

長庚大學 106 年 11 月份行政會議紀錄

壹、時 間：106 年 11 月 16 日（四）中午 12 時 10 分

貳、地 點：第一醫學大樓二樓簡報室

參、主 席：包家駒校長

記錄：廖麗雯

肆、出席人員：如簽到單

伍、主席致詞：(略)

陸、報告事項：

一、宣讀上次會議紀錄：紀錄確認。

柒、討論事項：

案由一、長庚大學「高等教育深耕計畫」計畫書審核，請討論。

(提案單位：校長室管理一組)

說 明：本案為本校申請教育部「高等教育深耕計畫」之規劃書如簡報檔。

辦 法：本計畫經行政會議通過，陳請校長核准後送教育部審定。

決 議：照案通過。

案由二、訂定「長庚大學公共關係事務委員會設置要點」案，請討論。

(提案單位：秘書室)

說 明：

一、為有效整合運用本校宣傳行銷經費及資源，研擬並執行全校媒體宣傳行銷方案，規劃成立「公共關係事務委員會」。

二、擬新訂「長庚大學公共關係事務委員會設置要點」，條文訂定說明及草案如附。

辦 法：本要點經行政會議通過，陳請校長核定後實施，修正時亦同。

決 議：

一、條文內容修正如下：

1. 第一點宗旨修正為「為有效整合規劃督導及審議本校公共關係事務及宣傳經費資源，成立...」。

2. 第二點組織，增加學務長為當然委員。

3. 第四點會議，刪除「或授權由主任委員徵詢委員意見後核決，再提本委員會追認」。

二、餘照案通過，修正後條文訂定說明表及修正後全文如附件一 pp.1-2。

案由三、訂定「長庚大學學生實習審議委員會設置辦法」案，請討論。

(提案單位：技合處)

說 明：

一、依教育部 106 年 9 月 22 日臺教技(三)字第 1060125350E 號函辦理。

二、擬新訂「長庚大學學生實習審議委員會設置辦法」，條文訂定說明及草案如附，亦修改建教合作合約書範本如附。

辦法：本辦法經行政會議通過，陳請校長核定後實施，修正時亦同。

決議：刪除第三條第三點最後「之處理」字眼，餘照案通過，修正後條文訂定說明表、修正後全文及建教合作合約書範本如附件二 pp.3-5。

案由四、「長庚大學資訊安全管理辦法」部分規定修正草案，請討論。

(提案單位：資訊中心)

說明：

一、修正長庚大學資訊安全管理辦法，變更資訊安全長資格及委員遴選方式，其他條文依現況略為調整文字。

二、「長庚大學資訊安全管理辦法」修正條文前後對照表、修正後全文如附件三 pp.6-14。

辦法：本辦法經行政會議通過，陳請校長核定後實施，修正時亦同。

決議：照案通過。

捌、臨時動議：無。

玖、散會：中午 12 時 35 分。

【長庚大學公共關係事務委員會設置要點】訂定說明表

(106.11.16)

規定	說明
<p>一、宗旨</p> <p>為有效整合規劃督導及審議本校公共關係事務及宣傳經費資源，成立「公共關係事務委員會」，以下簡稱本委員會。</p>	<p>為有效整合運用本校宣傳行銷經費及資源，爰訂定本要點。</p>
<p>二、組織</p> <p>本委員會職責為各項媒體宣傳行銷事務規劃、督導及審議，副校長、主任秘書、教務長、學務長、研發長、技合長為當然委員，另由三院及通識中心各推派一位資深教師，校長室、教務處及總務處各推派一位組長級以上主管為委員，委員任期一年。主任委員由校長自委員中指派一人擔任，召集並主持會議及督導年度計劃之執行。</p>	<p>依媒體宣傳行銷業務需求，訂定委員之組成、人數、遴選、聘期及職掌等。</p>
<p>三、職掌</p> <p>本委員會職責為各項媒體宣傳行銷事務規劃、督導及審議：</p> <p>(一)每學年全校媒體宣傳行銷經費規劃審議。</p> <p>(二)全校媒體宣傳行銷方案研擬與建議。</p> <p>(三)各單位擬執行媒體宣傳行銷案之審議。</p> <p>(四)督導各單位執行媒體宣傳行銷成果。</p> <p>(五)其他與媒體宣傳行銷相關事務。</p> <p>本委員會行政事務由秘書室兼辦。</p>	
<p>四、會議</p> <p>(一)本委員會會議每學期舉行一次，必要時得召開臨時會議。</p> <p>(二)主任委員兼任會議主席，因故無法出席時，得指定一名委員為代理人。</p> <p>(三)得視需要邀請相關人員列席。</p>	<p>訂定會議召開原則。</p>
<p>五、實施及修正</p> <p>本要點經行政會議通過，陳請校長核定後實施，修正時亦同。</p>	<p>訂定本要點實施與修訂原則。</p>

