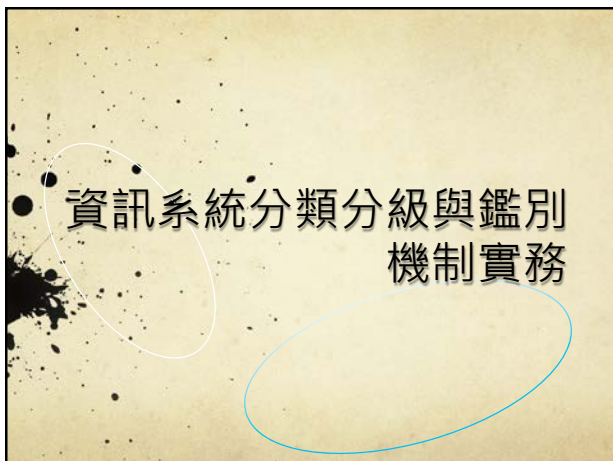
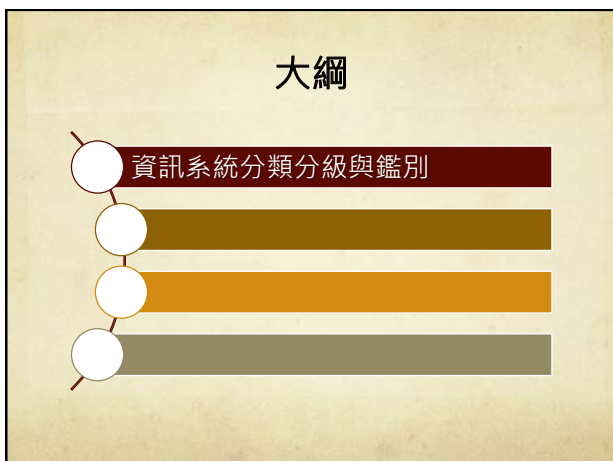








依據

政府機關資訊安全責任
等級分級作業規定

104年1月30日修正

資訊系統分級與資安防護基
準作業規定

104年7月修正

政府機關資訊安全責任 等級分級作業規定

政府機關

學術機構

國(公)營事業、醫療機構及
其它

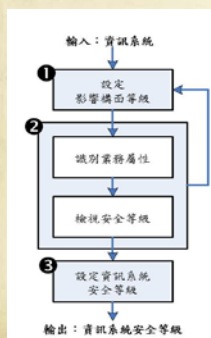
資訊系統分級與資安防護 基準作業規定



大綱

安全等級評估表

安全等級評估流程



- ❶：由業務承辦人依機密性、完整性、可用性、法律遵循性四大影響構面，分別評估對各資訊系統之影響衝擊，並據以設定影響構面等級。
- ❷：識別資訊系統所支援之業務屬性，並由承辦單位主管檢視業務承辦人所設定安全等級之合理性。
- ❸：資訊系統安全等級經承辦單位主管、資訊主管確認後，最後由資訊安全長核定。

程序說明-1

處理程序	工作項目	相關人員
輸入：資訊系統	輸入資訊系統。	承辦單位主管 (或其授權人員)
步驟❶： 設定影響構面等級	1. 由業務承辦人評估當發生資安事件時，對機密性、完整性、可用性、法律遵循性四大影響構面之衝擊程度，並參照「五、安全等級設定原則」填寫影響構面安全等級，安全等級區分為【普】、【中】、【高】三級，對於不適用之影響構面，安全等級以NA (Not Applicable)表示。 2. 資訊系統之安全等級，取其四大影響構面安全等級最高者。	業務承辦人

程序說明-2

處理程序	工作項目	相關人員
步驟●： 1. 識別業務屬性 2. 檢視安全等級	1. 識別資訊系統之業務屬性，並由承辦單位主管檢視設定安全等級之合理性。 2. 資訊系統依其支援之單位及業務屬性，分為行政與業務二類，說明如下： ◦ 行政類：指機關內部輔助單位之業務（如人事、薪資等），惟若輔助單位工作與機關職掌相同或兼具業務單位性質，機關得視情形調整其類別。 ◦ 業務類：指機關內部業務單位之業務（如交通監理、便民服務等）。 本步驟所進行各項異動均須記錄異動原因。	承辦單位主管（或其授權人員）

