威弱點評估表

文件編號：Takming-ISMS-D-005					機密等級：內部使用				版　　次：2.0				
紀錄編號：									填表日期：				
資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級			弱點等級			風險值
						低	中	高	低	中	高	
	CM			通訊服務失效	維護服務回應時間過長效							
				通訊服務失效	通訊線路未適當保護							
				通訊服務失效	缺乏有效變更控制							
				通訊服務失效	連線電纜失效							
				線路受損	未適當保護通訊線路							
				通訊滲透	未適當保護通訊線路							
				通訊滲透	未適當保護機敏性資料的傳輸							
				通訊設備或元件失效	維護服務回應時間過長							
				通訊設備或元件失效	缺乏硬體耗損控管							
				網路效能低落	缺乏正確使用通訊設備與訊息控管的政策							
				網路效能低落	網路管理不足							
				訊息路徑錯誤或被繞道	缺乏正確使用通訊設備與訊息控管的政策							
				訊息路徑錯誤或被繞道	網路管理不足							
				未經授權存取或使用	未確實陪同外部人員或清潔人員執行相關作							
				未經授權存取或使用	存取權限授與不當或未定期審查							
				未經授權存取或使用	通行碼管理不足							
				未經授權存取或使用	離開工作站未進行「登出」作業							
				未經授權存取或使用	缺乏監督與稽核機制							
				未經授權存取或使用	撥接線路未適當控管							
				未經授權存取或使用	識別與認證機制不足							
				操作失誤	複雜的操作介面							
				操作失誤	操作文件不足							
				操作失誤	專業訓練不足							
				蓄意破壞	缺乏實體之保護							
	DA			資料外洩	儲存媒體的報廢或再使用未適當處理							
				資料外洩	識別與認證機制不足							
				資料外洩	文件或檔案未適當存放							
				儲存媒介劣化	儲存媒體維護不足或安裝瑕疵							
				儲存媒介劣化	缺乏資料備份							
				未經授權存取或使用	缺乏監督與稽核機制							
				未經授權存取或使用	存取權限授與不當或未定期審查							
				未經授權存取或使用	未落實桌面淨空或螢幕鎖定							

威弱點評估表

文件編號：Takming-ISMS-D-005					機密等級：內部使用				版　　次：2.0				
紀錄編號：									填表日期：				
資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級			弱點等級			風險值
						低	中	高	低	中	高	
				未經授權存取或使用	文件或檔案未適當儲存							
	DC			遺失	人員安全訓練不足							
				遺失	缺乏適當管理機制							
				失竊	人員安全訓練不足							
				失竊	外部人員缺乏人員陪同作業							
				失竊	未經控管之資料複製							
				失竊	缺乏安全警覺							
				失竊	資料銷毀機制或程序不夠嚴謹							
				資料外洩	人員安全訓練不足							
				資料外洩	外部人員缺乏人員陪同作業							
				資料外洩	未經控管之資料複製							
				資料外洩	缺乏安全警覺							
				資料外洩	資料銷毀機制或程序不夠嚴謹							
				蓄意破壞	人員安全訓練不足							
				蓄意破壞	建築物、房間的實體進出控制不足							
				蓄意破壞	缺乏安全警覺							
				未經授權存取或使用	缺乏監督與稽核機制							
				未經授權存取或使用	存取權限授與不當或未定期審查							
				未經授權存取或使用	未落實桌面淨空或螢幕鎖定							
				未經授權存取或使用	文件或檔案未適當儲存							
	HW			火災	人員安全訓練不足							
				火災	消防設施的不足或缺乏消防器材的保護							
				火災	存放易燃物							
				失竊	建築物、房間的實體進出控制不足							
				失竊	缺乏安全警覺							
				失竊	缺乏建築物、門、窗等物質的保護							
				失竊	識別與認證機制的不足							
				地震	缺乏建築物、門、窗等物質的保護							
				灰塵	容易潮濕、有灰塵、穢物							
				空調失效	沒有作好維護的工作							
				空調失效	缺乏緊急應變機制							
				電源供應中斷	不穩定的供電							

