資通系統防護需求分級作業說明會

依據

- ~~資訊系統分級與資安防護基準作業規定~~
  - 停止適用：中華民國108年3月5日
- 資通安全責任等級分級辦法第 11 條
  - 施行日期：中華民國108年1月1日
  - 摘要內容：各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施

安全等級設定原則

- 安全等級分為【普】、【中】、【高】三級，由機關依機密性、完整性、可用性及法律遵循性四大影響構面，分別考量資訊系統於發生資安事件時可能造成之衝擊，即衡量資訊系統資料外洩、資料遭竄改、系統故障等情事時可能造成的後果嚴重程度，並據以評估、設定安全等級。

構面說明

- 機密性
  - 不讓資料遭未經授權者存取
  - 漏洞、不小心公開
- 完整性
  - 資料不被竄改或刪除
- 可用性
  - 系統不中斷
- 法律遵循性
  - 要遵守的法規
  - 違反將被罰款

構面說明

- 機密性
  - https
  - 資料加密
- 完整性
  - Hash
  - 程式碼版本控制、資料備份、紙本資料
- 可用性
  - 程式碼版本控制、資料備份
  - 增加主機資源
  - 資安設備
- 法律遵循性
  - 了解要遵守的法規是哪些

資訊系統分級與資安防護基準作業規定

- 已被廢止的規定，但有完整的說明文件，且安全等級的定義也較清楚，還是可以拿來參考。

機密性

安全等級	說明
普	未經授權之資訊揭露，在機關營運、資產或信譽等方面，造成可預期之有限負面影響，如： 一般性資料；資料外洩不致影響機關權益或僅導致機關權益輕微受損。
中	未經授權的資訊揭露，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響，如： 敏感性資料；資料外洩將導致機關權益嚴重受損。 涉及區域性或地區性個人資料，包含出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情形、社會活動及其他得以直接或間接識別個人之資料。

機密性

安全等級	說明
高	未經授權之資訊揭露，在機關營運、資產或信譽等方面，造成可預期之非常嚴重或災難性負面影響，如： 機密性資料；資料外洩將危及國家安全、導致機關權益非常嚴重受損。 凡涉及國家安全之外交、情報、國境安全、財稅、經濟、金融、醫療等重要機敏系統。 特殊屬性之個人資料（如：臥底警員、受保護證人、被害人等資料），資料外洩可能會使相關個人身心受到危害、社會地位受到損害、或衍生財物損失等情形。 涉及個人之醫療、基因、性生活、健康檢查、犯罪前科等資料，資料外洩將使個人權益非常嚴重受損。例如：醫療資訊系統、刑案資訊整合系統等。 涉及全國性個人資料，包含出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、聯絡方式、財務情形、社會活動及其他得以直接或間接識別個人之資料。例如：戶役政資訊系統、護照管理系統等。

完整性

安全等級	說明
普	未經授權之資訊修改或破壞，在機關營運、資產或信譽等方面，造成可預期之有限負面影響，如： 資料遭竄改不致影響機關權益或僅導致機關權益輕微受損。
中	未經授權之資訊修改或破壞，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響，如： 資料遭竄改將導致機關權益嚴重受損。
高	未經授權之資訊修改或破壞，在機關、資產或信譽等方面，造成可預期之非常嚴重或災難性負面影響，如： 資料遭竄改將危及國家安全、導致機關權益非常嚴重受損。

可用性

安全等級	說明
普	資訊、資訊系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之有限負面影響，如： 系統容許中斷時間較長（如：72小時）。 系統故障對社會秩序、民生體系運作不致造成影響或僅有輕微影響。 系統故障造成機關業務執行效能輕微降低。
中	資訊、資訊系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之嚴重負面影響，如： 系統容許中斷時間短。 系統故障對社會秩序、民生體系運作將造成嚴重影響。 系統故障造成機關業務執行效能嚴重降低。

可用性

安全等級	說明
高	資訊、資訊系統之存取或使用上的中斷，在機關營運、資產或信譽等方面，造成可預期之非常嚴重或災難性負面影響，如： 系統容許中斷時間非常短（如：30分鐘）。 系統故障對社會秩序、民生體系運作將造成非常嚴重影響，甚至危及國家安全。 系統故障造成機關業務執行效能非常嚴重降低，甚至業務停頓。

法律遵循性

安全等級	說明
普	系統運作、資料保護、資訊資產使用等若未依循相關法律規範辦理，造成可預期之有限負面影響，如： 　全球資訊網：必須符合智慧財產權相關法令尊重他人智慧財產，並遵守兒童及少年福利與權益保障法進行資訊內容管理，否則將涉及違反法律之遵循性。
中	系統運作、資料保護、資訊資產使用等若未依循相關法律規範辦理，造成可預期之嚴重負面影響，如： 　政府電子採購網：依「政府採購法」第27條規定，機關辦理公開招標或選擇性招標，應將招標公告或辦理資格審查之公告刊登於政府採購公報或公開於資訊網路。因此，若系統資料遭竄改導致公告資料錯誤，將影響採購作業透明化。