程序說明-3

處理程序	工作項目	相關人員
步驟●： 核定資訊系統安全等級	1. 由資訊單位綜整各資訊系統「安全等級評估表」中資訊，併同 共同性系統 （不需填安全等級），彙整至「資訊系統清冊」，資訊系統安全等級經相關主管確認後，最後由資訊安全長核定。 共同性系統之分級，統一由開發管理之機關進行評估與鑑別。 2. 本步驟所指之 共同性系統 ，包含共用性系統與共通性系統，共用性系統指單一機關主責系統開發與資料管理，其餘機關僅涉及使用操作，如國稅系統。共通性系統指單一機關主責系統開發與規格制訂，其餘機關除使用操作外，資料主要儲存於使用機關，如公文電子交換系統。	資訊安全長、相關主管、資訊人員

程序說明-4

處理程序	工作項目	相關人員
輸出： 資訊系統安全等級	1. 本程序所設定之資訊系統安全等級，將作為後續執行防護基準之依據。 2. 資訊系統安全等級列【高】者，可考量進一步實施詳細風險評鑑，俾利進行風險管理。	

資訊系統名稱

需要進行分級之資訊系統，以**自行或委外開發**之資訊系統為主。

套裝軟體、作業系統或防毒系統、防火牆系統、入侵偵測/防禦系統、弱點掃描系統、網頁/郵件內容過濾系統等屬資安防護處理相關控制措施，均**不需**進行資訊系統分級。

表單編號：「XXXX」安全等級評估表	
功能說明：	
業務屬性： ☐ 行政類 ☐ 業務類	日期：年 月 日
制訂/核准	

功能說明

表單編號：「XXXX」安全等級評估表	
功能說明：	
業務屬性： ☐ 行政類 ☐ 業務類	日期：年 月 日
制訂/核准	

說明資訊系統功能。
如：

「停車管理系統(參考範例)」安全等級評估表 功能說明：提供停車場停車資訊，以及汽機車系統管理系統功能。
「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諮詢服務，並提供線上查詢等服務。
「人事管理系統(參考範例)」安全等級評估表 功能說明：提供機關同仁之人事動態管理，以及人事管理之動態管理。

業務屬性-1

- **行政類**：指機關內部輔助單位之業務（如：人事、薪資等），惟若輔助單位工作與機關職掌相同或兼具業務單位性質，機關得視情形調整其類別。
- **業務類**：指機關內部業務單位之業務（如：交通監理、便民服務等）

表單編號：「XXXX」安全等級評估表		
功能說明：		
業務屬性： ☐ 行政類 ☐ 業務類	日期：年 月 日	
步驟2：說明業務屬性		
項目	業務屬性	應 用 說 明
輔助業務屬性	行政	
	業務	

業務屬性-2

「停車管理系统(參考範例)」安全等級評估表⁴

功能說明：提供停車場查詢，以及汽機車繳費資料查詢線上服務。⁴

業務屬性：☐行政類☒業務類 日期：__年__月__日⁴

步驟：識別業務屬性⁴

項目 ⁴	初估 ⁴	業務屬性	原因說明 ⁴
識別業務屬性 ⁴		業務類	本系統提供汽機車繳費資料查詢等對外資訊服務，屬機關業務類系統 ⁴
	異動 ⁴		

「全球資訊網(參考範例)」安全等級評估表⁴

功能說明：機關官方網站，提供機關簡介及政策服務介紹，並無提供線上申請等服務。⁴

業務屬性：☐行政類☒業務類 日期：__年__月__日⁴

步驟：識別業務屬性⁴

項目 ⁴	初估 ⁴	業務屬性	原因說明 ⁴
識別業務屬性 ⁴		業務類	本系統提供機關簡介、政策服務介紹等對外資訊服務，無涉及機關業務線上申請等其他服務，屬機關業務類系統 ⁴
	異動 ⁴		

業務屬性-3

「人事管理系统(參考範例)」安全等級評估表⁴

功能說明：提供機關同仁進行異動線上申請，以及人事單位進行相關人事異動管理。⁴

業務屬性：☒行政類☐業務類 日期：__年__月__日⁴

步驟：識別業務屬性⁴

項目 ⁴	初估 ⁴	業務屬性	原因說明 ⁴
識別業務屬性 ⁴		行政類	本系統支援機關內部人事管理層行政類資訊系統 ⁴
	異動 ⁴		

「會計管理系统(參考範例)」安全等級評估表⁴

功能說明：提供機關會計人員進行會計帳務作業及管理。⁴

業務屬性：☒行政類☐業務類 日期：__年__月__日⁴

步驟：識別業務屬性⁴

項目 ⁴	初估 ⁴	業務屬性	原因說明 ⁴
識別業務屬性 ⁴		行政類	本系統支援機關內部會計管理層行政類資訊系統 ⁴
	異動 ⁴		

業務類

•對外服務

行政類

•內部使用

影響構面等級-機密

- 資訊系統發生資安事件時，可能造成系統資料外洩或遭竄改等情事，導致資料機密性受到損害。

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	未經授權之資訊揭露，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。
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。