長庚大學公共關係事務委員會設置要點

106 年 11 月 16 日行政會議通過

一、宗旨

為有效整合規劃督導及審議本校公共關係事務及宣傳經費資源，成立「公共關係事務委員會」，以下簡稱本委員會。

二、組織

本委員會職責為各項媒體宣傳行銷事務規劃、督導及審議，副校長、主任秘書、教務長、學務長、研發長、技合長為當然委員，另由三院及通識中心各推派一位資深教師，校長室、教務處及總務處各推派一位組長級以上主管為委員，委員任期一年。主任委員由校長自委員中指派一人擔任，召集並主持會議及督導年度計劃之執行。

三、職掌

本委員會職責為各項媒體宣傳行銷事務規劃、督導及審議：

- (一)每學年全校媒體宣傳行銷經費規劃審議。
- (二)全校媒體宣傳行銷方案研擬與建議。
- (三)各單位擬執行媒體宣傳行銷案之審議。
- (四)督導各單位執行媒體宣傳行銷成果。
- (五)其他與媒體宣傳行銷相關事務。

本委員會行政事務由秘書室兼辦。

四、會議

- (一)本委員會會議每學期舉行一次，必要時得召開臨時會議。
- (二)主任委員兼任會議主席，因故無法出席時，得指定一名委員為代理人。
- (三)得視需要邀請相關人員列席。

五、實施及修正

本要點經行政會議通過，陳請校長核定後實施，修正時亦同。

【長庚大學學生實習審議委員會設置辦法】訂定說明表
(1061116)

條 文	說 明
<p>第一條 目的</p> <p>依教育部「專科以上學校產學合作實施辦法」第六條規定，訂定「長庚大學學生實習審議委員會（以下簡稱本委員會）辦法」。</p>	<p>依據教育部106年9月22日修正之「專科以上學校產學合作實施辦法」（以下簡稱實施辦法）第六條訂定。</p>
<p>第二條 委員會之組成</p> <p>本委員會置委員九位，由技合長擔任主任委員，其餘八位委員分別由醫學院、工學院、管理學院及建教合作中心各一位、校外法律專家一位、合作機構二位及學生代表一位組成，由校長聘任，聘期以二年一聘為原則，得續聘之。</p>	<p>依「實施辦法」第六條，「校級學生校外實習委員會，應包括辦理校外實習業務人員、合作機構代表、學生代表、校外法律學者專家」，考量本校現況，組成委員會，主任委員由技合長擔任。</p>
<p>第三條 委員會之職掌</p> <p>一、督導辦理學生實習合作機構之評估及選定。 二、檢核及確認學生實習書面契約。 三、評估學生實習成效及協調處理學生申訴、爭議及意外事件。 四、學生實習期滿前終止實習之處理與審議。 五、審議與合作機構訂定學生個別實習計畫。 六、督導實習輔導訪視之落實。 七、其他學生實習相關權益之保障事項。 八、督導各院學生校外實習委員會。</p>	<p>依「實施辦法」第六條，訂定委員會職掌。</p>
<p>第四條 委員會之運作</p> <p>一、本委員會每學年至少應召開委員會議一次，必要時得召開臨時會議。委員會議應有二分之一以上委員出席，始得開會，出席委員二分之一以上同意，始能作成決議。 二、本委員會之決議事項委由技術合作處建教合作中心公布與執行。</p>	<p>明訂委員會之運作方式。</p>
<p>第五條 實施與修正</p> <p>本辦法經行政會議通過，陳請校長核定後實施，修正時亦同。</p>	

