資安事件
風險因應與行動計畫

依照ISO27001資訊安全全景鑑別及風險評鑑程序 規範

1.嚴重程度評估：當該風險發生時，其可能造成之影響

評分	經濟損失	營運作業的影響	對商譽的影響	機密洩漏的影響	遵循性的影響
5	造成100萬(含)以上的費用損失。	影響本公司存續	對公司形象、商譽形象有嚴重的不良影響，會直接衝擊到公司業績。	極機密等級資料大量洩漏。	
4	造成50萬(含)以上的費用損失。	公司主要業務窒礙難行	對公司形象、商譽形象有不良影響。	1、極機密等級資料洩漏。 2、機密使用等級資料大量洩漏。	
3	造成10萬(含)以上的費用損失。	公司業務運作困難	對公司形象、商譽形象有短暫的不良影響。	機密使用等級資料洩漏。	部份不符合法規或主管機關要求。
2	造成1萬(含)以上的費用損失。	公司業務遭受阻礙	對公司形象、商譽形象有輕微的不良影響。	內部等級資料洩漏	
1	造成輕微的經濟損失。	不會影響公司營運/個人工作受到干擾	對公司形象、商譽形象不會有影響。	資料洩漏不會對公司造成影響。	符合法規會主管機關要求，但仍有改善空間。

2.發生機率評估：該風險發生之機率或可能性

量化質	潛在發生機率	已知發生頻率
5	非常可能 (90%)	總是發生(月)
4	很可能 (70%)	經常發生(季)
3	可能(50%)	屢次發生(年)
2	不太可能 (20%)	有時發生(兩年)
1	微乎其微	很少發生

3.依下列風險矩陣圖，判定風險值及等級

嚴重程度	1	2	3	4	5
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8
5	5	6	7	8	9

4..風險回應：

1. 針對風險值於6分以上之不可接受風險，需彙整於「風險因應行動表」中，並針對風險情境及造成該風險之弱點，研擬適當之因應措施。

4.風險因應行動表

風險情境	造成風險之弱點	因應行動	時程	人員	再評估		殘餘風險
					嚴重程度	發生機率	
未完全符合個資法要求	未指定代表與落實執行制度可能誤觸合規	指派個資法代表與落實制度	2024Q1	待指派	1	2	1
建立個資事故之預防、通報及應變機制	個資外流造成損失	落實建立個資盤點區隔與應變通報機制	2024Q1	待指派	2	2	3
個人資料應有遮罩	個資外流造成損失	修改應用程式與導入資料庫遮罩	2023/12/31	Rex	1	2	1
使用紀錄、軌跡資料及證據保存未滿6個月	難以查證追尋紀錄	建立LOG保存至少6個月	2023/12/31	Merlin	1	2	1
VPN遠端存取帳號可以被暴力破解	帳號資料外洩	建立多因素認證	2023/12/31	Merlin	3	1	2
使用者多重驗證CN區Android手機無法接收	帳號資料外洩	導入新世代遠端存取驗證方式	2024Q1	Merlin	2	2	3
防火牆官方憑證洩漏	造成金額損失,資料外流	下架全部舊有Fortigate火牆	2024Q1	Merlin	3	2	4
防火牆OS韌體存在外部風險	造成金額損失,資料外流	全區域替換防火牆	2024Q1	Merlin	3	2	4
駭客入侵營運中斷	造成金額損失,資料外流	建立委外24小時資訊安全監控中心(SOC)	2024Q1	Merlin	3	2	4
駭客入侵資料被加密	造成金額損失,資料外流	導入端點偵測防禦系統(EDR)回滾防禦	2023/12/31	Merlin	3	2	4
駭客入侵資料外流	造成金額損失,資料外流	導入資料洩漏防防護方案(DLP)阻擋	2024Q1	Merlin	3	2	4