影響構面等級-完整

- 資訊系統委外開發與營運時，若未有效執行資安防護作為，可能會造成系統完整性遭受破壞。

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。

影響構面等級-可用

- 資訊系統目的在輔助機關提升業務效能與服務品質，已成為機關業務運作不可或缺的一環，因此，系統故障（包含無法使用、異常運作等情形）可能導致業務執行效能降低，甚至業務中斷。
- 機關評估本影響構面安全等級時，應考量**資訊系統可容許中斷時間、服務受影響程度**等。一般而言，**行政類系統**（例如：人事管理系統、會計系統等）等，於系統故障時**通常不致**造成機關業務執行效能嚴重降低或業務中斷。

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。
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。

影響構面等級-法律遵循

- 本影響構面之危害程度評估係基於機關負有遵守法律規章之責任與義務下，如發生違法情事時，機關將面臨之衝擊，本影響構面衝擊後果之嚴重程度係取決於法令規定。
- 政府機關依法行政，資訊使用原則上應至少符合智慧財產權相關法令，資訊於網路揭露也應遵循「兒童及少年福利與權益保障法」及其相關規定。

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。
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護及資料儲存，將涉及從根本上違反法律之遵循性。

大綱

資訊系統清冊實作要項

安全等級評估-填寫部份

業務屬性： ☐ 行政類 ☐ 業務類		日期： 年 月 日	
影響範圍			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
步驟1：指定影響範圍			資訊系統安全等級：
影響範圍			安全等級
原因說明			
1. 機密性	初值		該值係影響範圍評估值
	異動		
2. 完整性	初值		
	異動		
3. 可用性	初值		
	異動		
4. 法律遵循性	初值		
	異動		

範例-1

「全球資訊網(參考範例)」安全等級評估表¹

功能說明：機關官方網站，提供機關簡介及政策落地介紹，並提供線上申辦等服務。²

業務屬性：☐行政類☒業務類 日期：__年__月__日³

影響場面 ⁴				資訊系統安全等級 ⁵
1. 機密性 ⁶	2. 完整性 ⁷	3. 可用性 ⁸	4. 法律遵循性 ⁹	
中 ¹⁰	中 ¹¹	中 ¹²	中 ¹³	中 ¹⁴
資訊系統安全等級： ¹⁵				中 ¹⁶

步驟②：依定影響場面等級¹⁷

影響場面 ¹⁸	安全等級 ¹⁹	原因說明 ²⁰
1. 機密性 ²¹	初估 ²² 中 ²³	網站資訊均為公開之一般性資料 ²⁴
	異動 ²⁵ 中 ²⁶	
2. 完整性 ²⁷	初估 ²⁸ 中 ²⁹	本網站主要提供資訊公布 ³⁰
	異動 ³¹ 中 ³²	
3. 可用性 ³³	初估 ³⁴ 中 ³⁵	本網站提供一般性資料瀏覽 ³⁶
	異動 ³⁷ 中 ³⁸	
4. 法律遵循性 ³⁹	初估 ⁴⁰ 中 ⁴¹	本網站必須符合智慧財產權相關法令，並遵守兒童及少年權利與權益保障法及其相關規定，惟不涉及其他未上達或法律之可能性，也不致因違反規範等致嚴重不良後果 ⁴²
	異動 ⁴³ 中 ⁴⁴	

範例-2

「人事管理系統(參考範例)」安全等級評估表¹

功能說明：提供機關同仁進行異動線上申請，以及人事單位進行相關人事異動管理。²

業務屬性：☒行政類☐業務類 日期：__年__月__日³

影響場面 ⁴				資訊系統安全等級 ⁵
1. 機密性 ⁶	2. 完整性 ⁷	3. 可用性 ⁸	4. 法律遵循性 ⁹	
中 ¹⁰	中 ¹¹	中 ¹²	中 ¹³	中 ¹⁴
資訊系統安全等級： ¹⁵				中 ¹⁶