長庚大學學生實習審議委員會設置辦法

民國 106 年 11 月 16 日行政會議通過

第一條 目的

依教育部「專科以上學校產學合作實施辦法」第六條規定，訂定「長庚大學學生實習審議委員會（以下簡稱本委員會）辦法」。

第二條 委員會之組成

本委員會置委員九位，由技合長擔任主任委員，其餘八位委員分別由醫學院、工學院、管理學院及建教合作中心各一位、校外法律專家一位、合作機構二位及學生代表一位組成，由校長聘任，聘期以二年一聘為原則，得續聘之。

第三條 委員會之職掌

- 一、 督導辦理學生實習合作機構之評估及選定。
- 二、 檢核及確認學生實習書面契約。
- 三、 評估學生實習成效及協調處理學生申訴、爭議及意外事件。
- 四、 學生實習期滿前終止實習之處理與審議。
- 五、 審議與合作機構訂定學生個別實習計畫。
- 六、 督導實習輔導訪視之落實。
- 七、 其他學生實習相關權益之保障事項。
- 八、 督導各院學生校外實習委員會。

第四條 委員會之運作

- 一、 本委員會每學年至少應召開委員會議一次，必要時得召開臨時會議。委員會議應有二分之一以上委員出席，始得開會，出席委員二分之一以上同意，始能作成決議。
- 二、 本委員會之決議事項委由技術合作處建教合作中心公布與執行。

第五條 實施與修正

本辦法經行政會議通過，陳請校長核定後實施，修正時亦同。

建教合作合約書

填入實習機構全銜（以下簡稱甲方），為協助長庚大學（以下簡稱乙方）培育學生實務經驗，提供乙方學生實習機會，經雙方同意訂定建教合作合約書如下述：

一、職掌：

甲方應協助乙方安排學生之工作分配、報到、**考勤**、考核及輔導學生之生活言行。

乙方承辦學生實習有關業務或聯繫並負責指導學生實務實習。

二、實習期間自民國 年 月 日至 年 月 日止。

三、實習學生人數： 填入科系 ，男 人，女 人，合計 人。

四、課程名稱：_____。

五、實習工作項目

甲方請依實習計畫書(附件一)安排實習工作項目及場地安排應以不影響學生健康及安全的工作環境為原則。

六、實習報到：

1. 乙方應於實習前，將學生名單及報到資料寄達甲方。
2. 甲方於學生報到時，應安排學生參加職前安全衛生訓練。

七、學生輔導

1. 甲方指派之實習單位應協助安排學生實務工作，並嚴格要求敬業精神。
2. 實習期間，每位學生均由乙方實習教師及甲方指派之實習單位主管共同擔任指導教師，並共同督導學生實習工作內容及技能指導工作。

3. 甲乙雙方經協商討論後得支付實習輔導費或其他相關費用予對方。

八、實習考核

1. 實習期間，甲方指派之實習單位主管得配合乙方實習教師共同評核學生的實習成績。
2. 實習期間，學生考勤與請假應遵循勞動基準法規定辦理之，另甲方需協助提供學生的考勤紀錄予乙方。
3. 學生表現或適應欠佳時，由甲方指派之實習單位主管知會乙方輔導處理，經輔導未改善者得以退訓處分。

九、乙方學生實習工作項目以實習計畫書為準，若有額外勞務提供，應依勞動基準法規定辦理。

十、本合約書壹式貳份，甲、乙雙方各執壹份。

甲方代表

姓 名：

職 稱：

地址：

統一編號：

乙方代表

姓 名：包 家 駒

職 稱：校 長

地 址：桃園市龜山區文化一路 259 號

統一編號：02612701

中 華 民 國 年 月 日

【長庚大學資訊安全管理辦法】部分規定修正草案條文對照表

(1061116)