威弱點評估表

文件編號：Takming-ISMS-D-005					機密等級：內部使用				版　　次：2.0				
紀錄編號：									填表日期：				
資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級			弱點等級			風險值
						低	中	高	低	中	高	
				水災	位於易淹水的區域							
				颱風	缺乏建築物、門、窗等物質的保護							
				支援之公用設施失效	維護服務回應時間過長							
				支援之公用設施失效	規格不清楚或未盡完善							
				支援之公用設施失效	缺乏測試程序或測試不夠							
				支援之公用設施失效	缺乏保養/維護程序或不足							
				支援之公用設施失效	缺乏備援電力或備援電力不足							
	HW			硬體失效	維護服務回應時間過長							
				硬體失效	缺乏硬體耗損控管							
				硬體失效	缺乏有效變更控制							
				電源供應中斷	不穩定的電壓							
				未經授權存取或使用	未確實陪同外部人員或清潔人員執行相關作							
				未經授權存取或使用	存取權限授與不當或未定期審查							
				未經授權存取或使用	通行碼管理不足							
				未經授權存取或使用	離開工作站未進行「登出」作業							
				未經授權存取或使用	缺乏監督與稽核機制							
				操作失誤	複雜的操作介面							
				操作失誤	操作文件不足							
				操作失誤	專業訓練不足							
	PE			人員不足	缺乏職務代理機制							
				人員不足	職責分工不當							
				重要人員異動	工作負荷過重							
				重要人員異動	缺乏適當之人事管理制度							
				使用者失誤	複雜的使用者介面							
				使用者失誤	教育訓練不足							
				操作失誤	複雜的操作介面							
				操作失誤	操作文件不足							
				操作失誤	專業訓練不足							
				操作失誤	機密資料的外洩(E-mail or 儲存媒體)							
				資料外洩	缺乏人員安全審查程序							
				使用非法軟體	未使用合法版權軟體或下載受控管之軟體							
				使用非法軟體	未定期審查軟體使用情形							

威弱點評估表

文件編號：Takming-ISMS-D-005	機密等級：內部使用	版　　次：2.0
紀錄編號：		填表日期：

資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級			弱點等級			風險值
						低	中	高	低	中	高	
	SW			軟體失效	維護服務回應時間過長							
				軟體失效	缺乏有效變更控制							
				軟體失效	缺乏監督與稽核機制							
				軟體失效	未適當執行軟體測試							
				操作失誤	複雜的操作介面							
				操作失誤	操作文件不足							
				操作失誤	專業訓練不足							
				操作失誤	機密資料的外洩(E-mail or 儲存媒體)							
				未經授權存取或使用	存取權限授與不當或未定期審查							
				未經授權存取或使用	通行碼管理不足							
				未經授權存取或使用	離開工作站未進行「登出」作業							
				未經授權存取或使用	缺乏監督與稽核機制							
				未經授權存取或使用	識別與認證機制不足							
				未經授權存取或使用	文件或檔案未適當儲存							
				否認性	缺乏正確使用通訊設備與訊息控管的政策							
				否認性	缺乏傳送或接收訊息的證據							
				否認性	缺乏傳送者與接收者的識別與認證							
				非法使用軟體	未使用合法版權軟體或下載受控管之軟體							
				非法使用軟體	未定期審查軟體使用情形							
				非法使用軟體	缺乏安全警覺							
				使用者失誤	複雜的使用者介面							
				使用者失誤	教育訓練不足							
				惡意軟體攻擊	缺乏安全警覺							
				惡意軟體攻擊	人員安全訓練不足							
				惡意軟體攻擊	缺乏有效變更控制							
				惡意軟體攻擊	未適當執行軟體測試							
				惡意軟體攻擊	軟體漏洞							

主管簽核