

## 附件2 資訊及資通系統資產評鑑範例說明

### 1. 機密性

資訊及資通系統資產的機密性鑑價，乃針對資訊及其使用權限分級要求，評估其未經授權存取之影響。鑑價重點在於資訊處理之授權，只有取得存取權限的人員或程序才可以進行授權範圍內之資訊的處理作業，未經過授權、或不當的授權便進行資訊處理(包含使用設備及組織內提供之服務、執行程式、進入實體區隔之區域、透露或複製經手之業務資料)，可能會對組織內之業務運作造成程度不等之影響。鑑價原則如下表：

機密性分級	評等	說明與衝擊
普通	1	<ul style="list-style-type: none"><li>• 資訊：非敏感性資訊，可公開使用者。資訊遭洩漏，不會造成影響或影響可忽略</li><li>• 軟體：非敏感性資訊處理設施與系統資源等，可公開使用者。受到不當存取，不會造成影響或影響可忽略</li><li>• 人員：負責非敏感性業務之工作人員，不會因該人員的行為或負責業務對資訊安全產生影響。洩漏業務內容，不會造成影響或影響可忽略</li><li>• 服務：非敏感性之電力、空調、通訊與網路等支援性服務。受到不當存取，不會造成影響或影響可忽略</li><li>• 實體設備：可開放公眾進出之實體環境或可開放公眾使用之設備，且不會造成損失者。受到不當存取，不會造成影響或影響可忽略</li></ul>

機密性分級	評等	說明與衝擊
中	2	<ul style="list-style-type: none"> <li>• 資訊：敏感性之資訊，僅能開放給經過授權的人員使用。一旦洩漏，足以影響組織或專案之執行</li> <li>• 軟體：敏感性之資訊處理設施與系統資源，僅開放給經過授權的人員使用。一旦洩漏，足以影響組織或專案之執行</li> <li>• 人員：負責業務執行人員，其了解之業務資訊內容，具有敏感性。一旦洩漏，足以影響組織或專案之執行</li> <li>• 服務：提供系統或業務進行使用之電力、空調、通訊與網路等具有敏感性之支援性服務。一旦洩漏，足以影響組織或專案之執行</li> <li>• 實體設備：敏感性之資訊處理設施、系統資源與保護該設施與資源之實體環境。一旦洩漏，足以影響組織或專案之執行</li> </ul>
高	3	<ul style="list-style-type: none"> <li>• 資訊：具有機密之資訊，僅能開放給經過授權的人員使用。一旦洩漏，足以影響組織整體信譽及業務執行</li> <li>• 軟體：機密之資訊處理設施與系統資源，僅開放給經過授權的人員使用。一旦洩漏，足以影響組織整體信譽及業務執行</li> <li>• 人員：負責業務執行人員，其了解之資訊內容，具有高度機密性。一旦洩漏足以影響組織整體信譽及業務</li> <li>• 服務：提供系統或業務進行使用之電力、空調、通訊與網路等具有機密性之支援性服務。一旦洩漏，足以影響組織整體信譽及業務執行</li> <li>• 實體設備：機密之資訊處理設施、系統資源與保護該設施與資源之實體環境。一旦洩漏，足以影響組織整體信譽及業務執行</li> </ul>

## 2. 完整性

資訊及資通系統資產的完整性鑑價，乃針對資訊及其使用過程，必須正確地進行資訊處理的要求程度進行評估。鑑價重點在於評估資訊及運用過程在遭受變更、竄改、破壞等不當的變動或更改措施時(包含移動設備、改變組織內提供之服務內容、更改系統組態或檔案、破壞實體設施、改變傳輸內容、竄改資料庫或交易資訊、冒用或假借名義進行業務處理、人為錯誤或誤用設施)，可能對組織內之業務運作造成程度不等之影響。鑑價原則如下表：