修正條文	現行條文	說明
第三條 組織與權責 二、 <u>本委員會設置委員七至十一人，由副校長以上擔任資訊安全長並兼任本委員會召集人，資訊中心主任為執行秘書，其餘委員由本委員會召集人就本校業務相關主管或具資訊相關專長之教職員中遴選。</u>	第四條 本委員會之成員為校長、副校長、教務長、學務長、總務長、秘書室主任秘書、資訊中心主任、圖書館館長為當然委員， <u>其餘委員由三院及通識中心各推派教師代表一名擔任。本委員會委員為無給職，任期為二學年，連聘得連任。</u>	變更資訊安全長資格及委員遴選方式。
三、 <u>前項所遴選之委員為無給職，任期為二學年，連聘得連任。</u>	第五條 本校資訊安全長由 <u>校長</u> 擔任，兼任本委員會召集人，資訊中心主任為執行秘書，行政及技術相關事宜由資訊中心負責。本委員會視需要得聘請校內外具資訊安全專長人員為顧問。	委員遴選方式保留在第二點，僅保留任期。
第四條 電腦系統安全防護 一、所有電腦帳號須設定密碼，訪客等公用帳號須停用，使用者須善盡帳號密碼保管之責， <u>並定期更換。</u>	第八條 所有電腦帳號須設定密碼， <u>guest</u> 等公用帳號須停用，使用者須善盡帳號密碼保管之責。 <u>密碼至少每六個月更換一次，長度須為八位數（含）以上，且夾雜英數字或特殊符號。</u>	因應NIST密碼安全新標準更新。
四、所有電腦必須安裝防毒軟體，不可任意關閉或移除，且防毒軟體病毒碼須定期更新。 <u>若因教學管理需要不安裝防毒軟體，則應有其他措施進行防護。</u>	第十一條 所有電腦必須安裝防毒軟體，不可任意關閉或移除，且防毒軟體病毒碼須定期更新。	公用電腦教室之電腦可利用還原系統防護，不需安裝防毒軟體。
第十六條 <u>各單位伺服器每年須執行一次弱點掃描程序，並即時修補缺失，資訊中心將不定期進行檢測。</u>	第十六條 各單位伺服器每年須執行一次弱點掃描程序，並即時修補缺失，資訊中心將不定期進行檢測。	已有校園伺服器管理辦法，刪除本辦法之伺服器相關條文。
第十七條 <u>對於用戶端之連線，伺服器端必須設定閒置逾時期限，當閒置逾時發生時須自動切斷其連線。</u>	第十七條 對於用戶端之連線，伺服器端必須設定閒置逾時期限，當閒置逾時發生時須自動切斷其連線。	已有校園伺服器管理辦法，刪除本辦法之伺服器相關條文。
十、採取權限區隔，非專責處理特定 <u>機密或敏感</u> 資料者，不得具有存取或查閱 <u>機密或敏感</u> 資料之權限。	第十九條 採取權限區隔，非專責處理特定 <u>個人</u> 資料者，不得具有存取或查閱 <u>個人</u> 資料之權限。	將個人資料統一為機密或敏感資料。
十一、禁止人員使用即時通訊軟體傳輸 <u>機密或敏感</u> 資料檔案。	第二十條 禁止人員使用即時通訊軟體傳輸 <u>個人</u> 資料檔案。	統一為機密或敏感資料。

