出需經過確認，確保處理程序的正確性與適當性。	☐	☐	☐	☐	☐	

條款 章節	依據條文		稽核評分 A B C D E	稽核發現與說明
A.12.3	加密控制措施 —較適用於第一群			
A.12.3.1	資料加密	必須發展加密控制措施保護資訊之政策。 —較適用於第一群	☐ ☐ ☐ ☐ ☐	
A.12.3.2	憑證機構之技術安全	以一套公認之標準、流程及方法為金鑰管理系統之基礎，支援加密技術之運用。 —較適用於第一群	☐ ☐ ☐ ☐ ☐	
A.12.4	系統檔案安全			
A.12.4.1	作業軟體控制	需建立作業系統各個軟體實施的管制程序，避免軟體影響作業系統之完整。	☐ ☐ ☐ ☐ ☐	
A.12.4.2	系統測試資料之保護	系統之測試資料須予以保護與控管。 —較適用於第一群	☐ ☐ ☐ ☐ ☐	
A.12.4.3	原始程式庫資源之存取控制	原始程式庫 (Source Library)的存取必須採取嚴格的控制措施，避免在存取原始程式庫的程序中，造成原始程式庫的損毀。 —較適用於第一群	☐ ☐ ☐ ☐ ☐	
A.12.5	開發與支援作業的控制 —較適用於第一群			
A.12.5.1	變更作業之控制程序	實施變更作業應依循嚴格的變更管制措施。 —較適用於第一群	☐ ☐ ☐ ☐ ☐	

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.12.5.2	作業系統變更之技術評估	應用系統必須有所變更時，需進行必要之技術審核及測試。 —較適用於第一群	☐	☐	☐	☐	☐	
A.12.5.3	套裝軟體變更限制	避免修改套裝軟體，有必要修改時需採取嚴格管制。 —較適用於第一群	☐	☐	☐	☐	☐	
A.12.5.4	資訊洩漏控制	預防施行單位資訊遭洩漏的危機，制定適當的控管措施。 —較適用於第一群	☐	☐	☐	☐	☐	
A.12.5.5	軟體委外開發	軟體之委外、使用需採取適當之管制及檢查。 —較適用於第一群	☐	☐	☐	☐	☐	
A.12.6	系統弱點管理 —較適用於第一群							
A.12.6.1	系統弱點控制	應及時取得有關針對系統弱點的資訊，並評估該弱點暴露的程度及所造成的可能危機。 —較適用於第一群	☐	☐	☐	☐	☐	
A.13	資訊安全事件之反應及處理							
A.13.1	資訊安全事件與弱點之通報							
A.13.1.1	資訊安全事件與弱點通報	資安事件需即刻進行通報。	☐	☐	☐	☐	☐	
A.13.2	資訊安全事件之管理							

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.13.2.1	資安事件處理責任與程序建立	應建立處理資訊安全事件之作業程序，並課予相關人員必要的責任，以便迅速有效處理機關資訊安全事件。	☐	☐	☐	☐	☐	
A.13.2.2	從資安事件中學習	監控並紀錄事件的過程與結果，必要時進行檢討會議，討論改善之事宜。	☐	☐	☐	☐	☐	
A.13.2.3	資安事件證據之收集	電腦稽核軌跡及相關的證據，應以適當的方法保護。	☐	☐	☐	☐	☐	
A.14	業務永續運作管理 —較適用於第一群							
A.14.1	永續運作管理之規劃 —較適用於第一群							
A.14.1.1	業務永續運作之規劃程序	施行單位應建立業務永續運作之程序及架構，鑑定測試及維護之優先順序，訂定與維護永續運作之計畫。 —較適用於第一群	☐	☐	☐	☐	☐	
A.14.1.2	永續運作計畫之測試及更新	永續運作計畫應進行測試與維護，確保該計畫的有效性。 —較適用於第一群	☐	☐	☐	☐	☐	
A.15	相關法規與施行單位政策之符合性							
A.15.1	法規之遵守							