法律遵循性

安全等級	說明
高	系統運作、資料保護、資訊資產使用等若未依循相關法律規範辦理，造成可預期之非常嚴重或災難性負面影響，如： 機密性資料：依「國家機密保護法施行細則」第28條第4款規定，國家機密之保管方式直接儲存於資訊系統者，須將資料以政府權責主管機關認可之加密技術處理，該資訊系統並不得與外界連線。因此，機關若未依循規定儲存資料，將涉及從根本上違反法律之遵循性。 醫療機構醫囑暨電子病歷系統：依「醫療機構電子病歷製作及管理辦法」第3條、第4條規定，電子病歷資訊系統之建置、電子病歷之製作及儲存應符合相關規定。因此，機關若未依循相關規定進行系統建置維運及資料儲存，將涉及從根本上違反法律之遵循性。

資通安全責任等級分級辦法

- 取代舊有的規定。
- 分級定義內容說明較模糊。
- 沒其他相關說明文件可參考。

附表九 資通系統防護需求分級原則

防護需求等級 / 構面	高	中	普
機密性	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。
完整性	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。
可用性	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。
法律遵循性	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。	其他資通系統設置或運作於法令有相關規範之情形。

範例

「停車管理系統(參考範例)」安全等級評估表

功能說明：提供停車場所查詢，以及汽機車未繳費資料查詢線上服務。

業務屬性：□行政類■業務類　　日期：__年__月__日

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
中	高	普	中	高
		資訊系統安全等級：		高

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	中	本系統資料屬敏感性資料，資料保護不當，將遭受一定程度之影響
	異動		
2. 完整性	初估	高	本系統目的在提供車輛未繳費資料查詢服務，若資料未妥適保存或發生資安事件造成資料外洩，可能造成資料完整性受損
	異動		
3. 可用性	初估	普	本系統容許中斷時間較長(超過 24 小時)，且服務中斷不致影響業務運作
	異動		
4. 法律遵循性	初估	中	本系統資料包含車號與未繳費資料明細等，應依「個人資料保護法」規定辦理
	異動		

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	業務類	本系統提供汽機車未繳費資料查詢等對外資訊服務，屬機關業務類系統
	異動		

「全球資訊網(參考範例)」安全等級評估表

功能說明：機關官方網站，提供機關簡介及政策措施介紹，並無提供線上申辦等服務。

業務屬性：□行政類■業務類　　日期：__年__月__日

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
普	普	普	普	普
		資訊系統安全等級：		普

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	普	網站資訊均為可公開之一般性資料
	異動		
2. 完整性	初估	普	本網站主要提供資訊公告
	異動		
3. 可用性	初估	普	本網站提供一般性資料瀏覽
	異動		
4. 法律遵循性	初估	普	本網站必須符合智慧財產權相關法令，並遵守兒童及少年福利與權益保障法及其相關規定，惟不涉及從根本上違反法律之可能性，也不致因違反規範導致嚴重不良後果
	異動		

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	業務類	本系統提供機關簡介、政策措施介紹等對外資訊服務，無涉及機關業務線上申辦等其他服務，屬機關業務類系統
	異動		

「人事管理系統(參考範例)」安全等級評估表

功能說明：提供機關同仁進行差勤線上申請，以及人事單位進行相關人事差勤管理。

業務屬性：■行政類□業務類　　日期：__年__月__日

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
中	普	普	普	中
		資訊系統安全等級：		中

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	中	本系統資料屬敏感性資料，資料保護不當，將遭受一定程度之影響
	異動		
2. 完整性	初估	普	本系統目的在提供人事管理服務，不對外提供服務，若個人資料未妥適保存或發生資安事件造成資料外洩，可能造成資料完整性受損
	異動		
3. 可用性	初估	普	本系統容許中斷時間較長(超過 24 小時)，且服務中斷不致影響業務運作
	異動		
4. 法律遵循性	初估	普	本系統包含同仁基本個人資料，應依「個人資料保護法」規定辦理；惟資料筆數不多，且多屬個人基本資料，評估若未完成遵循個人資料保護法辦理資料保護，可能伴隨輕微不良後果
	異動		

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	行政類	本系統支援機關內部人事管理屬行政類資訊系統
	異動		