修正條文	現行條文	說明
十二、 禁止人員使用校外網頁式電子郵件傳輸 <u>機密或敏感</u> 資料檔案。	第二十一條 禁止人員使用校外網頁式電子郵件傳輸 <u>個人</u> 資料檔案。	統一為機密或敏感資料。
十四、 禁止人員在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之 <u>機密或敏感</u> 資料。	第二十三條 禁止人員在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之 <u>個人</u> 資料。	統一為機密或敏感資料。
第五條 存取控管 一、 各單位利用網路公佈及流通資訊時，應評估資料安全等級，未經當事人同意之 <u>機密或敏感</u> 資料及文件，不得上網公佈。	第二十四條 各單位利用網路公佈及流通資訊時，應評估資料安全等級， <u>機密、敏感性</u> 或未經當事人同意之 <u>個人隱私</u> 資料及文件，不得上網公佈。	統一為機密或敏感資料。
二、 <u>機密或敏感</u> 資料及文件，欲利用電子郵件傳送時，須以適當的加密或電子簽章等安全技術處理。	第二十五條 <u>機密性或敏感性之</u> 資料及文件，欲利用電子郵件傳送時，須以適當的加密或電子簽章等安全技術處理。	統一為機密或敏感資料。
三、 電腦內的資料若須開啟網路分享，務必設定密碼及可存取之帳號，嚴禁未設權限控管開放電腦資料供人任意存取之行為，以防電腦病毒侵害及 <u>機密或敏感</u> 資料洩露或損毀，且重要資料務必定期備份。	第二十六條 電腦內的資料若須開啟網路分享，務必設定密碼及可存取之帳號，嚴禁未設權限控管開放電腦資料供人任意存取之行為，以防電腦病毒侵害及 <u>機密、敏感</u> 資料洩露或損毀，且重要資料務必定期備份。	統一為機密或敏感資料。
四、 各單位離職人員須 <u>依規定期限內</u> 取消使用單位內各項資源之所有權限，並列入人員離職之必要手續。	第二十七條 各單位離職人員須 <u>立即</u> 取消使用單位內各項資源之所有權限，並列入人員離職之必要手續。	依實際行政流程修改。
六、 應指定專人負責管理儲存 <u>機密或敏感</u> 資料檔案之資訊設備與其他相關設施，並檢視、處理其錯誤或異常事件等訊息。	第二十九條 應指定專人負責管理儲存 <u>個人</u> 資料檔案之資訊設備與其他相關設施，並檢視、處理其錯誤或異常事件等訊息。	統一為機密或敏感資料。
七、 儲存 <u>機密或敏感</u> 資料之資訊設備應置放於實體安全區域（如：門禁控管之辦公區域、機房），避免有心人士或非授權人員存取。	第三十條 儲存 <u>個人</u> 資料之資訊設備應置放於實體安全區域（如：門禁控管之辦公區域、機房），避免有心人士或非授權人員存取。	統一為機密或敏感資料。
八、 儲存 <u>機密或敏感</u> 資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，應指定專人管理，並置於實體保護之環境（如：上鎖之防潮箱、書櫃），必要時應建立備援機制，以防止資料損壞、遺失或遭竊取。相關儲存媒體非經權責單位同意並留存紀錄，不得任意攜出或拷貝複製。	第三十一條 儲存 <u>個人</u> 資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，應指定專人管理，並置於實體保護之環境（如：上鎖之防潮箱、書櫃），必要時應建立備援機制，以防止資料損壞、遺失或遭竊取。相關儲存媒體非經權責單位同意並留存紀錄，不得任意攜出或拷貝複製。	統一為機密或敏感資料。