步驟②：依定影響場面等級¹⁷

影響場面 ¹⁸	安全等級 ¹⁹	原因說明 ²⁰
1. 機密性 ²¹	初估 ²² 中 ²³	本系統資料屬敏感性質資料，資料保護不當，將遭受一定程度之影響 ²⁴
	異動 ²⁵ 中 ²⁶	
2. 完整性 ²⁷	初估 ²⁸ 中 ²⁹	本系統目的在提供人事管理服務，不對外提供服務，屬個人資料未妥適保存或發生資料遺失或資料外洩，可能造成資料完整性受損 ³⁰
	異動 ³¹ 中 ³²	
3. 可用性 ³³	初估 ³⁴ 中 ³⁵	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 ³⁶
	異動 ³⁷ 中 ³⁸	
4. 法律遵循性 ³⁹	初估 ⁴⁰ 中 ⁴¹	本系統包含個人基本個人資料，應依「個人資料保護法」規定辦理；惟資料筆數不多，且屬個人基本資料，詳情並未完全透過個人資料保護法辦理資料保護，可能導致輕微不良後果 ⁴²
	異動 ⁴³ 中 ⁴⁴	

範例-3

「停車管理系統(參考範例)」安全等級評估表¹

功能說明：提供停車場所查詢，以及汽機車車主繳費資料查詢線上服務。²

業務屬性：☐行政類☒業務類 日期：__年__月__日³

影響場面 ⁴				資訊系統安全等級 ⁵
1. 機密性 ⁶	2. 完整性 ⁷	3. 可用性 ⁸	4. 法律遵循性 ⁹	
中 ¹⁰	高 ¹¹	中 ¹²	中 ¹³	高 ¹⁴
資訊系統安全等級： ¹⁵				高 ¹⁶

步驟②：依定影響場面等級¹⁷

影響場面 ¹⁸	安全等級 ¹⁹	原因說明 ²⁰
1. 機密性 ²¹	初估 ²² 中 ²³	本系統資料屬敏感性質資料，資料保護不當，將遭受一定程度之影響 ²⁴
	異動 ²⁵ 中 ²⁶	
2. 完整性 ²⁷	初估 ²⁸ 高 ²⁹	本系統目的在提供車輛未繳費資料查詢服務，屬資料未妥適保存或發生資料遺失或資料外洩，可能造成資料完整性受損 ³⁰
	異動 ³¹ 中 ³²	
3. 可用性 ³³	初估 ³⁴ 中 ³⁵	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 ³⁶
	異動 ³⁷ 中 ³⁸	
4. 法律遵循性 ³⁹	初估 ⁴⁰ 中 ⁴¹	本系統資料包含車主姓名及繳費資料等，應依「個人資料保護法」規定辦理 ⁴²
	異動 ⁴³ 中 ⁴⁴	

[illegible]

共同性系統：包含**共用性**系統與**共通性**系統。

- 共用性系統指單一機關主責系統開發與資料管理，其餘機關僅涉及使用操作，如**國稅系統**。
- 共通性系統，指單一機關主責系統開發與規格制訂，其餘機關除使用操作外，資料主要儲存於使用機關，如**電子公文交換系統**。

防護基準重點概要說明

防護基準選擇

機關完成資訊系統分級後，應依資訊系統【高】、【中】、【普】等級，執行相對應之防護基準。

- 【高】等級資訊系統執行【高】等級防護措施，
- 【中】、【普】等級資訊系統，則執行【中】、【普】等級防護措施。
- 機關可依其資源，調整控制措施之優先順序。

防護基準

存取控制(Access Control)-3

稽核與可歸責性(Audit and Accountability)-6

營運持續計畫(Contingency Planning)-2

識別與鑑別(Identification and Authentication)-5

系統與服務獲得(System and Services Acquisition)-8

系統與通訊保護(System and Communications Protection)-2

系統與資訊完整性(System and Information Integrity)-3

範例

控制措施	安全等級		
	普	中	高
存取控制(Access Control)(3)			
帳號管理 (Account Management)	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。	1. 執行等級「普」之所有控制措施。 2. 資訊系統已逾期之臨時或緊急帳號應刪除或禁用。 3. 應禁用資訊系統開置帳號。 4. 應定期審核資訊系統帳號之建立、修改、啟用、禁用及刪除動作。	1. 執行等級「中」之所有控制措施。 2. 當超過機關所規定之預開置時間或可使用期限時，系統應自動將使用者登出。 3. 資訊系統應依照機關所規定之情況及條件(如上班時間或指定IP來源)，使用資訊系統。 4. 監控資訊系統帳號以發現違常使用，並於發現帳號違常使用時回報管理者。

Q & A