資通安全管理制度內部稽核紀錄表					
文件編號	TWVS-ISMS-D-039	機密等級	限閱	版次	2.0

條款 章節	依據條文		稽核評分					稽核發現與說明
			A	B	C	D	E	
A.15.1.1	適用法規之鑑別	蒐集相關法律條文（智慧財產權、資料隱私保護及其他相關法規）、管理規定及合約要求，了解與資訊處裡設施、軟體系統的關係，並予以書面或其他方式留存。	☐	☐	☐	☐	☐	
A.15.1.2	適用法規之遵循	需制定適當的流程與管制，保護重要紀錄，並確保遵守智慧財產權、個人資料保護及隱私等條文規範，防止資訊處理設施遭不當之使用。	☐	☐	☐	☐	☐	
A.15.2	安全政策與技術符合性之檢驗							
A.15.2.1	確保遵守安全政策與規範	確保單位內所有區域或作業流程皆定期審查及確保遵守安全政策及規範。	☐	☐	☐	☐	☐	
A.15.2.2	資訊系統符合性審查	為確保資訊系統之運行符合既定之安全實施標準，應進行定期的審查，並予以書面或其他方式留存。	☐	☐	☐	☐	☐	
A.15.3	系統稽核的考量							
A.15.3.1	系統稽核控制	為避免作業系統稽核造成系統中斷的危險，應進行審慎、一致的規劃；必要時可向外部專家顧問尋求協助。	☐	☐	☐	☐	☐	
A.15.3.2	系統稽核工具之保護	系統稽核之相關工具需建立適當的保護措施，並視需求設立備援及緊急應變方案。	☐	☐	☐	☐	☐	

資通安全管理制度內部稽核紀錄表					
文件編號	TWVS-ISMS-D-039	機密等級	限閱	版次	2.0

稽核人員：_____　　稽核日期：_____

資通安全管理制度內部稽核報告					
文件編號	TWVS-ISMS-D-041	機密等級	敏感	版次	2.0

紀錄編號：　　填表日期：　　年　　月　　日

1　稽核目的

為落實及評估國立曾文高級家事商業職業學校（以下簡稱本校）執行資訊安全管理制度之成效，以確保資訊安全政策、法令、技術及現行作業之有效性及可行性。

2　稽核範圍

本校資訊機房維運及核心業務系統。

3　稽核項目

3.1 適用性聲明書之確認

3.2 ISMS 建置步驟

3.3 ISMS 建置需求

3.4 資訊安全政策訂定與評估

3.5 資訊安全組織

3.6 資訊資產分類與管制

3.7 人員安全管理與教育訓練

3.8 實體與環境安全

3.9 通訊與作業安全管理

3.10 存取控制安全

3.11 系統開發與維護之安全

3.12 資訊安全事件之反應及處理

3.13 業務永續運作管理

3.14 相關法規與施行單位政策之符合性

3.15 個人資料保護

4　資訊安全稽核小組

組長：

組員：

5 稽核日期

XX 年 XX 月 XX 日

6 稽核期間

自 XX 年 XX 月 XX 日至 XX 年 XX 月 XX 日

7 稽核結果及其他建議事項

項次	稽核項目	稽核發現	建議事項
1			
2			
3			
其他建議事項			

8 缺失矯正與預防處理

受稽部門於接獲稽核報告後，應依據「矯正預防措施管理程序書」之規定，最晚於十個工作天內將該單位之缺失分析原因及擬採行之矯正與預防措施填列於「矯正與預防處理單」內，且經主管核定後回覆資訊安全稽核小組。

9 附件

資訊安全管理制度內部稽核表

資訊安全稽核小組		受稽單位		資通安全執行秘書	
日期	/ /	日期	/ /	日期	/ /

矯正與預防處理單					
文件編號	TWVS-ISMS-D-040	機密等級	限閱	版次	1.0

紀錄編號：　　填表日期：　　年　　月　　日

<table>
<tr><td>提出單位</td><td></td><td>提出人員</td><td></td><td>提出日期</td><td></td></tr>
<tr><td>處理單位</td><td></td><td>處理人員</td><td></td><td></td><td></td></tr>
<tr><td>事件分類
（外部稽核）</td><td colspan="2">□主要不符合事項 □觀察事項
□次要不符合事項 □建議事項</td><td>事件來源</td><td colspan="2">□內部稽核 □外部稽核
□資訊安全事件 □自行提出
□其他＿＿＿＿＿＿＿＿</td></tr>
<tr><td>問題或不符合事項說明</td><td colspan="5"></td></tr>
<tr><td>原因分析</td><td colspan="5"></td></tr>
<tr><td rowspan="6">矯正與預防措施評估</td><td colspan="5">暫時性對策：（控制不符合事項的擴大或消除單一事件的影響）</td></tr>
<tr><td>預訂完成日期</td><td colspan="2"></td><td>追 蹤 人</td><td></td></tr>
<tr><td>追 蹤 日 期</td><td colspan="2"></td><td>確認結果</td><td></td></tr>
<tr><td colspan="5">長期性對策：（消除不符合事項或潛在風險的根本原因，防止類似事件發生）</td></tr>
<tr><td>預訂完成日期</td><td colspan="2"></td><td>追 蹤 人</td><td></td></tr>
<tr><td>追 蹤 日 期</td><td colspan="2"></td><td>確認結果</td><td></td></tr>
</table>