修正條文	現行條文	說明
九、儲存 <u>機密或敏感</u> 資料檔案之電腦或相關設備如須報廢或移轉他用時，應確實刪除該設備所儲存之 <u>機密或敏感</u> 資料檔案。	第三十二條 儲存 <u>個人</u> 資料檔案之電腦或相關設備如須報廢或移轉他用時，應確實刪除該設備所儲存之 <u>個人</u> 資料檔案。	統一為機密或敏感資料。
第六條 可攜式儲存媒體 三、將 <u>機密或敏感</u> 資料存放於可攜式設備與媒體時，須採取適當加密處理或保護措施，避免遺失時洩漏資訊。	第三十六條 將 <u>機密或敏感</u> 資料存放於可攜式設備與媒體時，須採取適當加密處理或保護措施，避免遺失時洩漏資訊。	統一為機密或敏感資料。
第三十九條 辦公環境內須置放適當之消防設備（如：手提式滅火器、煙霧偵測器等），設備存放環境須保持淨空，以確保其可用性，並定期檢測與紀錄。	第三十九條 辦公環境內須置放適當之消防設備（如：手提式滅火器、煙霧偵測器等），設備存放環境須保持淨空，以確保其可用性，並定期檢測與紀錄。	消防規定依建築法規及校內規定辦理，刪除本辦法之消防設備條文。
第七條 實體與安全環境管理 四、 <u>機密或敏感</u> 資料須放置於抽屜或儲櫃並上鎖。	第四十一條 敏感文件（內含姓名、身分證、出生年月日、地址等個人資料） 須放置於抽屜或儲櫃並上鎖。	統一為機密或敏感資料。
第九條 人員管理 四、處理 <u>機密或敏感</u> 資料檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重置密碼外，應視須要更換使用者識別帳號。	第四十七條 處理 <u>個人</u> 資料檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重置通行碼外，應視須要更換使用者識別帳號。	統一用字為機密或敏感資料及密碼。
第十一條 系統開發及委外管理 一、自行開發或委外處理 <u>機密或敏感</u> 資料檔案之資訊系統，應在系統開發生命週期之初始階段，將 <u>機密或敏感</u> 資料檔案的安全須求納入考量（如：邏輯測試）；系統之維護、更新、上線及版本異動等作業，應予安全管制，避免危害 <u>機密或敏感</u> 資料安全。	第五十一條 自行開發或委外處理 <u>個人</u> 資料檔案之資訊系統，應在系統開發生命週期之初始階段，將 <u>個人</u> 資料檔案的安全須求納入考量（如：邏輯測試）；系統之維護、更新、上線及版本異動等作業，應予安全管制，避免危害 <u>個人</u> 資料安全。	統一為機密或敏感資料。
二、維護人員或系統服務廠商避免以遠端登入方式進行牽涉 <u>機密或敏感</u> 資料的資訊系統維護或其他有關之運作；若因業務須要必須使用遠端登入方式進行維護時，應透過加密通道進行（如：HTTPS、SSH等）。	第五十二條 維護人員或系統服務廠商避免以遠端登入方式進行牽涉 <u>個人</u> 資料的資訊系統維護或其他有關之運作；若因業務須要必須使用遠端登入方式進行維護時，應透過加密通道進行（如：HTTPS、SSH等）。	統一為機密或敏感資料。
三、自行開發或委外處理 <u>機密或敏感</u> 資料檔案之資訊系統，應將 <u>機密或敏感</u> 資料施予妥善之保護與控管。	第五十三條 自行開發或委外處理 <u>個人</u> 資料檔案之資訊系統，應將 <u>個人</u> 資料（ 包含測試用個人資料 ）施予妥善之保護與控管。	統一為機密或敏感資料。

修正條文	現行條文	說明
四、 <u>機密或敏感</u> 資料檔案若委外建檔，應於委外合約中載明所處理之 <u>機密或敏感</u> 資料保密義務、資訊安全相關責任及違反之罰則。	第五十四條 <u>個人</u> 資料檔案若委外建檔，應於委外合約中載明所處理之 <u>個人</u> 資料保密義務、資訊安全相關責任及違反之罰則。	統一為機密或敏感資料。
第十二條 附則 本辦法經行政會議通過， <u>陳請</u> 校長核定後實施，修正時亦同。	拾貳、附則 第五十六條 本辦法經行政會議通過， <u>呈</u> 校長核定後公告實施，修正時亦同。	文字略為修飾。

長庚大學資訊安全管理辦法

中華民國 98 年 9 月 10 日行政會議通過
中華民國 103 年 2 月 27 日行政會議修訂
中華民國 105 年 5 月 12 日行政會議修訂
中華民國 106 年 11 月 16 日行政會議修訂

第一條 目的

長庚大學（以下簡稱本校）為強化資訊安全管理，督促改善資訊安全防護，有效降低因人為疏失、蓄意或天然災害等導致之資訊資產遭竊、不當使用、洩漏、竄改或破壞等風險，特訂定「長庚大學資訊安全管理辦法」（以下簡稱本辦法）。