風險防禦由外至內

合規

⇩

強化身分驗證

⇩

強化遠端存取

⇩

強化邊緣防禦

⇩

建立威脅監控

⇩

防禦深度攻擊入侵與回滾

⇩

防禦資料外洩

5.風險分類

合規

風險情境	造成風險之弱點	因應行動	時程	人員	再評估		殘餘風險
					嚴重程度	發生機率	
未完全符合個資法要求	未指定代表與落實執行制度可能誤觸合規	指派個資法代表與落實制度	2024Q1	待指派	1	2	1
建立個資事故之預防、通報及應變機制	個資外流造成損失	落實建立個資盤點區隔與應變通報機制	2024Q1	待指派	2	2	3
個人資料應有遮罩	個資外流造成損失	修改應用程式與導入資料庫遮罩	2023/12/31	Rex	1	2	1
使用紀錄、軌跡資料及證據保存未滿6個月	難以查證追尋紀錄	建立LOG保存至少6個月	2023/12/31	Merlin	1	2	1
強化身分驗證							
VPN遠端存取帳號可以被暴力破解	帳號資料外洩	建立多因素認證	2023/12/31	Merlin	3	1	2
強化遠端存取							
使用者多重驗證CN區Android手機無法接收	帳號資料外洩	導入新世代遠端存取驗證方式	2024Q1	Merlin	2	2	3
強化邊緣防禦							
防火牆官方憑證洩漏	造成金額損失,資料外流	下架全部舊有Fortigate火牆	2024Q1	Merlin	3	2	4
防火牆OS韌體存在外部風險	造成金額損失,資料外流	全區域替換防火牆	2024Q1	Merlin	3	2	4
建立威脅監控							
駭客入侵營運中斷	造成金額損失,資料外流	建立委外24小時資訊安全監控中心(SOC)	2024Q1	Merlin	3	2	4
防禦深度攻擊入侵與回滾							
駭客入侵資料被加密	造成金額損失,資料外流	導入端點偵測防禦系統(EDR)回滾防禦	2023/12/31	Merlin	3	2	4
防禦資料外洩							
駭客入侵資料外流	造成金額損失,資料外流	導入資料洩漏防防護方案(DLP)阻擋	2024Q1	Merlin	3	2	4

6.風險分類執行計畫

合規

因應行動	說明	專案名稱	預計完成時程	人員	2024完成月份		
指派個資法代表與落實制度	建立與導入整套個資制度與定期執行	個資管理辦法與實行作業規則建立	2024Q1	待指派	1/22		
落實建立個資盤點區隔與應變通報機制	導入前先盤點個資存在處與建立應變通報	個資盤點與應變通報建立	2024Q1	待指派	1/31		
修改應用程式與導入資料庫遮罩	需要在資料庫建立敏感資料欄位遮蔽	資料庫欄位加密遮罩	2023/12/31	Rex			
建立LOG保存至少6個月	需要建立集中式log存放中心	集中式事件存放中心	2023/12/31	Merlin			

強化身分驗證

建立多因素認證	身分驗證MFA強制套用		2023/12/31	Merlin			

強化遠端存取

導入新世代遠端存取驗證方式	放棄舊有VPN存取模式改用雲端集中登入	雲端安全存取服務邊緣(SASE)	2024Q1	Merlin		2/2	

強化邊緣防禦

下架全部舊有Fortigate火牆	防火牆產品生命週期皆已EOD	防火牆切換與替換 1.替換:總部/IDC/磐石/北京/廣州/沛富/合康 2.切換:金山/靜安	2024Q1	Merlin		2/8	
全區域替換防火牆	官方曾經發生大量洩漏自家防火牆憑證,因此不在使用該牌防火牆						

建立威脅監控

建立委外24小時資訊安全監控中心(SOC)	建立時刻有專業背景的人加以監看處理	資安作業監控中心建立	2024Q1	Merlin		2/23	

防禦深度攻擊入侵與回滾

端點偵測防禦系統(EDR)回滾防禦	事前:偵測預防.事中:緩解,事後:回滾復原	事前:導入深度防禦偵測ATP 事中:導入端點偵測防禦EDR與復原	2023/12/31	Merlin			

防禦資料外洩

資料洩漏防防護方案(DLP)阻擋	資料被上傳:使用DLP偵測阻擋通知並錄影 資料被竊取:使用加密防止讀取	1.導入與建置DLP 2.資料夾加密	2024Q1	Merlin			3/15 3/29