「會計管理系統(參考範例)」安全等級評估表

功能說明：提供機關會計人員進行會計帳務作業及管理。

業務屬性：■行政類□業務類　　日期：__年__月__日

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
中	普	普	中	中
		資訊系統安全等級：		中

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	中	系統包含本機關收入、支出明細資料，屬敏感資料
	異動		
2. 完整性	初估	普	本系統目的在提供會計帳務管理，本系統不對外提供服務，惟會計帳務屬敏感性資料，若遭入侵完整性可能會有影響
	異動		
3. 可用性	初估	普	本系統容許中斷時間較長(超過 24 小時)，且服務中斷不致影響業務運作
	異動		
4. 法律遵循性	初估	中	會計系統資料包含受款人資料(包含姓名、戶籍地址、身分證字號、金融帳號等)及帳務往來明細等，應依「個人資料保護法」規定辦理
	異動		

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	行政類	本系統支援機關內部會計管理屬行政類資訊系統
	異動		

本校範例

「個資盤點系統」安全等級評估表

功能說明：提供全校各單位進行個資檔案盤點作業。

業務屬性： ☑行政類☐業務類　　**日期：**___年___月___日

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
普	普	普	普	普
		資訊系統安全等級：		普

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	普	本系統資料僅包含各單位所屬個人資料檔案盤點清單。
	異動		
2. 完整性	初估	普	若本系統資料完整性受損，仍可由當初填報人重新填報。
	異動		
3. 可用性	初估	普	本系統僅在個資盤點時提供服務，可容許中斷時間較長(超過 24 小時)。
	異動		
4. 法律遵循性	初估	普	本系統資料包含姓名、職稱、單位等，多屬可公開資料，依「個人資料保護法」規定辦理資料保護。
	異動		

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	行政類	本系統支援機關內部個資盤點作業屬行政類。
	異動		

「電子郵件系統」安全等級評估表

功能說明：供教職員生收送電子郵件用。

業務屬性： ☑行政類☐業務類　　**日期：** 105 年 3 月 10 日

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
中	普	中	普	普
		資訊系統安全等級：		中

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	中	本系統個人郵箱中，可能存有個人機密資料。
	異動		
2. 完整性	初估	普	若本系統保存之郵件資料完整性受損，可能影響收信人之權益。
	異動		
3. 可用性	初估	中	本系統提供本校教職生日常聯繫使用，若服務中斷，恐影響使用者收取重要信件權益。
	異動		
4. 法律遵循性	初估	普	本系統為管理所需，僅包含身分證字號，依「個人資料保護法」規定辦理資料保護。 個人電子郵件使用，若有機密資料外洩，屬個人行為，洩漏人須自行承擔相關法律責任。
	異動		

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	行政類	本系統支援本校教職員生日常聯繫屬行政類。
	異動		

「學籍系統」安全等級評估表

功能說明：學生個人資料管理

業務屬性：　□行政類■業務類　　日期：　105 年　3 月　23 日

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
中	中	中	中	中
		資訊系統安全等級：		中

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	中	本系統資料屬敏感性資料，資料保護不當造成個資外洩，將遭受一定程度之影響。
	異動		
2. 完整性	初估	中	本系統目的主要建置學生學籍資料，若資料未妥適保存或發生資安事件造成資料竄改，將造成資料完整性受損。
	異動		
3. 可用性	初估	中	本系統容許中斷時間短，於上班期間服務中斷，將造成核心業務資料服務更新停滯。
	異動		
4. 法律遵循性	初估	中	本系統資料包含學生個資，應依「個人資料保護法」規定辦理。
	異動		

步驟❷：識別業務屬性

項目		業務屬性	原因說明
識別業務屬性	初估	業務類	本系統提供學生個人資料及學籍狀況，屬機關核心業務。
	異動		

「招生系統」安全等級評估表

功能說明：提供本校招生選才

業務屬性：　□行政類■業務類　　日期：105 年 3 月 23 日

影響構面				資訊系統安全等級
1. 機密性	2. 完整性	3. 可用性	4. 法律遵循性	
中	中	中	中	中
		資訊系統安全等級：		中

步驟❶：設定影響構面等級

影響構面		安全等級	原因說明
1. 機密性	初估	中	本系統資料屬敏感性資料，若資料保護不當，將遭受一定程度之影響。
	異動		
2. 完整性	初估	中	本系統主要提供考生報名服務，若資料未妥善保存或發生資安事件造成資料竄改，將造成資料完整性受損。
	異動		
3. 可用性	初估	中	本系統容許中斷時間短（1-2 小時），於報名期間服務中斷，將造成業務執行效能降低。
	異動		
4. 法律遵循性	初估	中	本系統資料包含學生個人資料，應依「個人資料保護法」規定辦理。
	異動		