第二條 適用範圍

本校各項資訊資產使用者，含全校教職員生、合約廠商駐校人員及其它經授權使用之人員。

第三條 組織與權責

- 一、為強化本校資訊安全，健全資訊安全管理制度，特設立「長庚大學資訊安全委員會」（以下簡稱本委員會），以推動本校資訊安全管理業務之運作。
- 二、本委員會設置委員七至十一人，由副校長以上擔任資訊安全長並兼任本委員會召集人，資訊中心主任為執行秘書，其餘委員由本委員會召集人就本校業務相關主管或具資訊相關專長之教職員中遴選。
- 三、前項所遴選之委員為無給職，任期為二學年，連聘得連任。
- 四、本委員會權責如下：
 1. 訂定本校資訊安全政策及資訊安全管控機制。
 2. 督導資訊安全政策之實施。
 3. 資訊安全事件通報、緊急應變及危機處理。
 4. 規劃並督導資訊安全教育訓練及其他資訊安全相關事項。
 5. 協助推動本校資訊安全管理系統之認證。
- 五、本委員會每年開會一次為原則，得視業務需要召開臨時會議。會議須有應出席委員半數(含)以上出席始得開會，並得邀請相關人員列席。

第四條 電腦系統安全防護

- 一、所有電腦帳號須設定密碼，訪客等公用帳號須停用，使用者須善盡帳號密碼保管之責，並定期更換。
- 二、各類作業系統若有螢幕保護功能，必須啟用。啟動螢幕保護時間設定應小於十分鐘，且須設定繼續後以密碼保護功能。
- 三、各類作業系統及應用軟體須開啟自動更新功能或留意其更新資訊，隨時確保軟體的漏洞為已修補狀態。電腦因故重灌後，應立即重新完成所有之漏洞修補作業。
- 四、所有電腦必須安裝防毒軟體，不可任意關閉或移除，且防毒軟體病毒碼須定期更新。若因應教學管理需要不安裝防毒軟體應有其他措施進行防護。
- 五、當電腦中毒，病毒無法移除、隔離或作業不正常時，為避免產生大規模電腦病毒感染及擴散情形，應將電腦關機，並拔除網路連線，並通報資訊中心。
- 六、來路不明的軟體或檔案常為散播病毒的來源，為確保電腦使用安全，不得安裝使用。
- 七、電腦系統若具備防火牆功能，必須開啟，以提升電腦防護能力。
- 八、各單位架設伺服器依照本校「校園伺服器管理辦法」，須有專人負責維護並進行相關資訊安全作業。
- 九、禁止與他人共用電腦系統帳號。
- 十、採取權限區隔，非專責處理特定機密或敏感資料者，不得具有存取或查閱機密或敏感資料之權限。
- 十一、禁止人員使用即時通訊軟體傳輸機密或敏感資料檔案。
- 十二、禁止人員使用校外網頁式電子郵件傳輸機密或敏感資料檔案。
- 十三、禁止人員使用點對點（P2P）軟體及即時通訊軟體等相關工具下載或提供分享檔案。
- 十四、禁止人員在社群網站、部落格、公開論壇或其他利用網際網路形式公開業務所知悉之機密或敏感資料。

第五條 存取控管

- 一、各單位利用網路公佈及流通資訊時，應評估資料安全等級，未經當事人同意之機密或敏感資料及文件，不得上網公佈。

- 二、機密或敏感資料及文件，欲利用電子郵件傳送時，須以適當的加密或電子簽章等安全技術處理。
- 三、電腦內的資料若須開啟網路分享，務必設定密碼及可存取之帳號，嚴禁未設權限控管開放電腦資料供人任意存取之行為，以防電腦病毒侵害及機密或敏感資料洩露或損毀，且重要資料務必定期備份。
- 四、各單位離職人員須依規定期限內取消使用單位內各項資源之所有權限，並列入人員離職之必要手續。
- 五、各單位主機須限制外部人員以管理者權限帳號登入使用，如有設備保管人以外人士使用或維護設備的須求時，須經主管同意後由系統管理人員陪同下進行。
- 六、應指定專人負責管理儲存機密或敏感資料檔案之資訊設備與其他相關設施，並檢視、處理其錯誤或異常事件等訊息。
- 七、儲存機密或敏感資料之資訊設備應置放於實體安全區域（如：門禁控管之辦公區域、機房），避免有心人士或非授權人員存取。
- 八、儲存機密或敏感資料檔案之磁碟、磁帶，及紙本等相關儲存媒體，應指定專人管理，並置於實體保護之環境（如：上鎖之防潮箱、書櫃），必要時應建立備援機制，以防止資料損壞、遺失或遭竊取。相關儲存媒體非經權責單位同意並留存紀錄，不得任意攜出或拷貝複製。
- 九、儲存機密或敏感資料檔案之電腦或相關設備如須報廢或移轉他用時，應確實刪除該設備所儲存之機密或敏感資料檔案。
- 十、對重要資訊服務之日誌與紀錄等加以適度存檔，以便日後查核使用。