完整性分級	評等	說明與衝擊
低	1	<ul style="list-style-type: none"><li>• 資訊：遭受不當的破壞或篡改資訊，其所造成的業務衝擊可以忽略者</li><li>• 軟體：遭受不當的破壞或篡改資訊處理設施與系統資源，其所造成的業務衝擊可以忽略者</li><li>• 人員：不會因為人員的作業失誤造成傷害</li><li>• 服務：提供非敏感性系統或資源所使用之電力、空調、通訊與網路等支援性服務，遭受不當的破壞所造成的業務衝擊可以忽略者</li><li>• 實體設備：實體環境或設備被不當操作或破壞，所造成的業務的衝擊很少或可忽略者</li></ul>
中	2	<ul style="list-style-type: none"><li>• 資訊：不當的損失、破壞或篡改資訊，會對組織或計畫業務運作造成衝擊者</li><li>• 軟體：不當的損失、破壞或篡改資訊處理設施與系統資源，會對組織或計畫業務運作造成衝擊者</li><li>• 人員：人員對資訊內容之瞭解，於傳遞、公佈或交接過程不當或蓄意之錯誤，而對組織或計畫業務造成傷害者</li><li>• 服務：提供敏感性系統或資源所使用之電力、空調、通訊與網路等支援性服務，遭受不當的破壞會對組織或計畫業務造成衝擊者</li><li>• 實體設備：實體環境或設備被不當的操作或破壞，對組織或計畫造成傷害者</li></ul>

完整性分級	評等	說明與衝擊
高	3	<ul style="list-style-type: none"> <li>• 資訊：不當的破壞或篡改資訊，會對組織整體業務造成危害，甚至會造成業務中斷者</li> <li>• 軟體：不當的破壞或篡改資訊、資訊處理設施與系統資源，會對組織整體業務造成危害，甚至會造成業務中斷者</li> <li>• 人員：人員對資訊內容之瞭解，於傳遞、公佈或交接過程不當或蓄意之錯誤，而對業務造成重大傷害者</li> <li>• 服務：提供敏感性系統或資源所使用之電力、空調、通訊與網路等支援性服務，不當的破壞會對組織整體業務造成很大的危害，甚至會造成業務中斷者</li> <li>• 實體設備：實體環境或設備被不當的操作或破壞，對組織整體會造成嚴重的傷害甚至會造成業務中斷者</li> </ul>

### 3. 可用性

資訊及資通系統資產的可用性鑑價，乃針對資訊及其處理過程，獲得授權者對於資訊及處理設備於需要存取時，能夠正常使用的需求程度之評估。鑑價重點在於評估資訊及資通系統資產在運用過程中，必須保持正常運作之時間需求程度。影響資產可用性情況，例如：實體設施無法使用、實體區域無法進入、系統軟體或程式錯誤導致執行中斷、網路連線中斷、職務代理不明或未建立相關辦法。鑑價原則如下表：

可用性分 級	評 等	說明與衝擊
普	1	<ul style="list-style-type: none"> <li>• 資訊：無法使用，所造成的業務衝擊可以忽略者</li> <li>• 軟體：無法使用，所造成的業務衝擊可以忽略者</li> <li>• 人員：無法執行業務，所造成的業務衝擊可以忽略者</li> <li>• 服務：電力、空調、通訊與網路等支援性服務無法使用，所造成的業務衝擊可以忽略者</li> <li>• 實體設備：該實體環境或設備無法使用，所造成的業務衝擊可以忽略者</li> </ul>
中	2	<ul style="list-style-type: none"> <li>• 資訊：無法使用，會影響組織或專案業務執行</li> <li>• 軟體：無法使用，會影響組織或專案業務執行</li> <li>• 人員：無法執行業務，會影響組織或專案業務執行</li> <li>• 服務：電力、空調、通訊與網路等支援性服務無法使用，會影響組織或專案業務執行</li> <li>• 實體設備：該實體環境或設備無法使用，，會影響組織或專案業務執行</li> </ul>
高	3	<ul style="list-style-type: none"> <li>• 資訊：無法使用，會影響全機關業務執行</li> <li>• 軟體：無法使用，會影響全機關業務執行</li> <li>• 人員：無法執行業務，會影響全機關業務執行</li> <li>• 服務：提供所需之電力、空調、通訊與網路等支援性服務無法提供時，會影響全機關業務執行</li> <li>• 實體設備：實體環境或設備無法使用，會影響全機關業務執行</li> </ul>