第六條 可攜式儲存媒體

- 一、使用可攜式設備，須先確認電腦已安裝啟用防毒軟體，避免電腦、系統與網路受到病毒威脅。
- 二、使用可攜式設備與媒體時，須謹慎防範資訊洩漏或妨害本校利益等情節發生，資料攜入或攜出，使用者單位主管或廠商接洽窗口人員須盡控管之責。

- 三、將機密或敏感資料存放於可攜式設備與媒體時，須採取適當加密處理或保護措施，避免遺失時洩漏資訊。

第七條 實體與安全環境管理

- 一、外部人員及訪客須遵守各單位辦公區域安全管制相關規定，並於指定環境內執行作業，防止未經授權的存取、干擾及損害。
- 二、重要之出入口須有門禁管理機制，內部人員於進出時須隨時注意是否有非經授權人員跟隨進入，保持警覺，留意陌生人士。
- 三、使用影印機、印表機、傳真機或多功能事務機等資料複印設備後，須立即將相關資料取走，並清除可能暫存於該設備之資訊。
- 四、機密或敏感資料須放置於抽屜或儲櫃並上鎖。
- 五、下班時，必須實施桌面淨空，重要文件妥善保管，並關閉不須使用之電腦系統暨其週邊設備。

第八條 資安教育訓練與宣導

本校人員須定期參與資訊中心主辦的資訊安全教育訓練及宣導，建立並加強資訊安全認知，提升資訊安全水準。

第九條 人員管理

- 一、各單位對資訊相關職務及工作，須進行安全評估，並於人員進用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。
- 二、各單位對負責重要資訊系統管理、維護、設計及操作之人員，須妥適分工，分散權責，並視須要建立制衡機制，實施人員輪調，建立人力備援制度。
- 三、本校各級業務主管人員，須負責督導所屬員工之資訊作業安全，防範不法及不當行為。若有違反，由主管單位送請校方依本校相關法規懲處。
- 四、處理機密或敏感資料檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交，接辦人員除應於相關系統重置密碼外，應視須要更換使用者識別帳號。

- 五、處理機密或敏感資料檔案之人員，應簽訂保密切結書，並確認於離職時或合約終止時取消或停用其使用者識別帳號，且收繳其通行證及相關證件。

第十條 資安事件通報

- 一、學校內人員若發現有資訊安全可疑事件時，須儘速通報資訊中心。資訊中心做緊急必要之處理後會發出「資訊安全事件處理暨回覆單」給事件發生單位，事件發生單位須填寫後續處置情形，經主管核簽後回覆資訊中心存查。
- 二、各單位須設資安聯絡人及其職務代理人，負責資安事件之通報及處理等業務，並將名單送資訊中心存查。

第十一條 系統開發及委外管理

- 一、自行開發或委外處理機密或敏感資料檔案之資訊系統，應在系統開發生命週期之初始階段，將機密或敏感資料檔案的安全須求納入考量（如：邏輯測試）；系統之維護、更新、上線及版本異動等作業，應予安全管制，避免危害機密或敏感資料安全。
- 二、維護人員或系統服務廠商避免以遠端登入方式進行牽涉機密或敏感資料的資訊系統維護或其他有關之運作；若因業務須要必須使用遠端登入方式進行維護時，應透過加密通道進行（如：HTTPS、SSH 等）。
- 三、自行開發或委外處理機密或敏感資料檔案之資訊系統，應將機密或敏感資料施予妥善之保護與控管。
- 四、機密或敏感資料檔案若委外建檔，應於委外合約中載明所處理之機密或敏感資料保密義務、資訊安全相關責任及違反之罰則。
- 五、透過網路存取之相關系統應於上線前，確認所開發的系統架構是否已排除系統安全弱點之漏洞。

第十二條 附則

本辦法經行政會議通過，陳請校長核定後實施，修正時亦同。